Ethical Hacking and Countermeasures

Version6

Module LXI

Threats and Countermeasures

Domain Level Policies

Domain Level Policies are “Group Policy settings”

The built-in Default Domain Controller policy is

- Account policies, Default setting values for these policies are collectively referred as Account policies

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Policies

Types of Account policies

- Password policies
- Account lockout policies
- Kerberos authentication protocol policies

When these policies are applied to any other level in Active Directory, on the member server the local accounts list will only be affected

Default values are given in the built-in Default Domain Controller policy

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Policies (cont'd)

The domain Account policy is the default Account policy for a Windows computer which is a member of the domain

Another Account policy for the organizational unit is an exception for this rule

The default computer (local) policies are assigned to nodes that are in a workgroup are a domain and where no organizational unit Account policy or domain policy is associated

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Password Policy

A common way to hide user's identity is to use a secret password or a phrase

The assigned password prevents an unauthorized access to the user or administrative account

A regular change of the passwords decreases the threat of password attack

A password policy can be given to put into effect the use of strong passwords

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

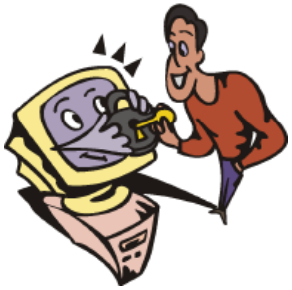
Password Policy (Cont'd)

Password policy settings control the intricacy and existence of passwords

The password policy settings are configured under the Object Editor of Group Policy at the location

- **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**

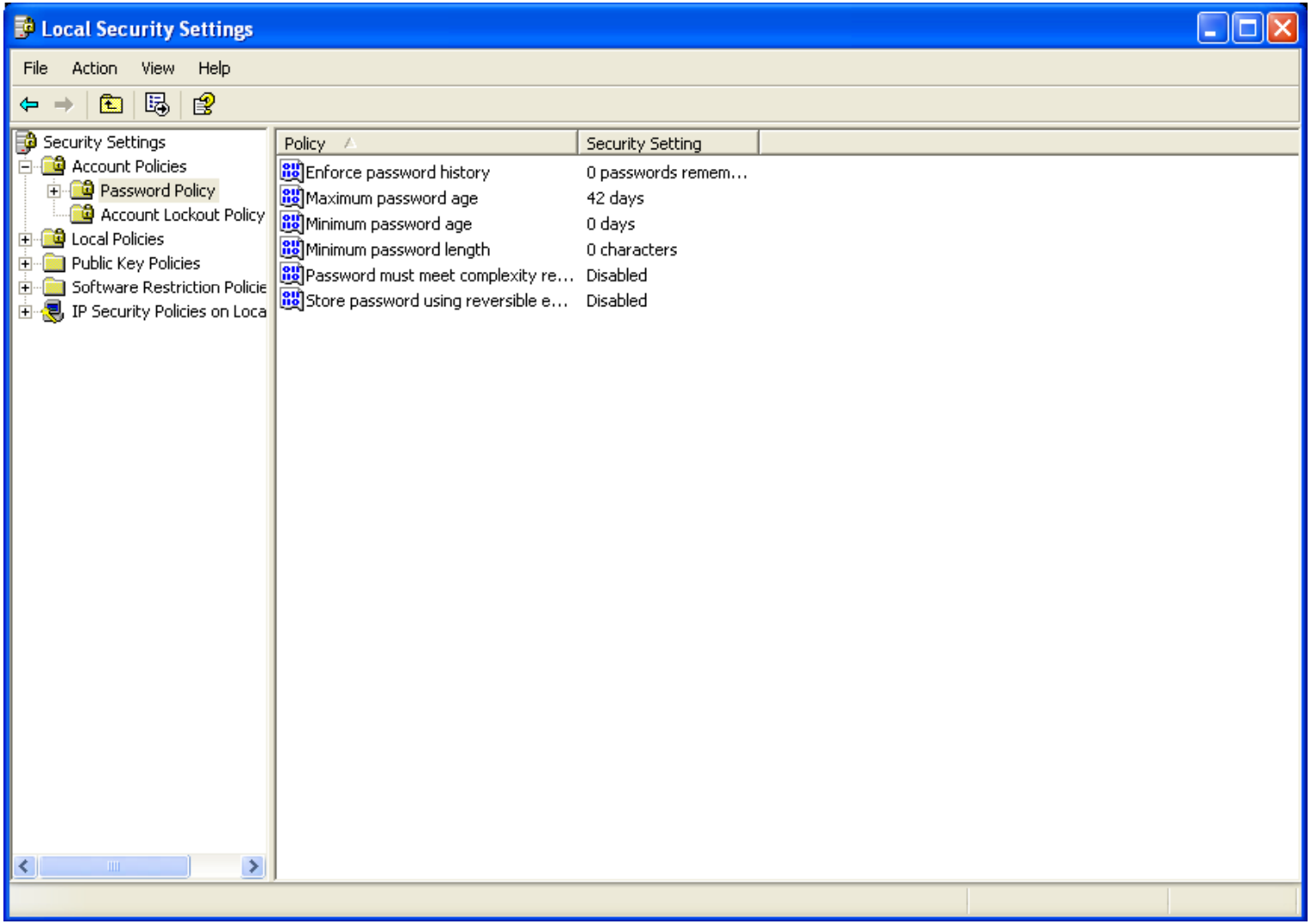
If various groups require different password policies, they must be divided into different sections (domains) depending on the additional requirements



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Password Policy



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Password Policy - *Policies*

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Passwords must meet complexity requirements
- Store password using reversible encryption for all users in the domain

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enforce Password History

This policy determines the various unique passwords that are connected with a user account before reusing the old password

The values for the **Enforce password history** setting are:

- A value between 0 and 24 specified by the user

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enforce Password History - *Vulnerability*

Brute-force attack can be used to determine the password, when the user is reusing the same password for an account for an extended period of time

The efficiency of a high-quality password policy is very much decreased, when a password change is necessary but password reusability is allowed

If **Minimum password age** setting are configured, users will not be able to change there passwords over and over, UN-less they stop reusing there old passwords

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enforce Password History - *Countermeasure*

To decrease the vulnerabilities raised by password reusing, set the **Enforce password history** option to **24** (maximum)

While configuring **Minimum password age** settings, no password should be changed immediately

The **Enforce password history** value should be set at a stage that combines a sensible utmost password age with a sensible password change interval requirement for the users

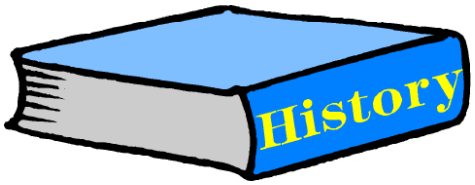
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enforce Password History - *Potential Impact*

The major impact of this pattern is that users has to generate a new password every time it is necessary to change the old one

Risk Involved

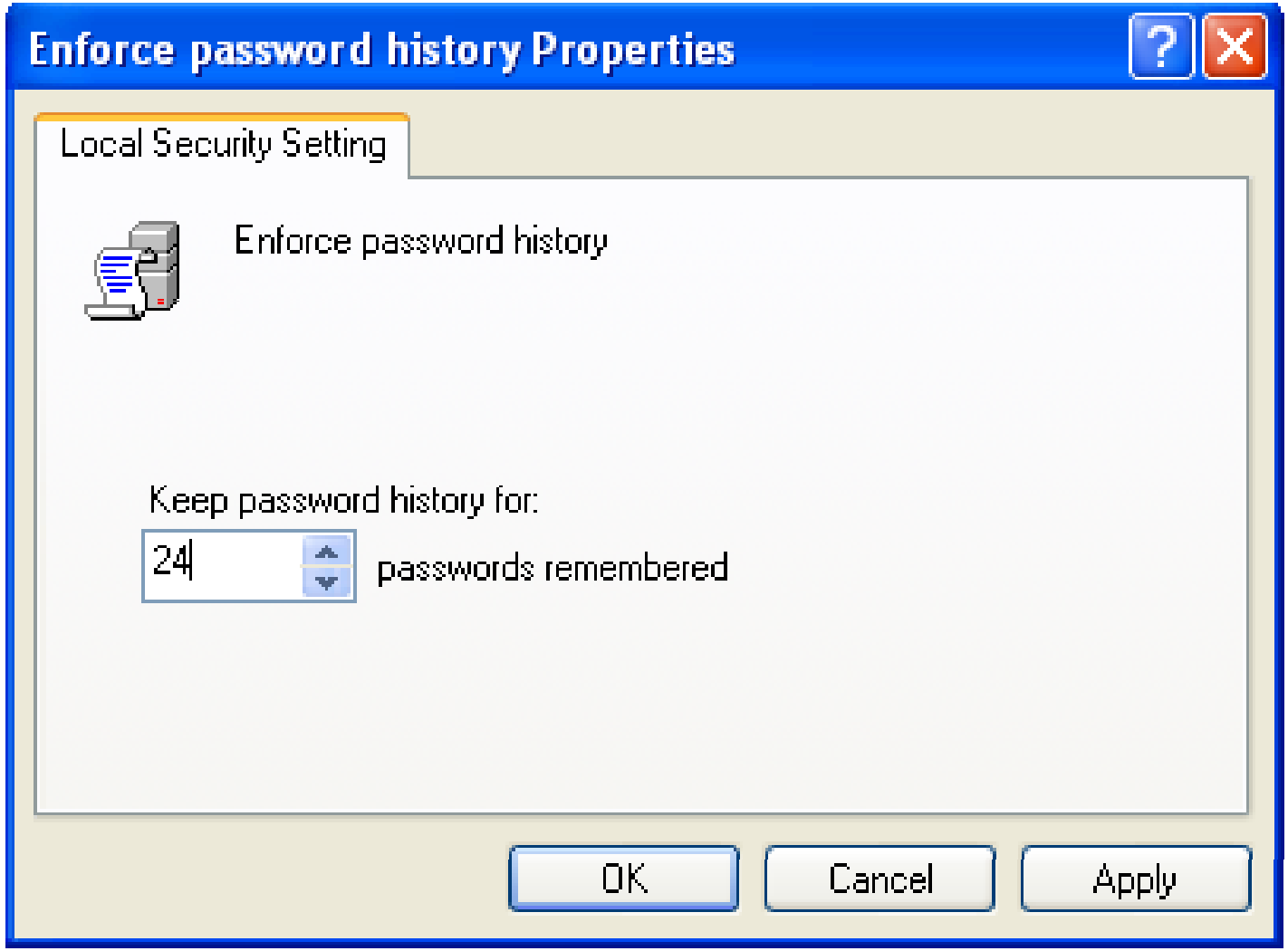
- If the user has to change the password to a new distinct phrase, the risk of writing the pass phrase is increased
- The users might generate passwords that change incrementally (as *password01*, *password02 …)* to ease its remembrance
- By decreasing the value of Minimum password age setting administrative overhead is maximized, as users who forget their pass phrase will be requiring assistance to reset it



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enforce Password History



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Password Age

This policy determines the duration (in days) that a password can be used before it is changed

The values for the Maximum password age setting are:

- The number of days between 0 and 999 as specified by the user.
- Not Defined

EC-Council

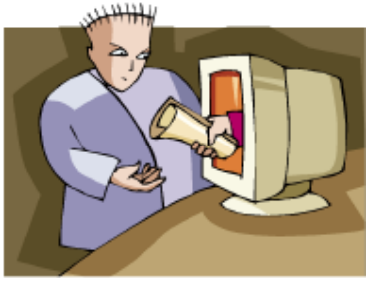
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Password Age - *Vulnerability*

A password attacker can always guess or crack a difficult password, Some policy settings make it tough to crack them

The risk of breaking a password can be reduced by making the users to change there passwords regularly

Maximum password age setting can be configured to never change the user passwords, but it might lead to a security risk



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Password Age - *Countermeasure*

Maximum password age settings can be configured as per user requirements

Maximum Password Age setting can be assigned to 0 so that passwords will never expire

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Password Age - *Potential Impact*

If the **Maximum password age** setting value is very less, the user has to modify their passwords frequently

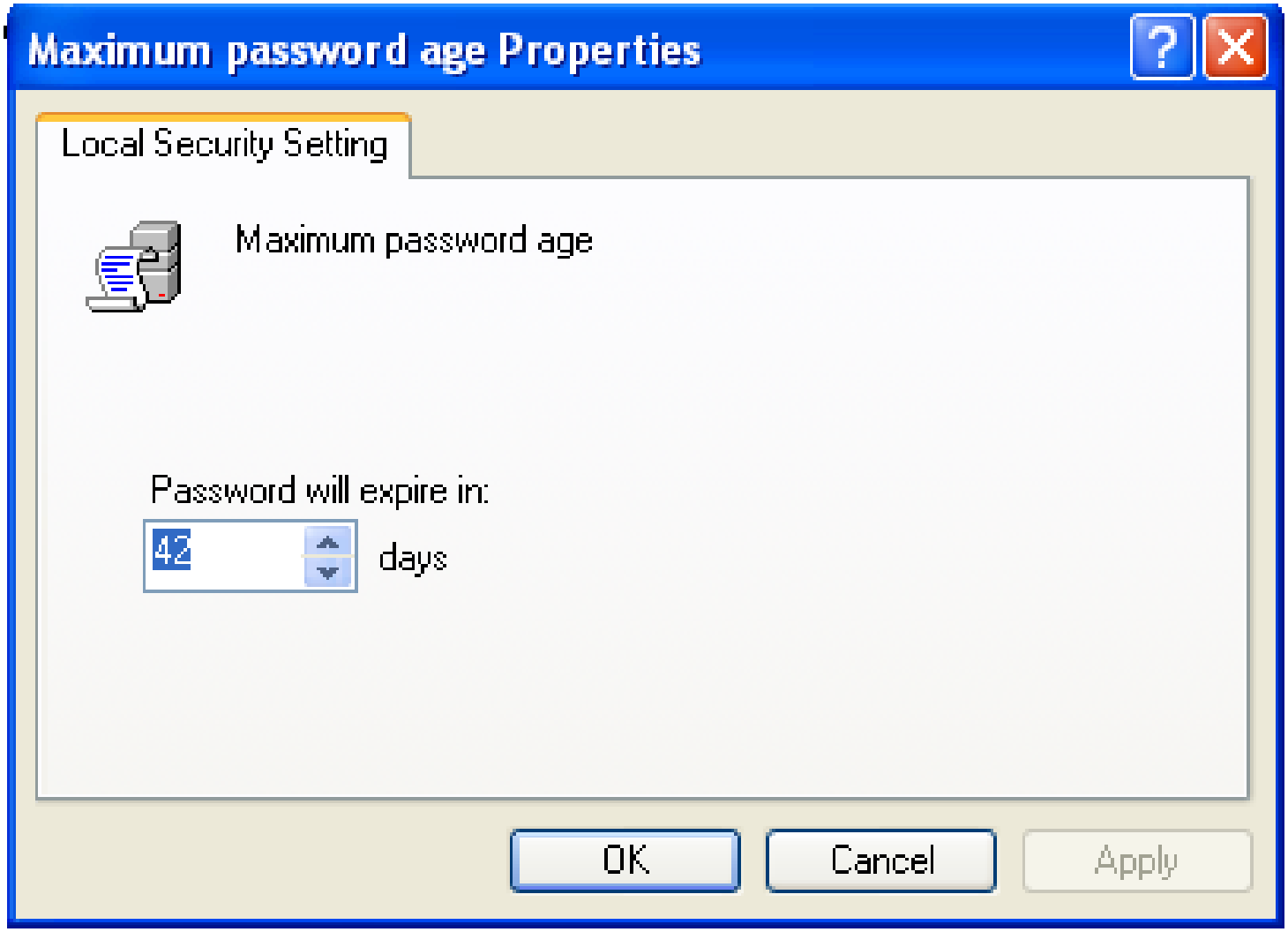
This kind of Configuration may decrease security, as the user may write the passwords somewhere by the fear of forgetting them and then they may lose information at some place

If value of the policy setting to set to maximum, the security level will be reduced as the attackers will get a large time span to crack the passwords

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Password Age



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Minimum Password Age

This policy setting is used to conclude the number of days in which the user has to change his password

To make **Enforce password history** setting efficient, set the policy value higher than 0

If this value is set to zero the user need not change his password regularly

The values for the Minimum password age setting are:

- The number of days between 0 and 998 as spesified by the user
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Minimum Password Age - *Vulnerability*

It is impractical to modify the password regularly, if the user cycles around to use his regular password

By using this policy setting with **Enforce password history** setting, prevents the use of old passwords

To make **Enforce password history** setting effective, set the policy value to higher than 0

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Minimum Password Age - *Countermeasure*

By setting the **Minimum password age** value to **0** days, immediate password changes would be allowed, which is not recommended

To have a limitation over the password change. Set the value to minimum **2** days

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Minimum Password Age - *Potential Impact*

To make a user change his password at his first logon

Administrator has to tick **User must change password at next logon** check box

This will allow the user to change his password on logging his account. In other case the user has to wait until next day

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Minimum Password Age

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Minimum Password Length

The policy settings conclude the minimum numeral characters to generate a password for an account

Many theories have been evolved to decide the password length; rather "pass phrase" is a suitable word than "password”

An expression “I am sick!" is an acceptable pass phrase. These expressions are significantly more robust than an 8 or 10 character strings and they are easier to remember

The values for the Minimum password length setting are:

- A number between 0 and 14 as user specified
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Minimum Password Length - *Vulnerability*

Various kinds of password attacks are implemented to get the password for an account.

- Dictionary attacks (Using general terms and expression)
- Brute force attacks (Possible grouping of characters)

Attackers also try to get hold of the user account database to utilize them to break the accounts and passwords.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Minimum Password Length - *Countermeasure*

If **Minimum password length** is set **0**, password is not necessary

To set a password, assign a value **8** or more. **8** character passwords give enough security from Brute force and Dictionary attacks

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Minimum Password Length - *Potential Impact*

Long passwords may cause account lockouts when the passwords are typed wrong by mistake which will maximize the work of help desk

Long Passwords

- Long passwords are hard to remember, so the personnel's might hard to write it down some where which can lead to insecurity of the password

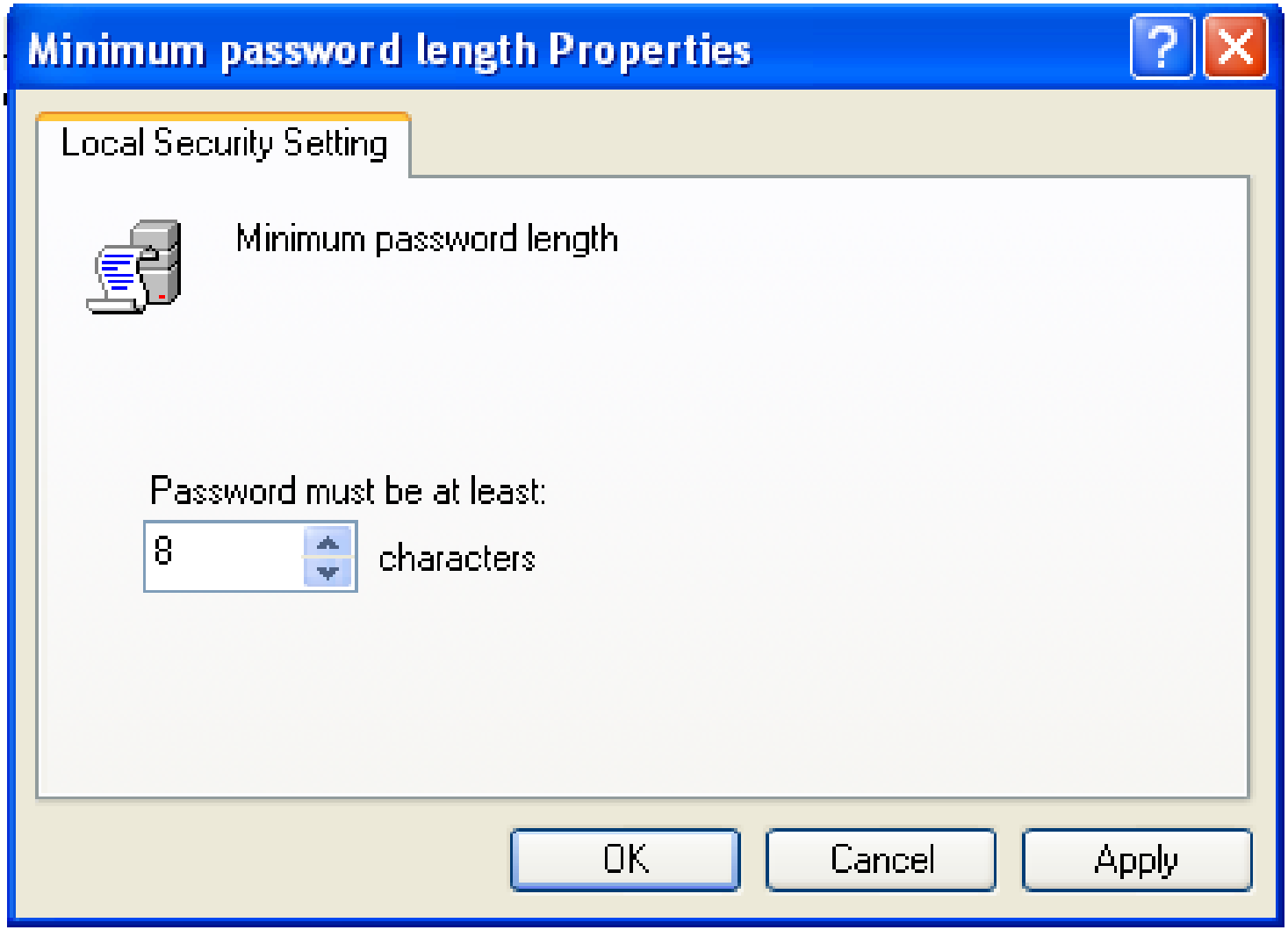
Short Passwords

- Short passwords can be easily broken using any tool which use brute force (or) dictionary attack

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Minimum Password Length



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Passwords Must Meet Complexity Requirements

If this policy setting is enabled, passwords must fulfill these requirements:

- The password length must be minimum 6 characters
- The password must contain characters from the below given groups:
  - Uppercase characters (A, B, C, ...)
  - Lowercase characters (a, b, c, ...)
  - Numerals (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)
  - Non-alphanumeric and Unicode characters (( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? / € Γ ƒ λ and space)

The password shouldn't include three or more successive characters from the user account name or display name

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Passwords must Meet Complexity Requirements (cont'd)

These complexity conditions are imposed upon password generation or modification.

The values for the Passwords must meet complexity requirements setting are:

- Enabled
- Disabled
- Not Defined

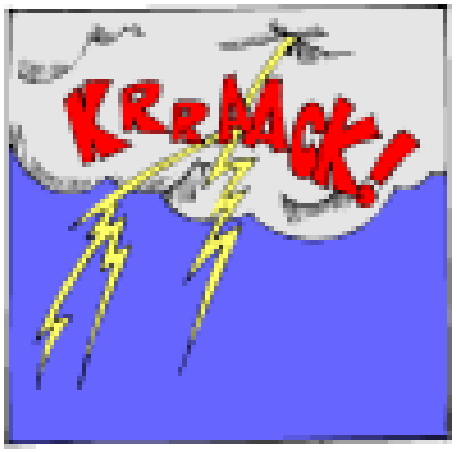
EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Passwords must Meet Complexity Requirements - *Vulnerability*

A password generated by the combination of letters and numeric characters is easy to break (crack)

Various character sets should be combined together to generate a passwords which can be prevented from Cracking



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Passwords must Meet Complexity Requirements - *Countermeasure*

Configure the **Passwords must meet complexity requirements** setting to **Enabled**.

By Combining **Minimum password length** of **8** with the above settings, the various possibilities for a password are so great that it is almost impossible for a brute force attack to be successful.

An attacker capable of processing 1 million passwords per second may crack the password in 7 and ½ days or less.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Passwords must Meet Complexity Requirements - *Potential Impact*

If the default password complexity configuration is hold, help desk calls may increase for locked-out accounts as users might not be able to remember the non alphabetic characters

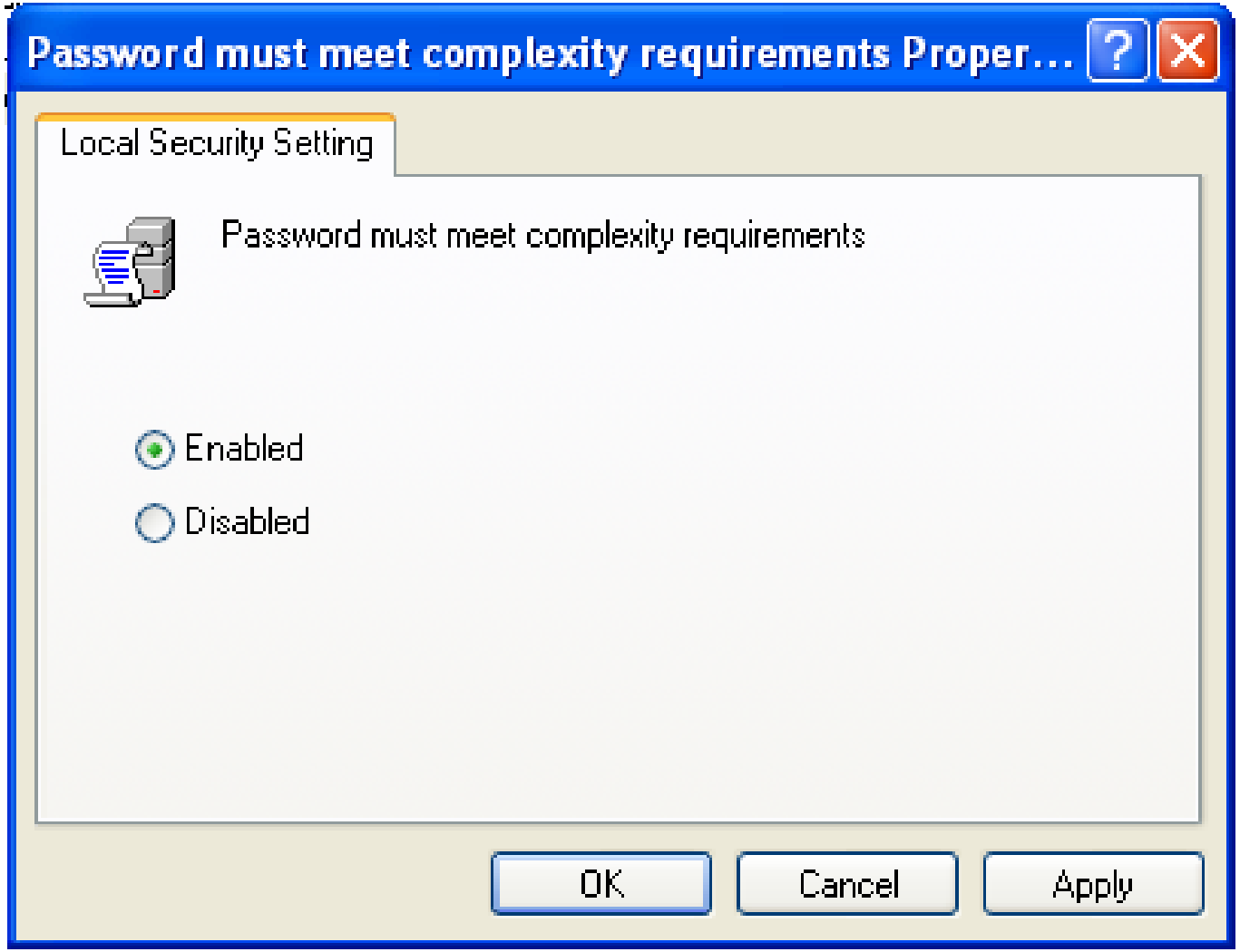
A custom password filter can be created which can perform a dictionary check to make sure the password is free from common words

The use of ALT key character grouping can increase the complexity of a password

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Passwords must Meet Complexity Requirements



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Store Password using Reversible Encryption for all Users in the Domain

The **Store password using reversible encryption for all users in the domain** setting offers support for application protocols that need information on the user's password for authentication purposes

Encrypted passwords that are stored can be decrypted. An attacker who manages break the encrypted password can logon on a compromised account

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Store Password Using Reversible Encryption for all Users in the Domain (Cont'd)

Using the Challenge Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Service (IAS) services need's the policy setting to be enabled.

The values for the Store password using reversible encryption for all users in the domain setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Store Password Using Reversible Encryption for all Users in the Domain (Cont'd)

Vulnerability

- This policy setting conclude that whether Windows Server 2003 will store passwords in a weaker format which is more vulnerable to compromise.

Countermeasure

- Configure the **Store password using reversible encryption for all users in the domain** setting to **Disabled**.

Potential Impact

- If an organization uses CHAP authentication protocol through remote access or IAS services (or) Digest Authentication in IIS, the policy settings should be configured **Enabled**.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Store Password Using Reversible Encryption for all Users in the Domain (Cont'd)

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Policy

An attacker might try to find out a password by trail and error method

The operating system can be set to disable the account after some number of unsuccessful attempts

Account lockout policy is responsible for taking necessary action for this threshold

You can configure the account lockout policy settings in the following location within the Group Policy Object Editor:

- **Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Policy

Local Security Settings

File Action View Help

- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignmen
    - Security Options
  - Public Key Policies
  - Software Restriction Policie
  - IP Security Policies on Loca

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon atte...
Reset account lockout counter after	Not Applicable

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Policy - *Policies*

1. • **Account lockout duration**
2. • **Account lockout threshold**
3. • **Reset account lockout counter after**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Duration

This policy setting decides the time period of a locked-out account to be unlocked automatically. The time period is within a range of 1 to 99,999 minutes

Configure the value to **0**, if the locked-out account is should be unlocked manually by the administrator

When an account lockout threshold is given, the **Account lockout duration** must be higher or similar to the reset time

The values for the Account lockout duration setting are:

- **A value in minutes between 0 and 99,999**
- **Not Defined**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Duration - *Vulnerability*

When an attacker neglect the **Account lockout threshold** and tries to logon to a specific account, a Denial of service (DoS) situation is created

If **Account lockout threshold** settings can be configured to lock out an account after some number of failed attempts

If the settings are configured to **0**, the administrator has to unlock it manually

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Duration - *Countermeasure*

Configure the **Account lockout duration** setting to a suitable value

Configure the value to **0,** to remain the account locked until an administrator manually unlocks it

When the settings are configured to a non-zero value. The automated password guessing attempts should wait for a specific interval

Automated guessing of a password can be made complex or useless, when **Account lockout threshold** settings are used

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

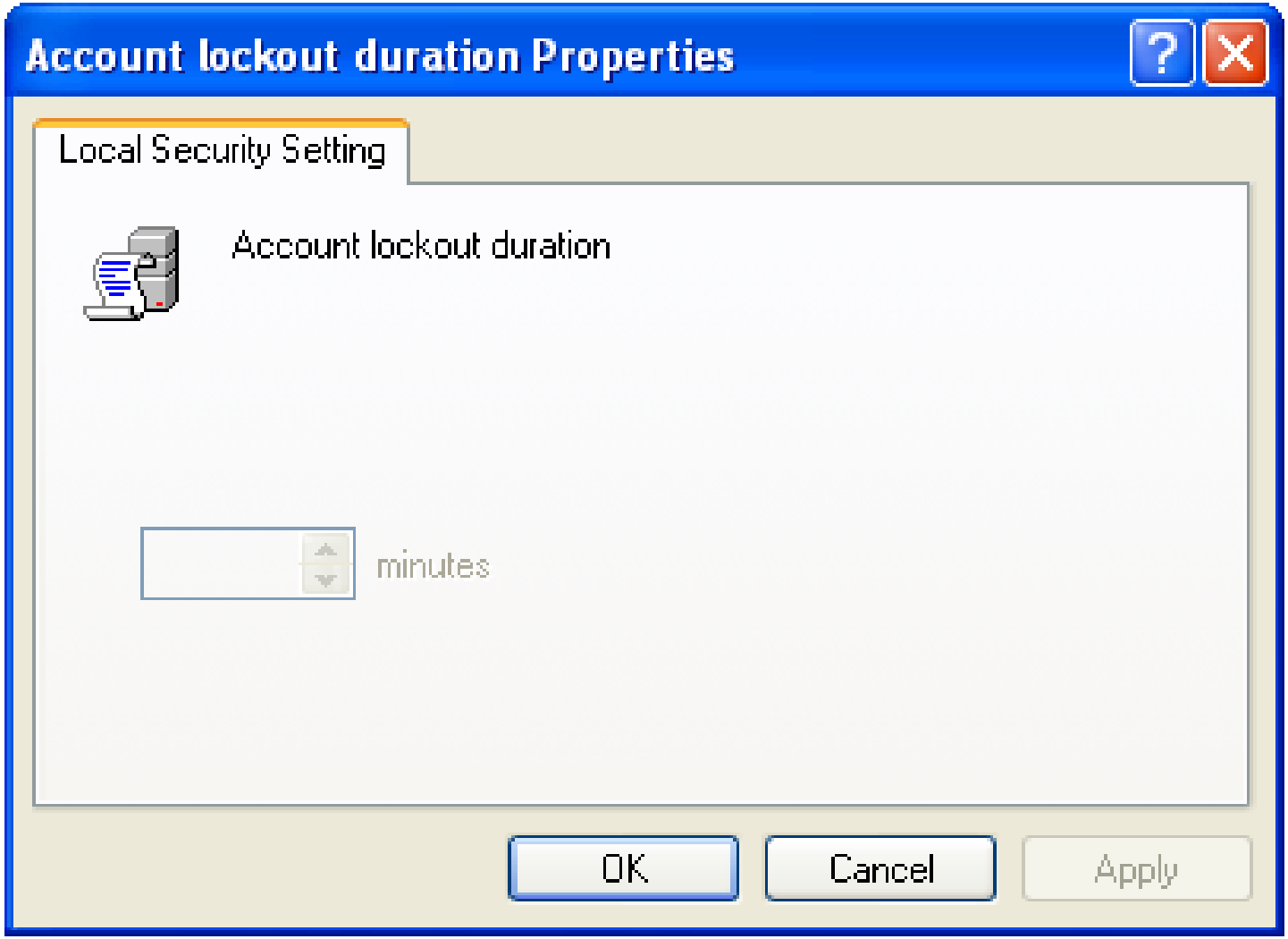
Account Lockout Duration - *Potential Impact*

The policy settings can be set to 'never automatically unlock an account'. This setting might maximize the help desk calls for unlocking an account

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Duration



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Threshold

This policy setting concludes the count of failed logon trails which caused an account to be locked out

To use a locked out account, the administrator has to reset the account or lockout duration should expire

- The failed logon attempts can be up to 999
- Setting the value to 0 indicates that the account will never be locked

If **Account lockout threshold** is given, then the **Account lockout duration** should be greater than or equal to the reset time

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Threshold

Unsuccessful password attempts which are locked through either CTRL+ALT+DELETE or password-protected screen savers do not count as failed logon attempts

Unless the policy setting **Interactive logon: Require Domain Controller authentication to unlock workstation** is enabled

The values for the Account lockout threshold setting are:

- **A value between 0 and 999**
- **Not Defined**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Threshold - *Vulnerability*

If a limit is set on the number of failed logon's performed, the password attackers will not perform any automated method on the account

Attacks

If an account lockout threshold is configured a DoS attack would be carried out.

Programmatically attempt a series of password attacks.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Threshold - *Countermeasure*

Vulnerabilities can occur in two situations

- When this value is configured
- When this value is not configured

The two countermeasure options are:

- Configuring the **Account Lockout Threshold** setting to **0**. With these configuration the accounts will not be locked out, and will prevent a DoS attack.
- As this configuration will not stop brute force attack, it should be chosen only if the below criteria's are met:
  - All users must have critical passwords of 8 or more characters
  - A mechanism should be assigned to alert the administrator when a failed logon occurs

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Threshold – *Countermeasure* (Cont'd)

If the earlier criteria cannot be met, configure **Account Lockout Threshold** settings to a greater value, by which the user can wrongly type the value various times

This value will be such that brute force password attack will still lock the account, but DoS attack cannot be prevented

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Threshold - *Potential Impact*

To use a locked out account, the administrator has to reset the account or lockout duration should expire

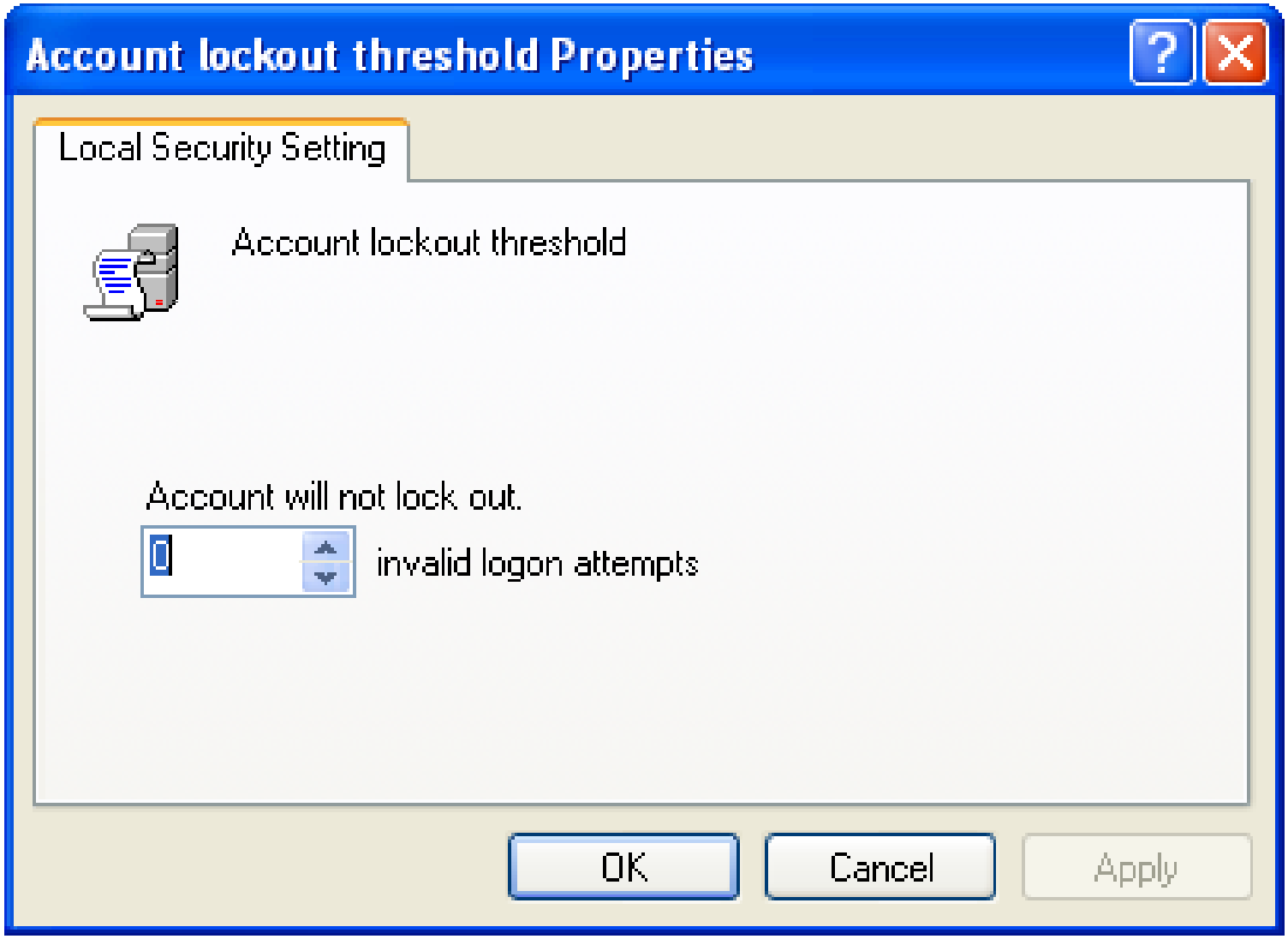
Long passwords may cause account lockouts when the passwords are typed wrong by mistake which will maximize the help desk calls

Configure the **Account Lockout Threshold** to **0.** A mechanism should be assigned to alert the administrator when a failed logon occurs

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Account Lockout Threshold



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Reset Account Lockout Counter After

This policy is set to keep track on the number of minutes that should pass before resetting the counters which hold the information on number of failed logon to **0**

The **Account lockout threshold** reset time should be less than or equal to the **Account lockout duration** setting configuration

The values for the Reset account lockout counter after setting are:

- **A number of minutes between 1 and 99,999**
- **Not Defined**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Reset Account Lockout Counter After

Vulnerability

- By typing a password multiple times the user can lock there account unintentionally.
- To minimize the possibility of unintended lockouts, the **Reset account lockout counter after** setting find out the number of minutes that should pass before resetting the counters which hold the information on number of failed logon to **0**

Countermeasure

- Configure the **Reset account lockout counter after** setting to **30 minutes**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Reset Account Lockout Counter After

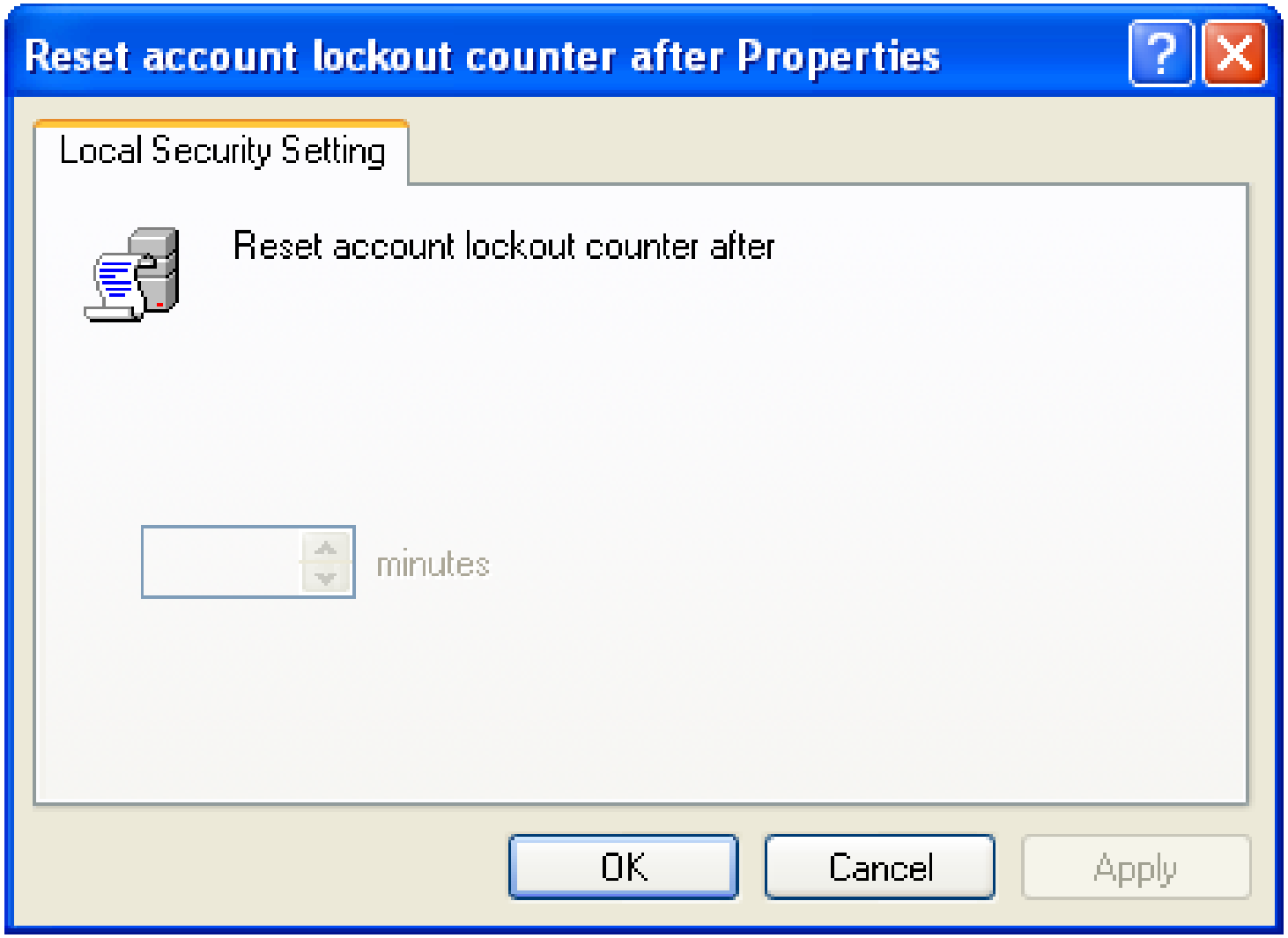
Potential Impact

- A DoS attack take place, if the policy is not configured (or) if the configured value has a long interval
- If **Reset account lockout counter after** is not set administrator has to unlock the account manually
- The value set for this policy, will keep the Locked user's account blocked for that amount of time
- Incase an account is locked. The user's must be informed about this value such that they can wait for that period of time, before accessing the account

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Reset Account Lockout Counter After



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Kerberos Policy

If the lifetime of Kerberos tickets is decreased, the risk of a valid user's credentials being stolen and lucratively used by an attacker decreases. However, authorization overhead increases

Modification of Kerberos policy settings are not done in most environments

These are domain level policy settings; the configuration of the default values is done at Default Domain Policy GPO in a default installation of a Windows 2000 or Windows Server 2003 Active Directory domain.

You can configure the Kerberos policy settings in the following location within the Group Policy Object Editor:

- **Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Kerberos Policy - *Policies*

- Enforce user logon restrictions
- Maximum lifetime for service ticket
- Maximum lifetime for user ticket
- Maximum lifetime for user ticket renewal
- Maximum tolerance for computer clock synchronization

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enforce User Logon Restrictions

This policy concludes that the Key Distribution Center (KDC) legalizes all requests for a session ticket with the user privileges policy

Validation of the requests for the session ticket kept optional, as the process may degrade the network access

The values for the Enforce user logon restrictions setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enforce User Logon Restrictions

Vulnerability	• Even if this policy is disabled, the users might get the session tickets for the services that they are unauthorized for, as the authorization is removed after they login
Countermeasure	• Configure the **Enforce user logon restrictions** setting to **Enabled**
Potential Impact	• None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Lifetime for Service Ticket

The maximum amount of time (minutes) granted for a session ticket is verified by this policy settings. The value can be set to 10 min's or greater and it should be less than or equal to the **Maximum lifetime for user ticket** setting

If a session ticket is expired a new ticket has to be requested for KDC

Once the connection is set, the ticket is not valid. Session tickets are necessary for a new connection. If the ticket expires during the session there will be no interruption in the process

The values for the Maximum lifetime for service ticket setting are:

- A user-defined value in minutes between 10 and 99,999. If you configure this policy setting to 0, service tickets do not expire.
- Not Defined.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Lifetime for Service Ticket

Vulnerability	• A user can access network resources outside of their logon hours, if a greater value is set to **Maximum lifetime for service ticket** setting • Users who are deactivated can also access the network with a valid service tickets issued before deactivating there accounts
Countermeasure	• Configure the **Maximum lifetime for service ticket** setting to **600 minutes**
Potential Impact	• None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Lifetime for User Ticket

The maximum time (in hours) of a user's ticket-granting ticket (TGT) is concluded by this policy

If a users TGT expires a new one should be requested (or) old one must be renewed

The values for the Maximum lifetime for user ticket setting are:

- **A user-defined value in hours between 0 and 99,999. The default value is 10 hours**
- **Not Defined**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Lifetime for User Ticket

Vulnerability

- A user can access network resources outside of their logon hours, if a greater value is set to Maximum lifetime for service ticket setting
- Users who are deactivated can also access the network with a valid service tickets issued before deactivating there accounts

Countermeasure

- Configure the **Maximum lifetime for user ticket** setting to 10 hours

Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Lifetime for User Ticket Renewal

This policy is used to set the time period (days), of renewing user's ticket-granting ticket (TGT)

The values for the Maximum lifetime for user ticket renewal are:

- **A value in minutes between 0 and 99,999**
- **Not Defined**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Lifetime for User Ticket Renewal

Vulnerability

- If this value is too high, it is possible to renew a old user ticket

Countermeasure

- Configure the **Maximum lifetime for user ticket renewal** setting to **10080 minutes** (7 days)

Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Tolerance for Computer Clock Synchronization

The maximum time (minutes) difference between client and server computers which is allowed by Kerberos protocol is determined by this policy

The values for Maximum tolerance for computer clock synchronization are:

- **A value in minutes between 1 and 99,999**
- **Not Defined**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Tolerance for Computer Clock Synchronization

Vulnerability

- Kerberos authentication protocol uses time stamps, for synchronizing the clocks of client and server computers
- This policy is used to set up the maximum elapsed time to complete the Kerberos negotiation
- Time stamp is necessary to calculate the elapsed time

Countermeasure

- Configure the **Maximum tolerance for computer clock synchronization** setting to **5 minutes**

Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Policy

Audit log is used to record the user actions, these actions are recorded as an entry

Both successful and failed entries are recorded

If there are any changes made in a network, the security system will also change, as the state of the operating system and applications on a computer are dynamic. If the made changes are not reset the security system will no longer be effective

Regular re-view of the security settings, helps the admin to follow security measures

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Policy (Cont'd)

The information acquired by this, is used to concentrate on security measures. The information helps to find out security flaws in the computer

The security audits are necessary to know a security breach

Failure log details are considerably important than successful as they allow to errors in the settings

Separate event logs are maintained for applications and system events

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Policy (Cont'd)

A Group policies event log contain information on application, security and security event log, as maximum log size, access rights for each log, and retention settings and methods

Before any audit processes are implemented, an organization should determine how they will collect, organize, and analyze the data

There is little value in large volumes of audit data if there is no underlying plan to exploit it. Also, audit settings can affect computer performance

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Policy (Cont'd)

The effect of a given combination of settings may be negligible on an end-user computer but quite noticeable on a busy server

Therefore, you should perform some performance tests before you deploy new audit settings in your production environment

A detailed plan should be set on how to collect, organize, and analyze the data before an audit process

As the audit settings shouldn't affect the server performance

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Policy (Cont'd)

You can configure the Audit policy settings in the following location within the Group Policy Object Editor:

- **Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Settings

In all the audit settings vulnerabilities, countermeasures, and potential impacts are similar

The options for each of the audit settings are:

- **Success.** An audit entry is generated when the requested action succeeds
- **Failure.** An audit entry is generated when the requested action fails
- **No Auditing.** No audit entry is generated for the associated action

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Settings

Vulnerability

- If audit setting is not configured it is difficult to find information on security process
- If the setting are configured the security event log be full of useless stuff
- Large number of objects in the audit settings may minimize the computer performance

Countermeasure

- To sense an unauthorized action audit policy settings are must

Potential Impact

- A legal obligation may be held with some industries, to log certain events and activities

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Account Logon Events

This policy setting is configured to state an audit success, audit failure or no audit

A success audit indicates that an attempt to login has succeeded

A Failure audits indicate a failed or false login attempt, this help in detecting intrusion detection

These setting create the possibility for a denial of service (DoS) attack. If **Audit: Shut down system immediately if unable to log security audits** setting is enabled, an attacker can force the computer to shut down by generating millions of logon failures

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Account Logon Events

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Account Management

This policy setting finds out either to audit each computer on logon or not.

Account management events

- A user account or group is created, changed, or deleted
- A user account is renamed, disabled, or enabled
- A password is set or changed

Configuring **Audit account management** setting:

- Enable to set an audit for success and failure events

When an account management event fails failure event is generated

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Account Management

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Directory Service Access

Whether to audit user access an active directory service object associated with system access control list (SACL) or not, is conclude by this policy. SACL is list of users and groups to perform audit on the network

By configuring **Audit directory service access** setting to enable, you actually mean to use the information that is generated

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Directory Service Access

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Logon Events

This policy finds out whether to audit each occasion of user login, logoff (or) only on the computer that records the audit event

If a successful logon event on a domain is recorded, workstation logon do not produce logon audits

Account logon events are created wherever the account lives

Logon events are created wherever the logon attempt occurs

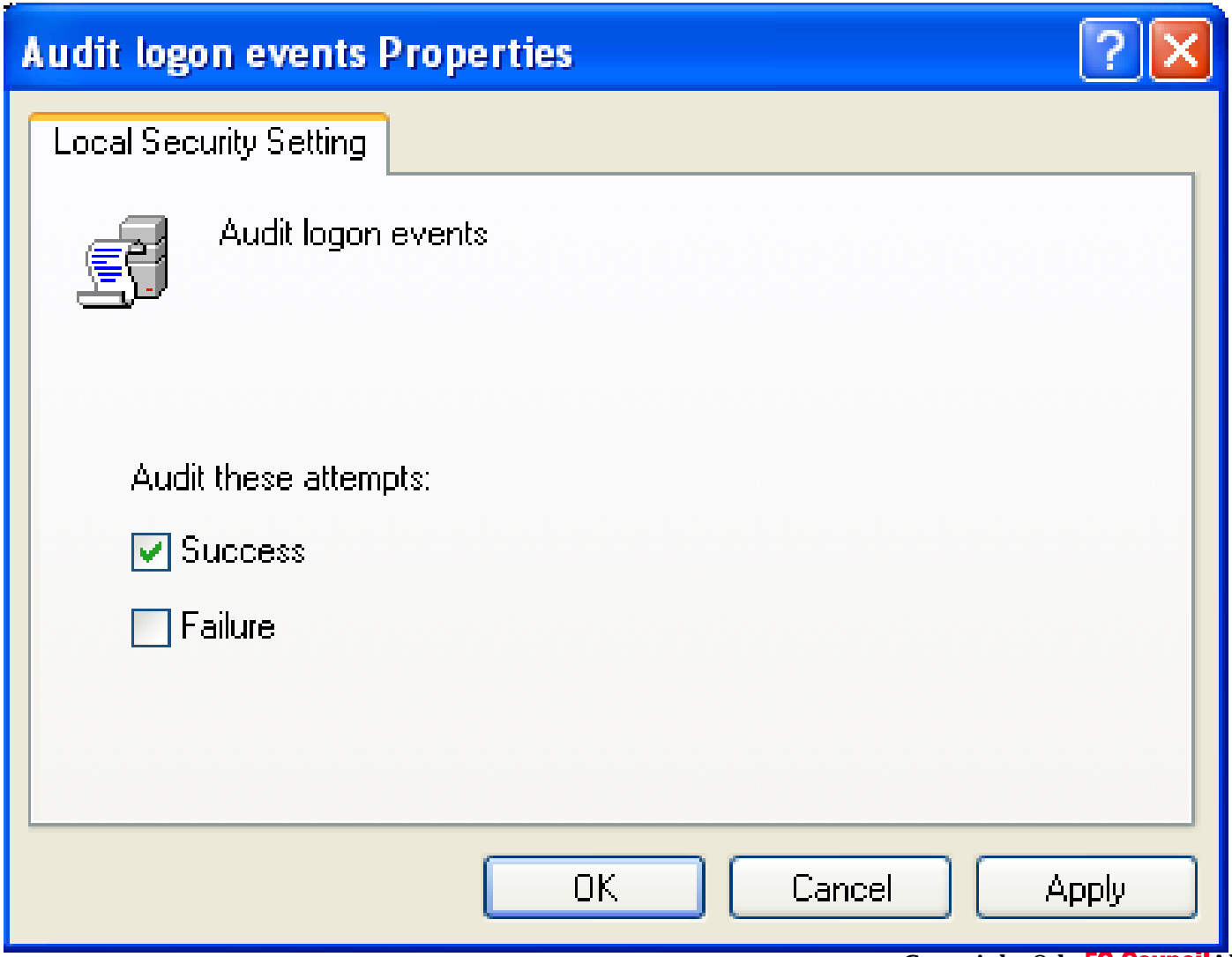
Configure **Audit logon events** setting, to indicate audit successes, audit failures, or not audit event

- The configuration also creates a DoS condition

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Logon Events



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Object Access

This policy concludes whether or not to access an object by a user

Configure **Audit object access** setting, audit successes, audit failures, or not audit

If failure auditing is enabled and SACL on the file, the event will be recorded, when ever it happens

Enabling metabase object auditing:

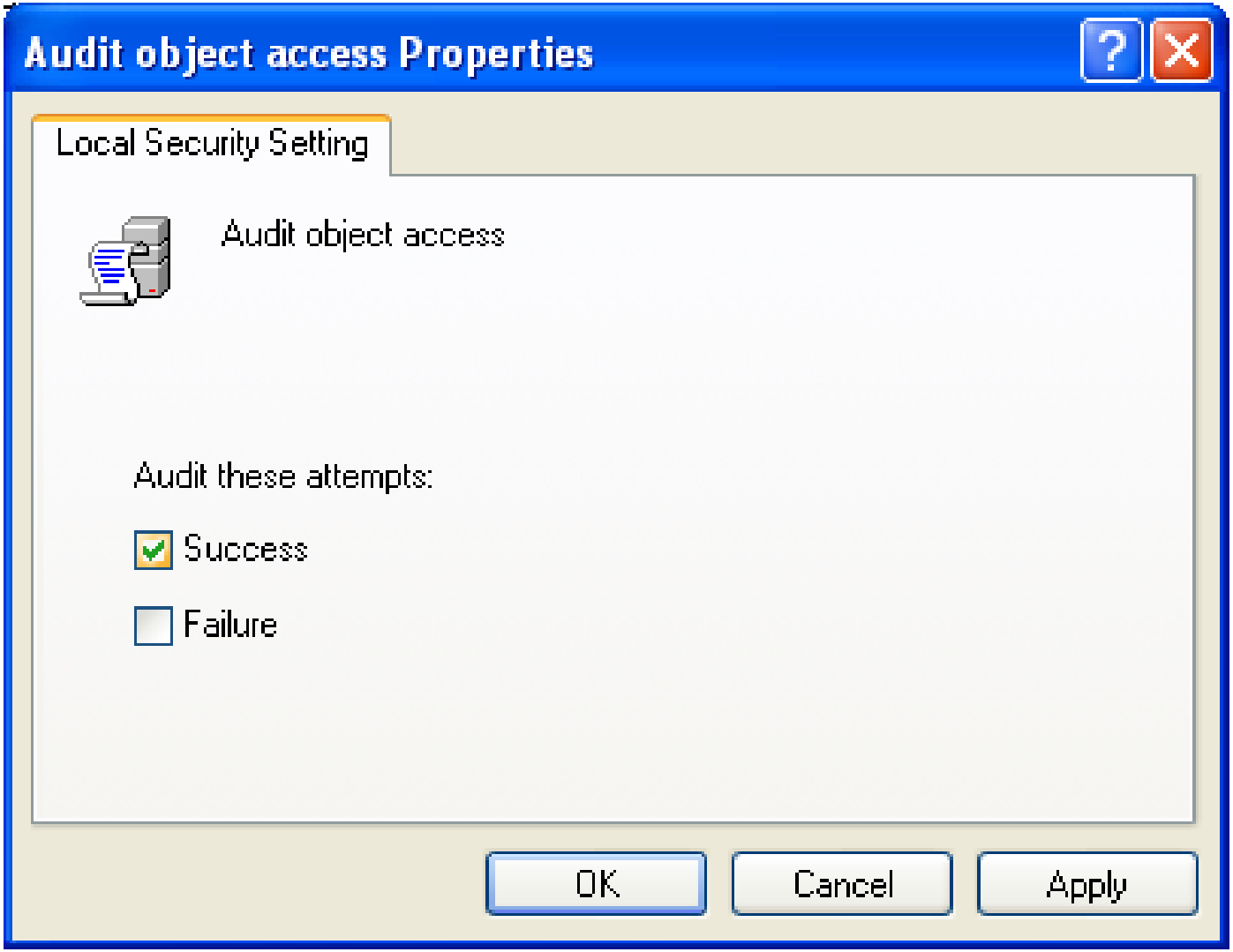
- Enable **Audit object access** on the target computer
- Set SACLs on metabase objects to audit

On configuring **Audit object access** policy setting and SACLs on objects. Large volume of entries can be created in the Security logs

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Object Access



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Policy Change

To conclude every modification to user rights assignment policies, Windows Firewall policies, Audit policies, or trust policies configure this setting

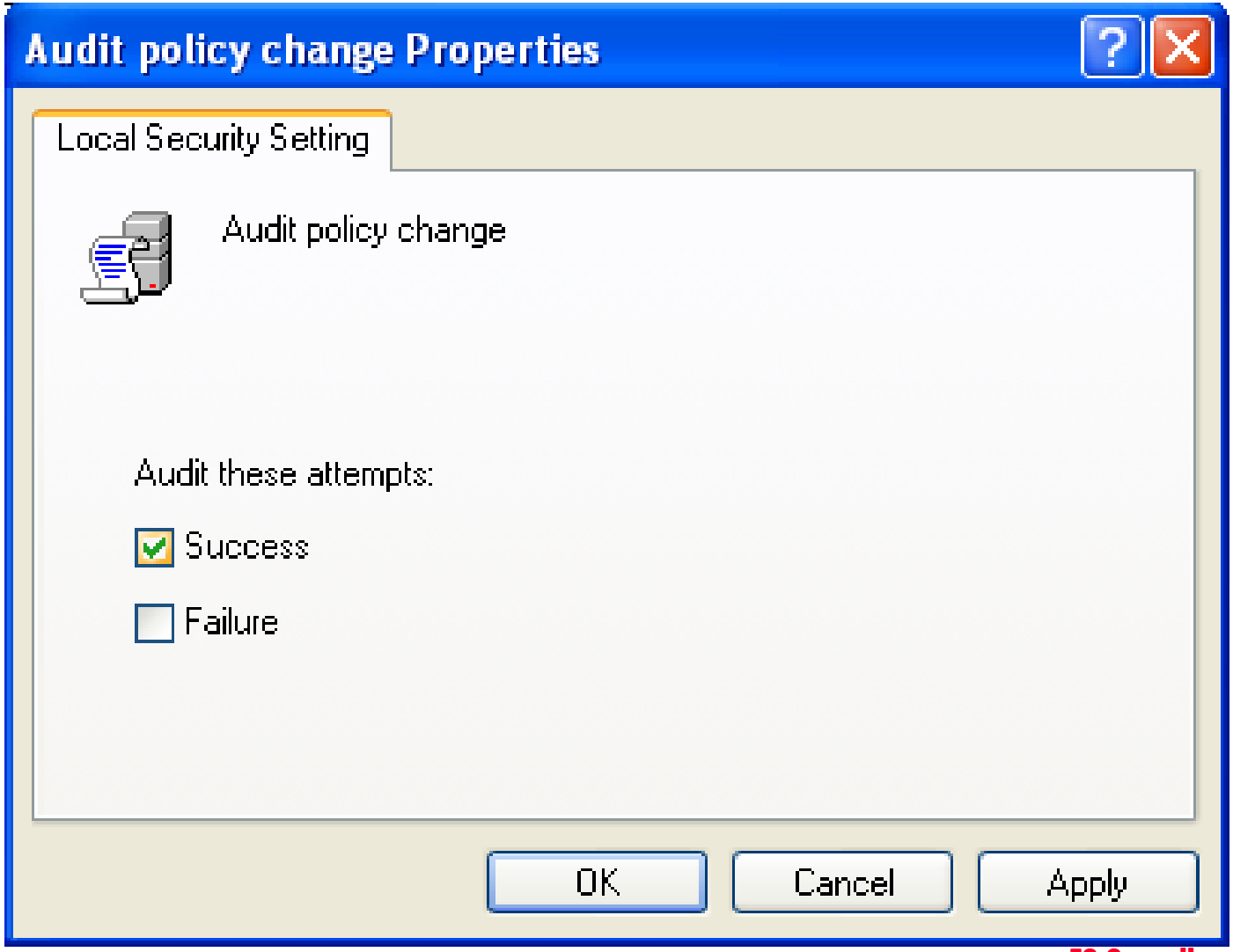
This policy specifies to audit successes, failures, or not audit. This helps in finding out the successful modifications done in a domain or computer

Configuration changes in Windows Firewall component are enabled when this policy setting are enabled for Windows XP with SP2 and Windows Server 2003 with SP1

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Policy Change



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Privilege Use

This policy is used to conclude an audit a user for his each instance, when he put into effect his rights

On configuring **Audit privilege use** setting, audits successes, failures, or no audit

This policy can generate large events, which might be complex to sort out

This policy should be enabled, with a plan to use the evolved output

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Privilege Use (Cont'd)

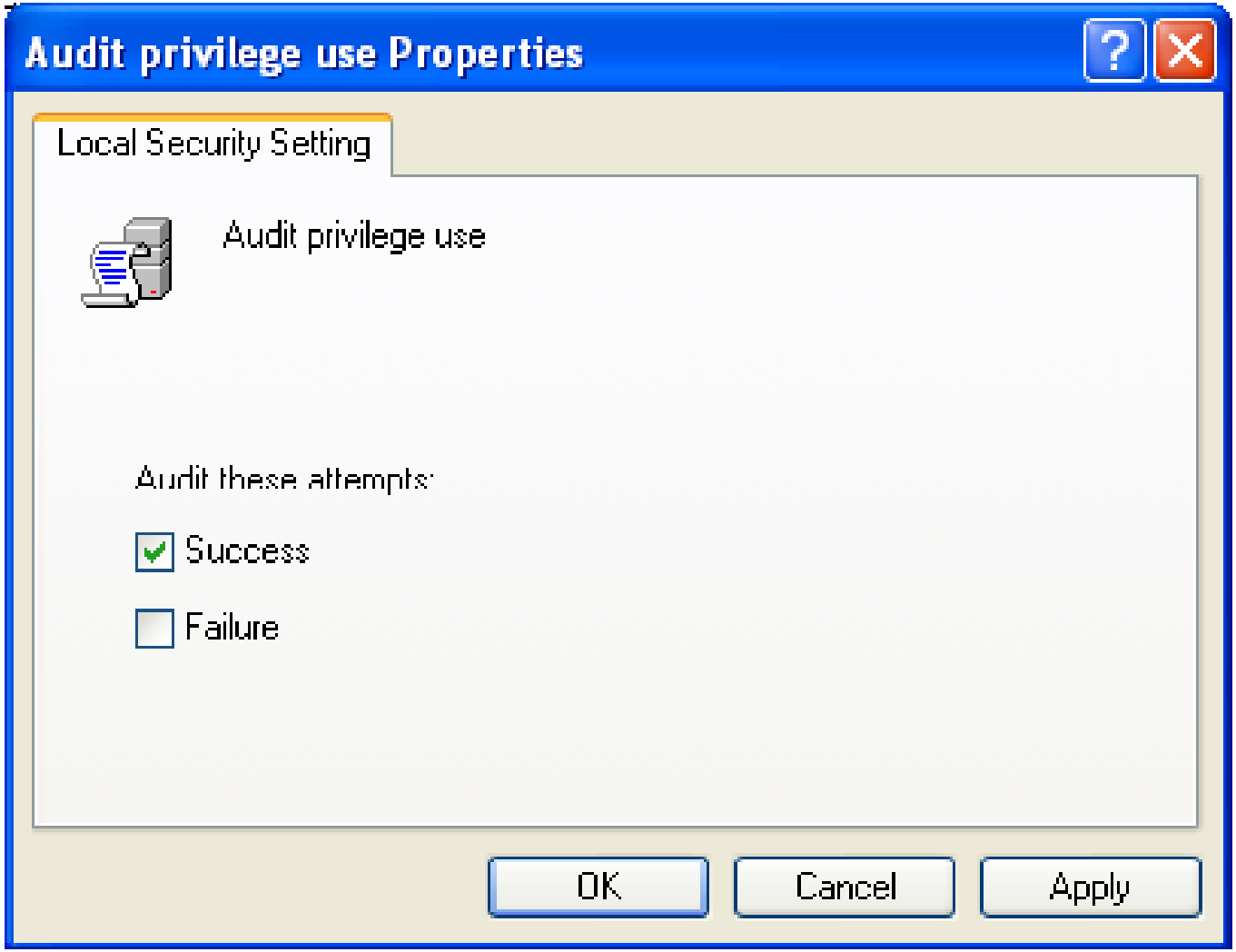
User rights which are not generated for audit event (Success or failure audit)

- Bypass traverse checking
- Debug programs
- Create a token object
- Replace process level token
- Generate security audits
- Backup files and directories
- Restore files and directories

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Privilege Use



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Process Tracking

Detailed tracking information such as program activation, process exit, handle duplication, and indirect object access can be audited by configuring this policy

On configuring **Audit process tracking** setting, audits successes, failures, or no audit

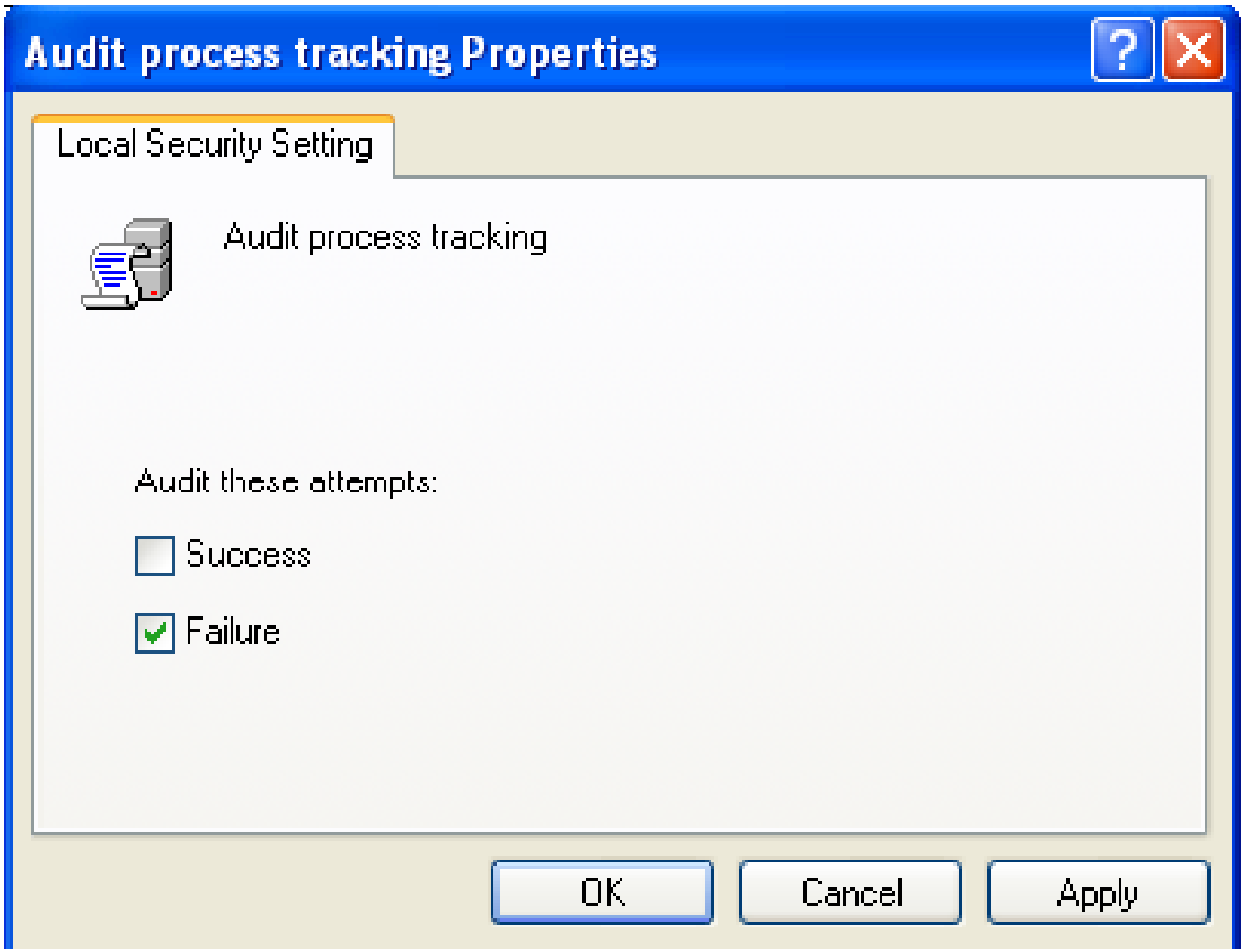
In Windows XP with SP2 and Windows Server 2003 with SP1, when this policy is enabled, it will log information on the operating mode and status of the Windows Firewall component

This policy generates large volume of events. General value of this policy is **No Auditing**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit Process Tracking



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit System Events

This policy concludes on auditing when user restarts or shutdown the computer, (Or) When an event affecting system security or security log

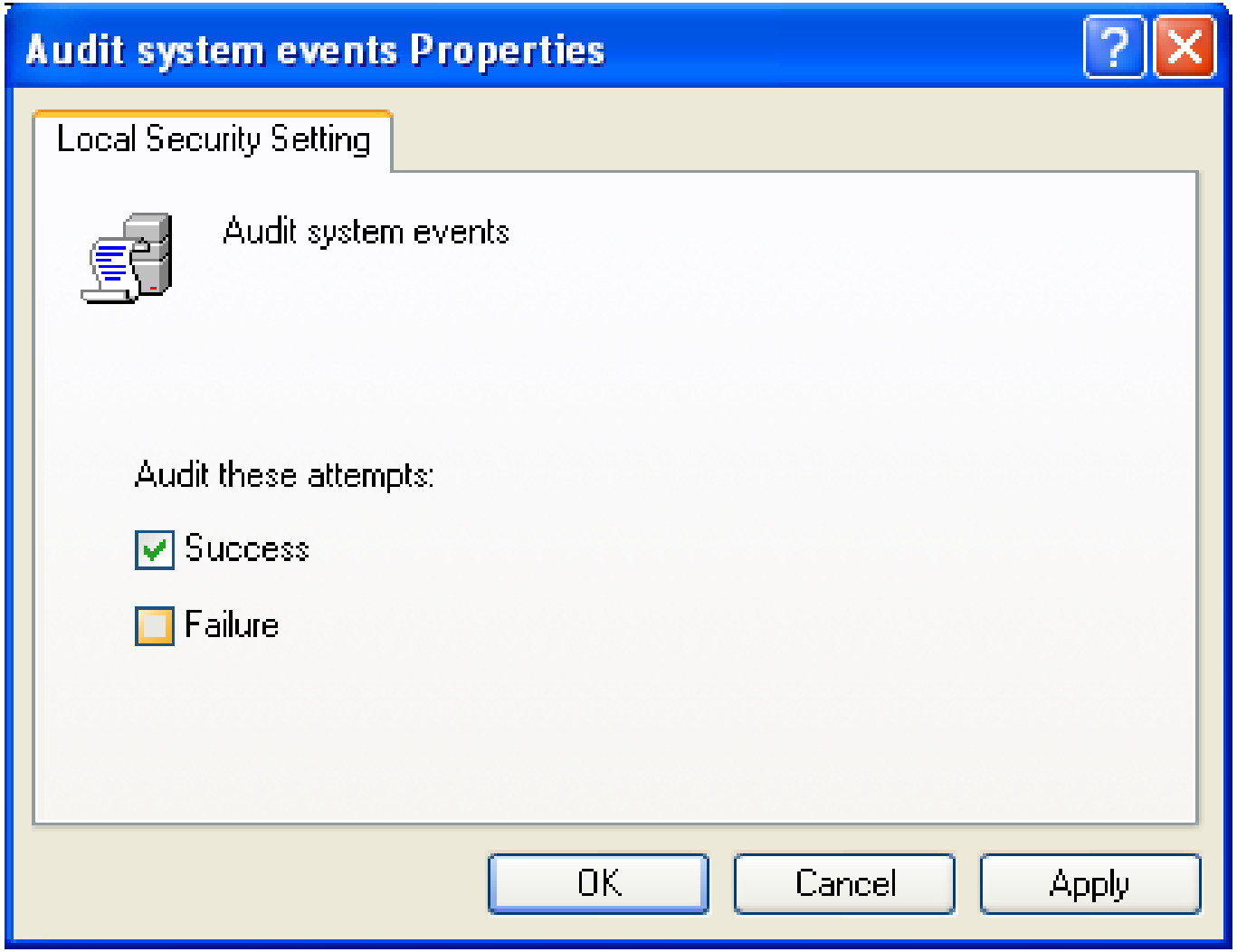
Audit system event generate audits successes, failures, or no audit

This policy should be set **Enabled** on all computers in the network

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit System Events



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

User Rights

User rights are to permit the user to perform a specific task on the domain; they include

- Logon rights – Only authorized personnel have to log on to the domain. (Example: Logging on to local computer)
- Privileges – Used to control user access. (Example: Shutting down the PC)

Individual and group user rights are set by the administrator.

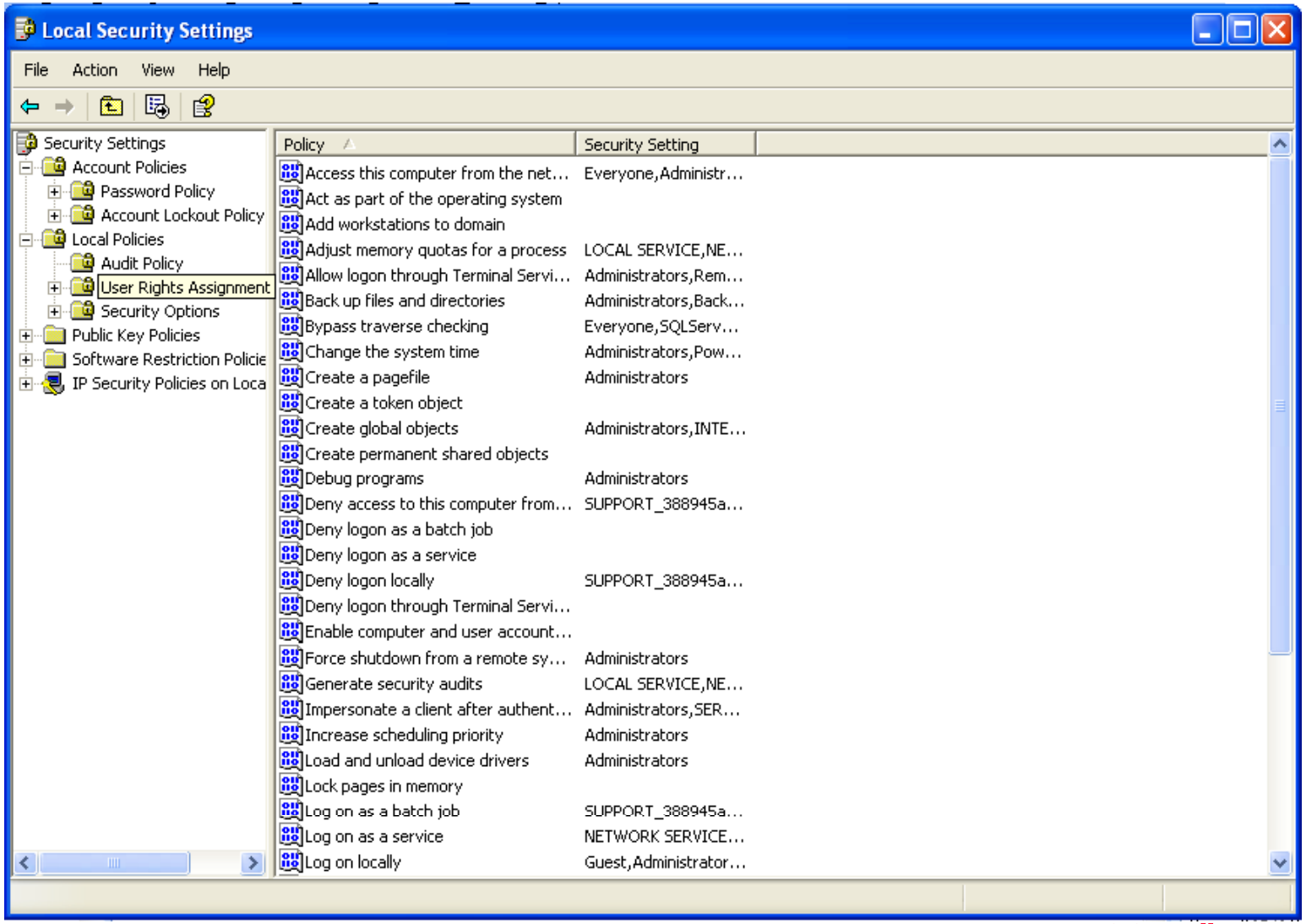
In a Group Policy Object Editor configure the **User Rights Assignment Settings** at:

- **Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

User Rights



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Access this Computer from the Network

This policy concludes that a user can connect to a computer from the network

Various network protocols as Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+) require this ability

The values for the Access this computer from the network setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Access this Computer from the Network

Vulnerability

- User's having privileges to resources on the other computers can access them through the network
- A user must have **Access this computer from the network** user right is necessary to share printers and shared folders

Countermeasure

- This right should be limited to only those users who should necessarily access the server

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Access this Computer from the Network

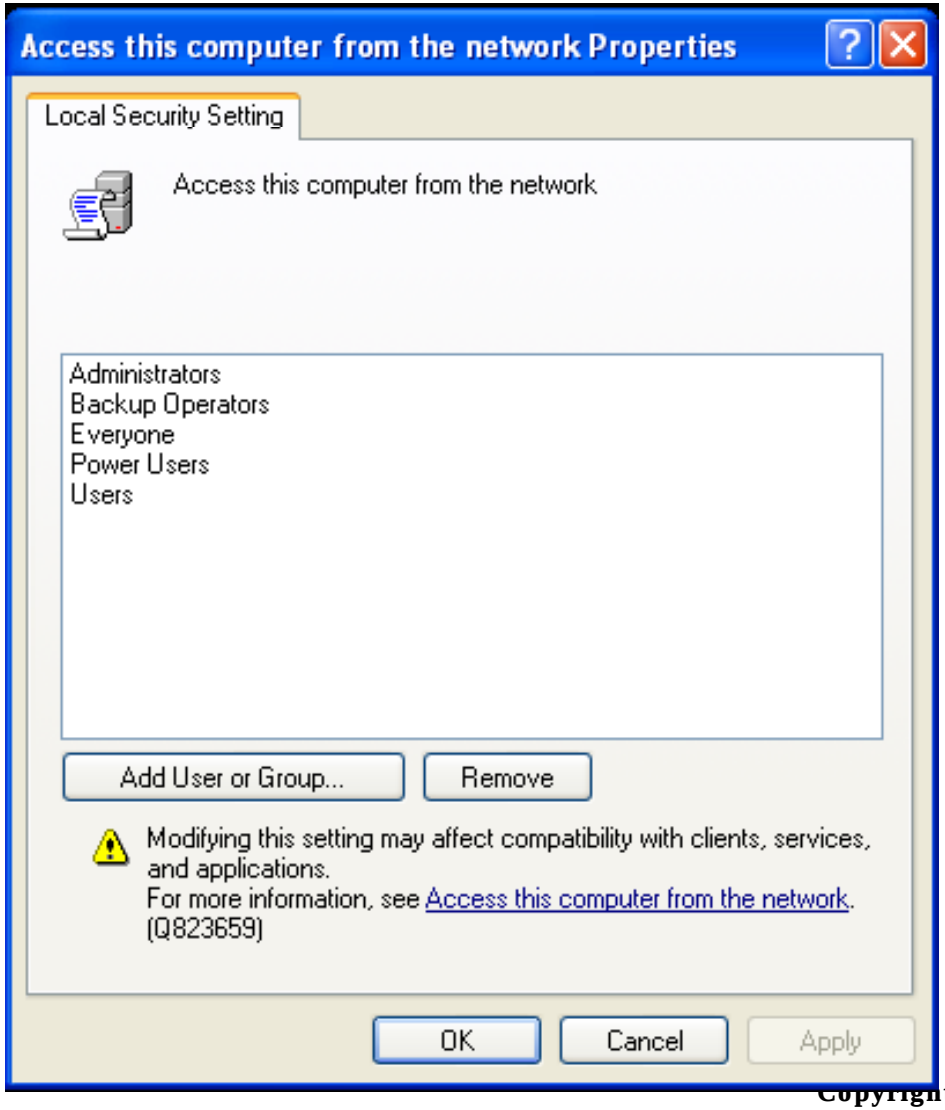
Potential Impact

- If this right is blocked on domain controller, the users will not be allowed to logon to the domain or use network resources
- If the right is removed on the member server, user will restricted to connect to the server
- If any additional (optional) components are installed, the users needing these components should be given the rights to access them

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Access this Computer from the Network



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Act as Part of the Operating System

This policy setting is used to decide that a process can use the identity of any user and access the resources authorized to the user

These user rights are given to low level users

The values for the **Act as part of the operating system** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Act as Part of the Operating System

Vulnerability

- This user right is very authoritative; it provides complete control over the computer

Countermeasure

- This user right should be assigned to only few accounts. Even administrators are not given these rights
- To assign this user right
- Configure the service to logon with the local system account (It has an inherent privilege)
- Don't create a separate account for assigning the user right

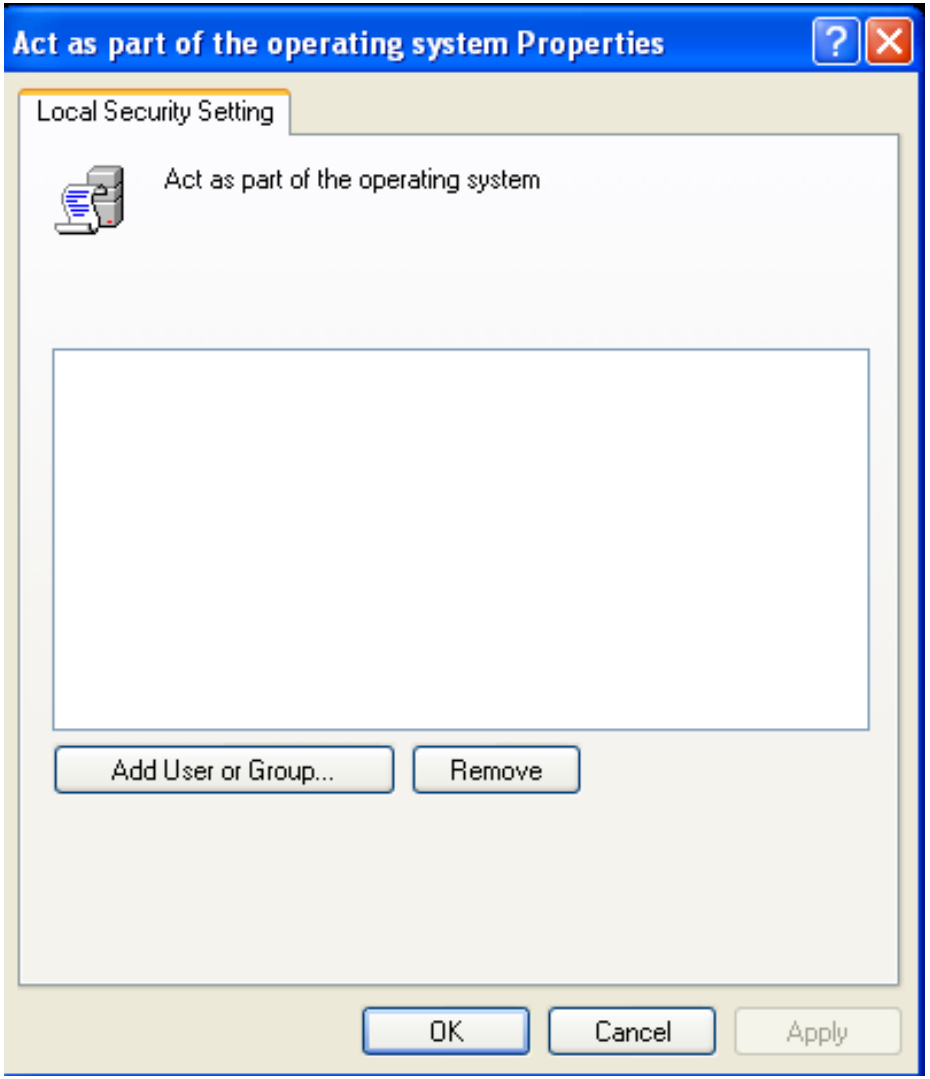
Potential Impact

- The impact provided should be very low as this user right is needed infrequently by accounts other than local system account

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Act as Part of the Operating System



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Add Workstations to Domain

This policy finds out that a user can add a computer to a specific domain or not. It must be assigned to one domain controller to make the policy condition affective. The limit on the number of workstations to add is up to 10

To add a computer to a domain the user must have permissions for **Create Computer Object**

The users with permission can add unlimited computers to the domain

The values for the Add workstations to domain setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Add Workstations to Domain

Vulnerability

- This right has a moderate vulnerability, which provides the right to add a computer to the domain configured to violate organizational security policy
- If a user with this right does not have an administrator privileges he can install windows and add to a domain, and can logon with that account and add them selves to the administrator group (local)

Countermeasure

- By configuring this setting only authorized members are allowed to add computers to the domain

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

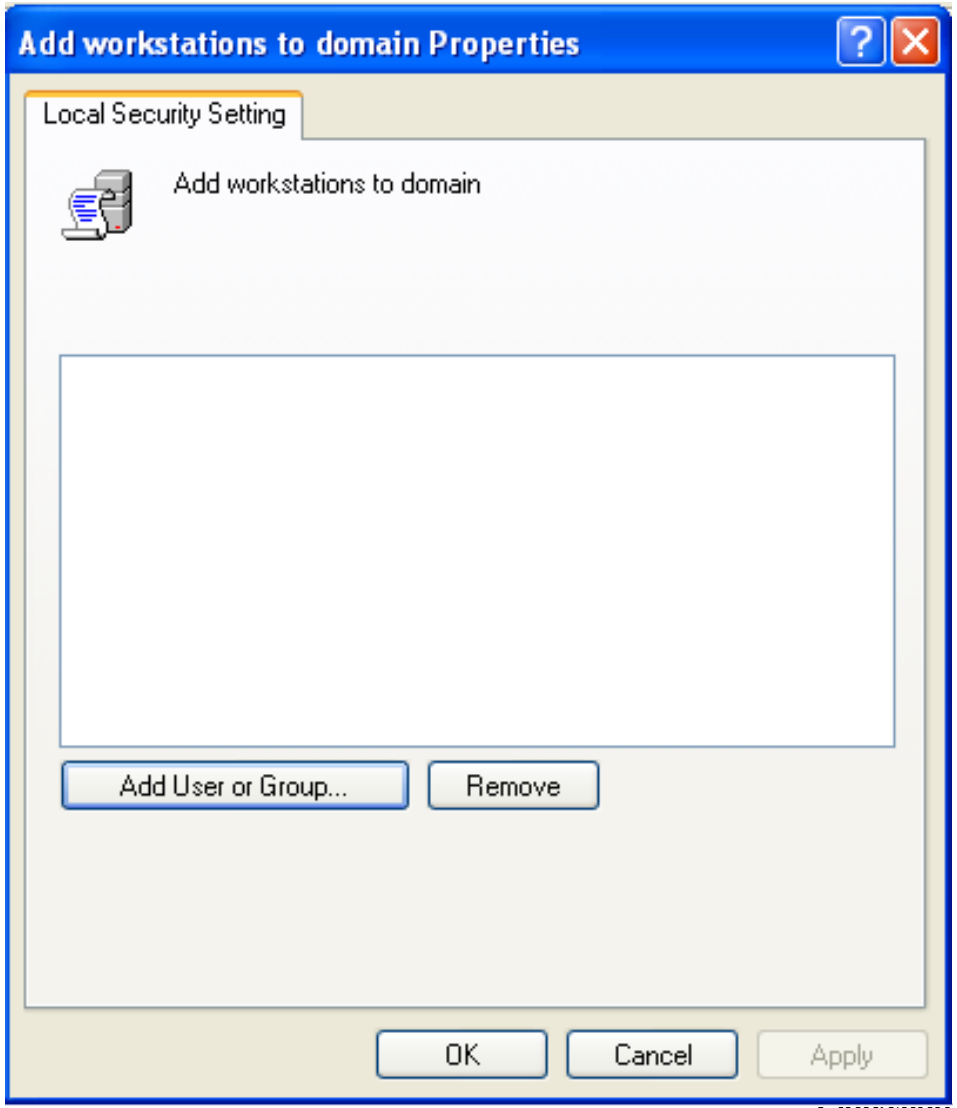
Add Workstations to Domain

Potential Impact

- This countermeasure won't be having any impact on the security policy, if the users are not allowed to configure there own computers and added them to the domain.
- In an organization if a user is allowed to configure there own computer, the organization has to set a process as a countermeasure.

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Add Workstations to Domain



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

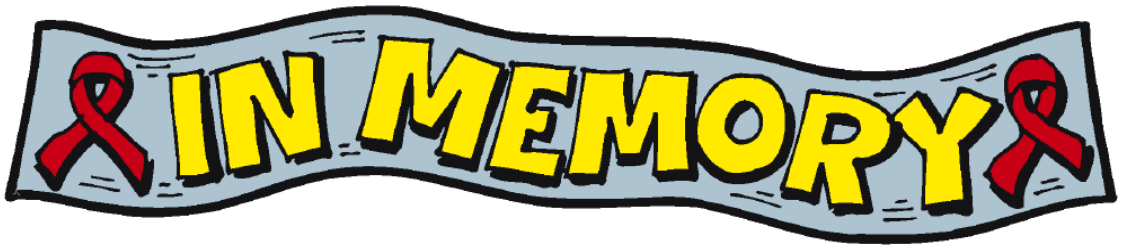
Adjust Memory Quotas for a Process

User concludes on allocating the maximum amount of memory available to a process. This is needed to tune computers.

This could even be used to start a launch denial of service (DoS) attack.

The values for the **Adjust memory quotas for a process** setting are:

- A user-defined list of accounts
- Not Defined



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Adjust Memory Quotas for a Process

Vulnerability	• A user with this privilege can minimize the amount of memory available a process, which can lead to slowing down or failing an business network application
Countermeasure	• This privilege must be given only to limited personnel's as application administrator or domain administrators
Potential Impact	• Organizations which are not following rule of limited privileges to the user, will find it difficult to follow this measure

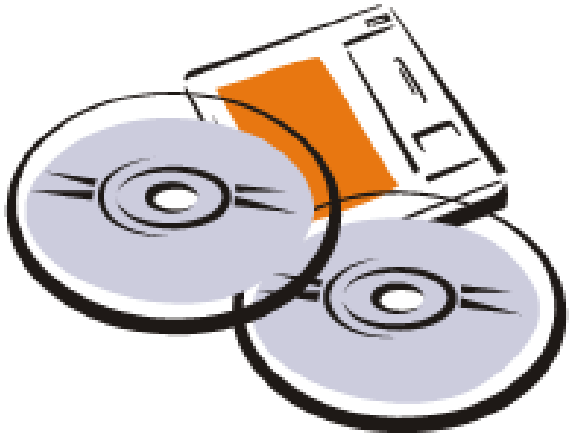
EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Adjust Memory Quotas for a Process

This privilege has to be assigned if the user is using optional components ASP.NET or IIS

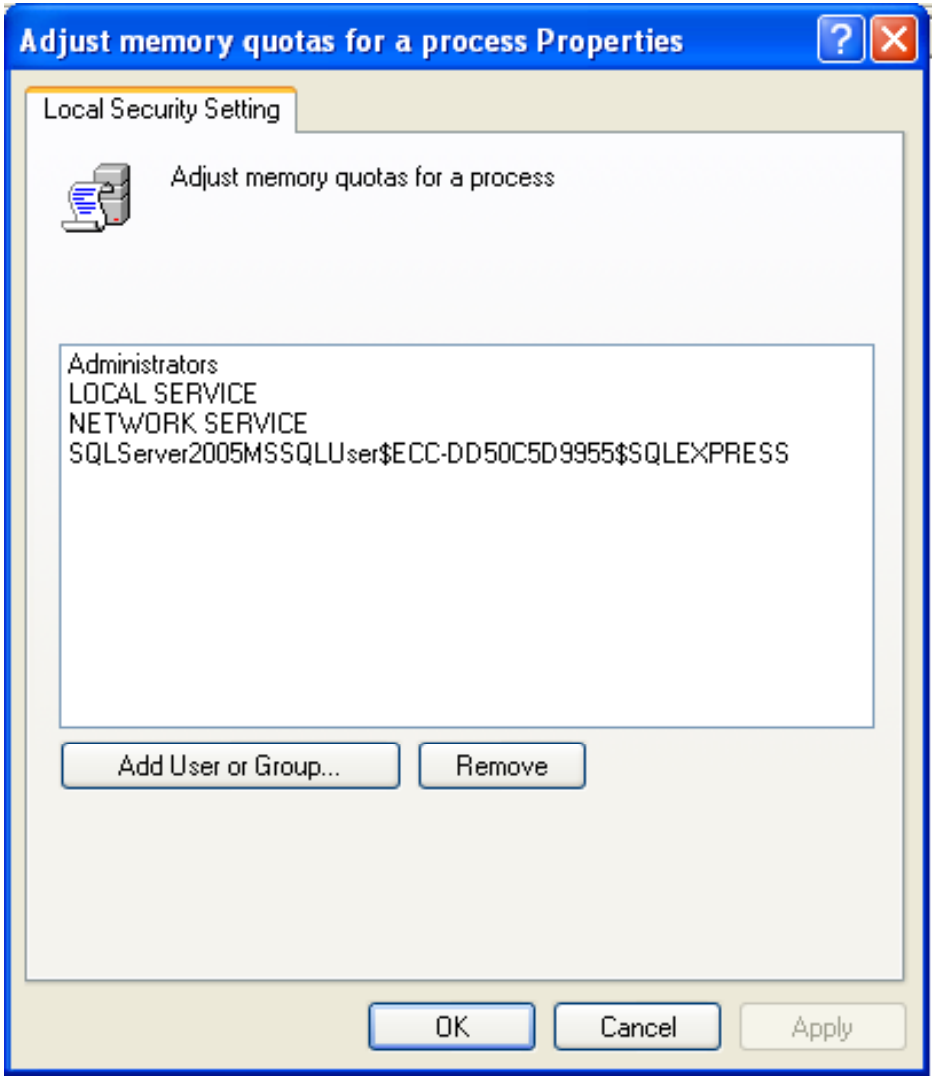
In IIS this privilege has to be given to IWAM_<*ComputerName*>, Network Service, and Service accounts



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Adjust Memory Quotas for a Process



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Log On Locally

This policy is used to start a interactive session on the computer

If **Allow logon through Terminal Services** right is given a remote interactive session can be started on the computer

The values for the **Allow log on locally** setting are:

- A user-defined list of accounts
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Log On Locally

Vulnerability

- This policy provides the right to logon to the console computer. AN unauthorized user with this right can logon and execute some malicious code

Countermeasure

- Give the right **Allow log on locally** to the **Administrators** group over domain controllers. On end-user computers allow this right to user groups

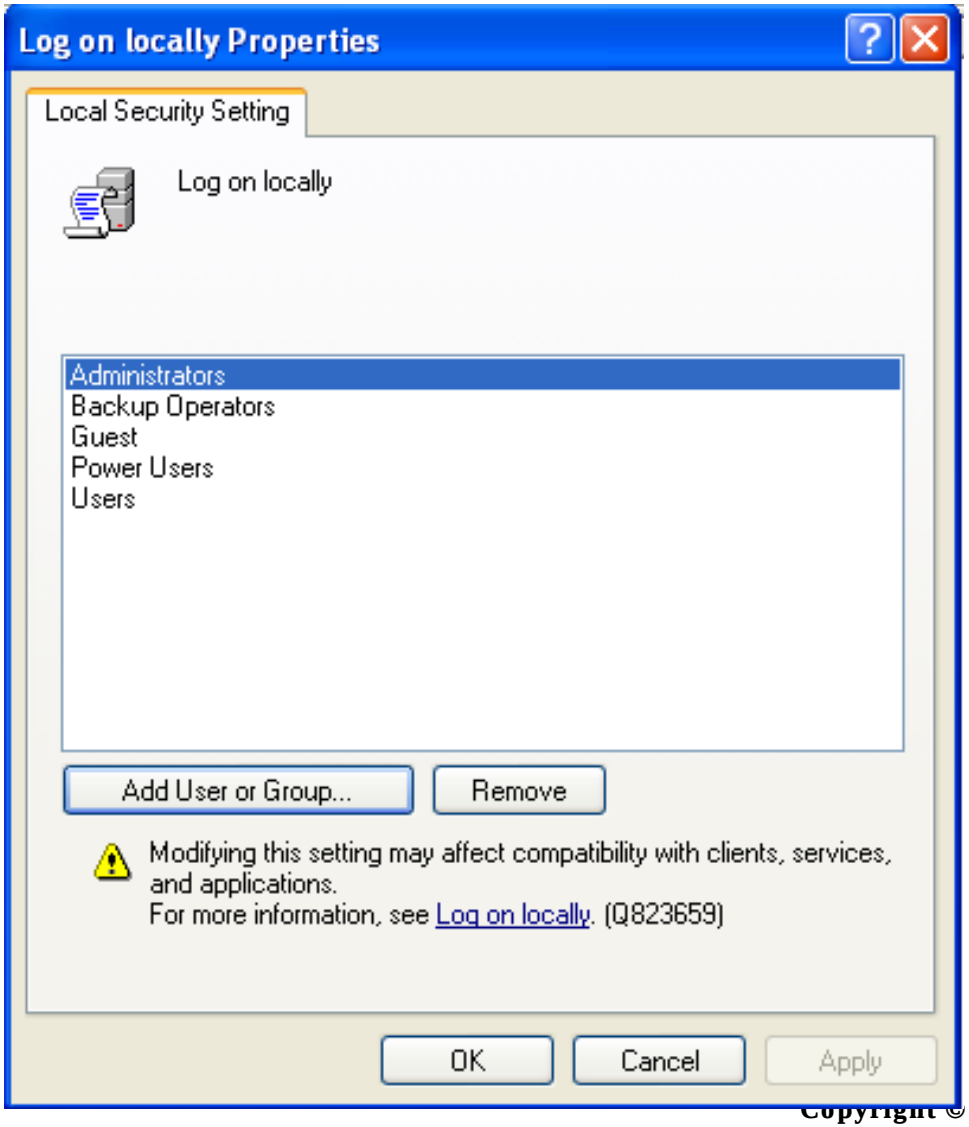
Potential Impact

- With a limitation on the default groups, it is possible to keep an eye on the allotted administrative privileges
- User with additional components as ASP.NET and IIS need this policy to be set

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Log On Locally



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Log On through Terminal Services

Allow log on through Terminal Services is used to figure out, whether a user can logon to another computer through a remote desktop connection

To keep a control on the personnel's opening a remote desktop connection is to add/remove them from **Remote Desktop Users** group

The values for the Allow log on through Terminal Services setting are:

- A user-defined list of accounts
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Log On through Terminal Services

Vulnerability

- If this right is not limited to legitimate personnel's, unauthorized personnel's can logon to the computer console and execute malicious code.

Countermeasure

- Assign the **Allow log on through Terminal Services** user right to the **Administrators** group on domain controllers.
- For server roles and end-user computers, also add the **Remote Desktop Users** group.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Log On through Terminal Services

Give **Deny Logon Through Terminal Services** right to groups as **Account Operators**, **Server Operators**, and **Guests**

As administrators may also be in **Deny Logon Through Terminal Services** group do not block there right

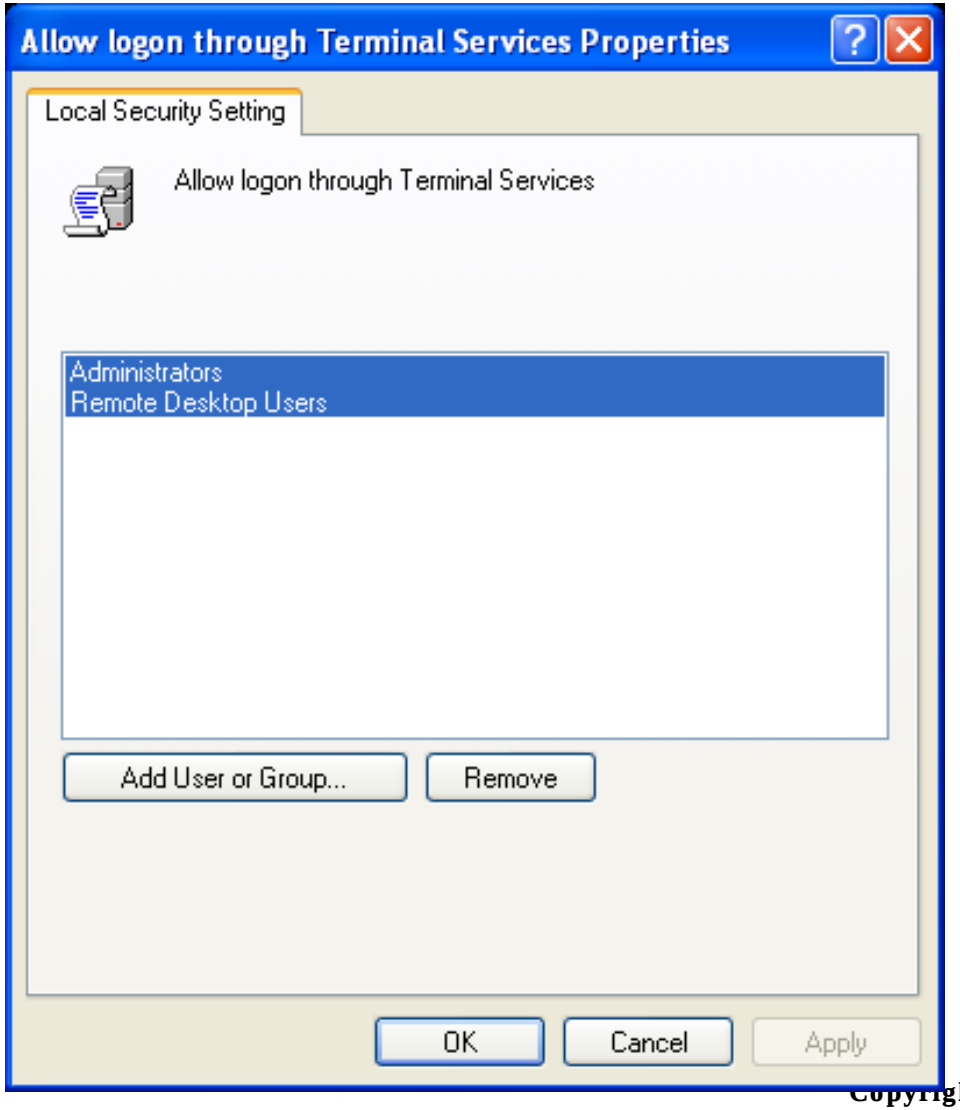
Potential Impact

- Confirm that hand over activities will not be adversely affected

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Log On through Terminal Services



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

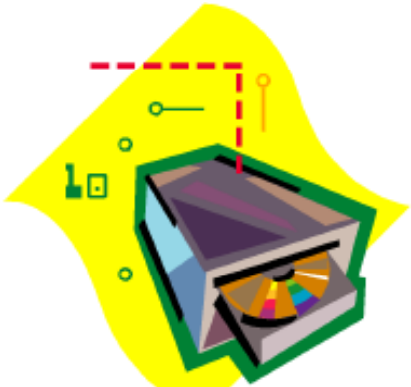
Back Up Files and Directories

This policy is used to conclude on avoiding file and directory permissions to take a back up of the computer

This right exists, when the application makes an NTFS backup, through a backup utility such as NTBACKUP.EXE

The values for the Back up files and directories setting are:

- A user-defined list of accounts
- Not Defined



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

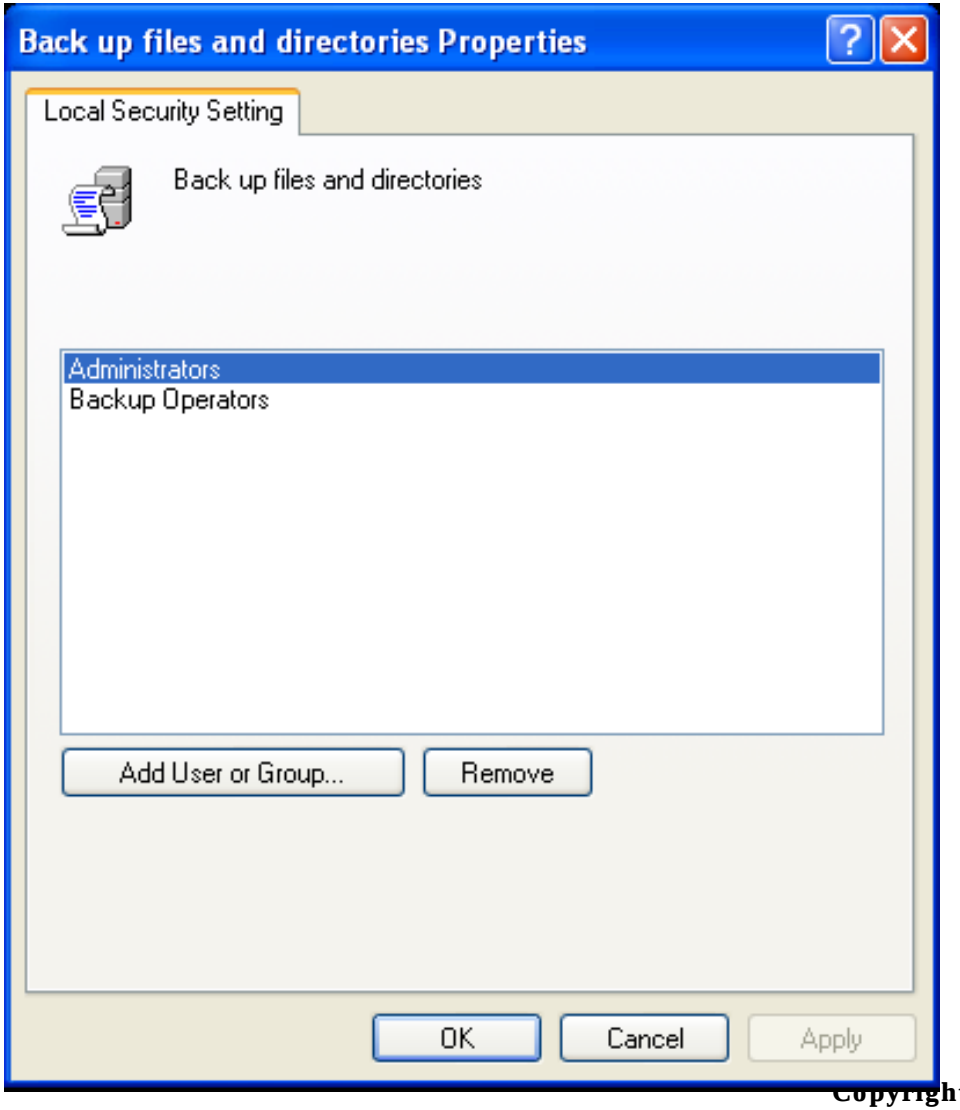
Back Up Files and Directories

Vulnerability	• Once the backup is taken the data can be moved to a non-domain computer, with administrative privileges. • After restoring the data they can view any unencrypted data in the backup
Countermeasure	• This right has to be given to people who need to perform this operation in a day-to-day job • If any software is used for taking backup using some service account then these account require the right
Potential Impact	• If any changes in the membership of the group are made, it has to make sure that the authorized personnel's are able to perform the backup task properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Back Up Files and Directories



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Bypass Traverse Checking

This policy concludes checking for permissions on the folders that are passed through “Traverse Folder”. As per the right user cannot list the folder contents but can traverse it

The values for the Bypass traverse checking setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Bypass Traverse Checking

Vulnerability

- By default this right is set to bypass traverse checking
- The administrator should have a keen understanding about the rights while assigning to the user

Countermeasure

- Organizations remove the **Everyone** group (or) **Users** group from the **Bypass traverse checking** user right
- A control should be made on traversal assignments to protect the sensitive information

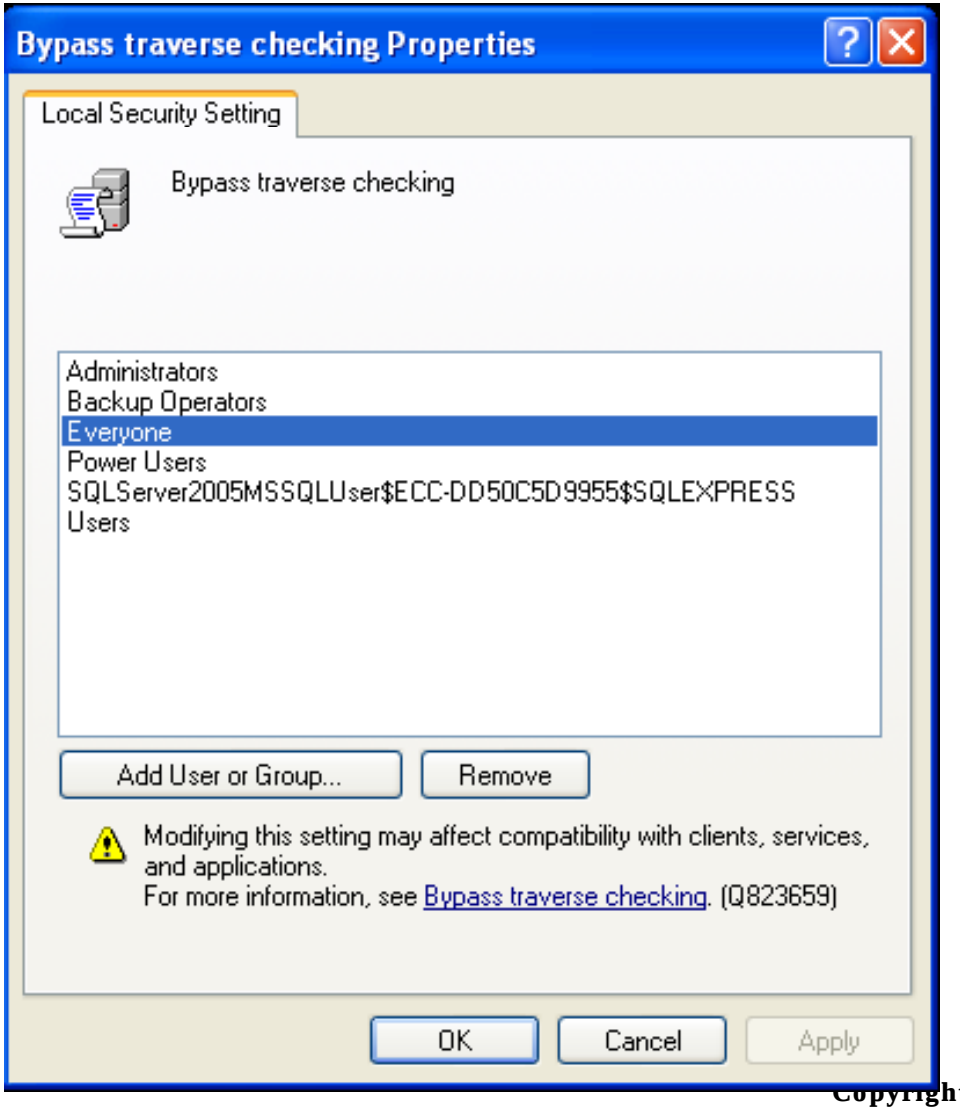
Potential Impact

- In Windows and many other applications **Bypass traverse checking** user right are assigned by default. So, the administrator must check the operations before making the changes
- The IIS and ASP.NET component users may need this user right

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Bypass Traverse Checking



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Change the System Time

This policy allows the user to change the system clock (internal). Changing Time zone and display settings of the system time doesn't require this policy setting

The values for the Change the system time setting are:

- A user-defined list of accounts
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Change the System Time

Vulnerability

- Kerberos need requestor's and authenticator's clocks synchronized
- Several problems caused when system time is changed by the users.
  - Time stamps on the event log could be inaccurate.
  - Time stamps on files and folders could be incorrect.
  - Computers on the domain could not authenticate themselves.
- An attacker may unable a Kerberos ticket by changing the system time.

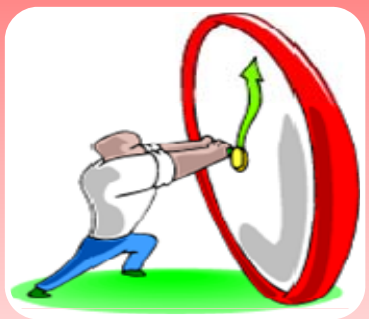
EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Change the System Time

The Windows Time service synchronizes time with domain controllers by design in the following ways:

- A domain controller acts as a inbound time partner between client desktop computers and member servers
- The Primary Domain Controller (PDC) is the inbound time partner for all domain controllers
- PDC emulates follow a hierarchy of domains for selecting an inbound time partner.
- PDC emulator (route) must be configured from an external time server



If an attacker changes the system time and reconfigure it with an inaccurate time server, this vulnerability is more severe.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Change the System Time

Countermeasure

- This right should be given only to he members of the IT team who are legitimate to change the system time

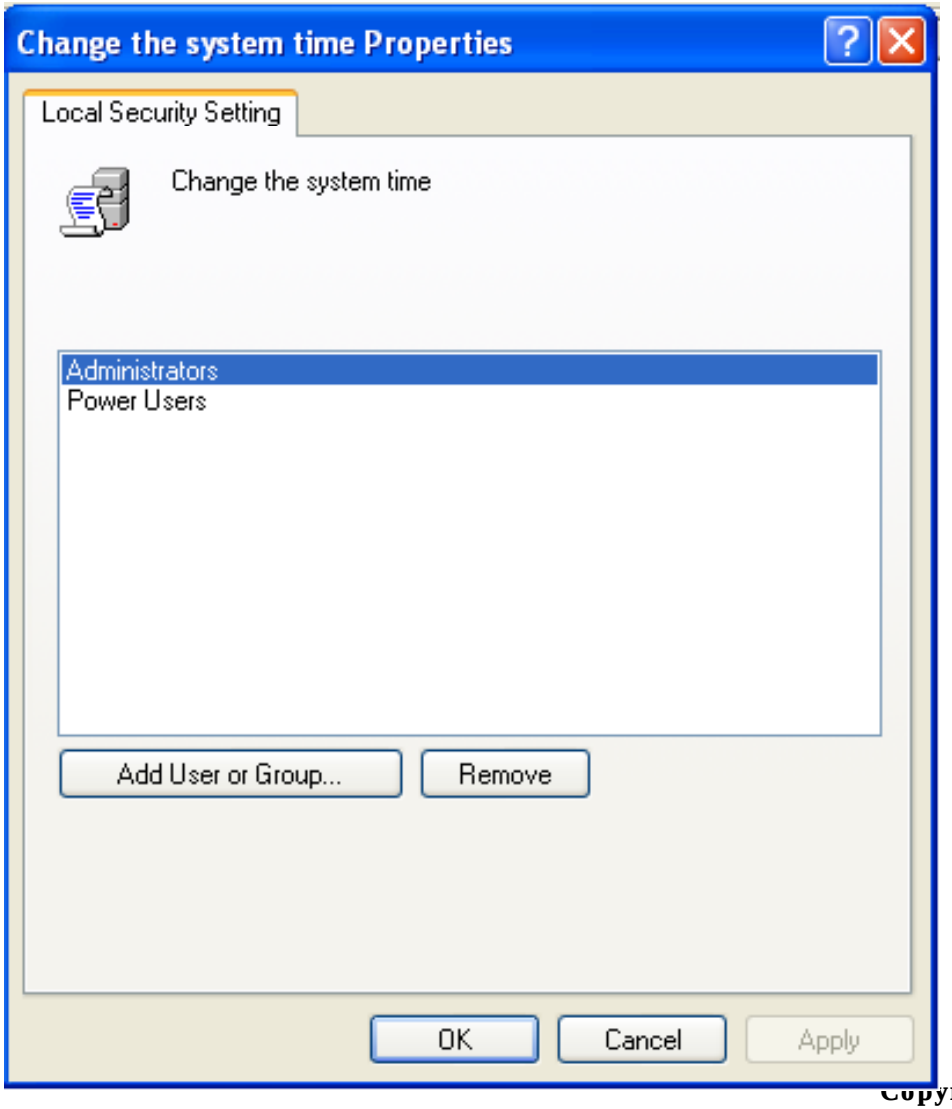
Potential Impact

- Time synchronization should be automated for all computers in domain
- Individual systems should be synchronized by the help of external resources

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Change the System Time



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create a Page File

This policy setting concludes that user can create and change the size of a page file

It is concluded by the policy that the page file size on a specific drive in the **Performance option** box placed under **Advanced** tab of the **System Property** dialog box can be crated or changed

The values for the Create a page file setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create a Page File

Vulnerability

- On changing the page file size to tremendously small (or) moving it to an extremely partitioned storage volume the user can reduce the system performance

Countermeasure

- This right should be given to the **Administrators** group only

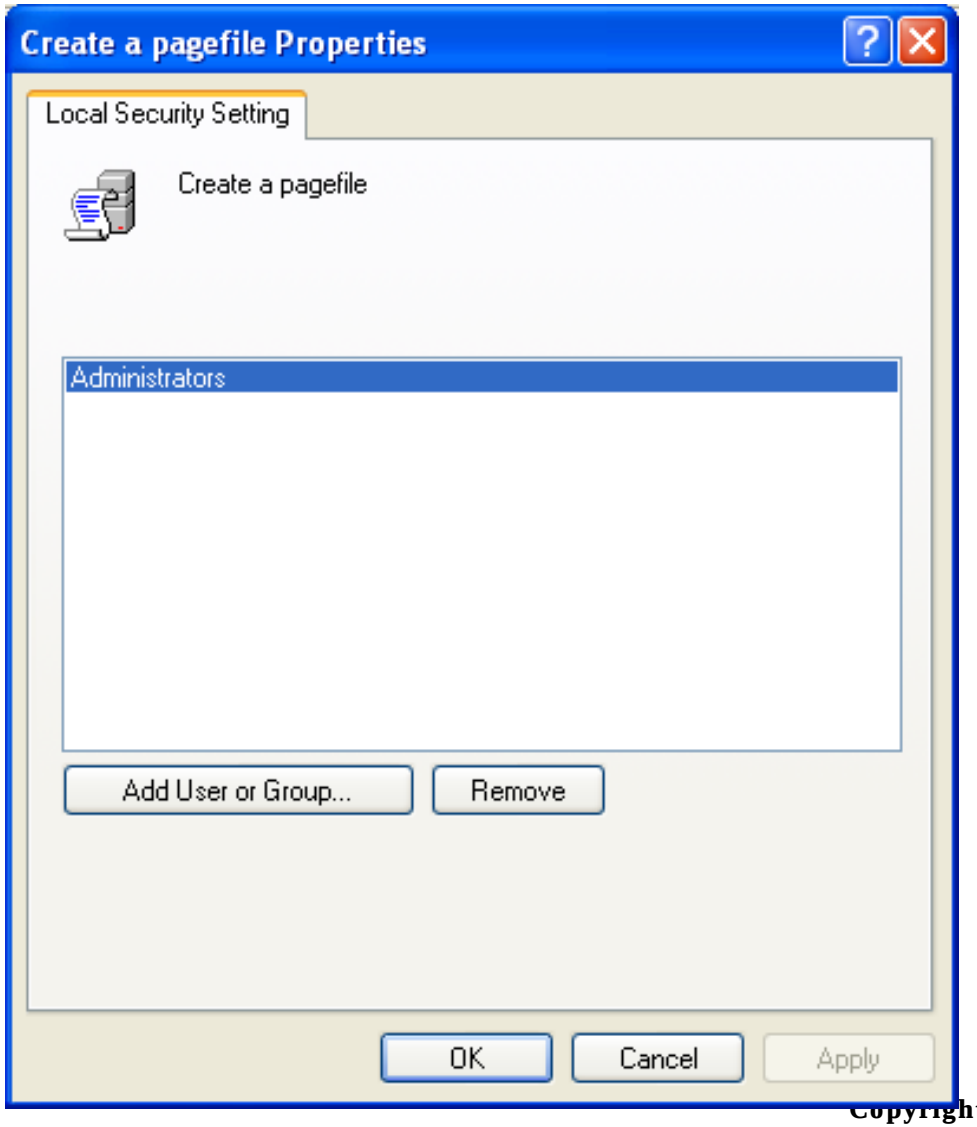
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create a Page File



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create a Token Object

This policy decides a application can create a token or not. Used to gain access to local resources while using NtCreateToken() or a token creation object

The values for the Create a token object setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create a Token Object

Vulnerability

- If a user connects to a local computer or remote computer on the network a token is created
- Access tokens specify the user privileges and his level
- A change in the privileges is at once recorded to the token but they are not effective until the user logon again
- A user with the ability to modify tokens can change his privileges or create a DoS condition

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

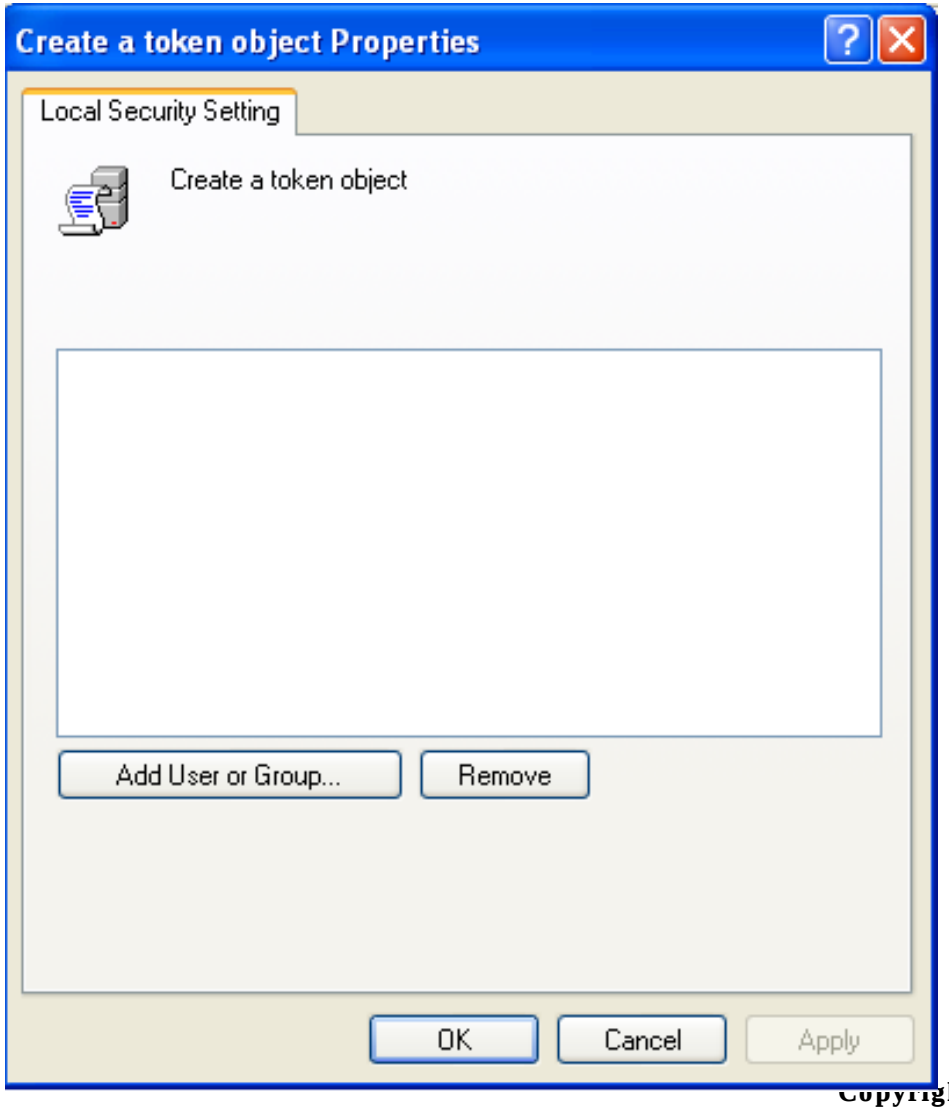
Create a Token Object

Countermeasure	• Any process in necessity of a right should use a system account, which holds the right • This right should not be assigned to a specific user
Potential Impact	• None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create a Token Object



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create Global Objects

This policy checks that the user can create a global object which will be accessible by all sessions

The values for the Create global objects setting are:

- A user-defined list of accounts
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

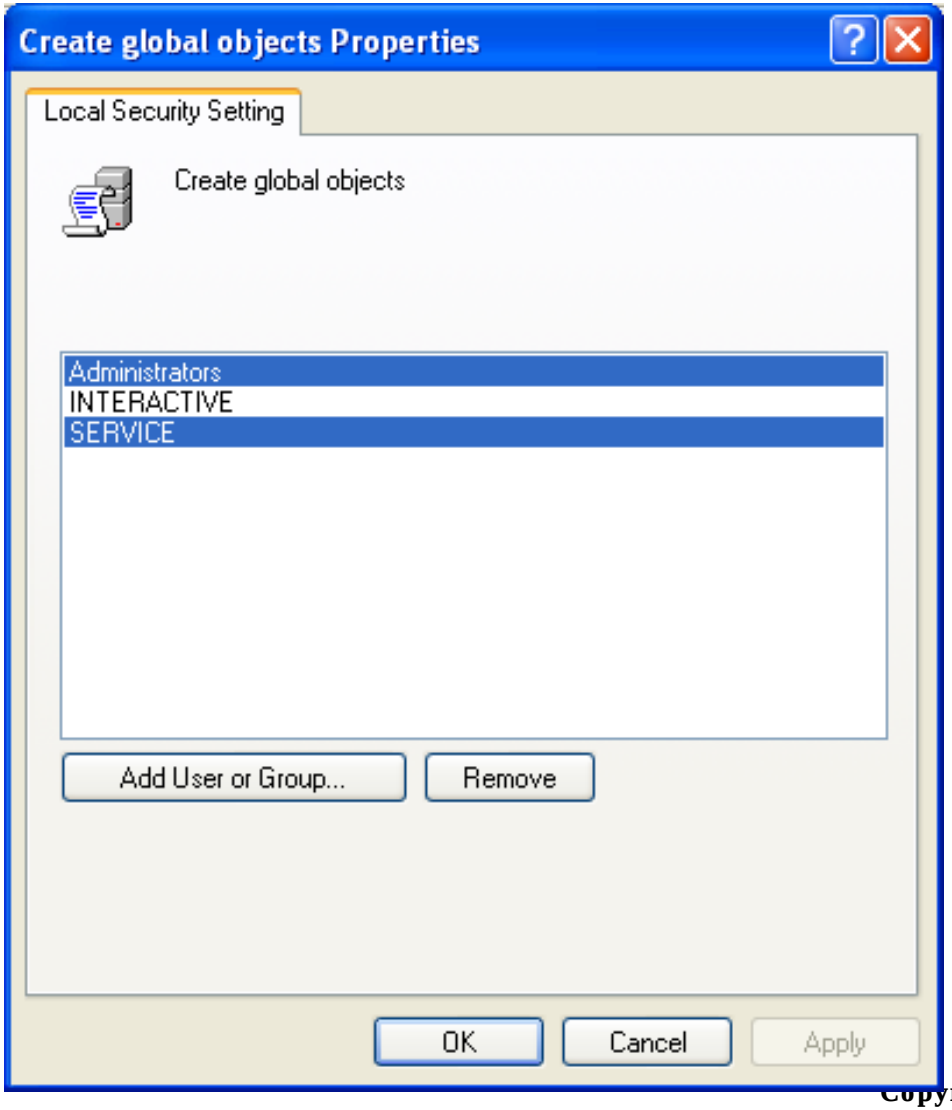
Create Global Objects

Vulnerability	• The created global object could have an effect on processes of other users. This could lead to application failure or data corruption.
Countermeasure	• This right should be given to local **Administrators** and **Service** groups.
Potential Impact	• None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create Global Objects



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create Permanent Shared Objects

This policy concludes on creating a directory objects in the object manager, with which users can create permanent shared objects, including devices, semaphores, and mutexes. Kernel mode components can use this right to extend object namespace

The values for the Create permanent shared objects setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create Permanent Shared Objects

Vulnerability

- Users with this right can create new shared objects and reveal sensitive data to the network

Countermeasure

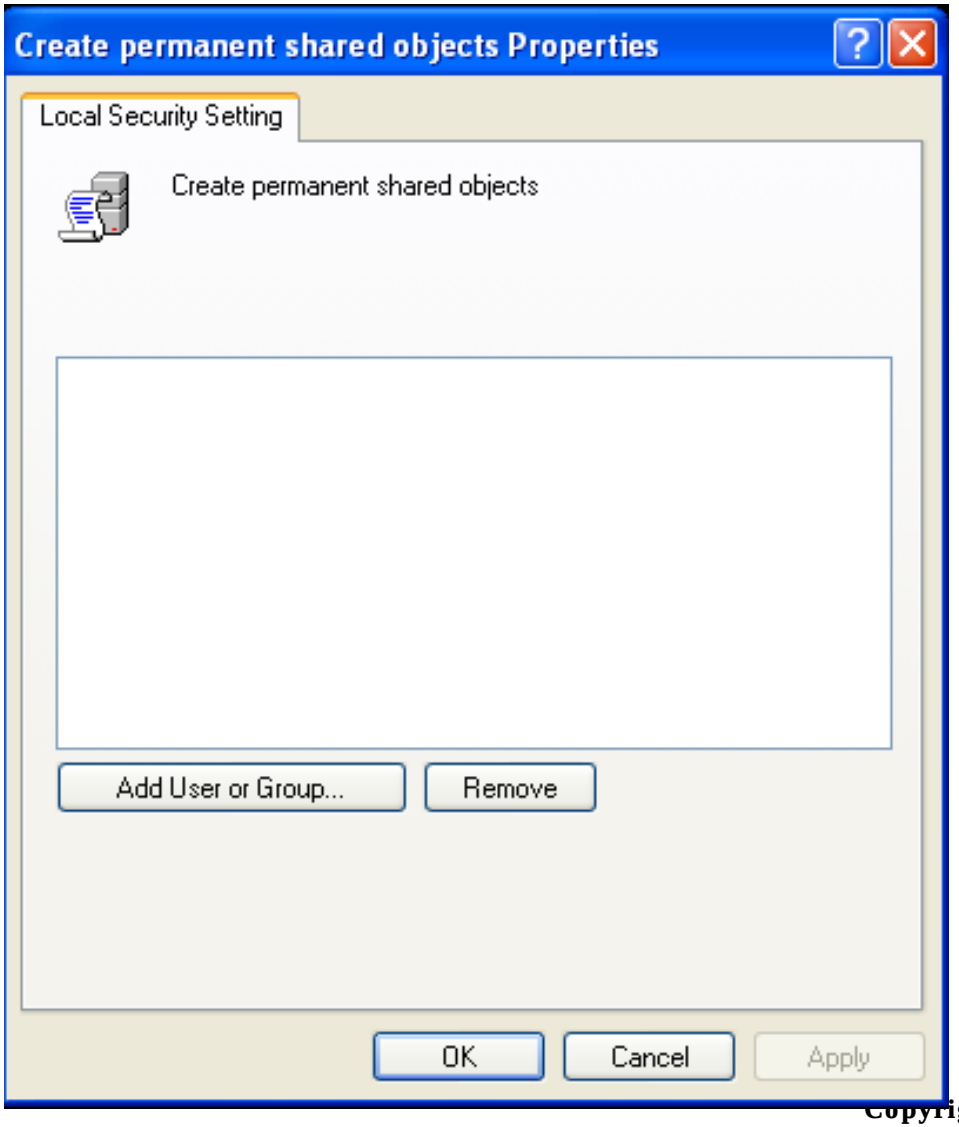
- Processes which need this right must work with the system account (which already includes this user right)

Potential Impact

- None

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Create Permanent Shared Objects



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Debug Programs

This policy checks that users can open or attach to any process, even if they don't own it.

This right gives access to sensitive and critical operating system components.

The values for the Debug programs setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Debug Programs

Vulnerability

- It congregates sensitive information from system memory (or) gain entry to kernel or application structure and changes it.
- Attacks are made through this right to get passwords from hashed tables and gain access to other security information.
- This right is only assigned to an administrator.

Countermeasure

- Timely change this right from users who do not require it.

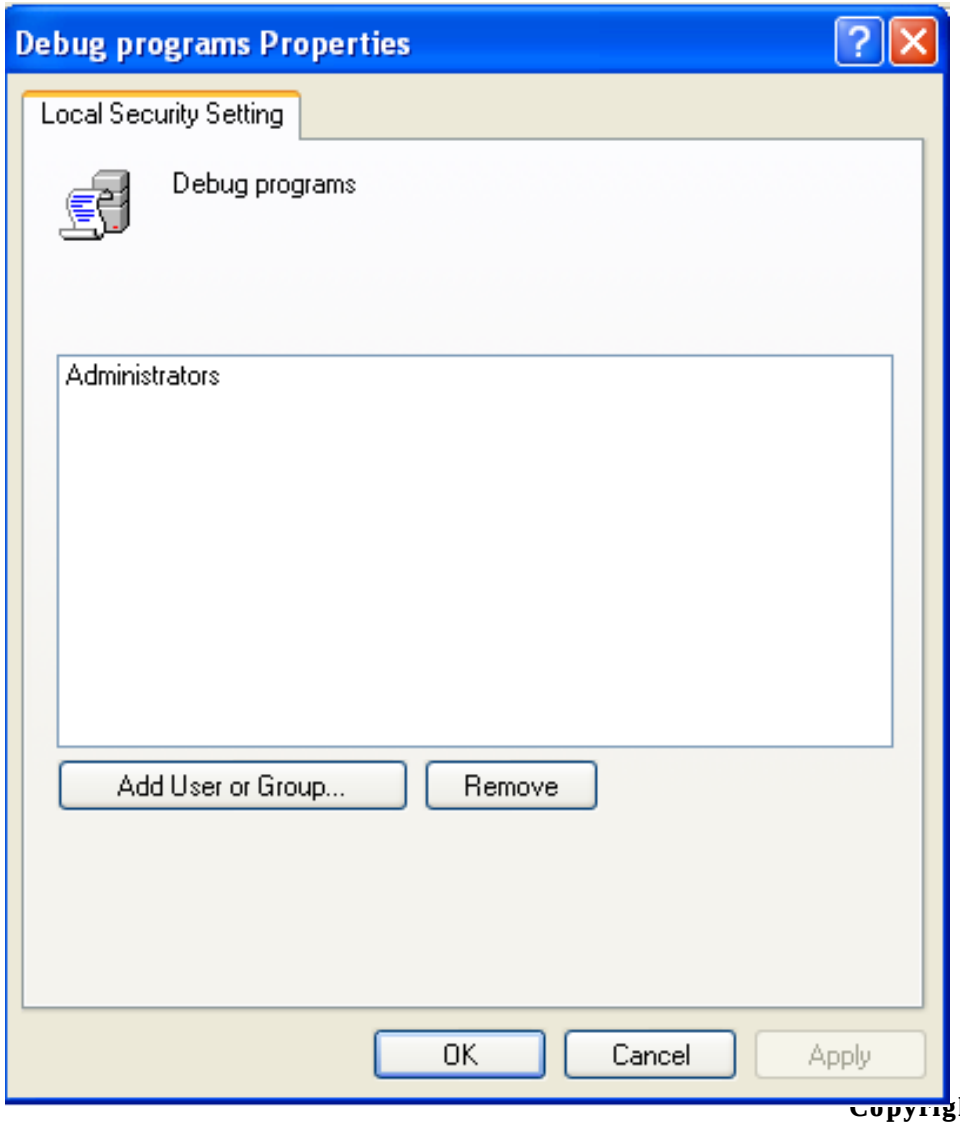
Potential Impact

- If this right is revoked no program can be debugged.
- This right is necessary for service accounts, which acts as a cluster service.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Debug Programs



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Access to this Computer from the Network

This policy ascertains that user can connect to the computer from the network.

The values for the **Deny access to this computer from the network** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Access to this Computer from the Network

Vulnerability

- By setting this policy a user can be restricted from accessing some particular resources, as shared folders and files
- Without this right the user can access, view and modify the data over the network
- This right gives a limitation over some accounts as a guest account who don't need to access the shared files

Countermeasure

- This right should be allocated to:
  - ANONYMOUS LOGON
  - The built-in local Administrator account
  - The local Guest account
  - The built-in Support account
  - All service accounts
- This right is useful while configuring servers and workstations with sensitive information

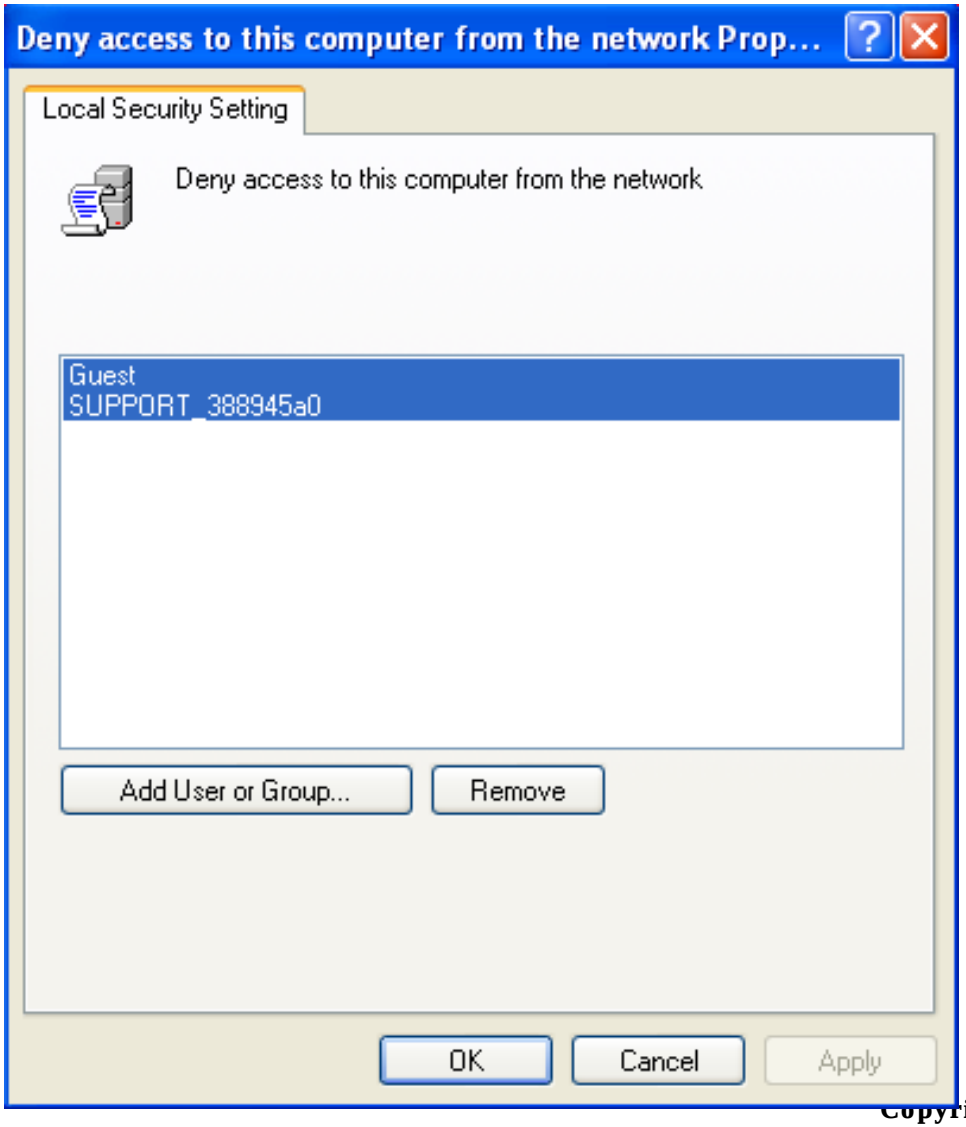
Potential Impact

- The user abilities can be affected by assigning this user right

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Access to this Computer from the Network



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On as a Batch Job

This protocol determines if you can log on through a batch-queue facility or not. Its characteristics in Windows Server 2003 are used to schedule and launch a task automatically one or more times.

This right is used to start a scheduled task.

The possible values for the **Deny log on as a batch job** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On as a Batch Job

Vulnerability

- This protocol schedules a task that consumes huge computer resources and causes a DoS state.

Countermeasure

- This right is given to the built-in Support account and the local Guest account.

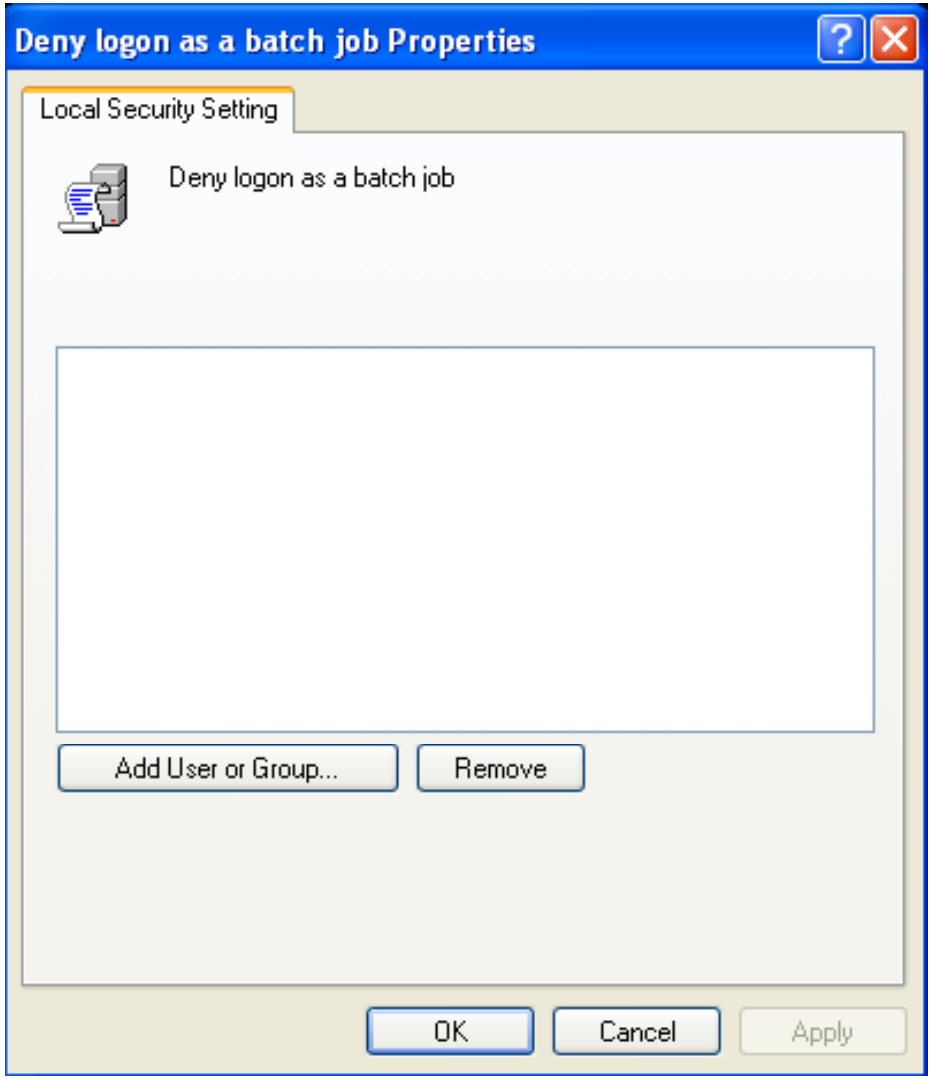
Potential Impact

- By allotting this right you can deny users assigned to administrative roles (the ability to perform their required job activities).
- On a computer that runs Windows Server 2003 the account do not fit in to the **Guests** group, but on a computer which is upgraded from Windows 2000 this account is associated to a **Guests** group.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On as a Batch Job



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On as a Service

Check whether a user can logon to a service or not

The values for the **Deny log on as a service** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

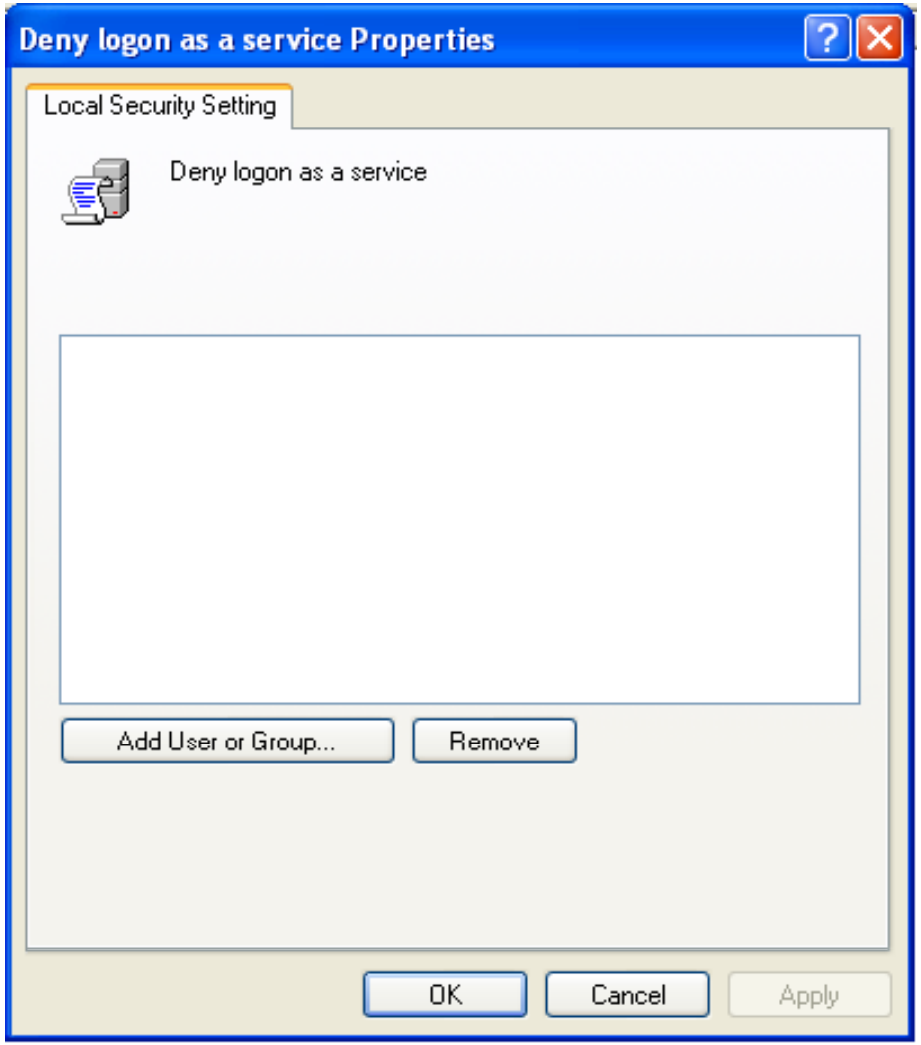
Deny Log On as a Service

Vulnerability	• Users with accounts capable of logging on as a service can start new unauthorized services as keylogger or any malware • As per the countermeasures only accounts with administrative privileges can install and configure the services
Countermeasure	• It is suggested not to avail this right to the accounts with default configuration
Potential Impact	• If this right is assigned to specific accounts, services may not start and could raise DoS condition

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On as a Service



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On Locally

These settings conclude whether you can logon directly on a computers keyboard.

The values for the **Deny log on locally** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On Locally

Vulnerability

- If this right is not limited to justifiable users, unauthorized users can download and execute malicious code
- An account with the ability to log on locally could be used to log on at the console

Countermeasure

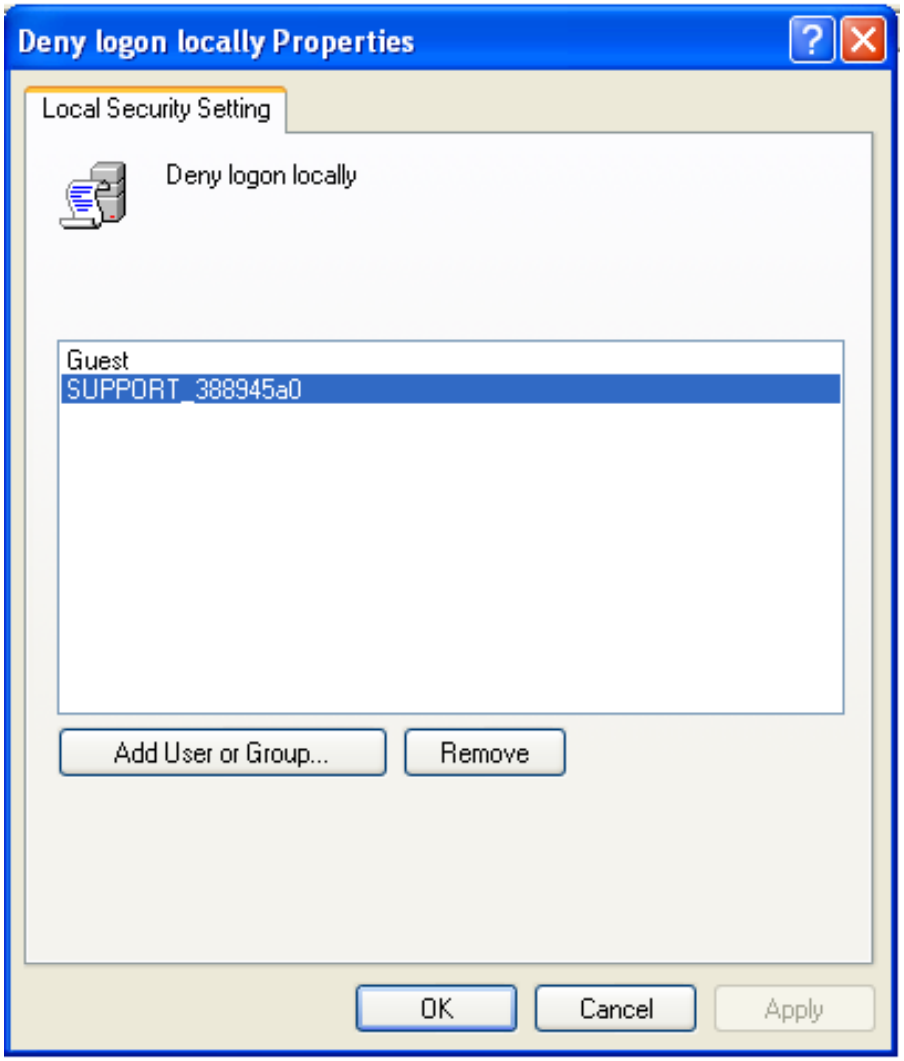
- This right can be given to built-in Support account
- This user right might have to be given to additional accounts that use ASP.NET Components

Potential Impact

- This right should be allotted to user having ASP.NET and IIS 6.0
- It should be confirmed that assigned activities will not be adversely affected

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On Locally



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On through Terminal Services

This determines on the user right to logon to the computer through a remote desktop connection.

The values for the **Deny log on through Terminal Services** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On through Terminal Services

Vulnerability

- If users are not restricted for logging on from a distinct console, then unauthorized users may download and install malicious code

Countermeasure

- This right has to be assigned to local Administrator account and all service accounts
- Users with ASP.NET components might need this right

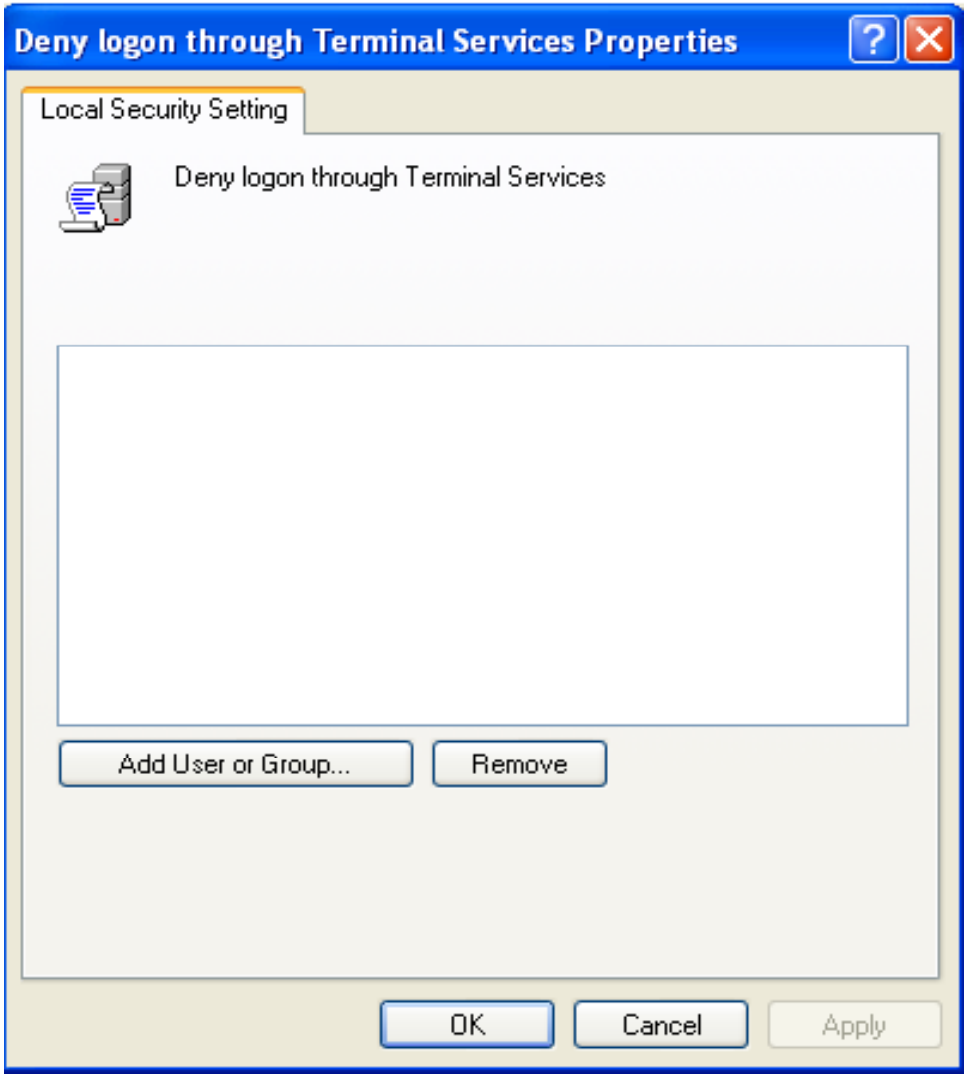
Potential Impact

- Assigning this right to other group could restrict the abilities of users with specific administrative roles in your environment
- Accounts with this user right are unable to connect to a computer through either Terminal Services or Remote Assistance

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log On through Terminal Services



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enable Computer and User Accounts to be Trusted for Delegation

This right checks that a user can modify the **Trusted for Delegation** settings on a user or computer object in Active Directory

Users with this right must have write access to the account control flags on the object

Delegation of authentication is an ability that is used by multi-tier client/server applications, through which a front-end service uses client identification to authenticate to a back-end service

Both client and server accounts must be trusted for delegation

The values for the **Enable computer and user accounts to be trusted for delegation** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enable Computer and User Accounts to be Trusted for Delegation

Vulnerability

- By unauthorized use of the right, users on the network might be impersonated
- An attacker can gain access to network resources

Countermeasure

- This right should be assigned with a clear need for its functionality
- While assigning this right, you should investigate on the use of constrained delegation to control the activities of a delegated account

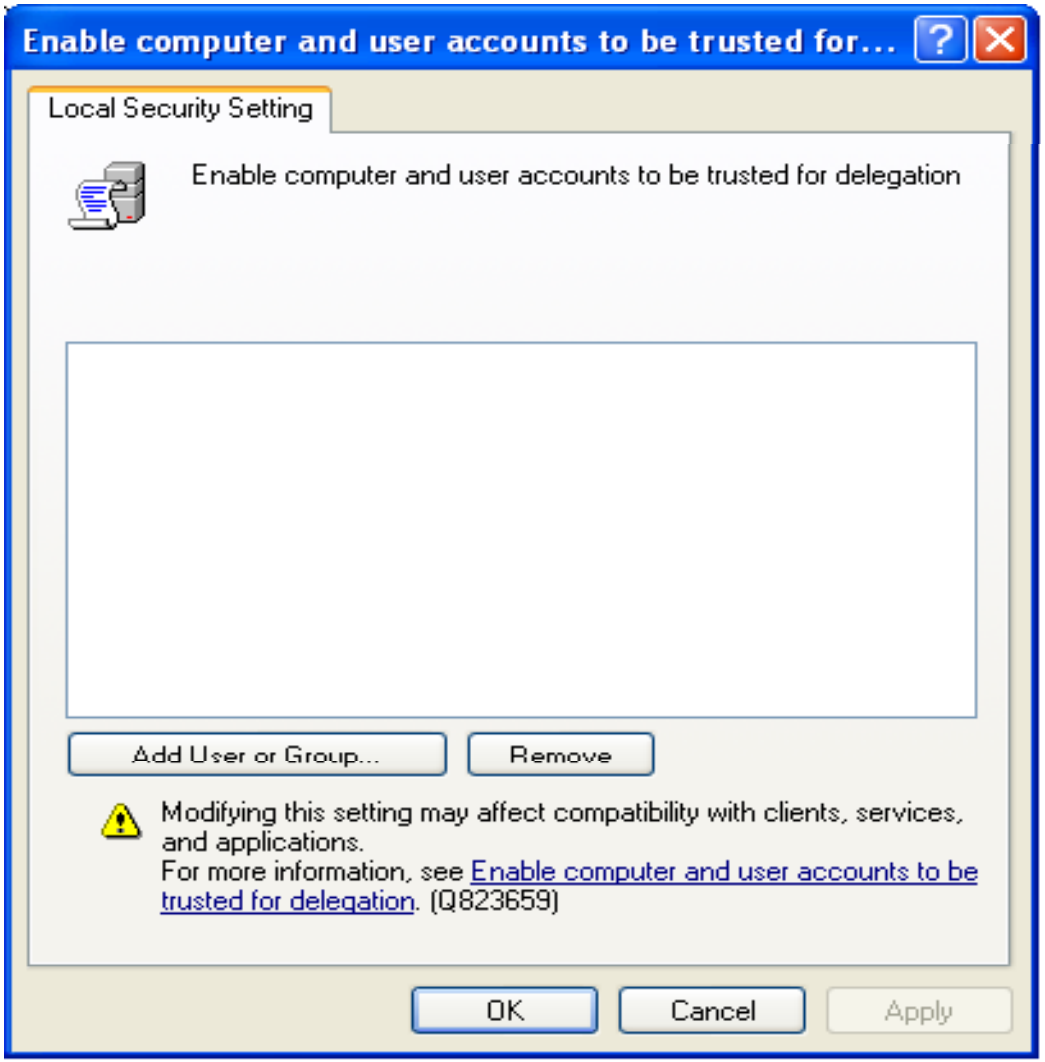
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enable Computer and User Accounts to be Trusted for Delegation



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Force Shutdown from a Remote System

This right gives the ability to shut down a computer from a remote location on the network.

The values for the **Force shutdown from a remote system** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

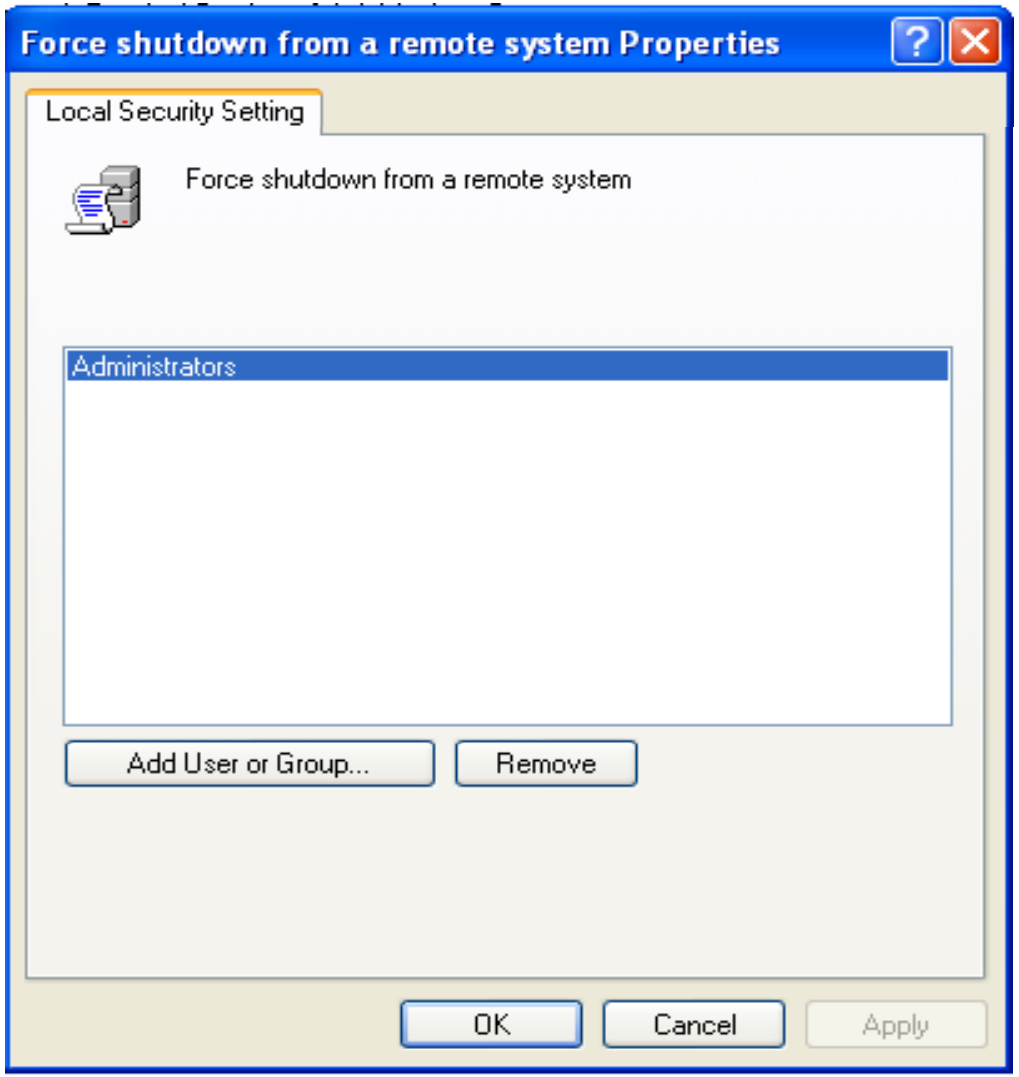
Force Shutdown from a Remote System

Vulnerability	• This right should be restricted as if a computer not shutdown properly a DoS condition may occur.
Countermeasure	• This right should only be given to Administrators or other personnel are who needed to perform some administrative operations.
Potential Impact	• By restricting this right to the server operator group, you may limit specific administrative roles.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Force Shutdown from a Remote System



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Generate Security Audits

This policy can determine that a process can generate audit records in the Security log

The information in the Security log can trace unauthorized computer access

The values for the **Generate security audits** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Generate Security Audits

Vulnerability

- If an attacker gets access to a computer capable of writing security logs could fill that log with meaningless data. An attacker can clear the evidence of an unauthorized activity if the computer is configured to overwrite events
- If the computer is configured to shut down on unable of writing to Security log and it is not set to take a backup, this method could be used to create a denial of service

Countermeasure

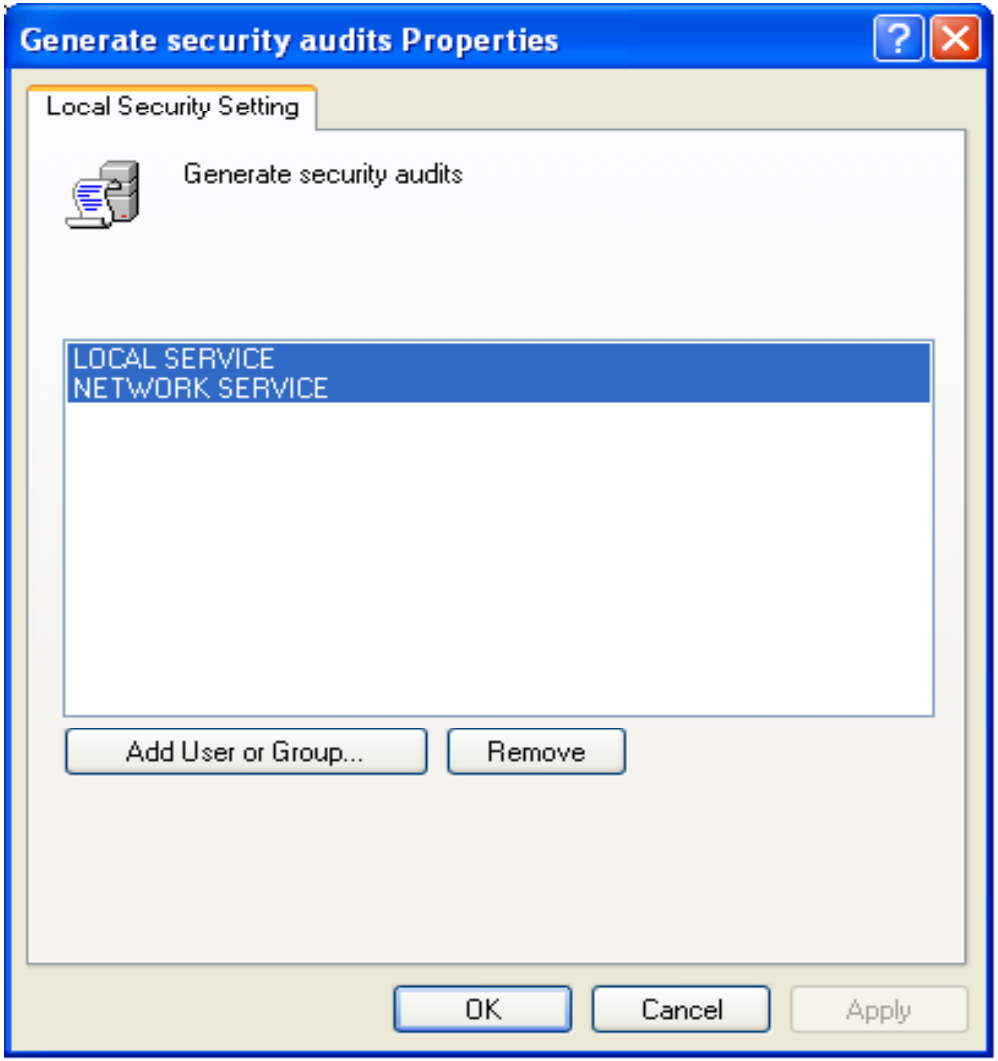
- This right should be given to the Service and Network Service accounts

Potential Impact

- None

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Generate Security Audits



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Impersonate a Client after Authentication

This right allows programs that run on behalf of a user to impersonate that user or account

By this kind of impersonation, an unauthorized user can not convince a client to connect

Services started by the Service Control Manager and COM servers started by the COM infrastructure and configured to run under a specific account, have a built-in **Service** group added to their access tokens

These processes are assigned this user right when they are started

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Impersonate a Client after Authentication

A user can impersonate an access token if any of the following conditions exist:

- The access token that is being impersonated is for this user
- The user, in this logon session, logged on to the network with explicit credentials to create the access token
- The requested level is less than Impersonate, such as Anonymous or Identify.

Users do not usually need to have this user right assigned

The values for the **Impersonate a client after authentication** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Impersonate a Client after Authentication

Vulnerability

- An attacker with this right can create a service to trick a client and make them connect to the service to impersonate that client and elevate his level of access to the clients

Countermeasure

- This right has to be with **Administrators** and **Service** groups
- Computers that run IIS 6.0 must have this user right assigned to the IIS_WPG group

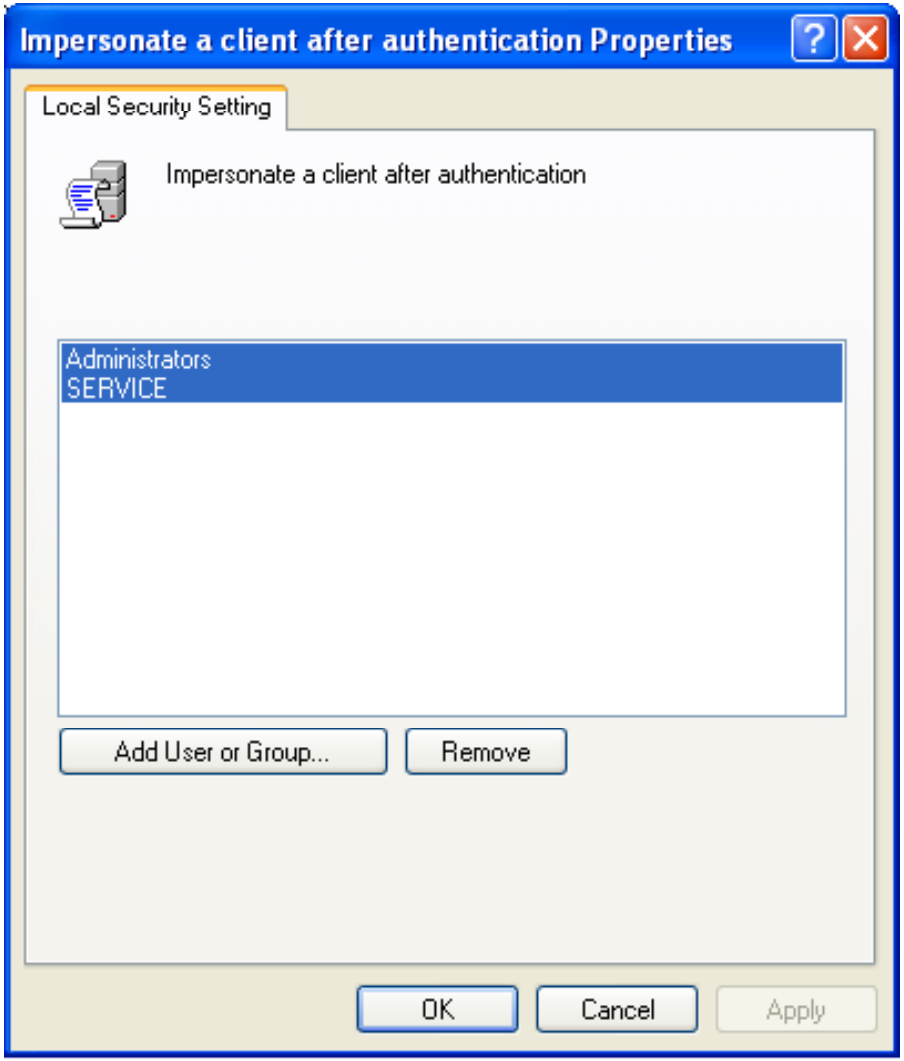
Potential Impact

- If there are any optional components as ASP.NET or IIS, this right has to be given to those accounts

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Impersonate a Client after Authentication



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Increase Scheduling Priority

The Base priority class of a process can be increased by this policy.

This right might be required by software development tools.

The values for the **Increase scheduling priority** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Increase Scheduling Priority

Vulnerability

- With this right the user can increase the scheduling priority of a process, which might lead to a DoS condition as very less amount of processing time will be left for other processes

Countermeasure

- *This right should be only with Administrators*

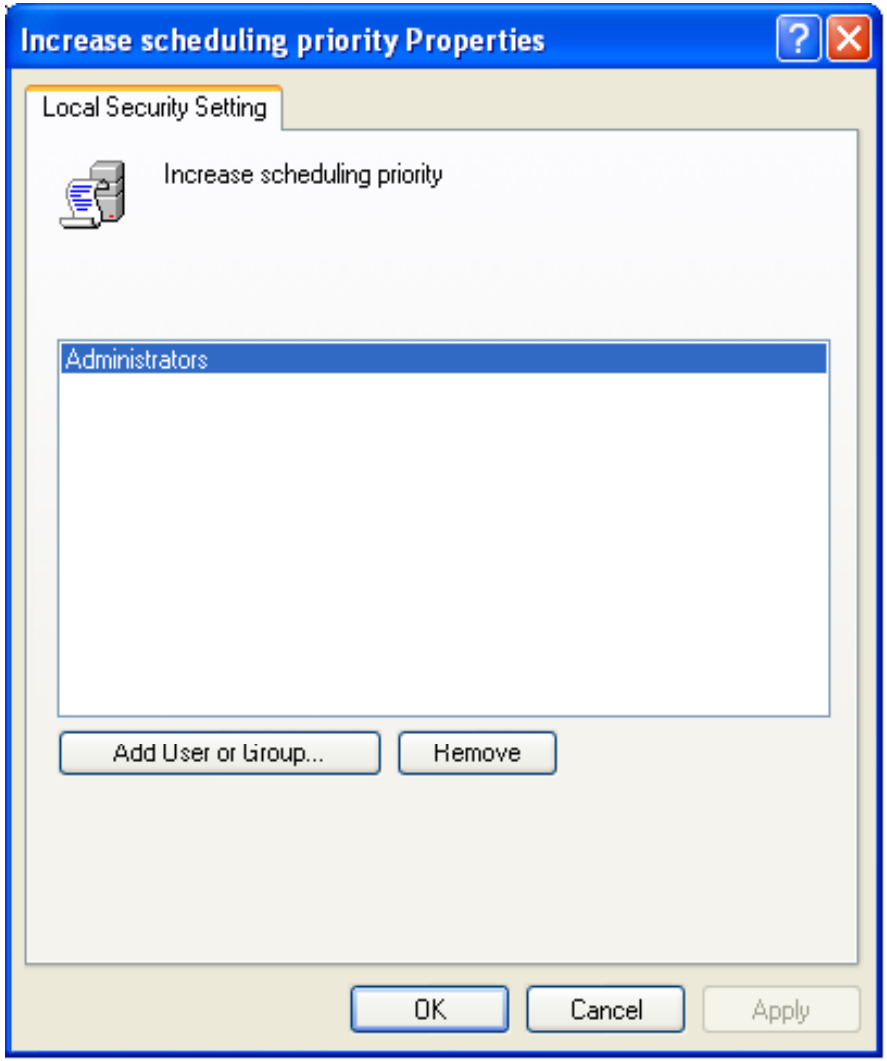
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Increase Scheduling Priority



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Load and Unload Device Drivers

This policy checks on dynamically loading and unloading device drivers. If a signed driver for the hardware already exists in the Driver.cab file, setting this right is not necessary

The values for the **Load and unload device drivers** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Load and Unload Device Drivers

Vulnerability

- Device drivers are highly privileged codes. Administrators should take extra care and install only drivers with verified digital signatures

Countermeasure

- Only **Administrators** on member servers should have this right. On domain controllers this right has to be given only to **Domain Administrators**

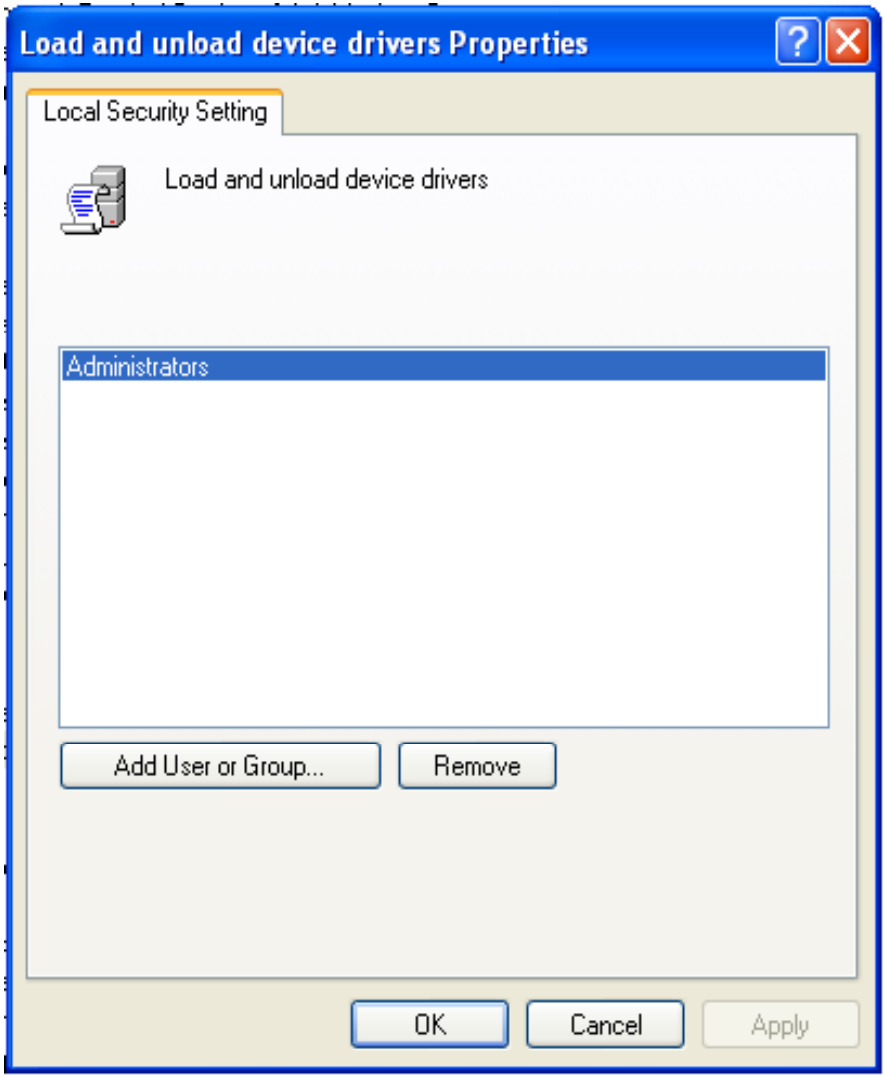
Potential Impact

- By restricting this right to **Print Operators** group or other accounts, the abilities of users with administrative roles are limited

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Load and Unload Device Drivers



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Lock Pages in Memory

This right permits a process to store data in physical memory and prevents the data from paging to virtual memory

With this right the computer performance can be decreased

The values for the **Lock pages in memory** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

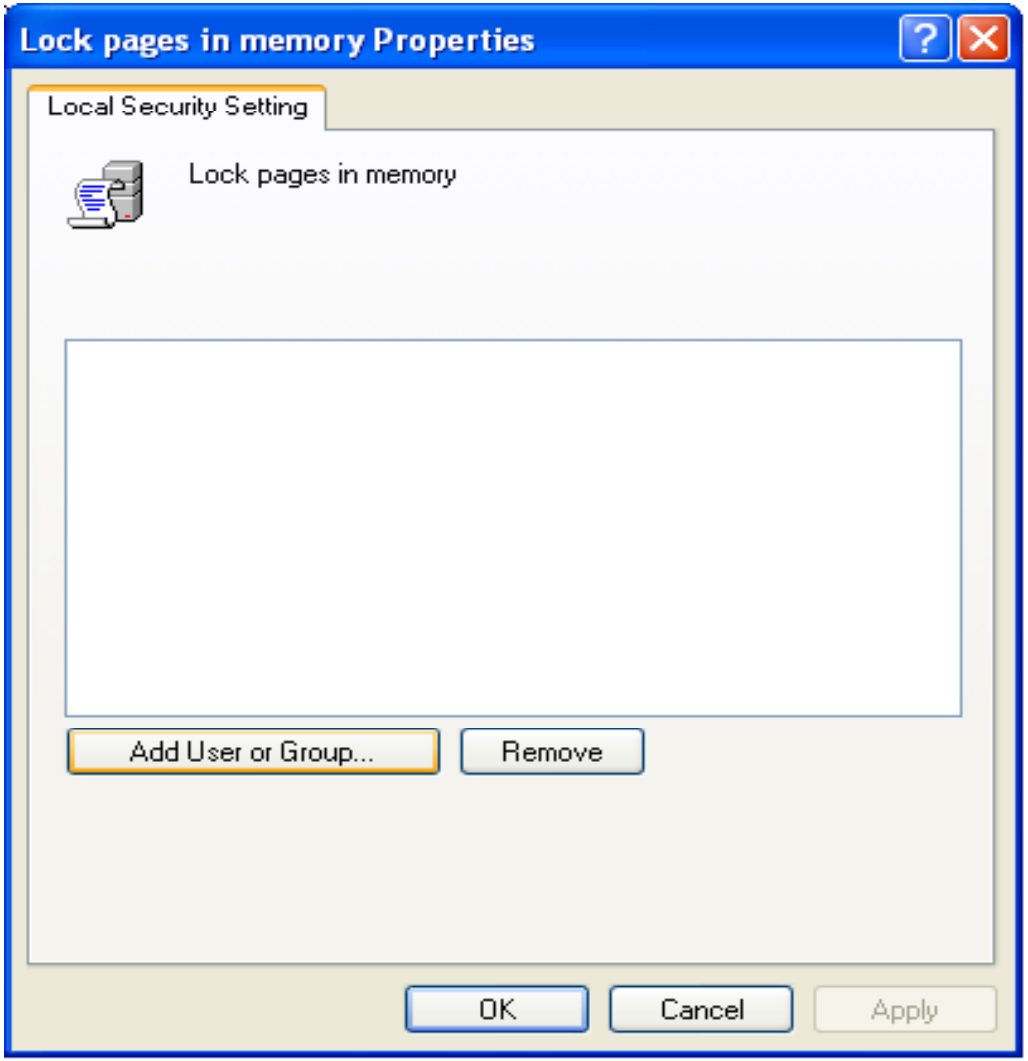
Lock Pages in Memory

Vulnerability	• This right can assign physical memory to several processes, which could lead to no RAM for other processes and create a DoS condition
Countermeasure	• This right should not be assigned to any account
Potential Impact	• None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Lock Pages in Memory



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Log On as a Batch Job

By this policy a user logs on a batch-queue facility such as the Task Scheduler service

When Add Scheduled Task wizard is used to run under a particular user name and password, that user automatically gets this right assigned to him

The values for the **Log on as a batch job** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Log On as a Batch Job

Vulnerability

- This right has low-risk vulnerability

Countermeasure

- This right has to be managed automatically, if scheduled tasks have to run for specific user accounts. If Task Scheduler is not to be used in this manner, configure the right for only the Local Service account and the local support account

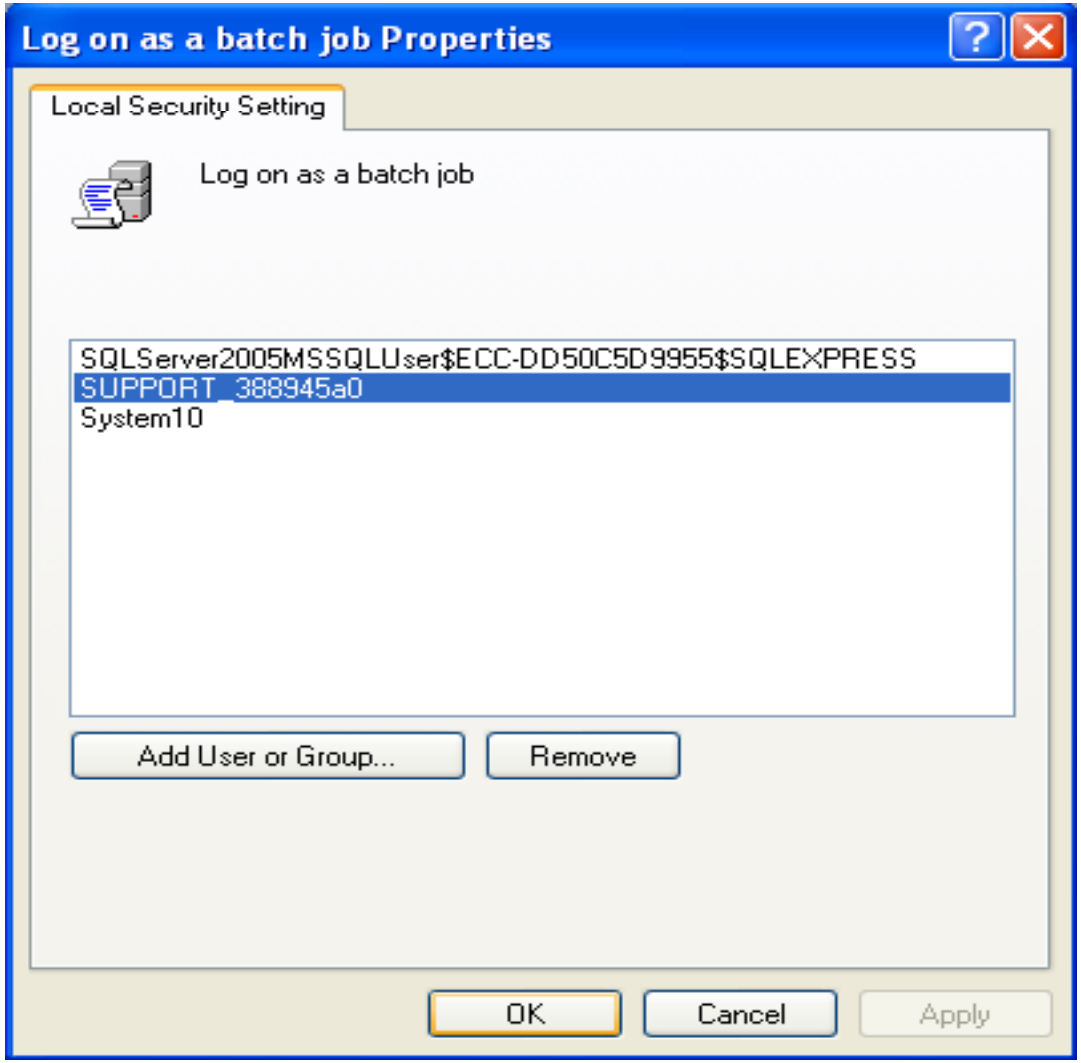
Potential Impact

- Configure settings for domain–based Group Policies; the computer will not be able to assign the user right to accounts that are used for scheduled jobs in the Task Scheduler
- If optional components as ASP.NET or IIS or used, you might need to assign this user right to additional accounts that are required by those components

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Log On as a Batch Job



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Log On as a Service

This policy decides whether a security principal can log on as a service, these services can be configured to run under the Local System, Local Service, or Network Service accounts

A service running under a different user account should have this right

The values for the **Log on as a service** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

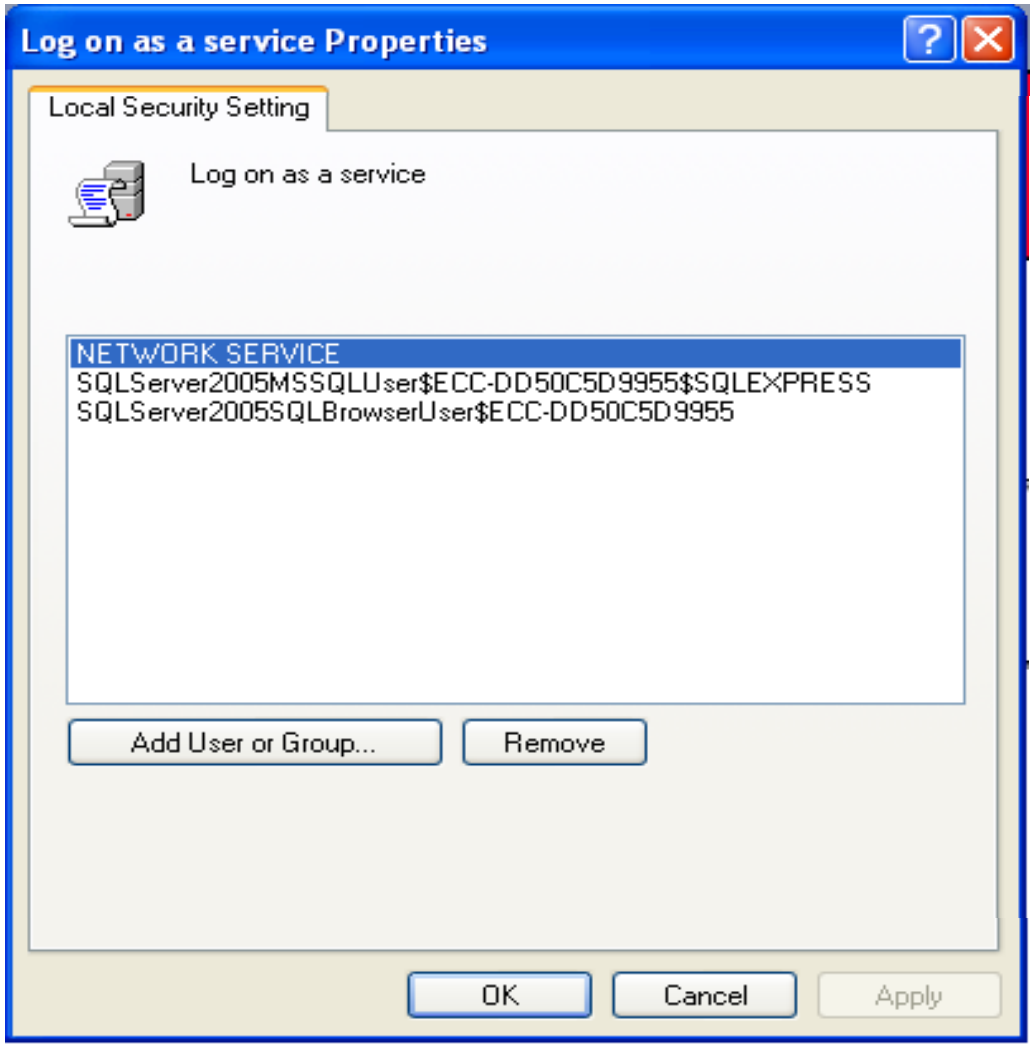
Log On as a Service

Vulnerability	• This right allows users to network services or services which run without any assistance. • The installation and configuring of the services can only be performed by an administrator
Countermeasure	• This right is restricted to local accounts as Local System, Local Service, and Network Service • There should be a limit in assigning this user right
Potential Impact	• This right is a default configuration on most of the computers • Computers having optional components as ASP.NET and IIS should have this user right

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Log On as a Service



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Manage Auditing and Security Log

This policy checks whether you can specify object access audit option for individual resources such as files, Active Directory objects, and registry keys.

Object access audits have to be enabled through **Audit Policy**, which is located under **Security Settings**, **Local Policies**

A user with this right can view and clear the Security event log from Event Viewer

The values for the **Manage auditing and security log** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Manage Auditing and Security Log

Vulnerability

- Managing security event log is a powerful right. A user with this right can clear the security log and erase the necessary log information

Countermeasure

- This user right should be assigned only to local **Administrators** group

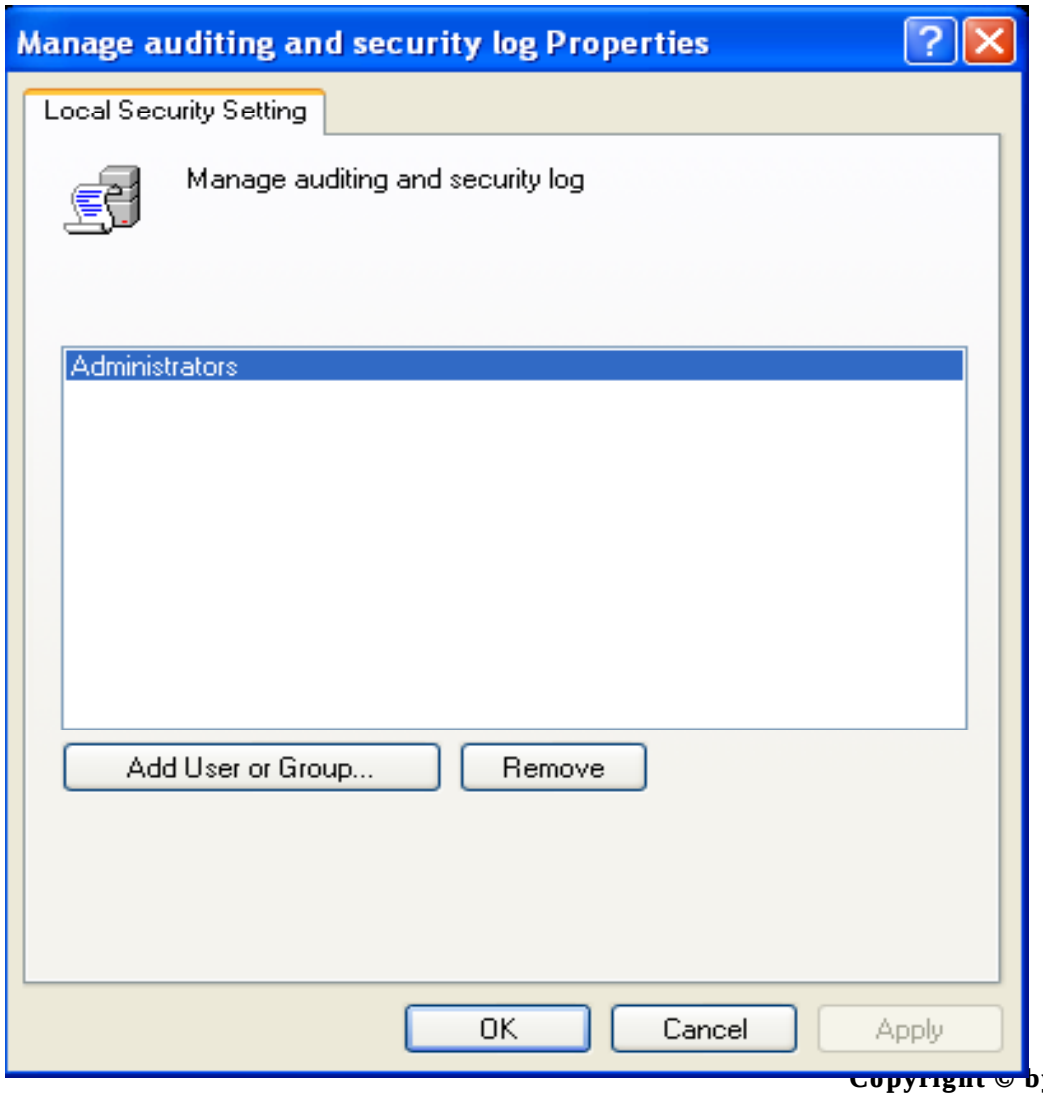
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Manage Auditing and Security Log



EC-Council
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Modify Firmware Environment Values

By this right the user can modify system environment variables either by a process (API) or by a user through System Properties

The values for the **Modify firmware environment values** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Modify Firmware Environment Values

Vulnerability

- Any one with this right can configure a hardware and cause it to fail

Countermeasure

- This right should be assigned only to local **Administrators** group

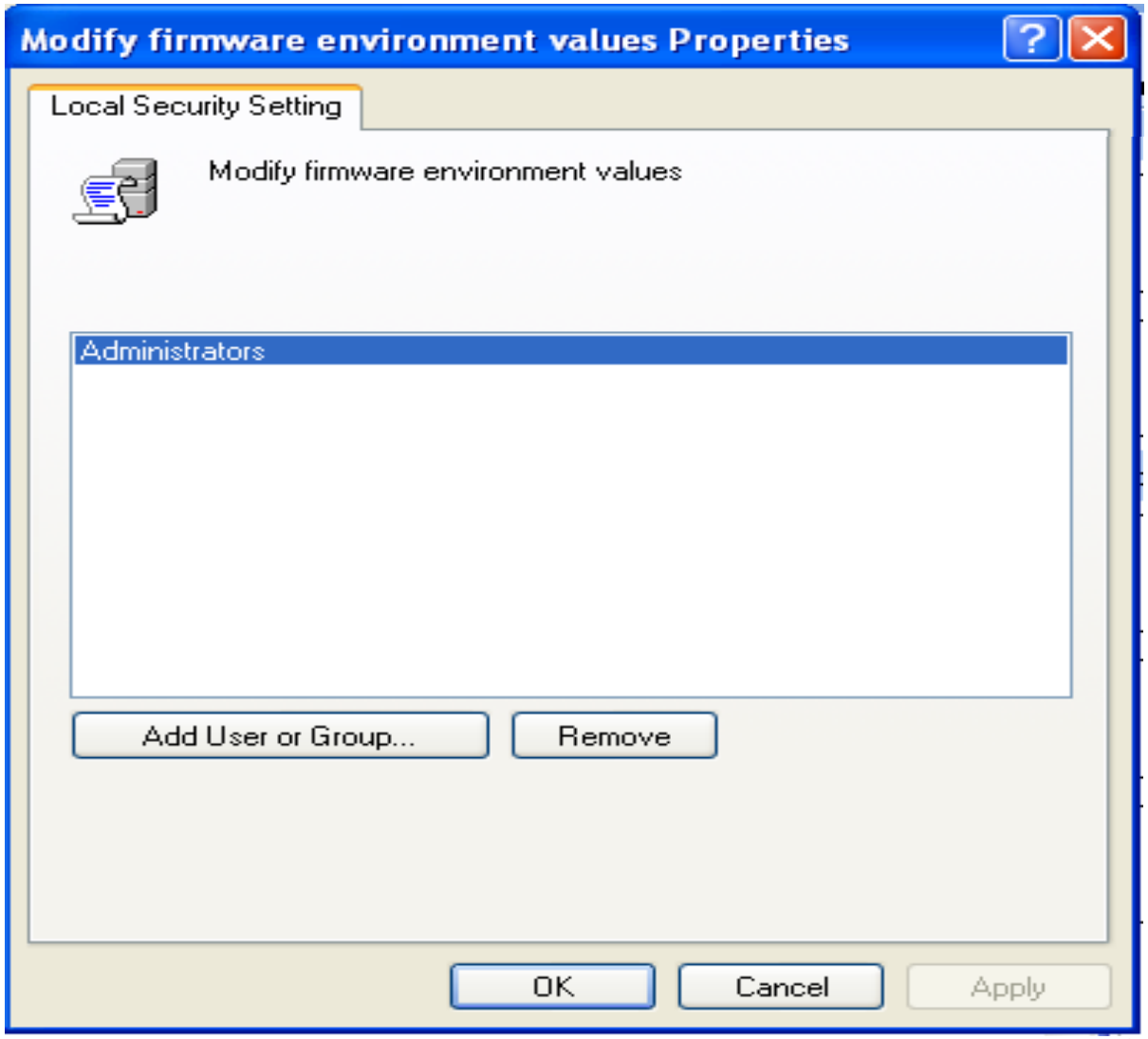
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Modify Firmware Environment Values



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Perform Volume Maintenance Tasks

This policy concludes on performing volume and disk management tasks by non-administrative or remote users as defragmenting an existing volume, create or remove volume and running the Disk Cleanup tool

Windows Server 2003 checks this right in user's access token when process runs in security context calls SetFileValidData()

The values for the **Perform volume maintenance tasks** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

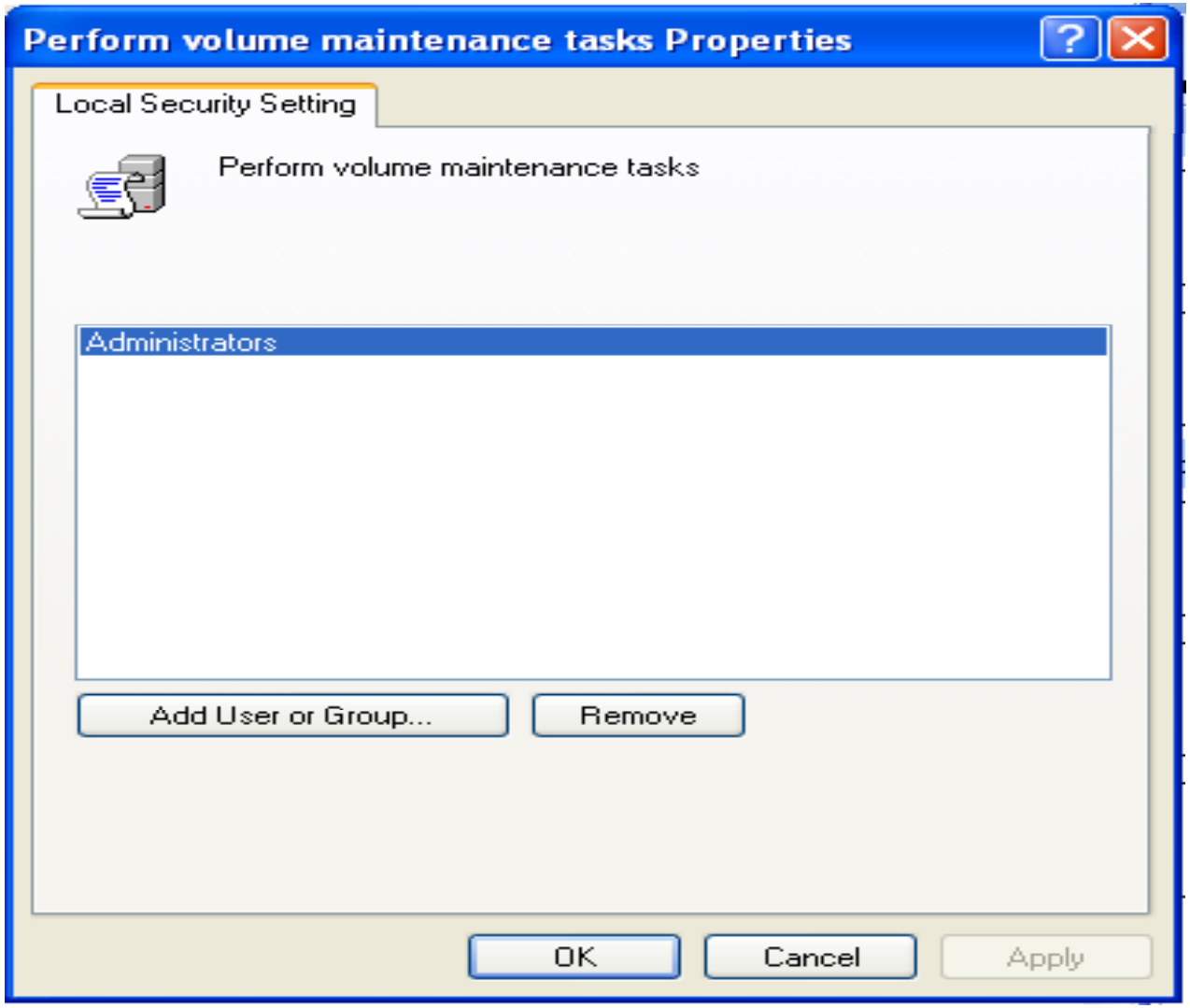
Perform Volume Maintenance Tasks

Vulnerability	• With this right the user can delete a volume, which leads to loss of data or a DoS condition
Countermeasure	• Only local **Administrators** group should have this right
Potential Impact	• None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Perform Volume Maintenance Tasks



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Profile Single Process

By this right you can examine the performance of an application process

You don't need this right for using Microsoft Management Console (MMC) Performance snap-in

You do need this right to collect data through Windows Management Instrumentation (WMI) while System Monitor is configured

The values for the **Profile single process** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Profile Single Process

Vulnerability

- Attacker with this user right can
  - Monitor computer's performance to help identify critical processes that they might wish to attack directly
  - Check what processes run on the computer to identify countermeasures to avoid, as antivirus software, an intrusion-detection system

Countermeasure

- Only Local **Administrators** group should have this right

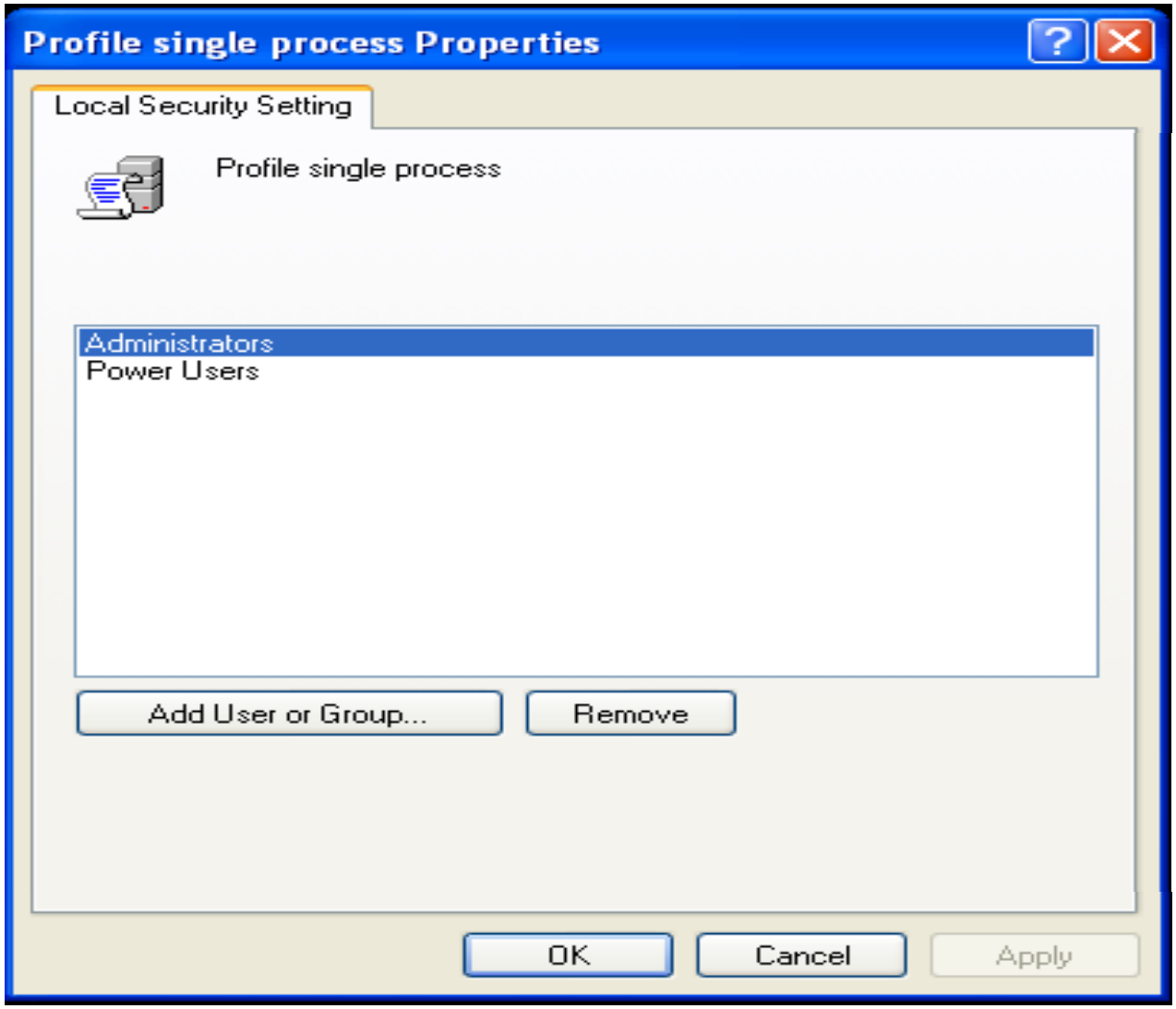
Potential Impact

- By restricting this right to **Power Users** group or other accounts, the abilities of this group are limited

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Profile Single Process



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Profile System Performance

These settings allow the user to sample the performance of computer system processes.

If MMC Performance snap-in is configured to collect data through WMI this right is necessary.

To use the performance snap-in this right is not needed.

The values for the **Profile system performance** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Profile System Performance

Vulnerability

- This right has a moderate vulnerability
- Attacker with this right
- Monitor's a computer's performance to help identify critical processes that they might wish to attack directly
- Check the processes which are active on the computer to identify countermeasures to avoid, as antivirus software or an intrusion detection system

Countermeasure

- Only local **Administrators** group should be assigned by this right

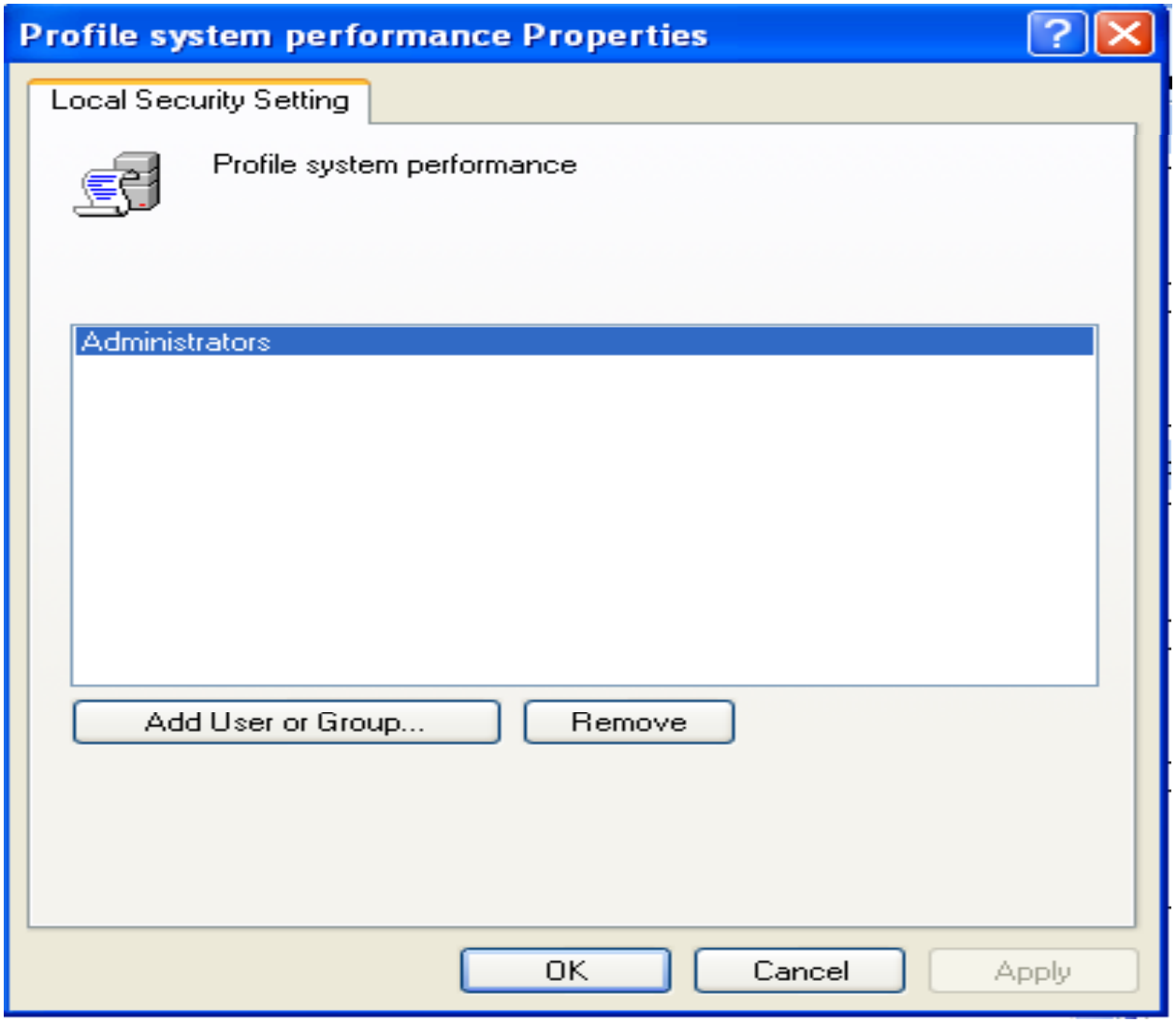
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Profile System Performance



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remove Computer from Docking Station

The policy checks whether the users with portable computers can click **Eject PC** on the **Start** menu to undock the computer

The values for the Remove computer from docking station setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remove Computer from Docking Station

Vulnerability

- Any user with this right can remove a portable computer from its docking station
- The value of this countermeasure is reduced by the following factors:
- An attacker could remove it from the docking station after the BIOS starts but before the operating system launches, if he can restart the computer
- Servers are not affected by these settings as they are not installed in docking stations
- An attacker could steal the computer and the docking station together

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remove Computer from Docking Station

Countermeasure

- This right is assigned only to local **Administrators** and **Power Users** groups

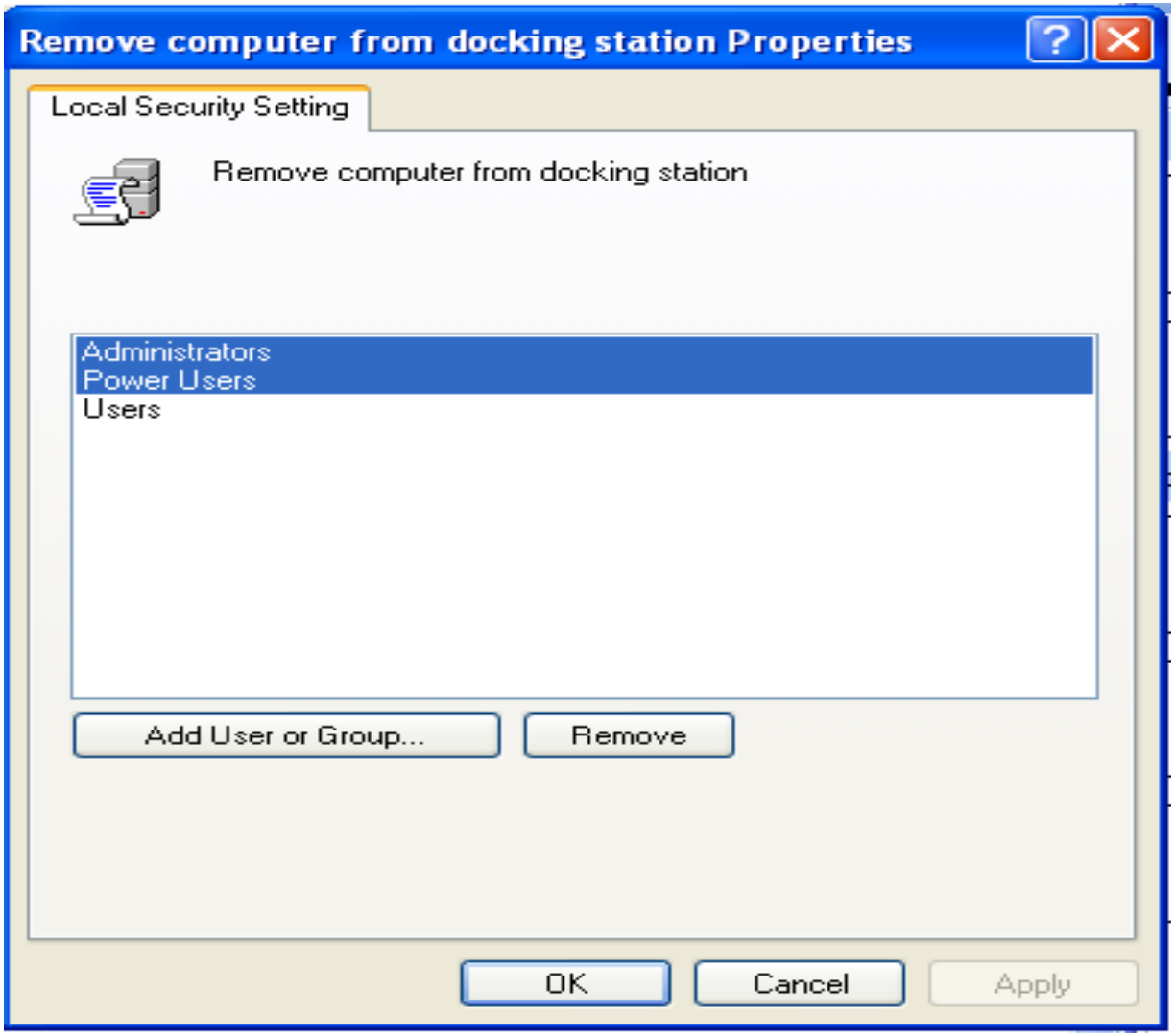
Potential Impact

- This right is of default setting but it has a little impact
- If organization users are not members of the **Power Users** or **Administrators** groups, they will be unable to remove their own portable computers from their docking stations without shutting them down first

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remove Computer from Docking Station



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Replace a Process Level Token

By this right a parent process can replace the access token that is associated with a child process

The possible values for the Replace a process level token setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

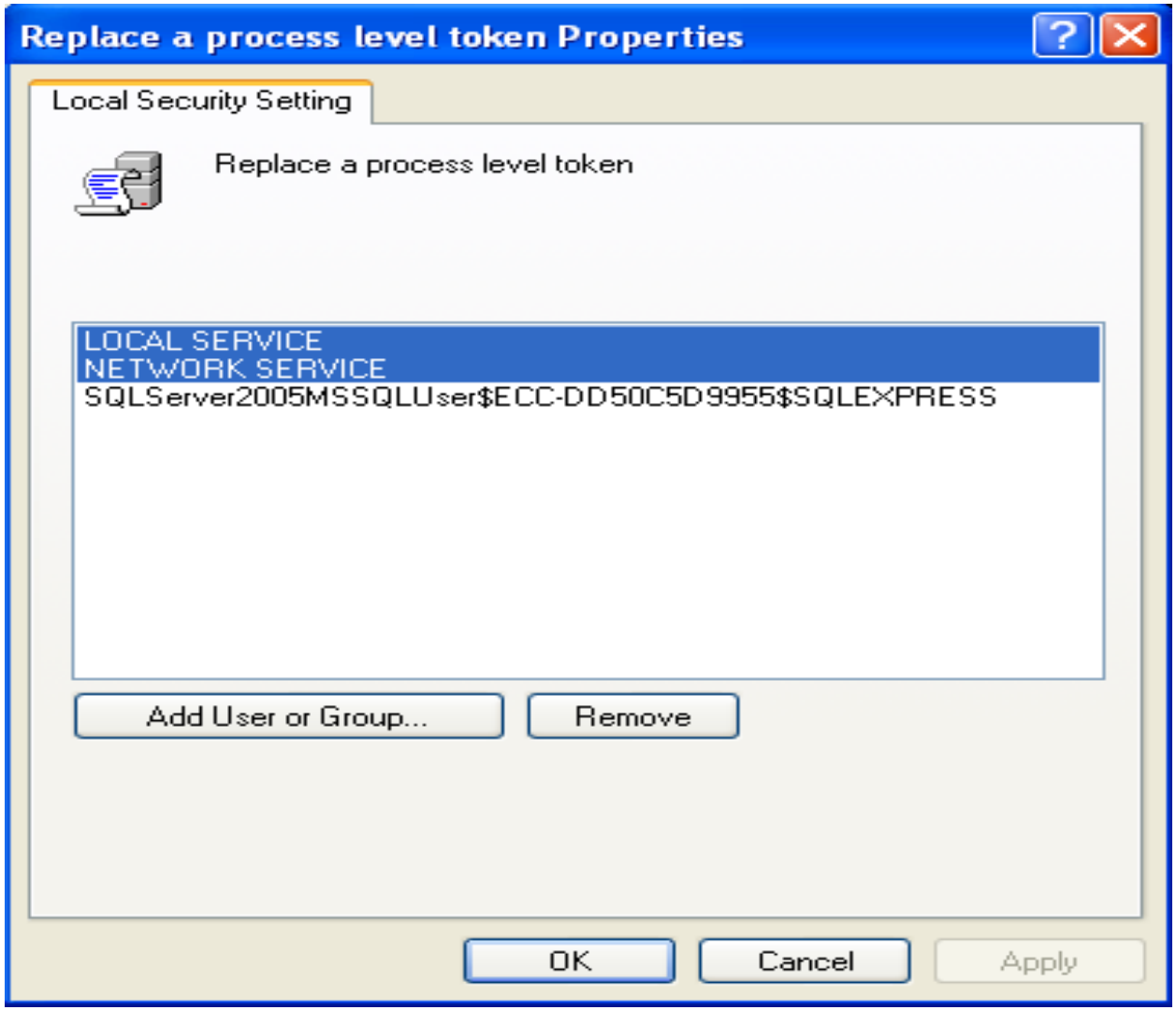
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Replace a Process Level Token

Vulnerability	• A user with this right can launch processes as other users • Using this method there unauthorized actions can be hidden
Countermeasure	• For member servers, only the Local Service and Network Service accounts have this right
Potential Impact	• Most computers have impact of this setting as this is the default configuration • If optional components as ASP.NET or IIS are installed, this right might be necessary

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Replace a Process Level Token



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Restore Files and Directories

The policy check whether the user can circumvent file and directory permissions when they restore backed up files and directories and can they set any valid security principal as the owner of an object

The values for the Restore files and directories setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Restore Files and Directories

Vulnerability

- Attacker with this right can restore sensitive data to a computer and overwrite some data which is important and can create denial of service.
- Attacker could overwrite executable files used by legitimate administrators or system services and install backdoors for continued access to the computer.

Countermeasure

- Only local **Administrators** group should assign the right.

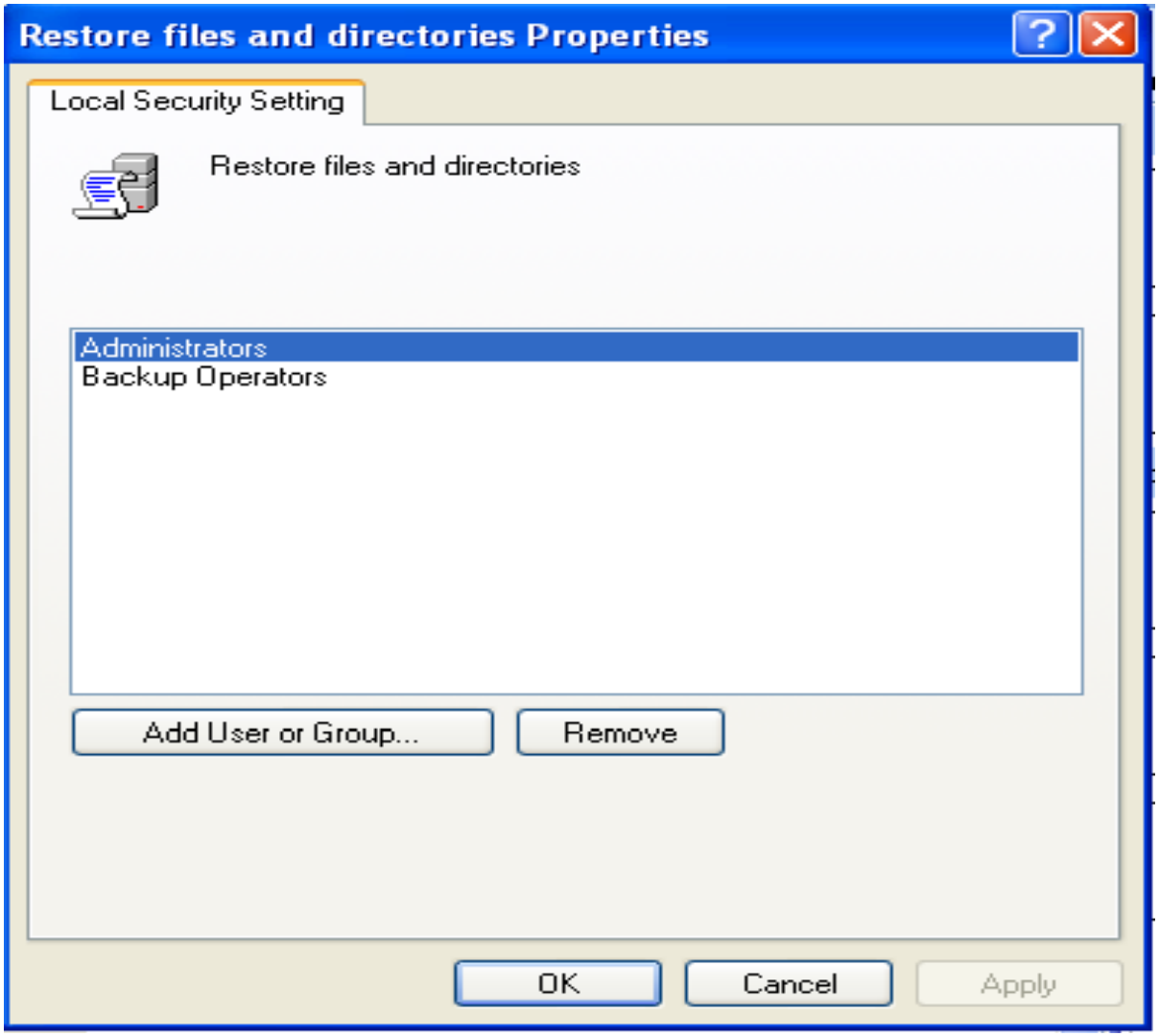
Potential Impact

- If this right is removed from **Backup Operators** group and other accounts, the tasks assigned to them can not be performed.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Restore Files and Directories



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shut Down the System

By setting this right user can shut down the local computer.

The values for the **Shut down the system** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shut Down the System

Vulnerability

- The ability to shut down domain controllers should be given only to some trusted administrators
- Users with these rights have the ability to log on to the server, the accounts and groups that are allowed to shut down a domain controller should be very careful
- After shutting down the domain controller it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries

Countermeasure

- Only **Administrators** and **Backup Operators** are assigned the right on member servers and that only **Administrators** have it on domain controllers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

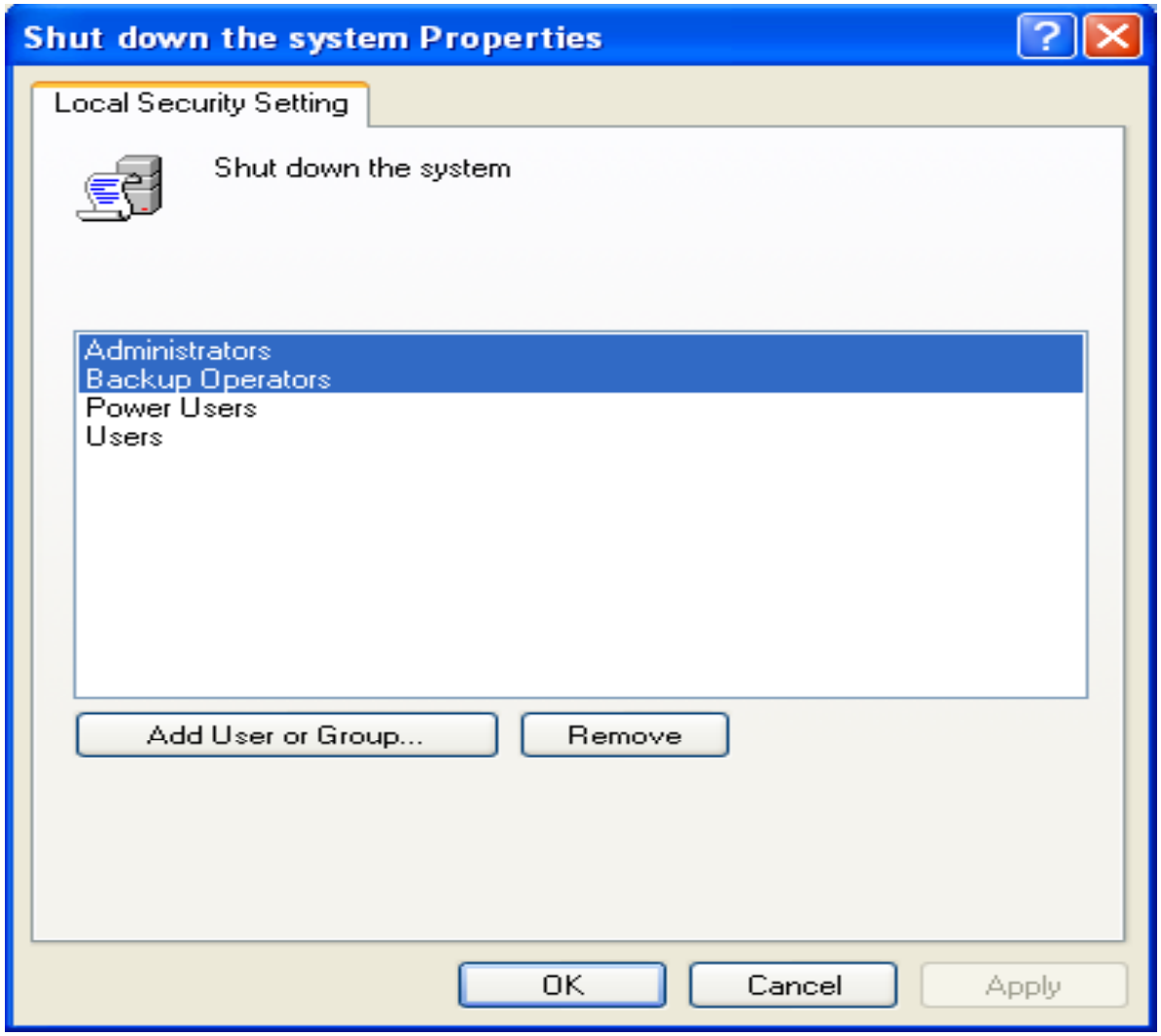
Shut Down the System

Potential Impact

- By restricting default groups from this right you could limit the delegated abilities of assigned roles in your environment

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shut Down the System



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Synchronize Directory Service Data

By this right a process can read all objects and properties in the directory, regardless of the protection on the objects and properties

The privilege is required to use LDAP directory synchronization (dirsync) services

The values for the Synchronize directory service data setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Synchronize Directory Service Data

Vulnerability

- This right affects domain controllers, which should be able to synchronization directory service data
- Domain controllers have this right inherited, as the synchronization process runs the context of the System account
- An attacker with this right can view all information stored within the directory then they could help other attackers to expose some sensitive data

Countermeasure

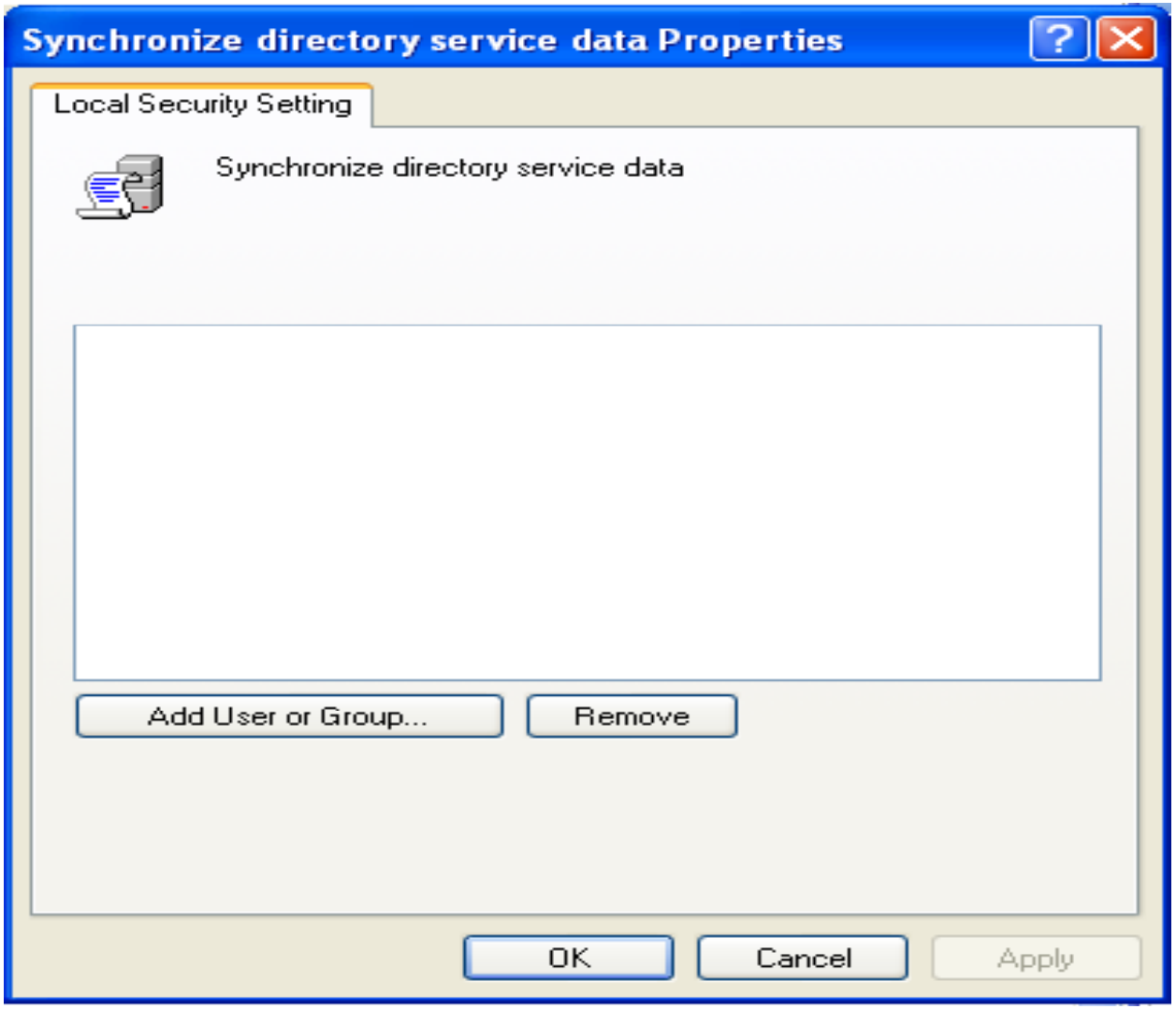
- No account should have this right

Potential Impact

- None

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Synchronize Directory Service Data



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Take Ownership of Files or Other Objects

This policy determines whether user can take ownership of any securable object in the computer, including Active Directory objects, NTFS files and folders, printers, registry keys, services, processes, and threads

The values for the **Take ownership of files or other objects** setting are:

- A user-defined list of accounts
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

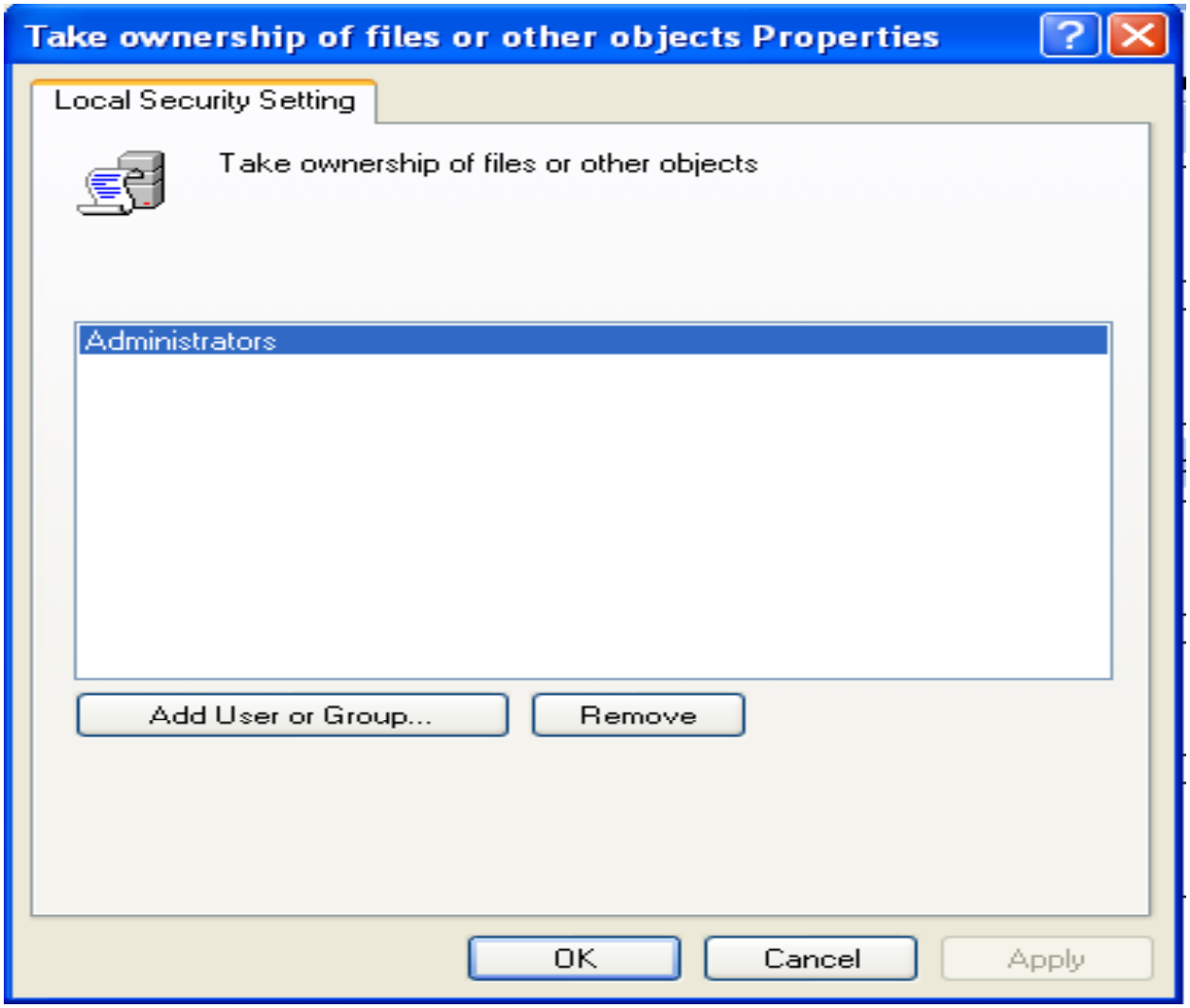
Take Ownership of Files or Other Objects

Vulnerability	• A user with this right can take control of any object, regardless of the permissions on that object, and make any changes to that object
Countermeasure	• Only local **Administrators** group should have this right
Potential Impact	• None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Take Ownership of Files or Other Objects



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Options

The Security Options section of Group Policy is used to enable or disable computer security settings such as digital data signatures, Administrator and Guest account names, access to floppy disk and CD-ROM drives, driver installation behavior, and logon prompts

Security Options Settings

- You can configure the security options settings in the following location:
  - **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Administrator Account Status

This policy setting enables or disables the Administrator account for normal operational conditions

If a computer is started in safe mode, the administrator account is always enabled, no matter what the configuration settings are

The values for the **Accounts: Administrator account status** setting is:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Administrator Account Status - *Vulnerability*

The Administrative account is disabled as:

- It is very difficult to maintain a schedule for periodic password change in some organizations.
- It is impossible to login regardless of the number of attacks occurring, which makes it a target for brute force attack.
- The administrative account has a security identifier (SID) and third party tools which allow authentication by using SID than account name. An brute force attacker can attack an using SID even the account name is changed

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Administrator Account Status

Countermeasure

- **Configure** this policy to **Disable**

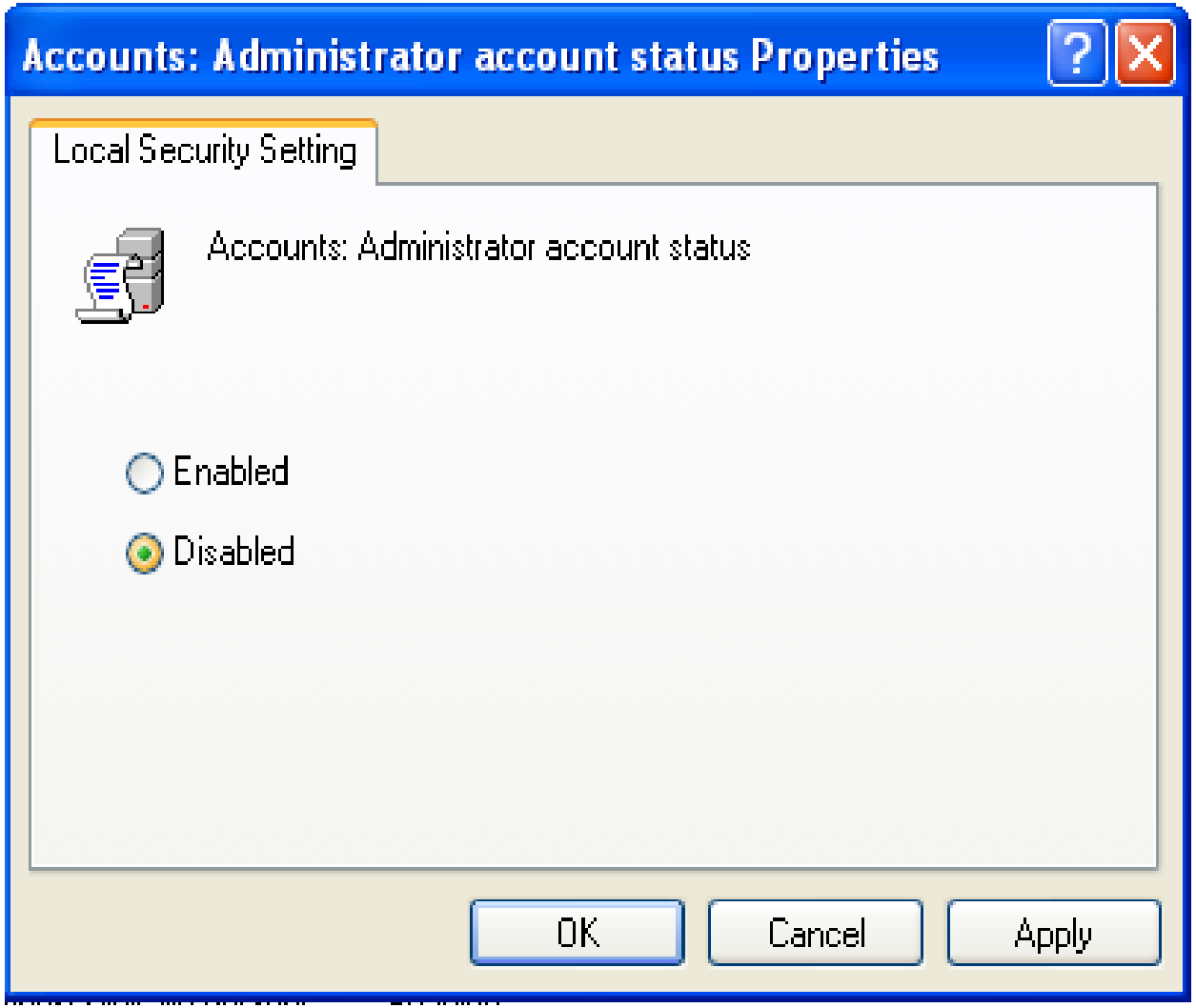
Potential Impact

- Maintenance will be a big measure under the circumstances when the administrator account is disabled, as if any channel between member computer and the domain controller fails in an environment it is a must to logon is safe mode state to set the connection

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Administrator Account Status



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Guest Account Status

This policy helps to ascertain whether the Guest account is enabled or disabled

The values for the Accounts: Guest account status setting is:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Guest Account Status

Vulnerability

- The unauthorized users are permitted to logon on a Guest account with no passwords. This user can access any document with in the network which is accessible to the guest account
- Any data with permissions to Guest account, the **Guests** group, or the **Everyone** group will be accessible and may lead to corruption of data

Countermeasure

- **Configure** this policy setting to **Disable,** to disable the guest account

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Guest Account Status

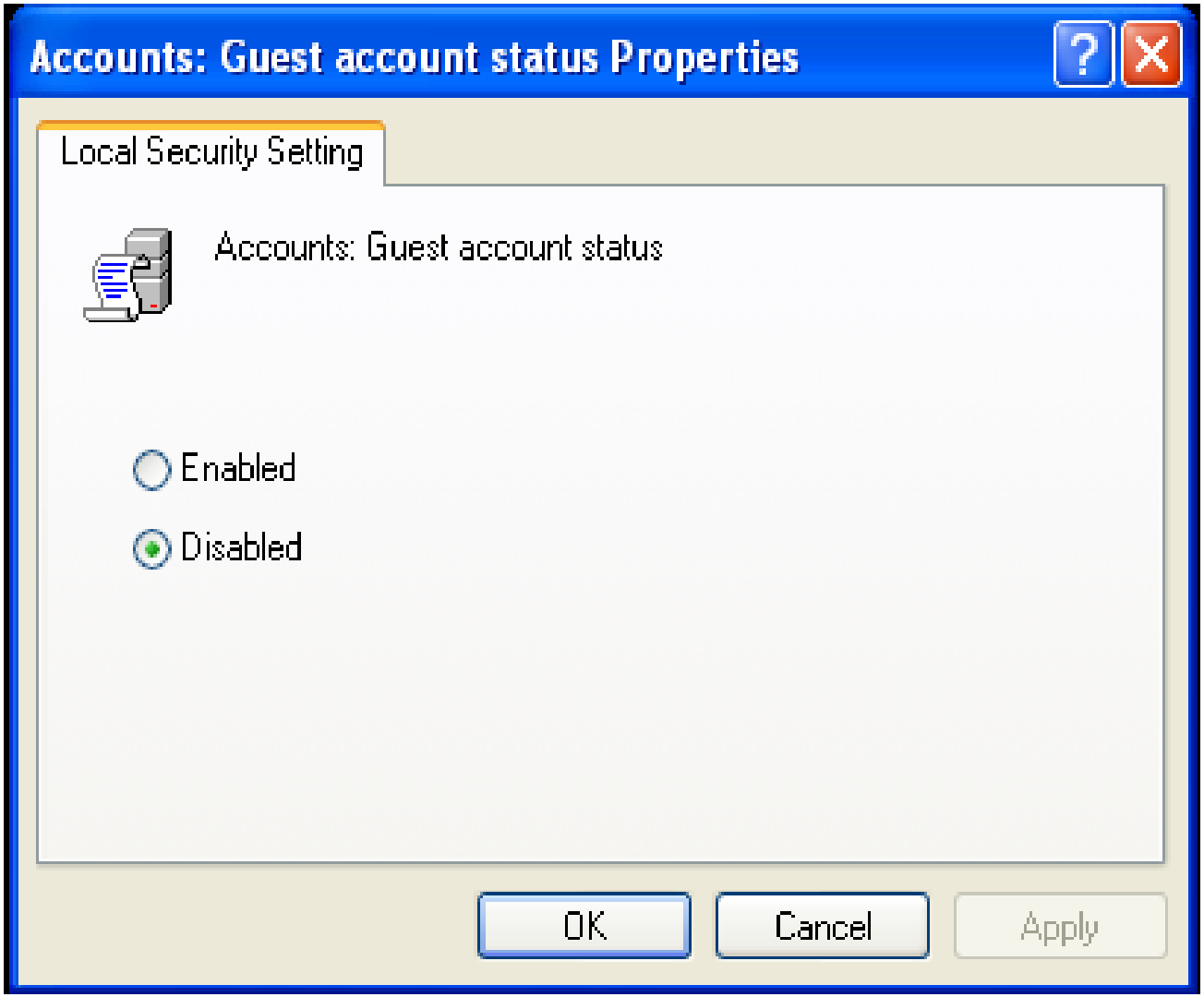
Potential Impact

- Authentication is very necessary to access shared resources. If the guest account is disabled and the **Network Access: Sharing and Security Model** option is set to **Guest Only.** In such case Network logons which are operated by Microsoft Network Server (SMB Service), will fail
- These setting have a minor impact on organizations as they are default setting in Microsoft Windows® 2000, Windows XP, and Windows Server™ 2003

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Guest Account Status



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Limit Local Account Use of Blank Passwords to Console Logon Only

This policies check on allowing remote interactive logons by network services as Terminal Services, Telnet, and File Transfer Protocol (FTP)

To perform an interactive or network logon from a remote client, a local account should have a non-blank password

The values for the **Accounts: Limit local account use of blank passwords to console logon only** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Limit Local Account Use of Blank Passwords to Console Logon Only

Vulnerability

- One of the serious threats to computer security is blank passwords, which should be forbidden by organization policies. The default setting of for Windows Server 2003 Active Directory® service domains need a password of seven characters

Countermeasure

- **Configure** this setting to **Enable**

Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Limit Local Account Use of Blank Passwords to Console Logon Only

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Rename Administrator Account

This policy settings checks if there is a different account name associated with the SID for the Administrator account

The values for the **Accounts: Rename administrator account** setting is:

- User-defined text
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Rename Administrator Account

Vulnerability

- The Administrator account exists in every computer that runs on the operating systems as Windows 2000, Windows Server 2003, or Windows XP Professional. If this account is renamed it is hard to guess the name and password to unauthorized users
- Any built-in Administrator account could not be locked out even a brute force attack is used; this capability makes the Administrator account a popular target for attack

Countermeasure

- Rename the **Administrator** account by specifying it in this policy setting

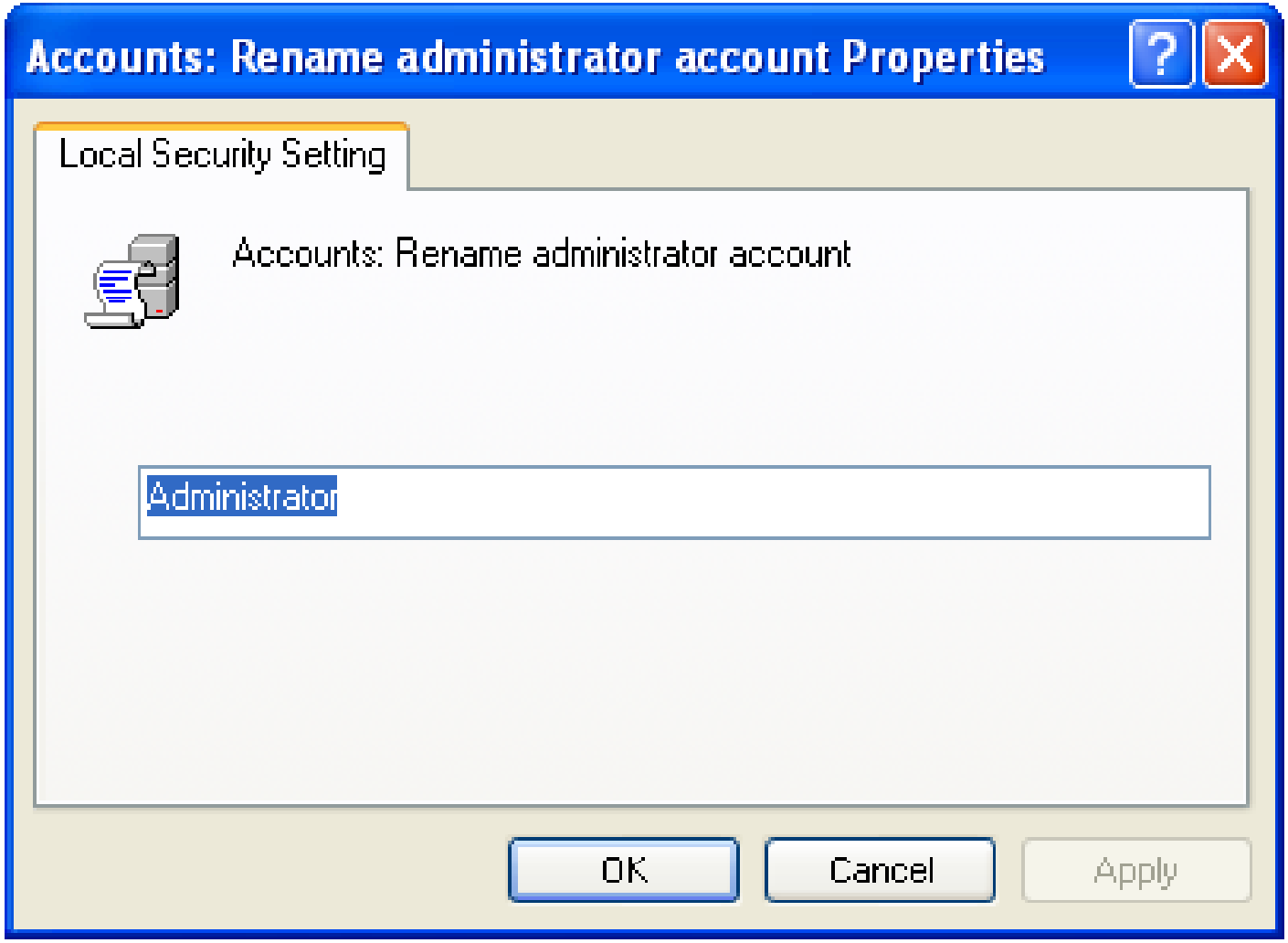
Potential Impact

- The new account name has to be notified to all the users authorized to use this account

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Rename Administrator Account



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Rename Guest Account

This policy check whether there is another name associated for the SID of the Guest Account

The values for this Group Policy setting are:

- User-defined text
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Rename Guest Account

Vulnerability

- In all operating systems as Windows 2000, Windows Server 2003, or Windows XP Professional a Guest account exists
- If this account is renamed it will be difficult to guess the account name and password

Countermeasure

- Rename the **Guest** account by setting this policy

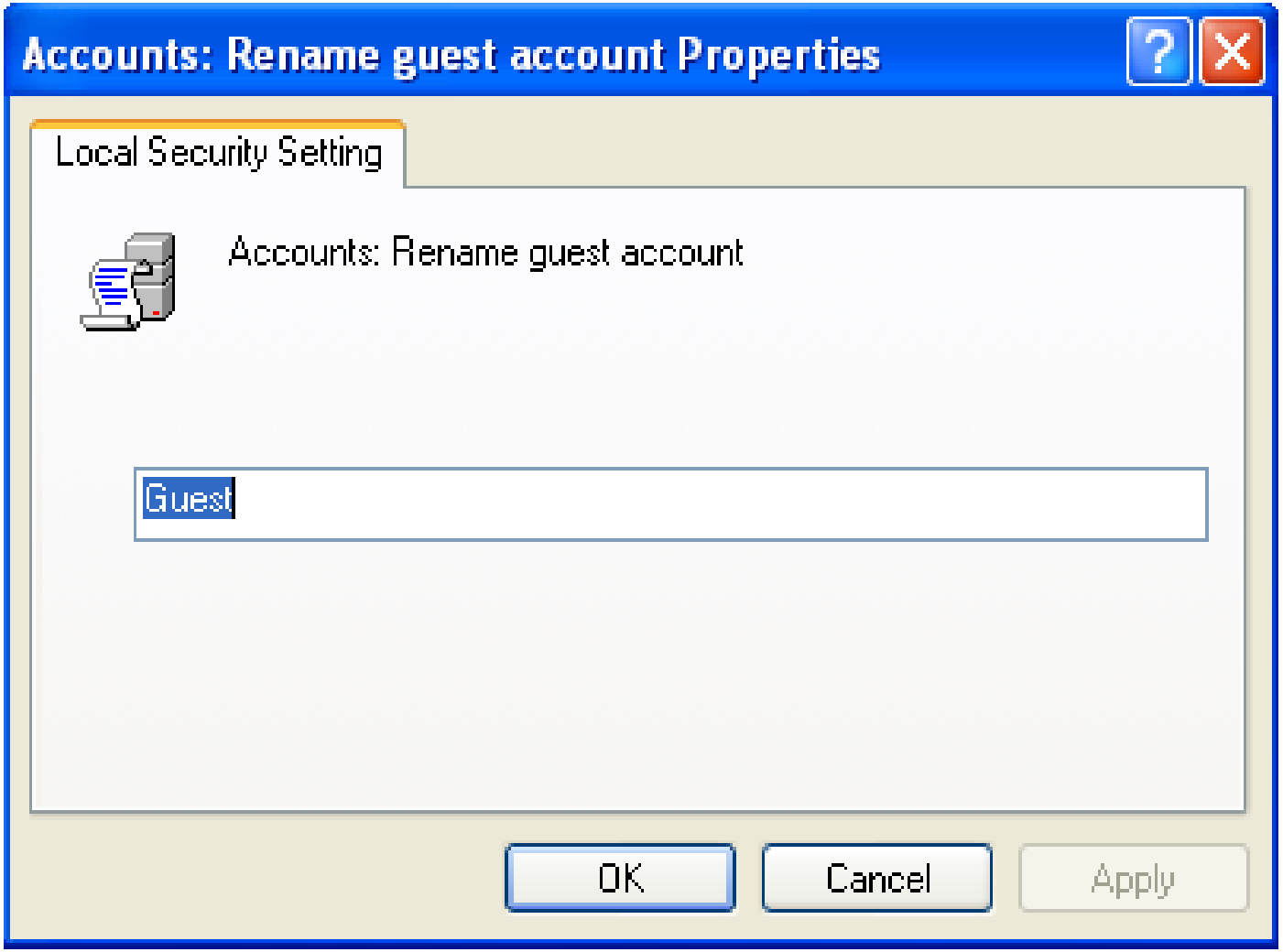
Potential Impact

- A minor impact is considered as the Guest account is disabled by default in the operating systems as Windows 2000, Windows XP, and Windows Server 2003

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Accounts: Rename Guest Account



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit: Audit the Access of Global System Objects

If this policy settings are enabled a default System Access Control List is applied when a object is created by the computer

If **Audit object access** audit setting is also enabled with it. Auditing for these objects will be started

The Global system objects as “base system objects” or “base named objects” are used to synchronize multiple applications or various parts of a complicated application

These objects have a NULL SACL. If this policy setting is enabled at startup time, the SALC is assigned by the kernel

The values for the Audit: Audit the access of global system objects setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

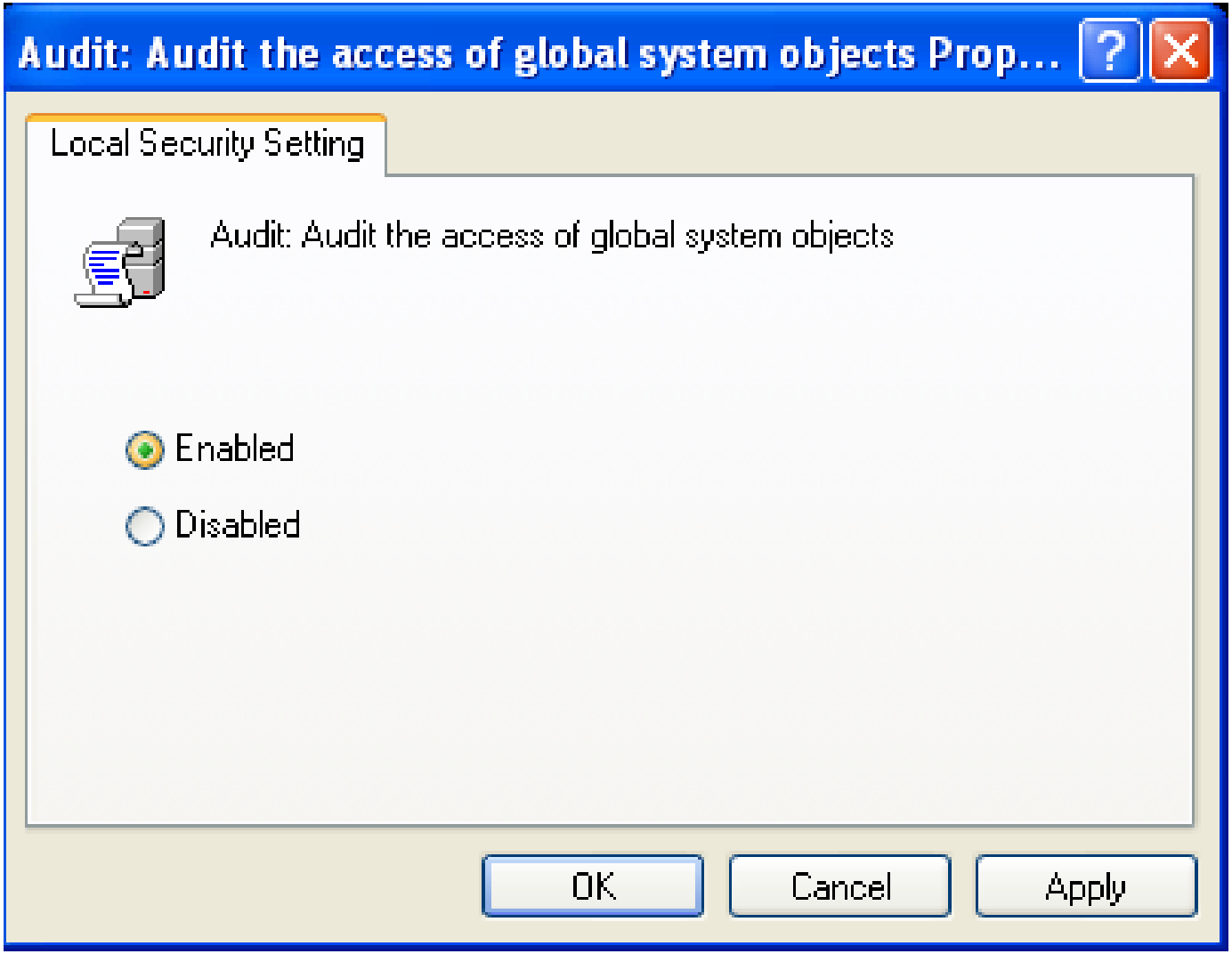
Audit: Audit the Access of Global System Objects

Vulnerability	• If an object is improperly secured any malicious code can act under it, if the object name is known • Risk of such occurrence is low
Countermeasure	• Configure this policy setting to **Enable**
Potential Impact	• A huge number of security events are generated when this policy setting are Enabled. These events can slow the server, as there is no limit on the recorded events • The policy can only be enabled or disabled, but it can not be restricted to record some specific logs

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit: Audit the Access of Global System Objects



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit: Audit the Use of Backup and Restore Privilege

When **Audit privilege use** policy setting is in effect, this policy determines whether you can audit the use of all user privileges, with Backup and Restore

When these both policy settings are enabled, for every backup and restore an audit event is generated

If this policy is disabled no events are recorded, even if **Audit privilege use** is enabled

The values for the **Audit: Audit the use of Backup and Restore privilege** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit: Audit the Use of Backup and Restore Privilege

Vulnerability

- When these both policy settings are enabled, for every backup and restore an audit event is generated. This information helps you to capture any accidental or malicious operations in unauthorized manner

Countermeasure

- **Enable** this policy setting and implement automatic log backup by configuring the AutoBackupLogFiles registry key

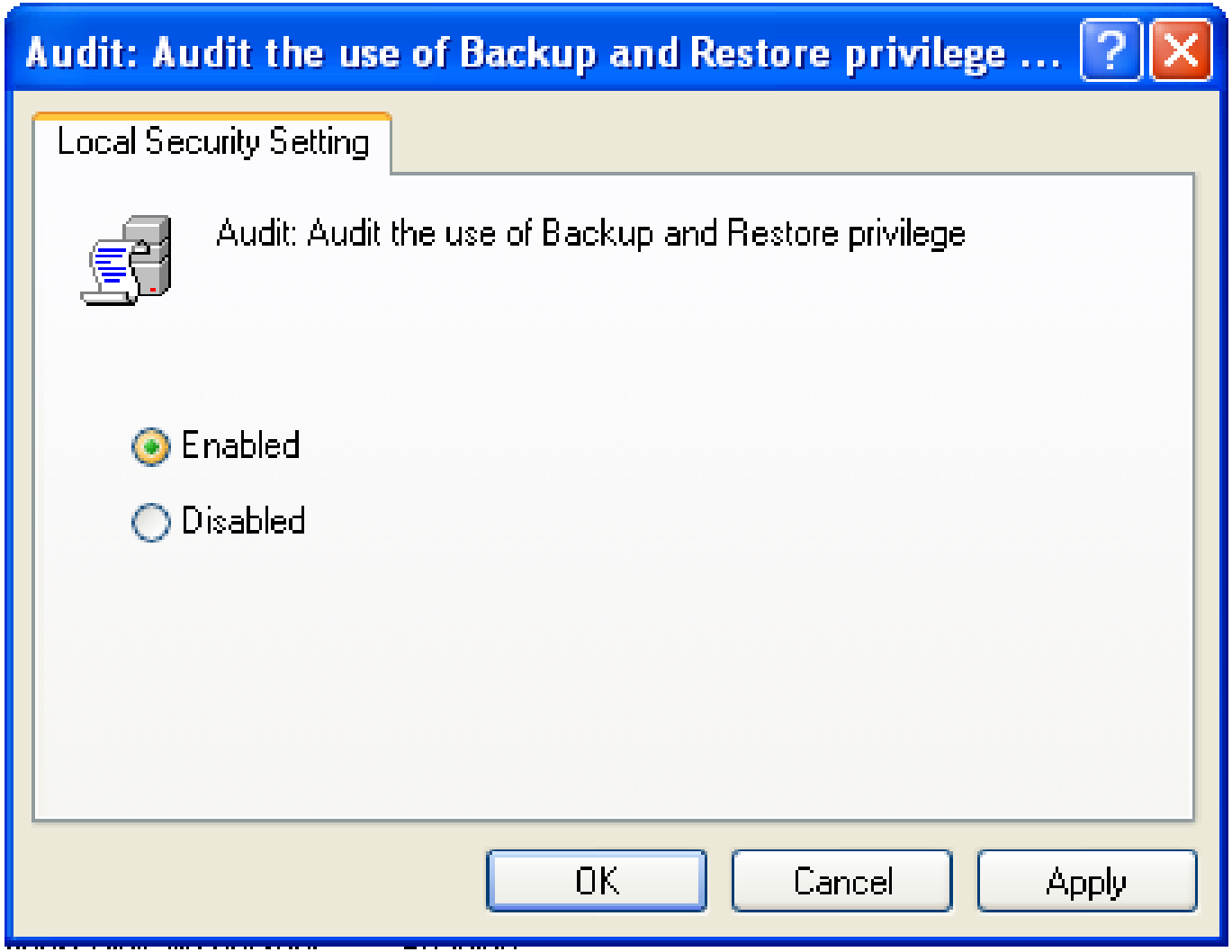
Potential Impact

- If this policy is enabled, the server could slow down as a large number of security events can generate
  If the size of the security log is increased to minimize frequent shutdown, a large log file may reduce the performance of the system

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit: Audit the Use of Backup and Restore Privilege



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit: Shut Down System Immediately if Unable to Log Security Audits

This settings check whether the computer can shutdown if it cannot generate the log file

It is required that the computer has to be able to prevent the auditable event occurrence if the audit system is unable to log, as per The Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certifications

When it is not possible to audit the event the Microsoft system has to display a stop message

If the security audit cannot be logged the computer stops, when ever this policy is enabled

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit: Shut Down System Immediately if Unable to Log Security Audits

By this policy setting a Stop message will be displayed when the security log is full

- STOP: C0000244 {Audit Failed}
- An attempt to generate a security audit failed

To recover the administrator has to logon, clear the log and disable this setting to restart the computer.

Next step is to clear the log manually and configure the policy settings to Enabled.

The possible for the **Audit: Shut down system immediately if unable to log security audits** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit: Shut Down System Immediately if Unable to Log Security Audits

Vulnerability

- If the computer is not able to record the happening events then important information will not be available to review the security measures
- Even an attacker can fill the log with huge data to force the system to shutdown

Countermeasure

- **Enable** this policy setting.

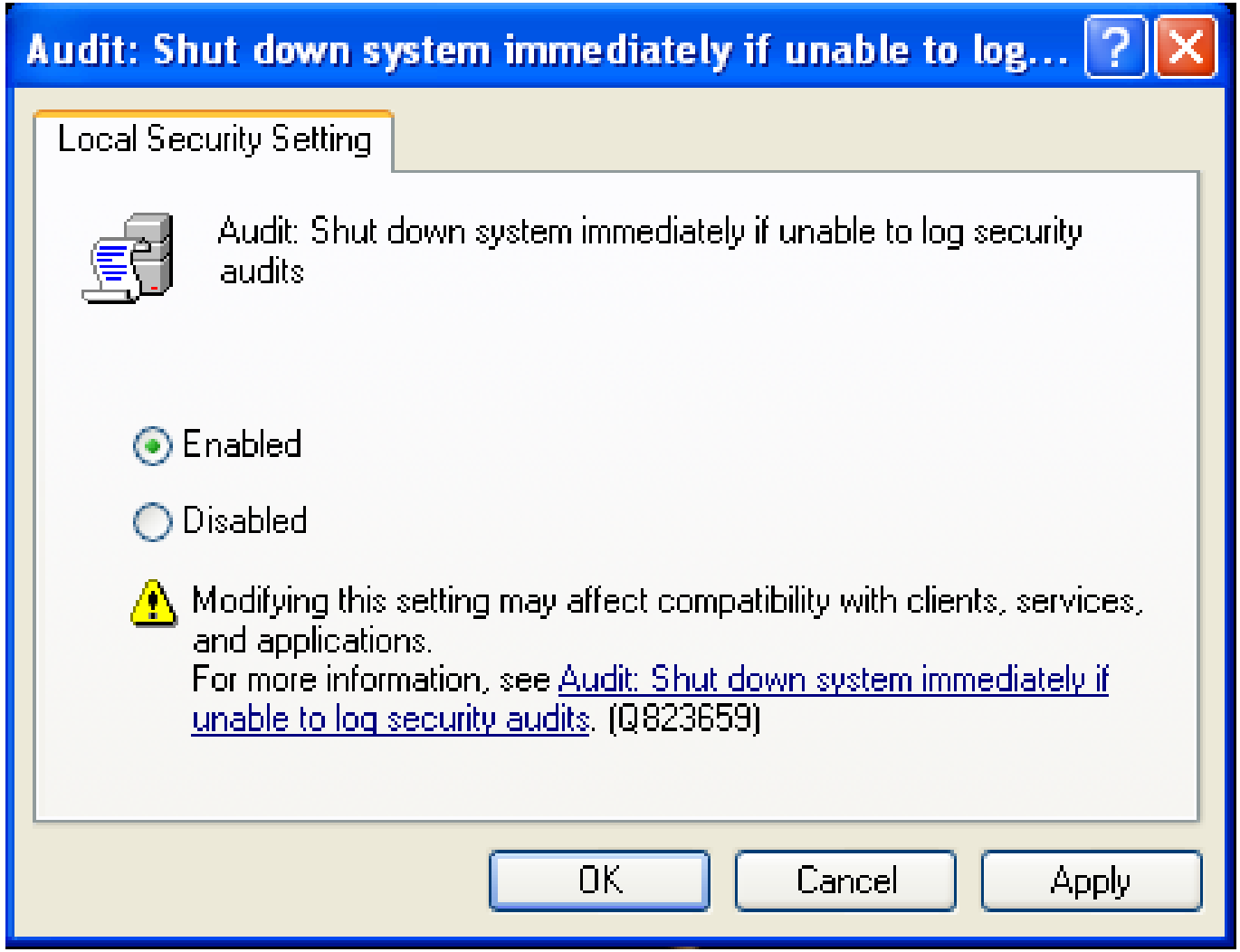
Potential Impact

- If this policy setting is enabled with retention method of Security log, Administrator's work load is increased. By this configuration a repudiation threat may raise and leads to DoS condition
- Even with repeated shutdowns damage to the operating system, applications, or data could result

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Audit: Shut Down System Immediately if Unable to Log Security Audits



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DCOM: Machine Access/Launch Restrictions in Security Descriptor Definition Language (SDDL)

This policy permits the administrators to define extra computer wide access control that direct access to all Distributed Component Object Model (DCOM)–based applications

An added access check call against a computer-wide access control list (ACL) for a call, activation, or launch of any COM server. If the check fails the request is denied

It provides less authorization rules to be passed

The policy right setting controls access permit to cover call rights

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DCOM: Machine Access/Launch Restrictions in Security Descriptor Definition Language (SDDL)

The ACL override weak security settings which are particular to a specific application through CoInitializeSecurity or application-specific security settings

The ACL provide a centralized location to set general authorization policy which are applied to all COM servers

This policy setting allows specifying an ACL in two different ways

- Type security details in SDDL
- Local and remote access permissions are granted or denied individually

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DCOM: Machine Access/Launch Restrictions in Security Descriptor Definition Language (SDDL)

Vulnerability

- COM application contains security-specific code. These settings cannot be overwritten by administrators for stronger security without modification of the application
- An attacker attack with a COM call and try to utilize week security
- A service called as RPCSS is included in COM which runs during computer start up and continue
- Attackers using remote, unauthenticated computers attack RPCSS

Countermeasure

- Set this policy setting to appropriate computer wide ACL, which protects COM based requests

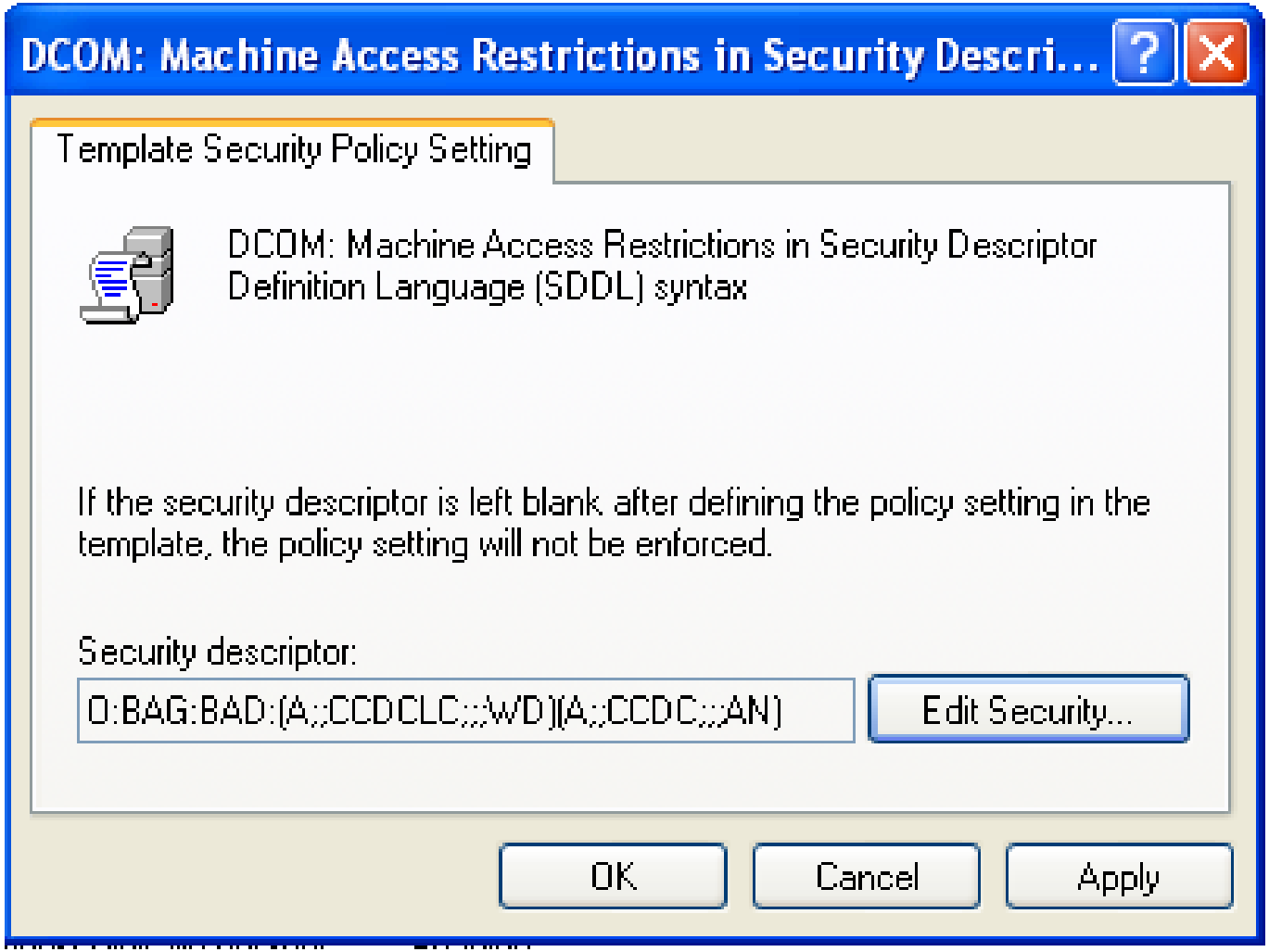
Potential Impact

- Make sure that the application-specific call permissions assigned are appropriate users implementing a COM server and override the default security settings

EC-Council

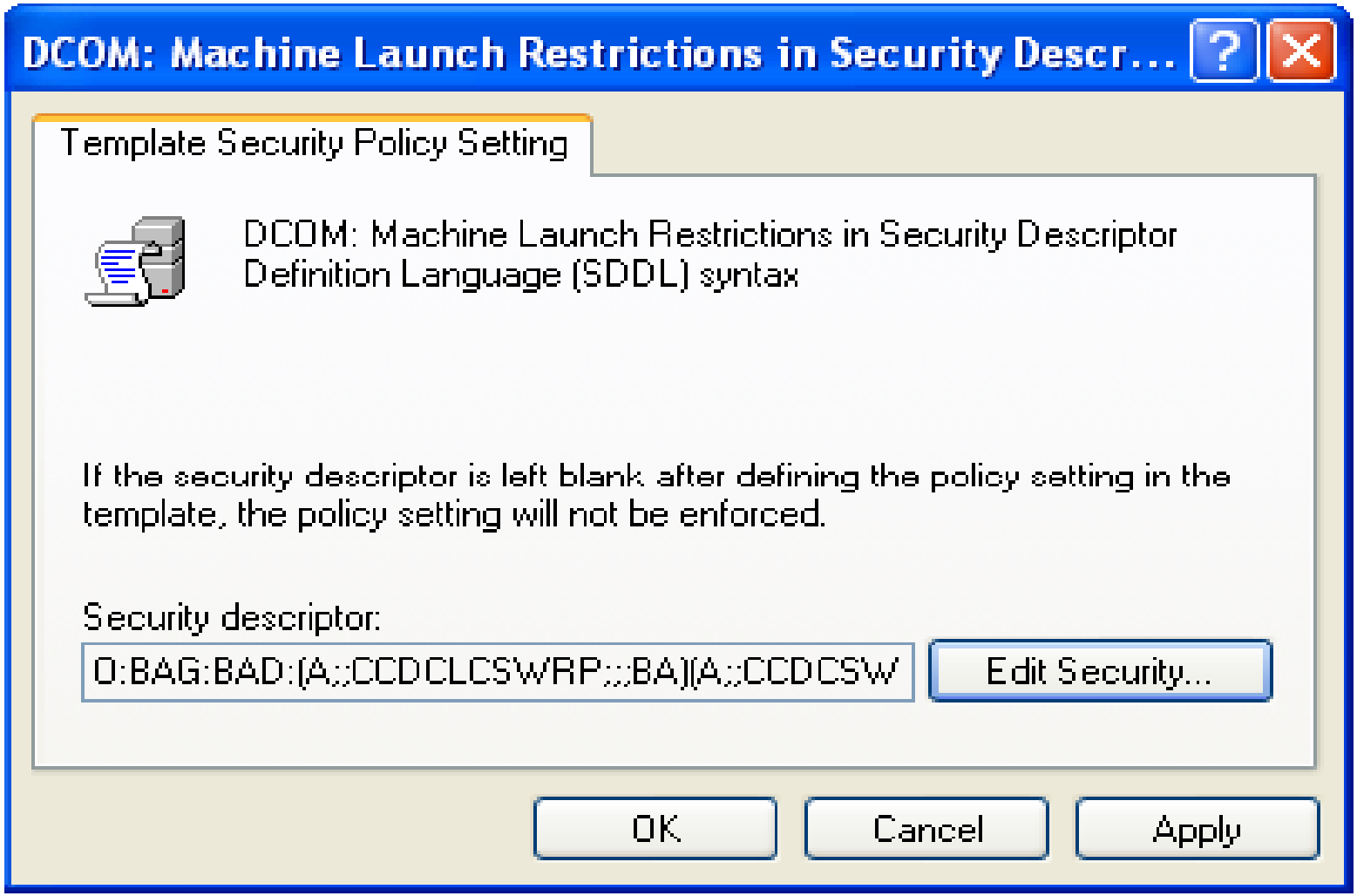
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL)



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Allow Undock without having to Log On

This setting checks whether the user has to logon to request permission to remove a portable computer from a docking station

Enabling this setting, allows physically ejecting or undocking the computer

Disabling this setting, the user should logon and receive permission to undock

Users with **Remove Computer from Docking Station** privilege will get this permission

The values for the Devices: Allow undock without having to log on setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

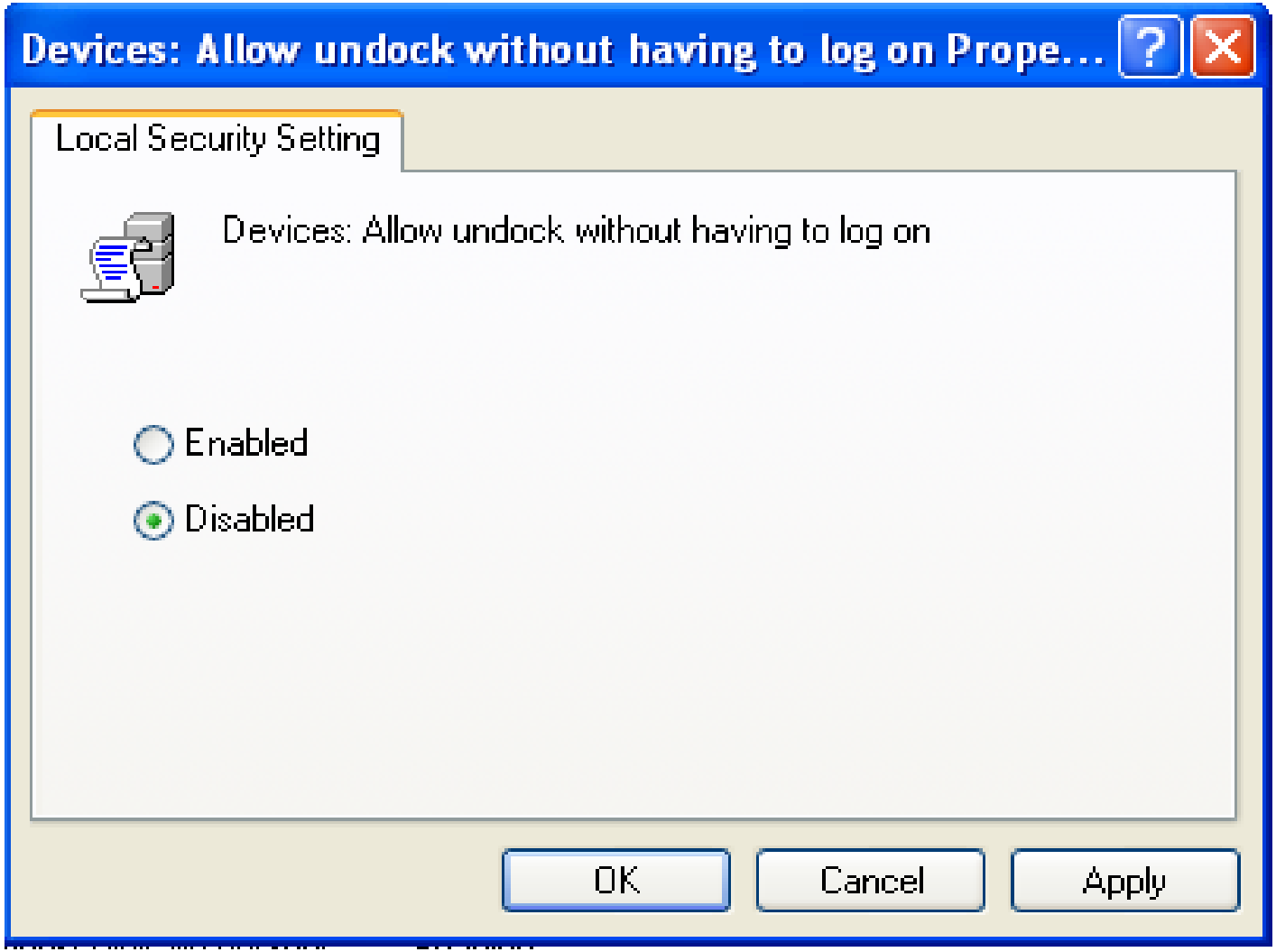
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Allow Undock without having to Log On

Vulnerability	• If this policy setting is enabled, users with access to a portable computer with in there docking station can possible tamper with them
Countermeasure	• **Disable** this policy setting
Potential Impact	• Users with docked systems have to logon to the local console before undocking there computers

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Allow Undock without having to Log On



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Allowed to Format and Eject Removable Media

By this policy it is determined, who has to format and eject removable media.

The values for the **Devices: Allowed to format and eject removable media** setting are:

Administrators

Administrators and Power Users

Administrators and Interactive Users

Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Allowed to Format and Eject Removable Media

Vulnerability

- Users with administrative privileges can
- Remove or move the disk to a different location
- View and modify files, grant permissions

Countermeasure

- Configure this policy setting to **Administrators**.

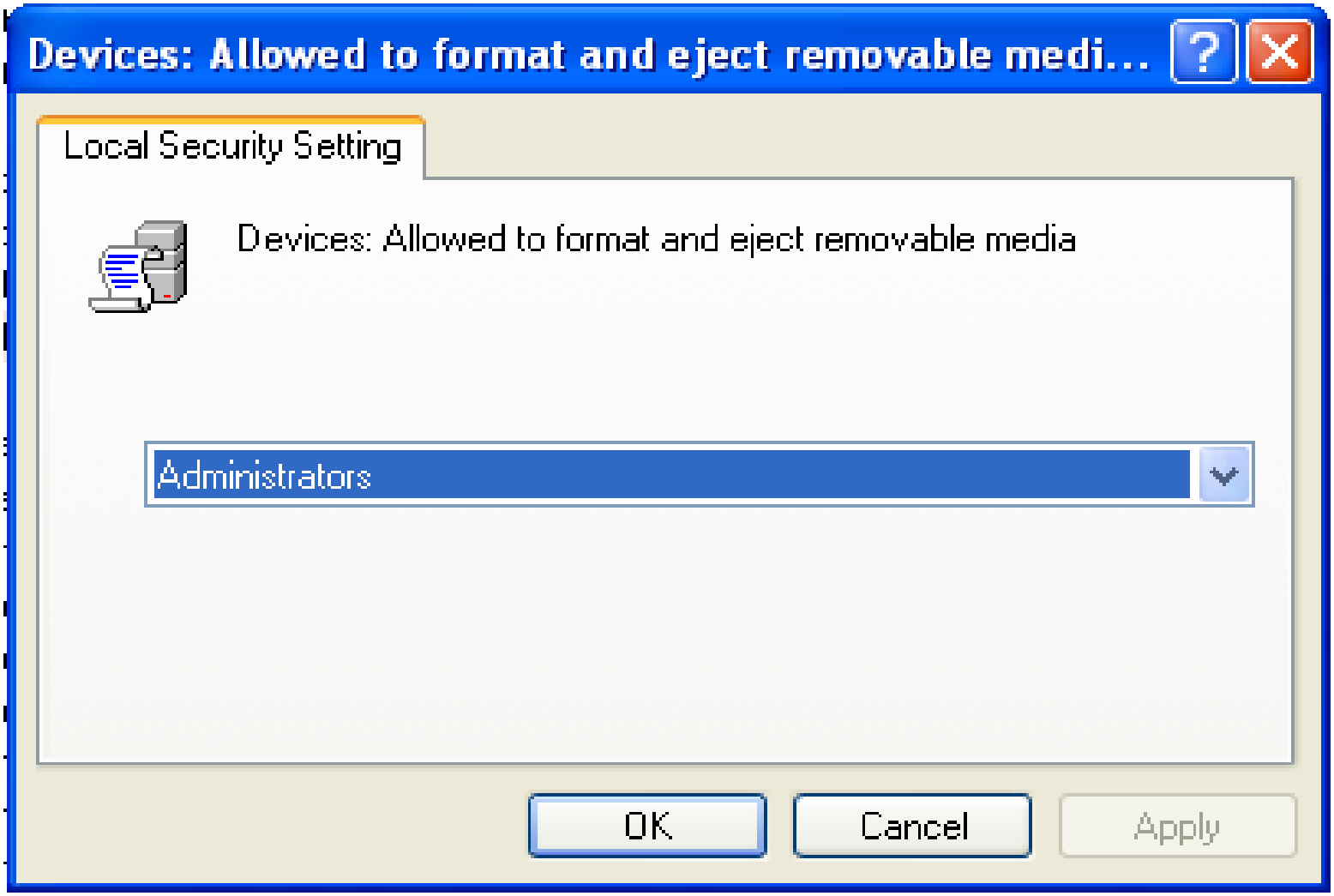
Potential Impact

- NTFS formatted media can be removed only by **Administrators**.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Allowed to Format and Eject Removable Media



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Prevent Users from Installing Printer Drivers

This policy checks who can install a network printer driver on the machine required to operate the printer from the remote machine

Members of **Administrators** and **Power Users** groups are allowed to perform install operations for the network printer when this policy is enabled

If this policy is disabled, any user can install printer drivers

The values for the Devices: Prevent users from installing printer drivers setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Prevent Users from Installing Printer Drivers

Vulnerability

- In some organizations users are allowed to install the drivers on there computer by themselves
- But only administrator should be given privileges to install them on the server, to avoid malicious code acting as a printer driver

Countermeasure

- **Enable** this policy setting

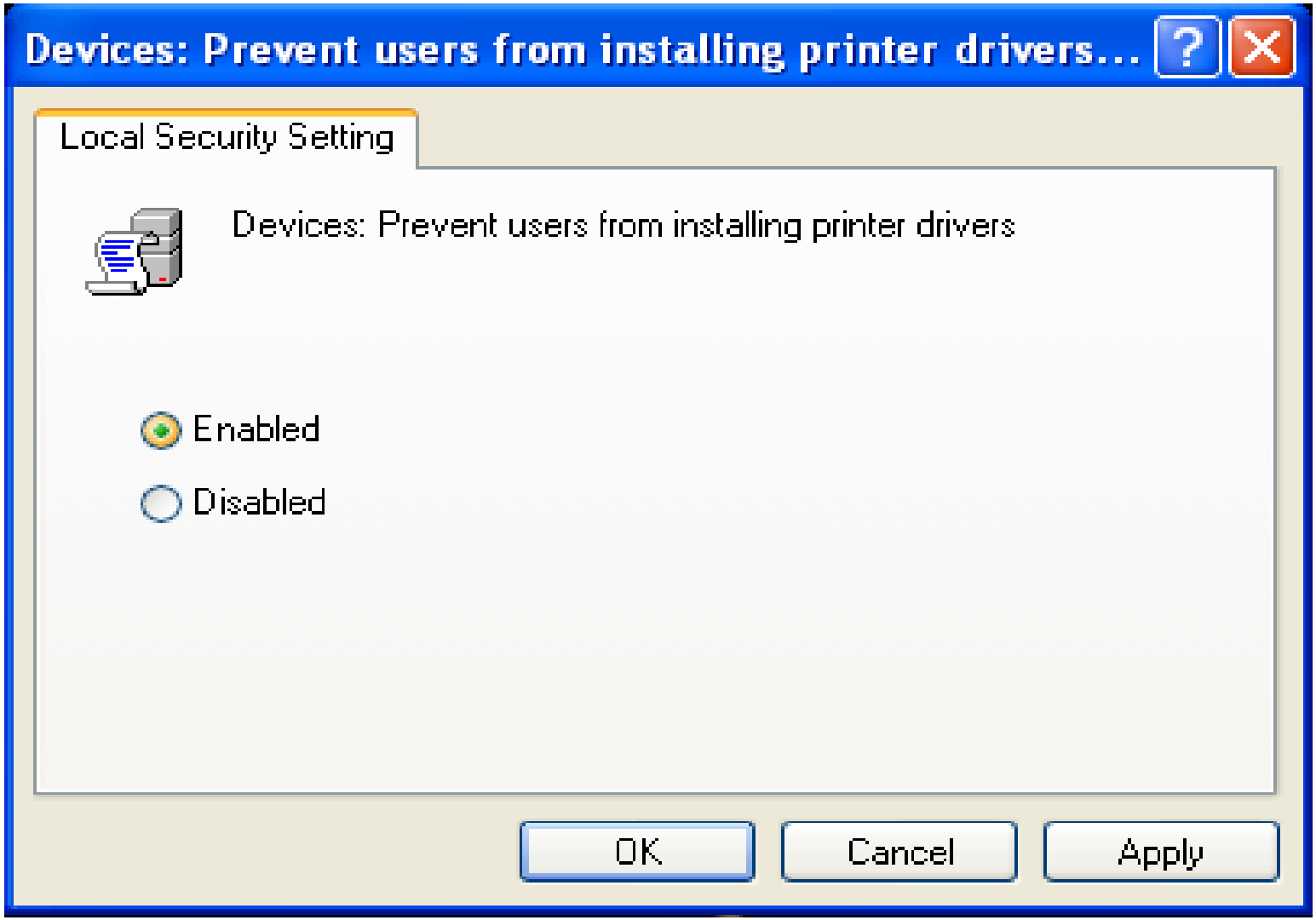
Potential Impact

- Users with Server Operator, Administrator or Power User privileges can only install the printer drivers on the server

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Prevent Users from Installing Printer Drivers



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Restrict CD-ROM/Floppy Access to Locally Logged-on User Only

On enabling this policy a CD-Rom/Floppy can be accessed by both local and remote user simultaneously by an interactively logged on user

The values for the Devices: Restrict CD-ROM/Floppy access to locally logged-on user only setting is:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Restrict CD-ROM /Floppy Access to Locally Logged-on User Only

Vulnerability

- Any user can view a CD-ROM/Floppy with sensitive information
- CD-ROM/Floppy drives have to be manually shared by the Administrator to make it accessible

Countermeasure

- Enable this policy setting

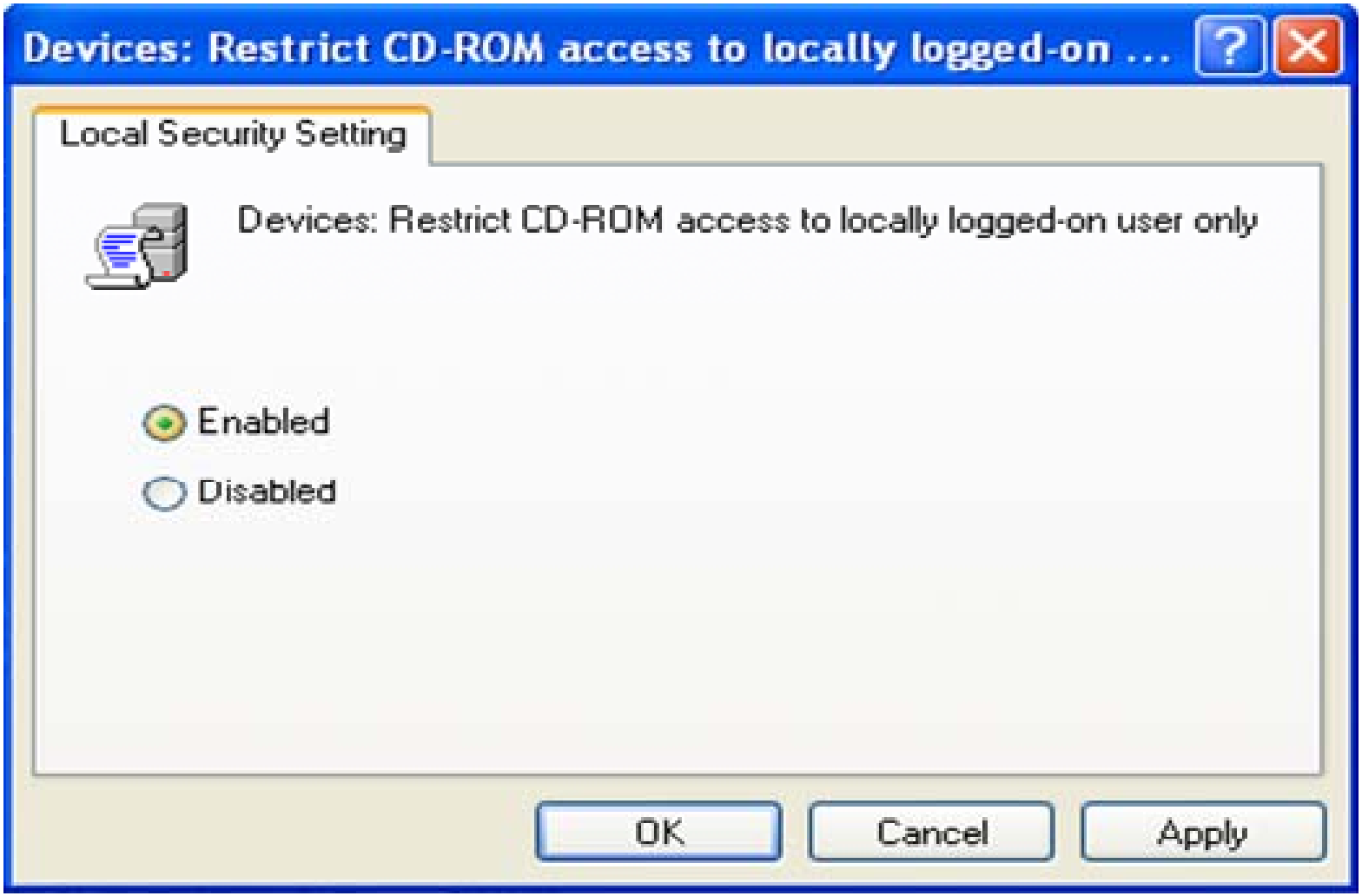
Potential Impact

- Users connected to the server over network can not use the CD-ROM/Floppy drive, installed on the server
- If a computer acts as a CD jukebox for a network, these setting are not suitable

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

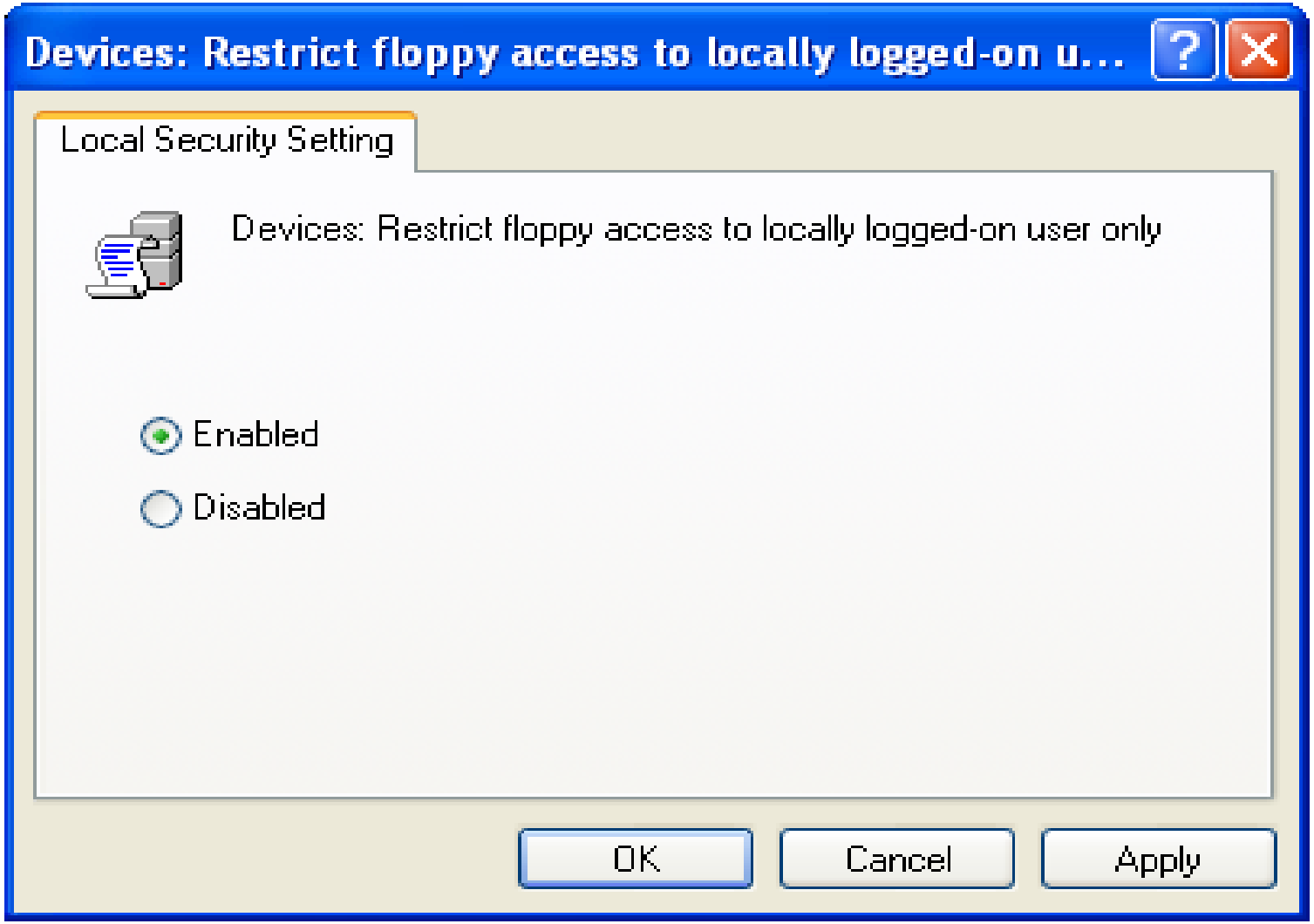
Devices: Restrict CD-ROM Access to Locally Logged-on User Only



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Restrict Floppy Access to Locally Logged-on User Only



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Unsigned Driver Installation Behavior

This policy concludes the outcome of installing a device driver that has not been certified and signed by the Windows Hardware Quality Lab (WHQL) by means of the Setup application programming interface (API)

The values for the **Devices: Unsigned driver installation behavior** setting is:

- Silently succeed
- Warn but allow installation
- Do not allow installation
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Unsigned Driver Installation Behavior

Vulnerability

- This policy interrupts an installation and warns the admin, if the driver is unsigned
- This policy cannot stop coping of a .sys file to start as system service

Countermeasure

- Configure the policy to **Warn but allow installation** for Windows XP with SP2 and **Not Defined** for Windows Server 2003

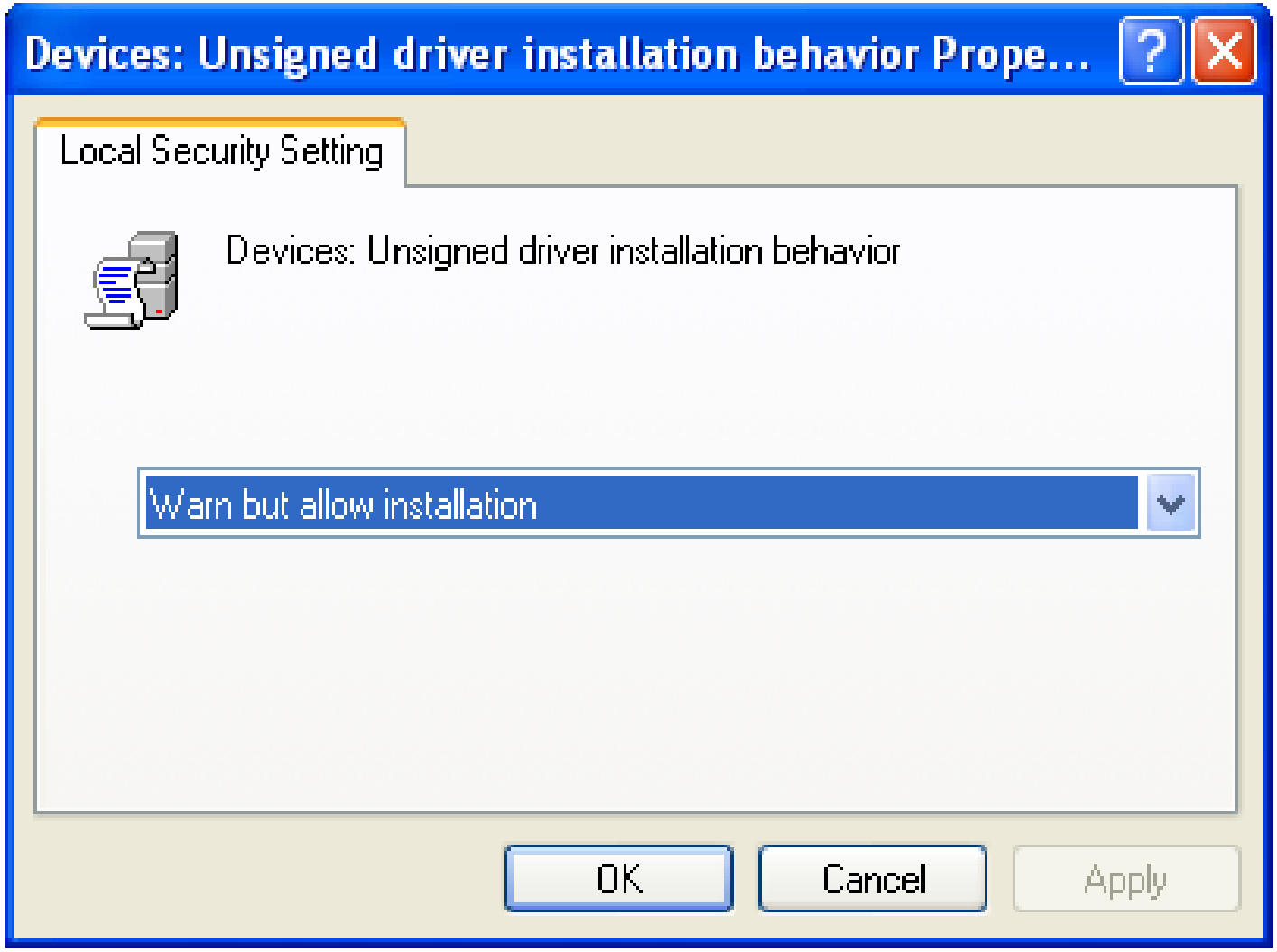
Potential Impact

- Users with this right can install unsigned drivers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Devices: Unsigned Driver Installation Behavior



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Controller: Allow Server Operators to Schedule Tasks

This policy concludes whether server operator can allow to submit jobs through AT schedule facility

The values for the Domain controller: Allow server operators to schedule tasks setting are:

- Enabled
- Disabled
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

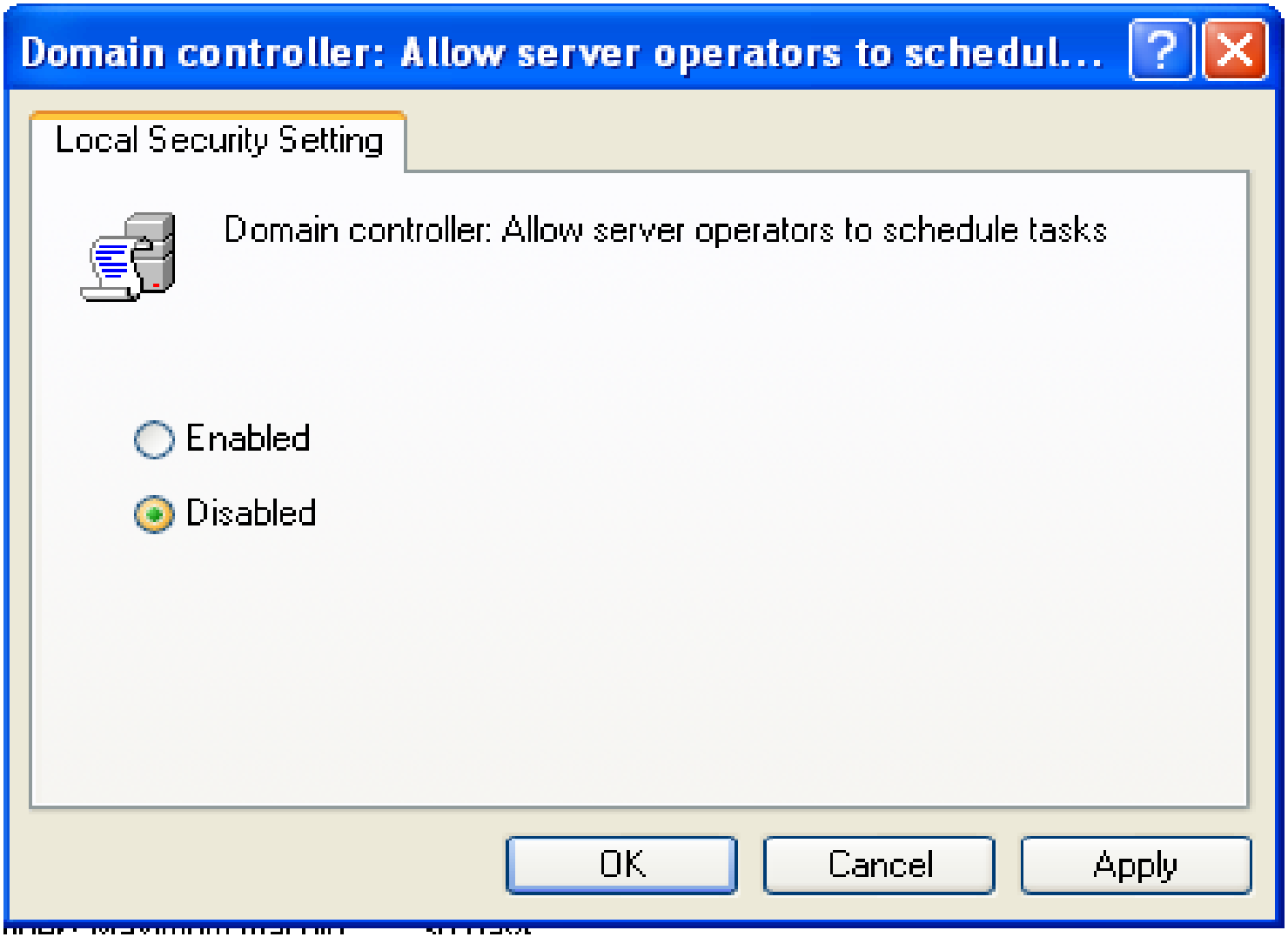
Domain Controller: Allow Server Operators to Schedule Tasks

Vulnerability	• Enabling this setting allows to execute the jobs created by server user in the context of the service running account (local system account)
Countermeasure	• Disable this policy setting
Potential Impact	• The effect is less in many organizations • Users are still able to create jobs through the Task Scheduler Wizard

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Controller: Allow Server Operators to Schedule Tasks



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Controller: LDAP Server Signing Requirements

Finding that the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing is performed by this policy

The values for the **Domain controller: LDAP server signing requirements** setting are:

- **None**. Data signature not necessary
- **Require signature**.
- **Not Defined**.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Controller: LDAP Server Signing Requirements

Vulnerability

- Man-in-the-middle attacks are performed on the unsigned network traffic. To prevent it Internet Protocol security (IPsec) authentication header mode (AH) can be applied, which performs mutual authentication and packet integrity for IP traffic

Countermeasure

- Configure this policy setting to **Require signature**

Potential Impact

- LDAP queries can not be executed over domain controllers by the clients who do not support LDAP signing. Third-party operating systems do not support LDAP signing
- Enabling this policy setting, do not allow those operating systems to access domain resources

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Controller: LDAP Server Signing Requirements

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Controller: Refuse Machine Account Password Changes

This policy checks whether or not a domain controller will accept password change requests for computer accounts

The values for the Domain controller: Refuse machine account password changes setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Controller: Refuse Machine Account Password Changes

Vulnerability

- By enabling this policy on the domain controller, users on the domain can not change there password

Countermeasure

- Disable this policy setting

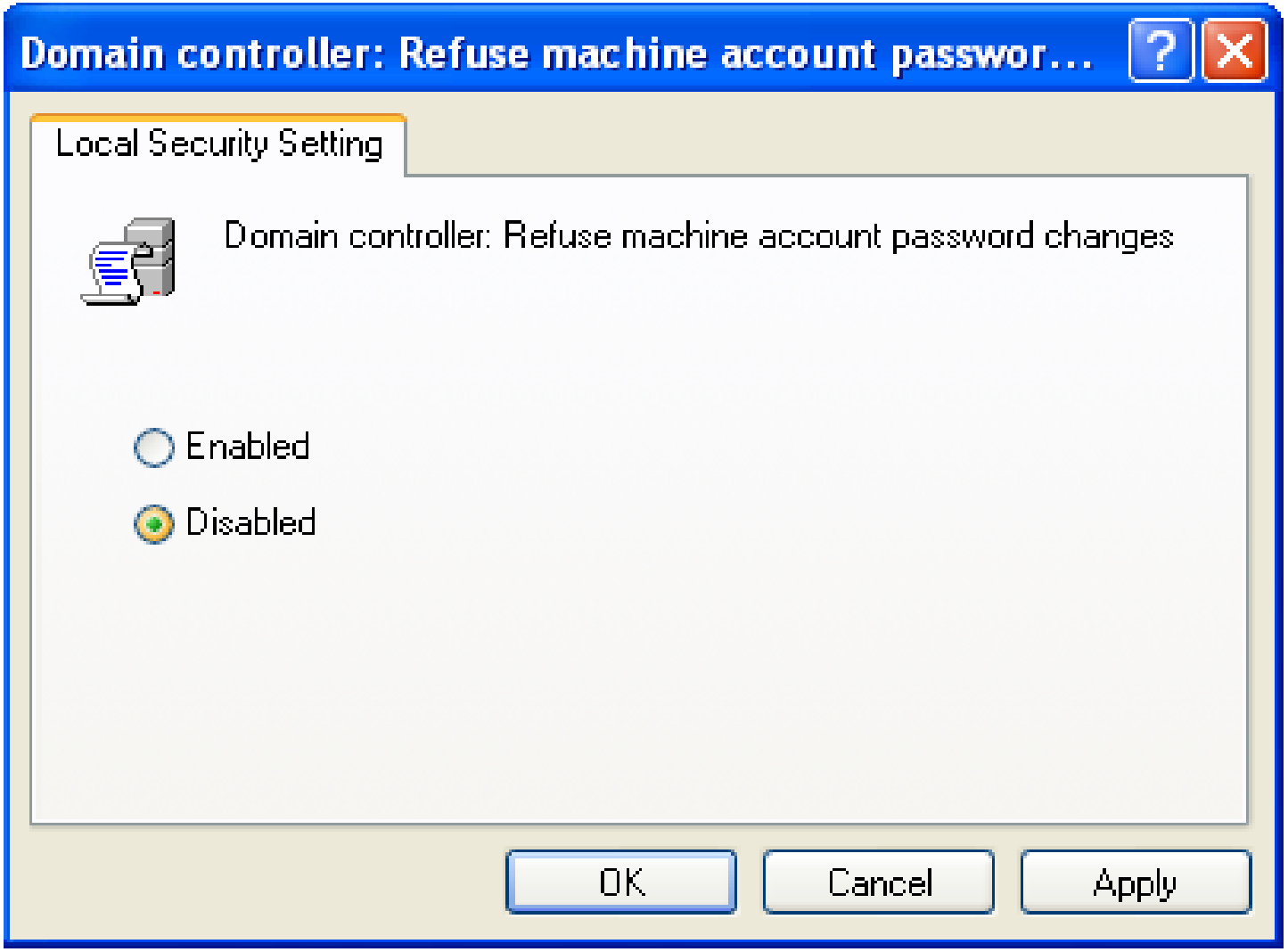
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Controller: Refuse Machine Account Password Changes



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Digitally Encrypt or Sign Secure Channel Data

By the following settings we can conclude whether a secure channel can be aquired with thw domain controller:

- **Domain member: Digitally encrypt or sign secure channel data (always)**
  - By enabling this setting, cannot set a secure channel with domain controller.
- **Domain member: Digitally encrypt secure channel data (when possible)**
  - This setting is enabled by enabling the above setting
- **Domain member: Digitally sign secure channel data (when possible)**

The possible values for this policy setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Digitally Encrypt or Sign Secure Channel Data

Vulnerability

- A secure channel cannot be encrypted or signed by the domain controller.
- A secure channel can be established, if the computer is set to encrypt or sign secure channel when possible. Encryption level is discussed

Countermeasure

- Configure the **Domain member: Digitally encrypt or sign secure channel data (always)** setting to **Enabled**
- Configure the **Domain member: Digitally encrypt secure channel data (when possible)** setting to **Enabled**
- Configure the **Domain member: Digitally sign secure channel data (when possible)** setting to **Enabled**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Digitally Encrypt or Sign Secure Channel Data

Potential Impact

- Enabling **Domain member: Digitally encrypt or sign secure channel data (always)** setting over domain controllers with windows 98 client is not possible
- Potential impacts can include the following:
- Create or delete down-level trust relationships will be disabled.
- Logons from down-level clients will be disabled
- Authenticate other domains' users from a down-level trusted domain will be disabled

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Digitally Encrypt or Sign Secure Channel Data

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Disable Machine Account Password Changes

This setting defines that a domain member can change his password from time-to-time or not

Enabled – Cannot change password

Disabled – Can change password

This setting should be avoided while supporting dual-boot scenarios

These setting are used with imaged computers (or) with hardware or software level change prevention

The values for the Domain member: Disable machine account password changes setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Disable Machine Account Password Changes

Vulnerability

- Windows Server 2003 based computers are automatically required to change the passwords in every 30 days. If the setting in these computers are disabled they will retain there passwords
- If the computers not able to modify there password by itself can be attacked for password guess

Countermeasure

- Disable this policy setting

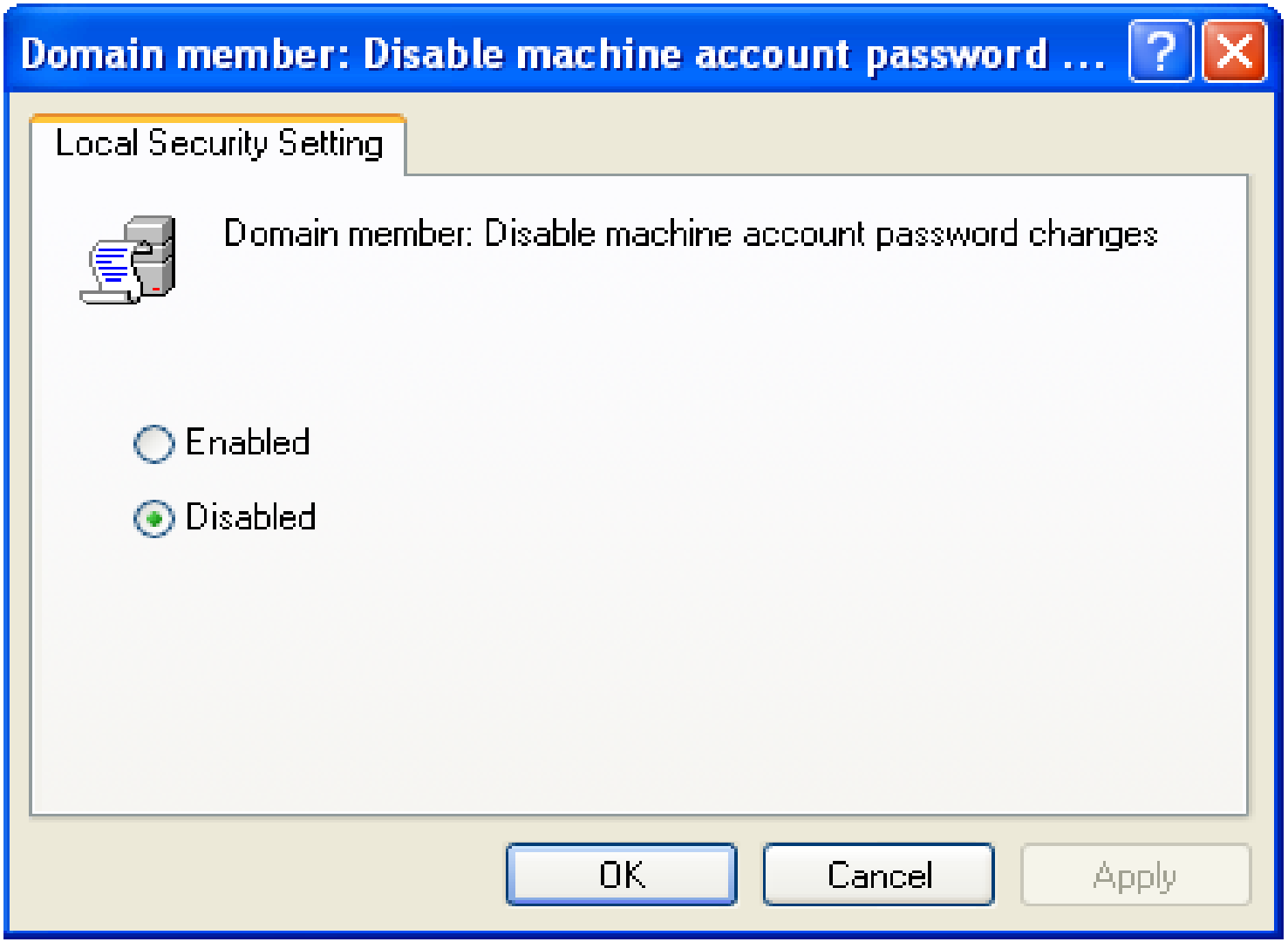
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Disable Machine Account Password Changes



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Maximum Machine Account Password Age

This policy helps to find out the maximum allowable age for a computer account password

The values for the **Domain member: Maximum machine account password age** setting is:

- A number of days between 0 and 999
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Maximum Machine Account Password Age

Vulnerability

- An Active Directory–based domain will have an account and password, which is changed for every 30 days by default
- If the password change event time span is increased or modified 0, an attacker will have much time to run brute force attack

Countermeasure

- Configure the password change setting to 30 days

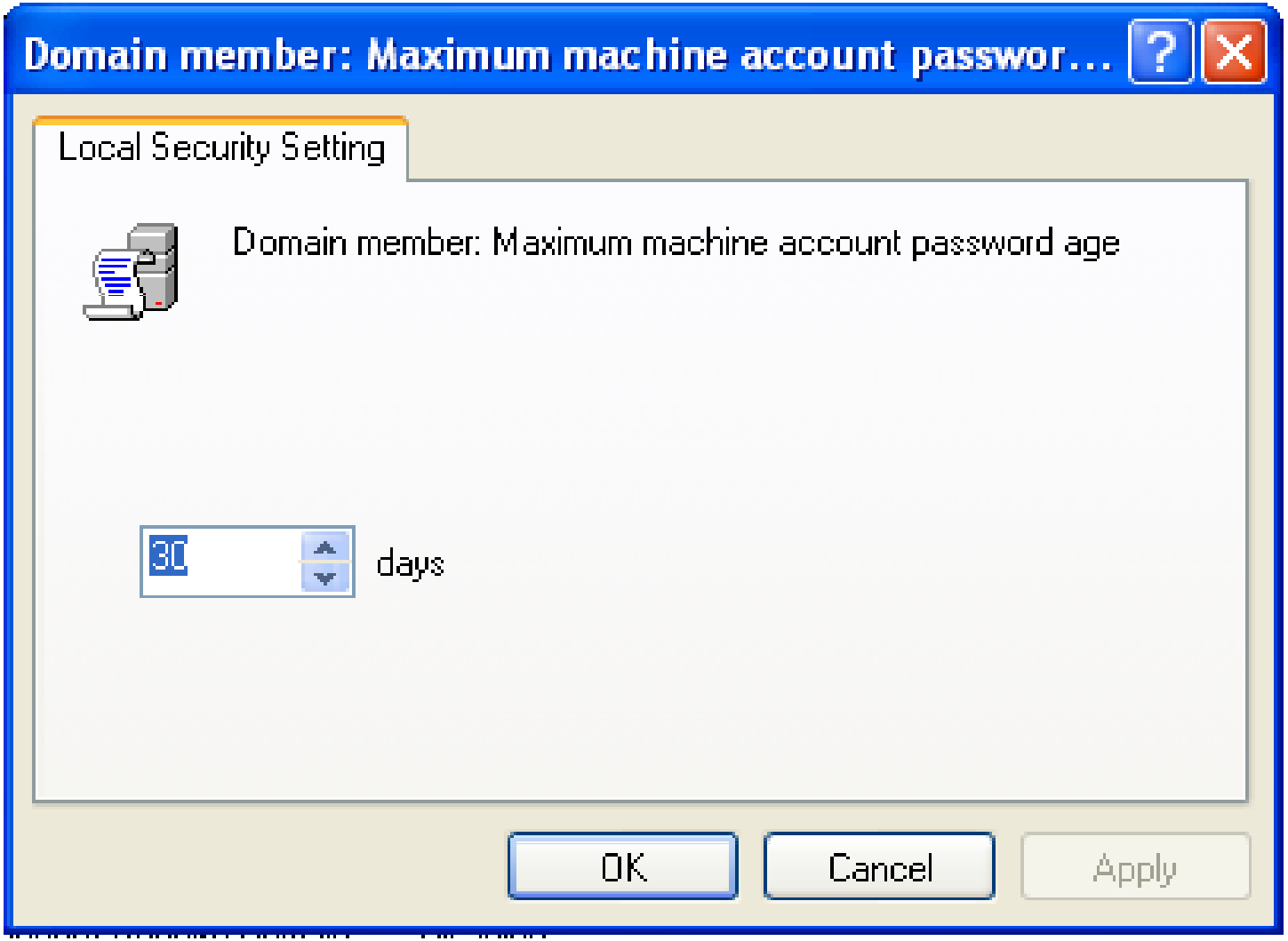
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Maximum Machine Account Password Age



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Require Strong (Windows 2000 or Later) Session Key

By this policy it can be determined that a secure channel can be started with a domain control which cannot encrypt the traffic with 128 bit session key

If this policy is enabled a secure channel cannot be started with a domain controller

By disabling this policy a 64-bit session keys are allowed

The values for the Domain member: Require strong (Windows 2000 or later) session key setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Require Strong (Windows 2000 or Later) Session Key

Vulnerability

- In Windows 2000 a much stronger session key is used to connect between a domain controller and member computer
- These advanced session keys should be used to protect communication from network hijackers and eavesdropping

Countermeasure

- **Enable** this policy setting
- **Disable** this policy setting to negotiate the key strength

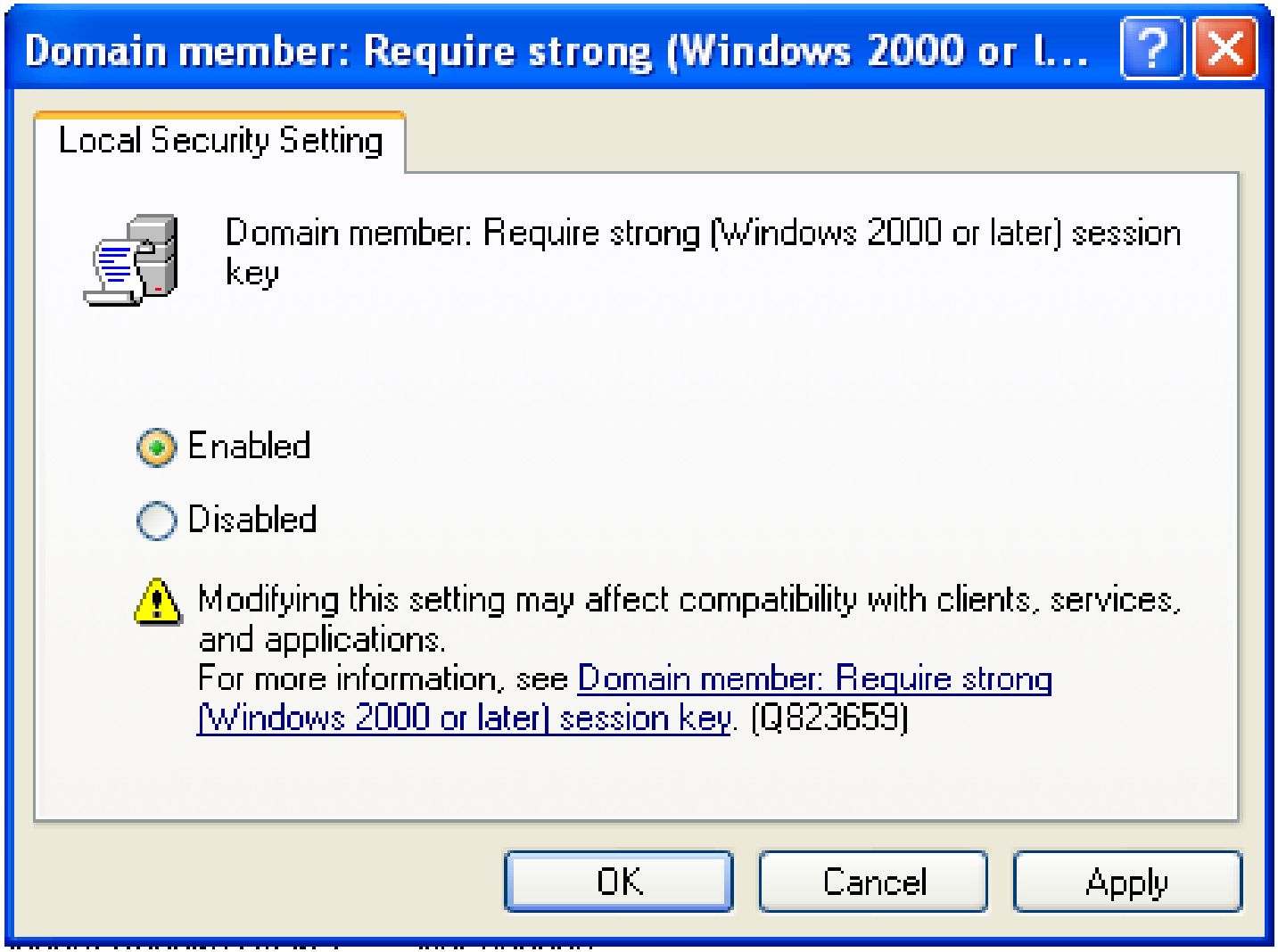
Potential Impact

- Computers that have this policy setting enabled will not be able to join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT-style domains may not work properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Domain Member: Require Strong (Windows 2000 or Later) Session Key



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Do Not Display Last User Name

This policy determines whether the logon box displays last logged on user name

- Enable – the name of the last user to successfully log on does not display.
- Disable – the name of the last user to log on will display.

The values for the **Interactive logon: Do not display last user name** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Do Not Display Last User Name

Vulnerability

- An attacker who can access the console can view the name of the last user logged on. Then the attacker can logon using dictionary words and brute force attack

Countermeasure

- Configure this policy setting to **Enable**

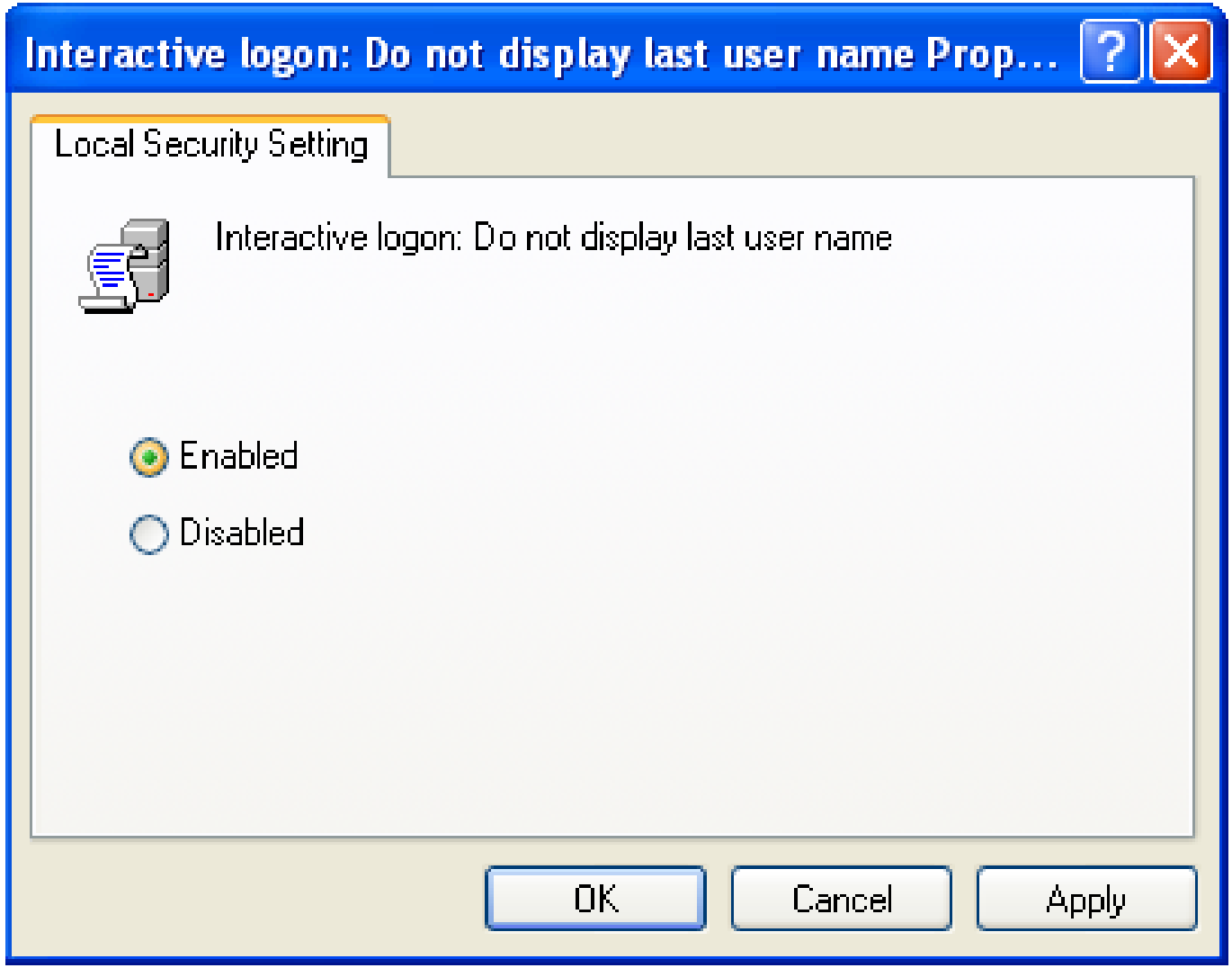
Potential Impact

- The user name should be inputted for every visit

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Do Not Display Last User Name



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Do Not Require CTRL+ALT+DEL

By this policy you can decide that users must press CTRL+ALT+DEL before they log in

- Enable – No need to press CTRL+ALT+DEL
- Disable – Must press CTRL+ALT+DEL

You can logon to Windows using a smart card. Which is a tamper-proof device used to stores security information

The values for the **Interactive logon: Do not require CTRL+ALT+DEL** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Do Not Require CTRL+ALT+DEL

Vulnerability

- This feature is included in Windows as if users are not required to press CTRL+ALT+DEL subsequent attack may happen for the password
- An attacker could install a Trojan horse program to capture the user login and password

Countermeasure

- Disable the policy setting.

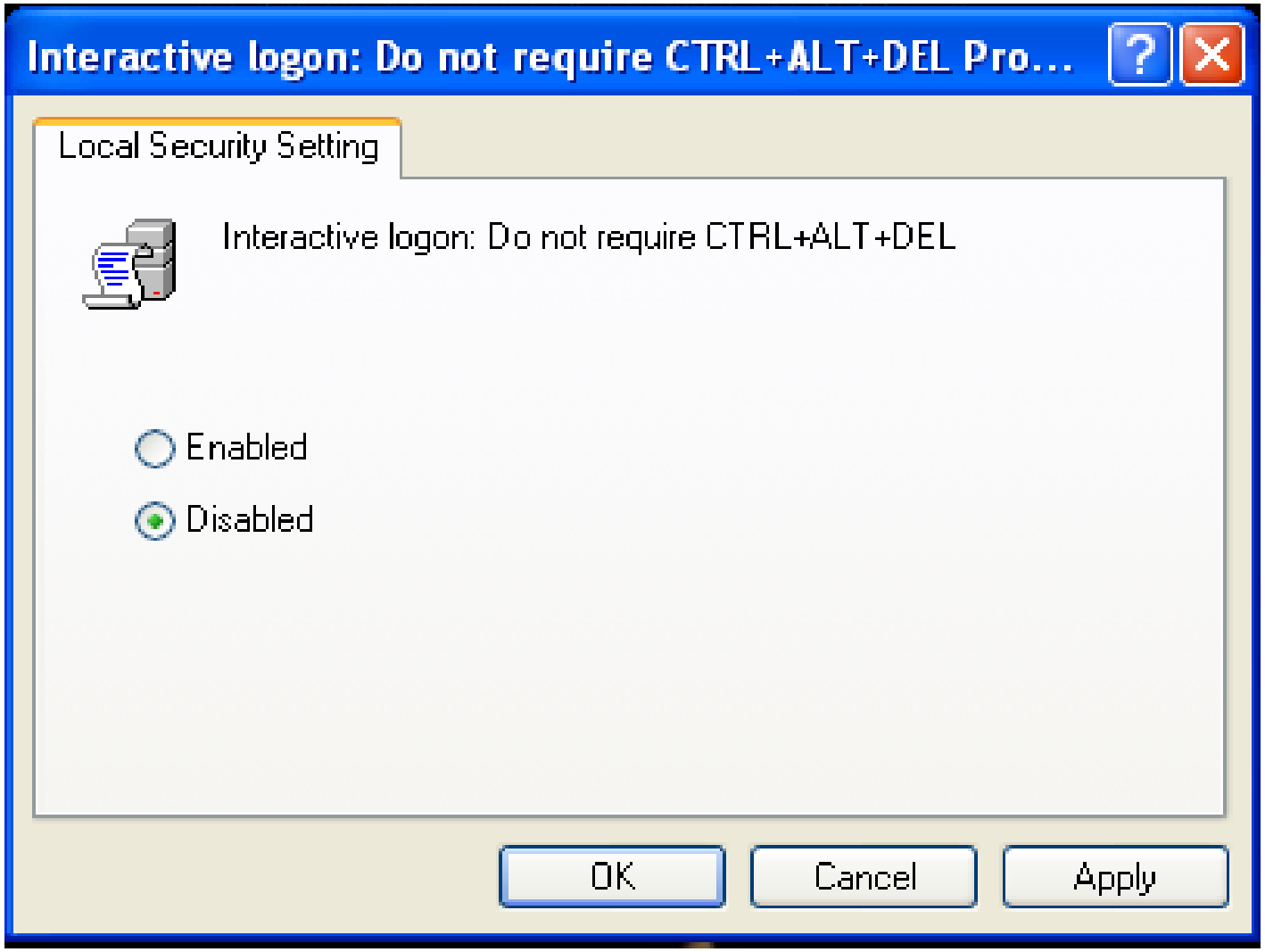
Potential Impact

- User has to press CTRL+ALT+DEL for the logon dialog box

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Do Not Require CTRL+ALT+DEL



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Message Text for Users Attempting to Log On

The **Interactive logon: Message text for users attempting to log on** and the **Interactive logon: Message title for users attempting to log on** settings are used for almost similar purpose.

The first policy setting displays a text message to the user, and the second policy setting display the message in title bar of the window.

The values for these policy settings are:

- User-defined text
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Message Text for Users Attempting to Log On

Vulnerability

- By displaying a warning message you can warn the attackers
- It even helps to inform employees about the company policies

Countermeasure

- Configure the **Message text for users attempting to log on** and **Message title for users attempting to log on** settings to a suitable value

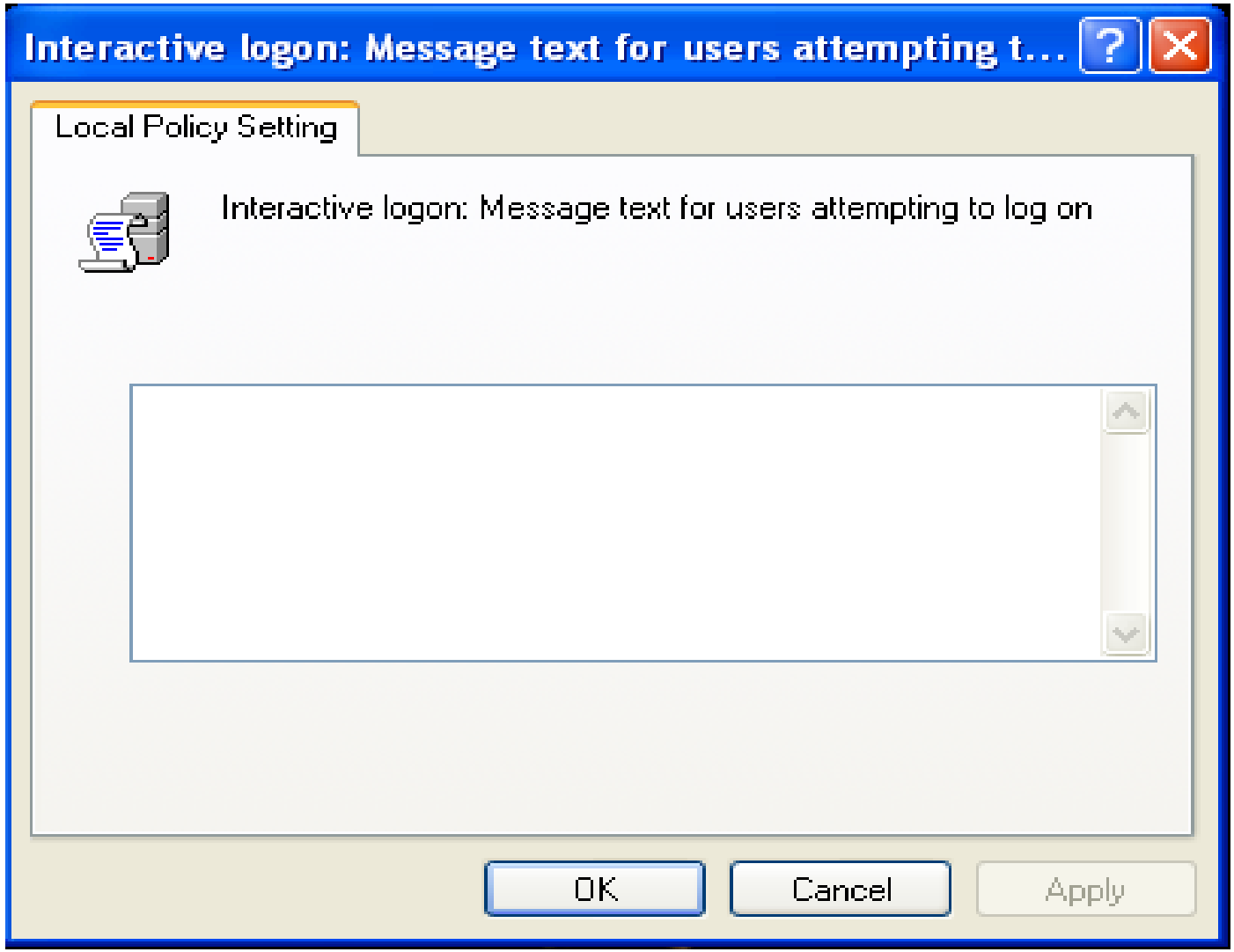
Potential Impact

- A message is displayed to the user before logging on to the server console

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Message Text for Users Attempting to Log On



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Number of Previous Logons to Cache

This policy finds the number of different unique users who have the capability of logging on to a window domain using cached information of an account

In rare cases if a domain controller cannot be contacted the locally cached information can be used to logon

This policy helps to find the number of user's information cached

When the domain controller is not reachable the following message is given to the users:

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Number of Previous Logons to Cache

A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on may not be available

If the domain controller is not available and the information is not cached, the following message is given:

- The system cannot log you on now because the domain <*DOMAIN_NAME*> is not available.

The values for the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting are:

- A number between 0 and 50
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Number of Previous Logons to Cache

Vulnerability

- This policy accepts a number which indicates the number of user information which has to be cached
- Once this number of cache are captured the next cached logon session is overwritten
- When a user logs on a server console the logon credentials are captured on the server.
- Once an attacker is able to get access to the file system of the server, he can find the cached information and attempt an attack

Countermeasure

- Configure the policy value to **0**

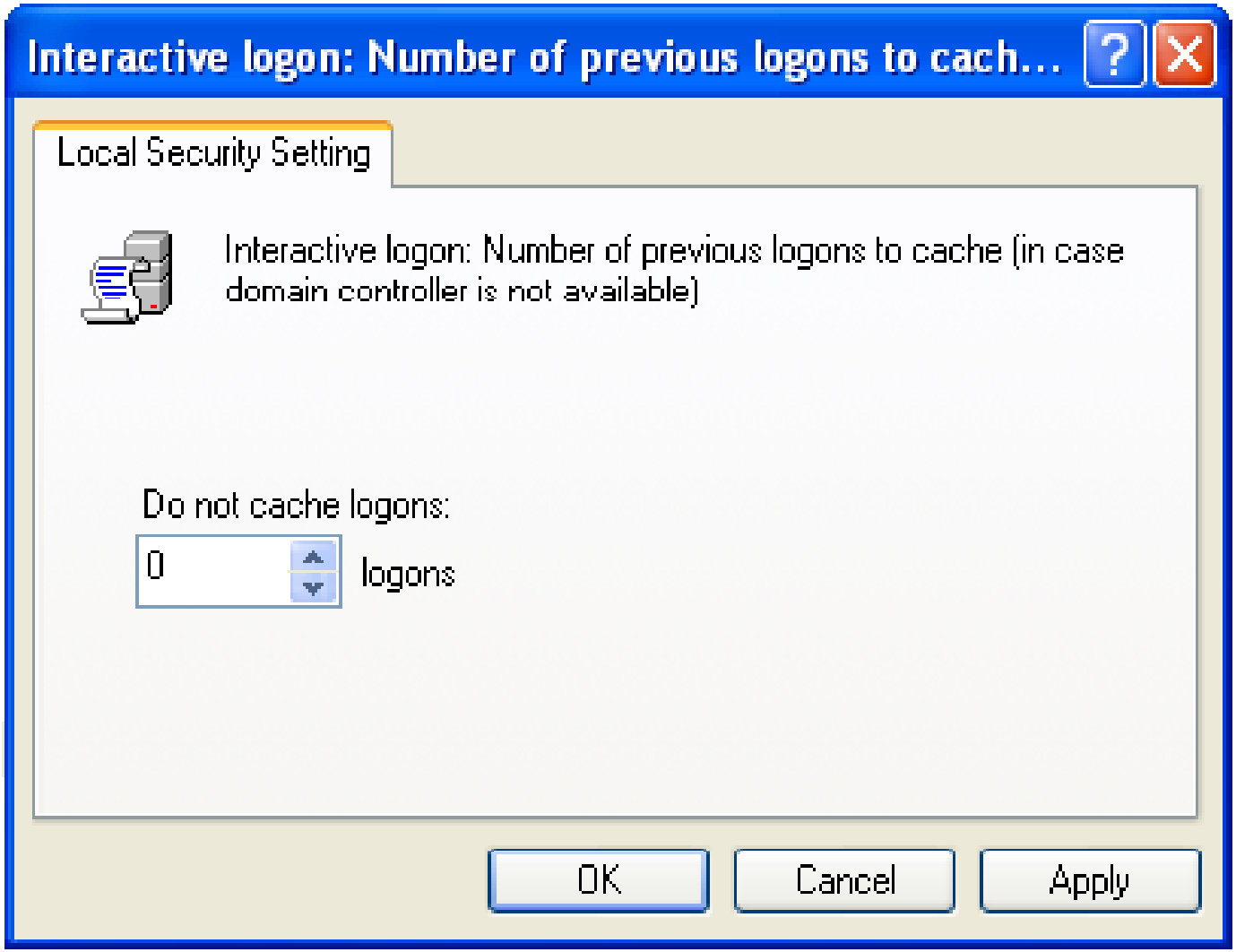
Potential Impact

- If there is no domain controller, users cannot logon to any computer

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Number of Previous Logons to Cache



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Prompt User to Change Password before Expiration

This policy is used to set the number of days in advance the users are given password change message. This helps the user in deciding a strong password

The values for the Interactive logon: Prompt user to change password before expiration setting are:

- Number of days between 1 and 999
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Prompt User to Change Password before Expiration

Vulnerability

- When the passwords are configured to change periodically, a message (warning) should be given to the user before the password expires.
- If there is no warning message given the computer may lock down as soon as the password expires.

Countermeasure

- Configure the setting to 14 days.

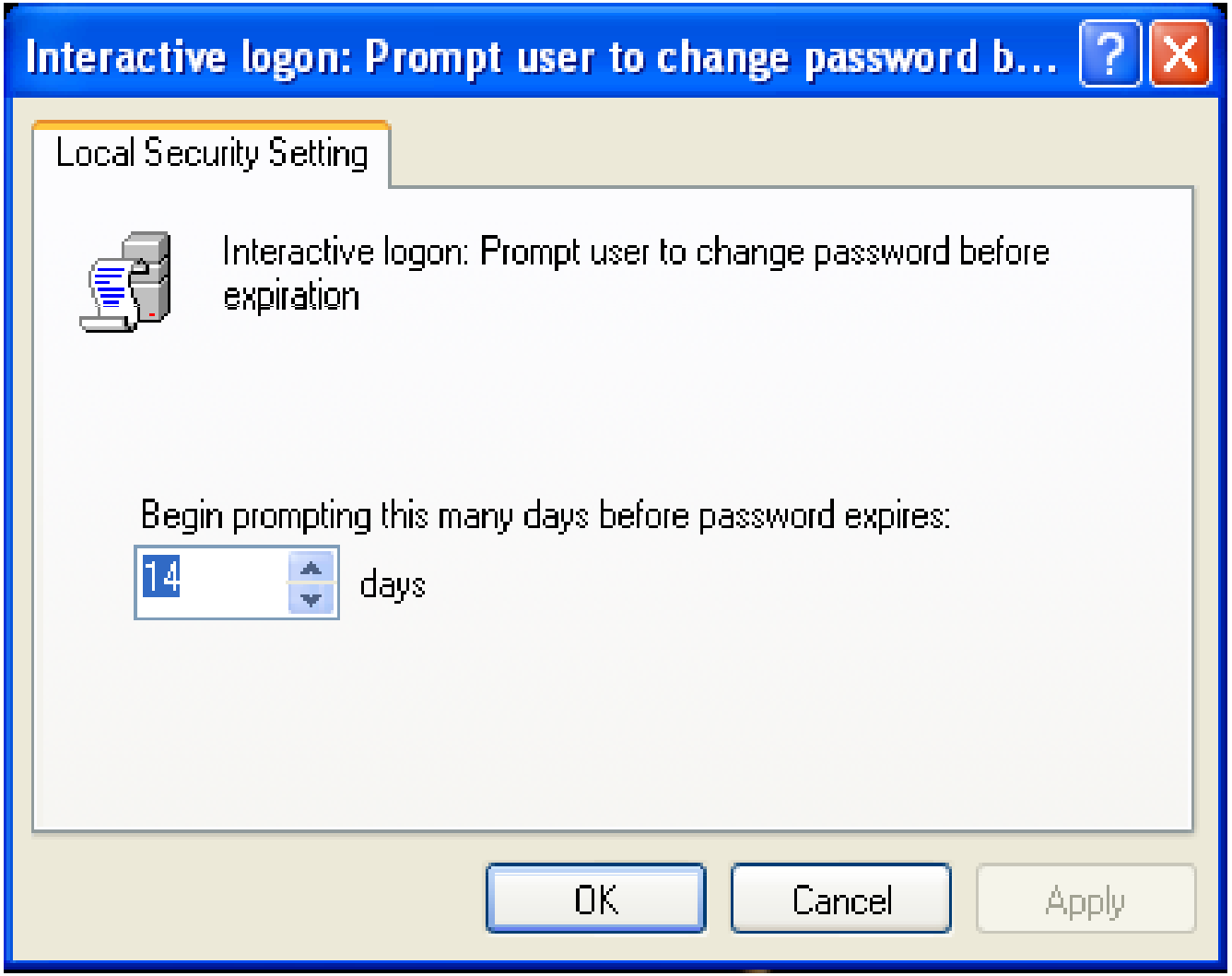
Potential Impact

- A dialog box to change the password should be prompted when ever the user password is in expiry limit.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Prompt User to Change Password before Expiration



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Require Domain Controller Authentication to Unlock Workstation

To unlock a locked computer logon information is required

This policy checks on contacting the domain controller is essential to unlock a computer

Enable – A domain must be authenticated by a domain controller

Disable – No need to contact the domain controller

The values for the **Interactive logon: Require Domain Controller authentication to unlock workstation** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Require Domain Controller Authentication to Unlock Workstation

Vulnerability

- When a user attempt to logon, the computer cache the logon information which is used to unlock the console
- While using cached credentials, the recently made account changes are not affected after unlocking the console

Countermeasure

- Configure this policy to **Enable**
- Configure the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** setting to **0**

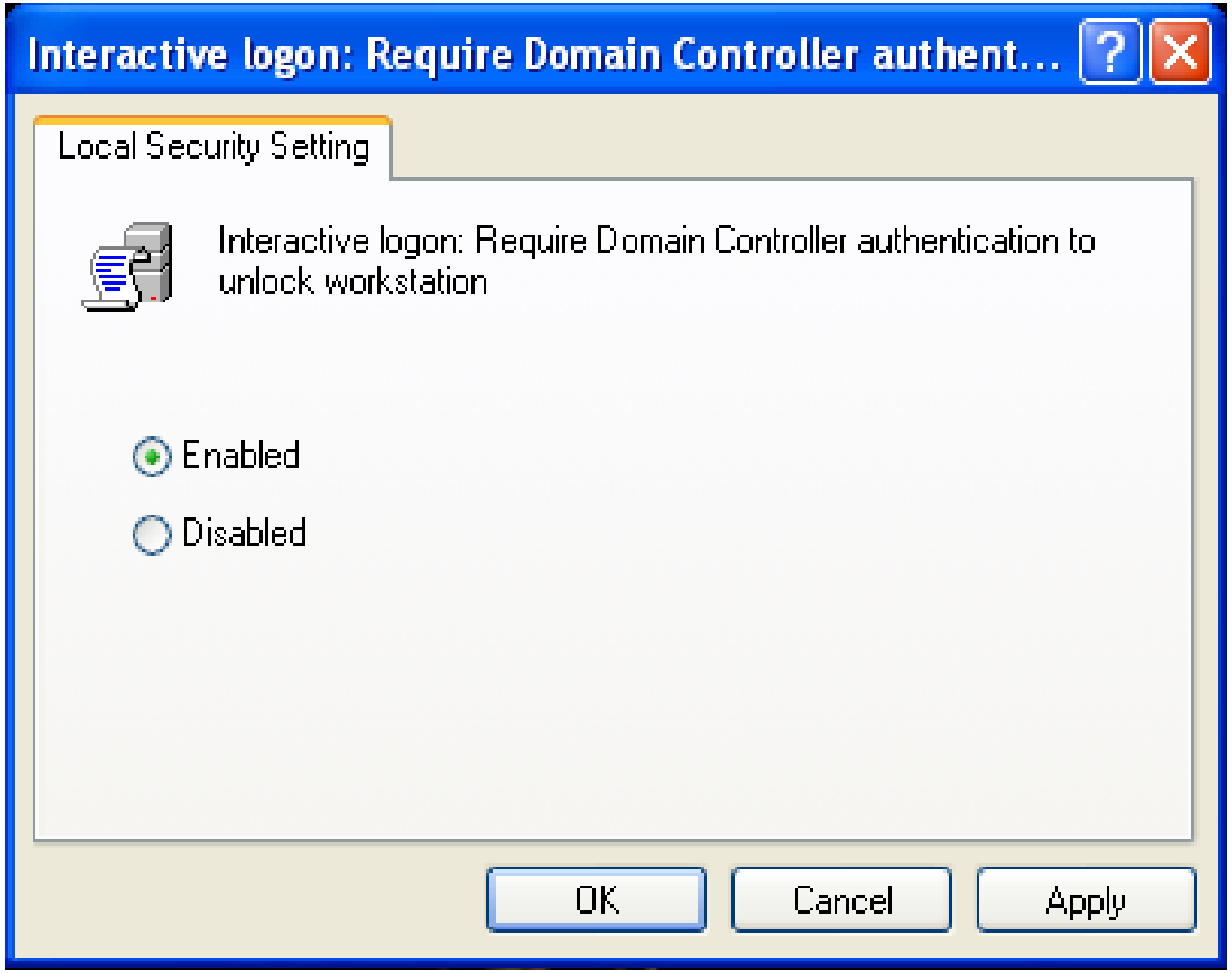
Potential Impact

- To unlock a computer which is locked automatically or by a screen saver needs a domain controller to re-authenticate it
- If **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** is configured to **0,** users without domain controllers are unavailable to log on

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Require Domain Controller Authentication to Unlock Workstation



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Require Smart Card

This policy decides whether users need a smart card to logon or not.

The values for the **Interactive logon: Require smart card** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Require Smart Card

Vulnerability

- The use of smart card increases security as using a smart card the user must provide the card and even know its Personnel Identification Number (PIN).
- Every time the user logs on a new session key is generated to encrypt the traffic

Countermeasure

- Issue smart cards and configure the account policy to Enable

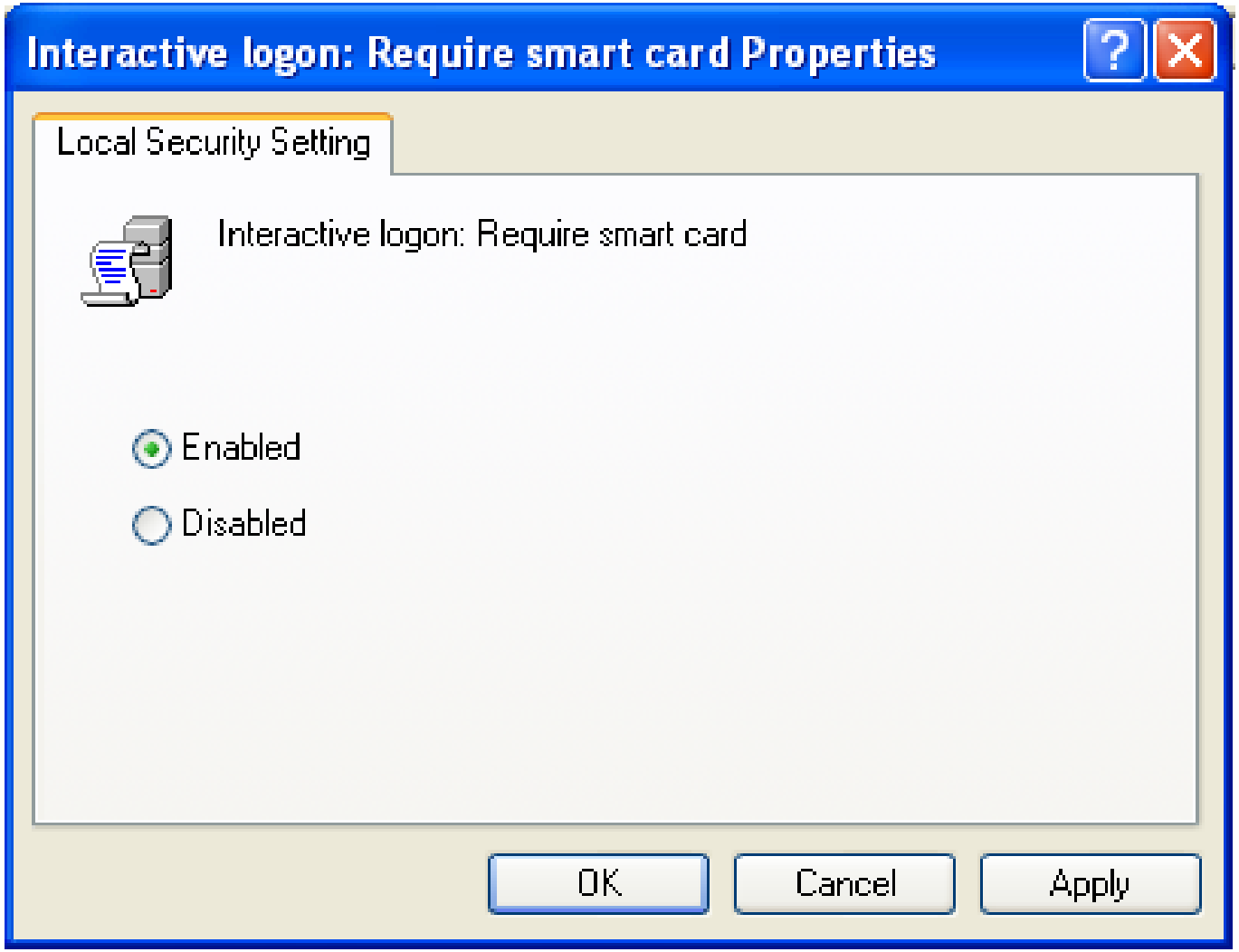
Potential Impact

- Windows Server 2003 includes Certificate Services, a highly advanced service for implementing and managing certificates.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Require Smart Card



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Smart Card Removal Behavior

This policy concludes on the outcome when a smart card is removed from the smart card reader

The values for the Interactive logon: Smart card removal behavior setting are:

- No Action
- Lock Workstation
- Force Logoff
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

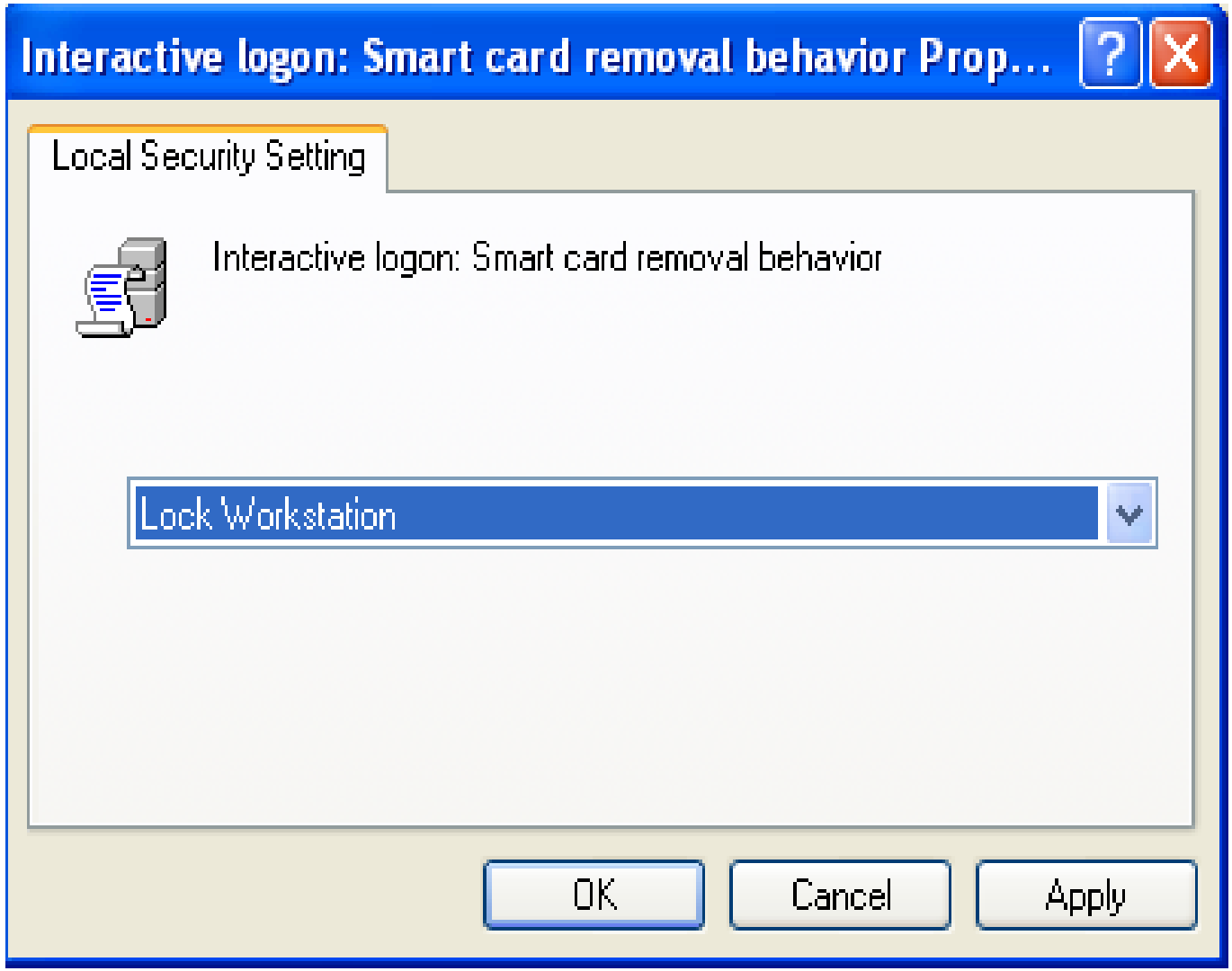
Interactive Logon: Smart Card Removal Behavior

Vulnerability	• When the smart card is removed from the reader the computer should automatically be removed. This will prevent unauthorized login
Countermeasure	• Configure this policy to Lock Workstation to lock the computer when the card is removed • With **Force Logoff Properties** the user is automatically logged off when the smart card is removed
Potential Impact	• The user should present his smart card and PIN to login the next time.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Interactive Logon: Smart Card Removal Behavior



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Client and Server: Digitally Sign Communications (Four Related Settings)

For Server Message Block (SMB) communications these properties are to be set:

- **Microsoft Network Client: Digitally Sign Communications (Always)**
- **Microsoft Network Server: Digitally Sign Communications (Always)**
- **Microsoft Network Client: Digitally Sign Communications (If Server Agrees)**
- **Microsoft Network Server: Digitally Sign Communications (If Client Agrees)**

The values for each of these policy settings are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Client and Server: Digitally Sign Communications (Four Related Settings)

Vulnerability

- Using digital signature helps in securing the network
- An attacker can intercept and modify unsigned SMB packets to modify the traffic to make the server perform undesirable actions
- Attacker can pose as a server or client after legitimate authentication to gain unauthorized access to data

Countermeasure

- Configure the settings as follows:
  - **Microsoft Network Client: Digitally Sign Communications (Always)** to **Disabled**
  - **Microsoft Network Server: Digitally Sign Communications (Always)** to **Disabled**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Client and Server: Digitally Sign Communications (Four Related Settings)

Microsoft Network Client: Digitally Sign Communications (If Server Agrees) to Enabled

Microsoft Network Server: Digitally Sign Communications (If Client Agrees) to Enabled

If these properties are made to **Enable**, this configuration may minimize the performance on client computer

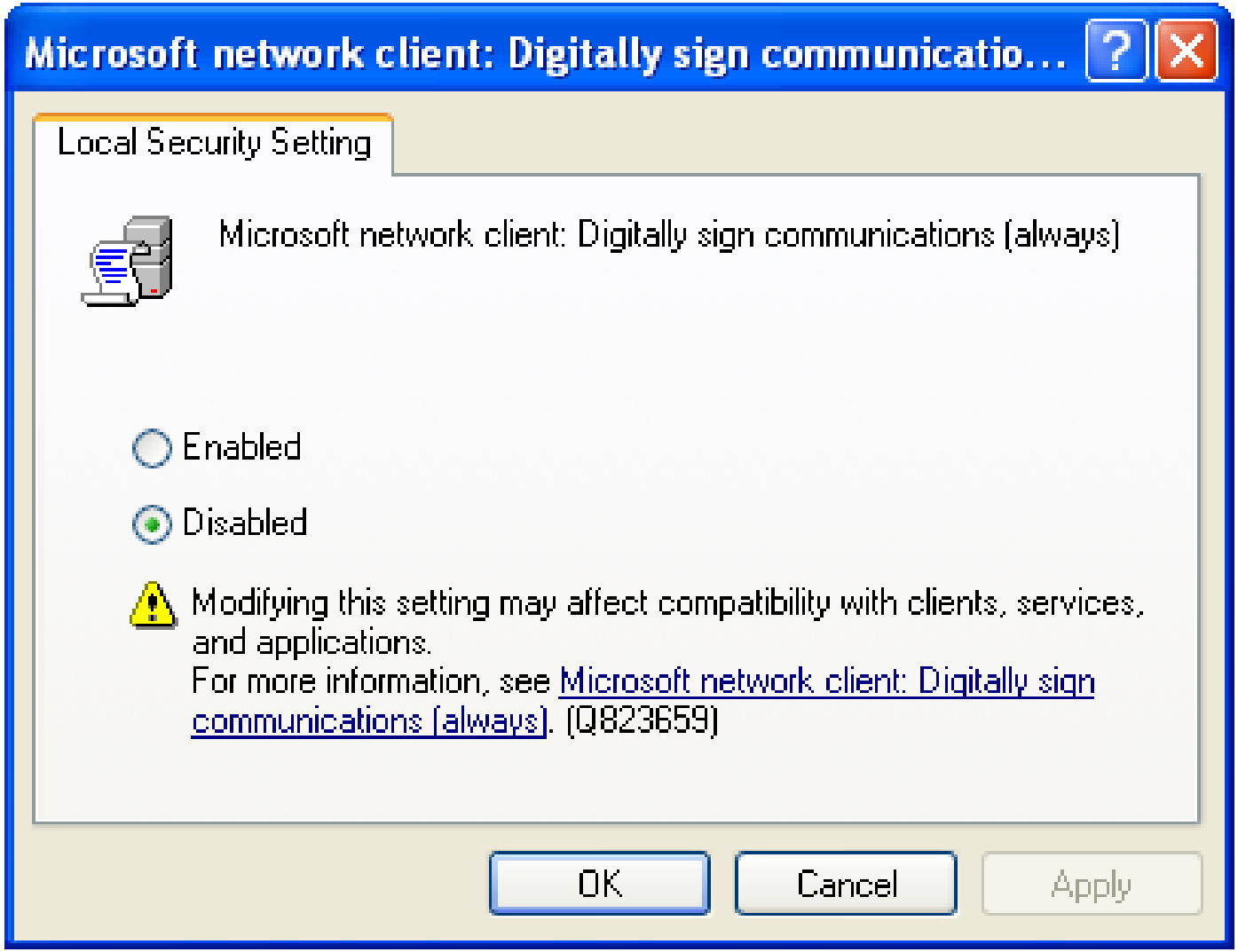
Potential Impact

- To prevent session hijacking attacks by implementing of the SMB file and print sharing protocol in The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, and Windows XP Professional

EC-Council

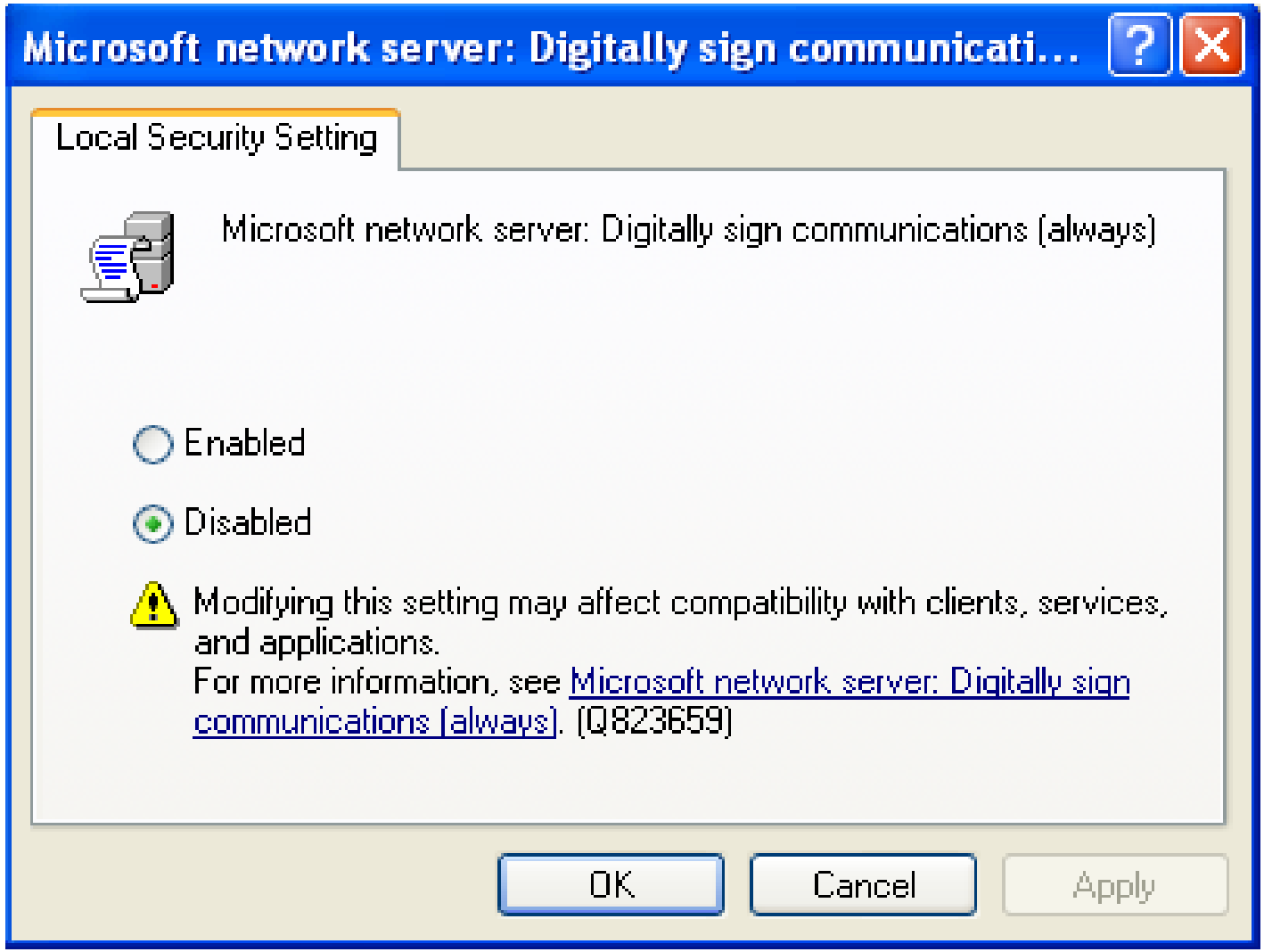
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Client and Server: Digitally Sign Communications (Four Related Settings)



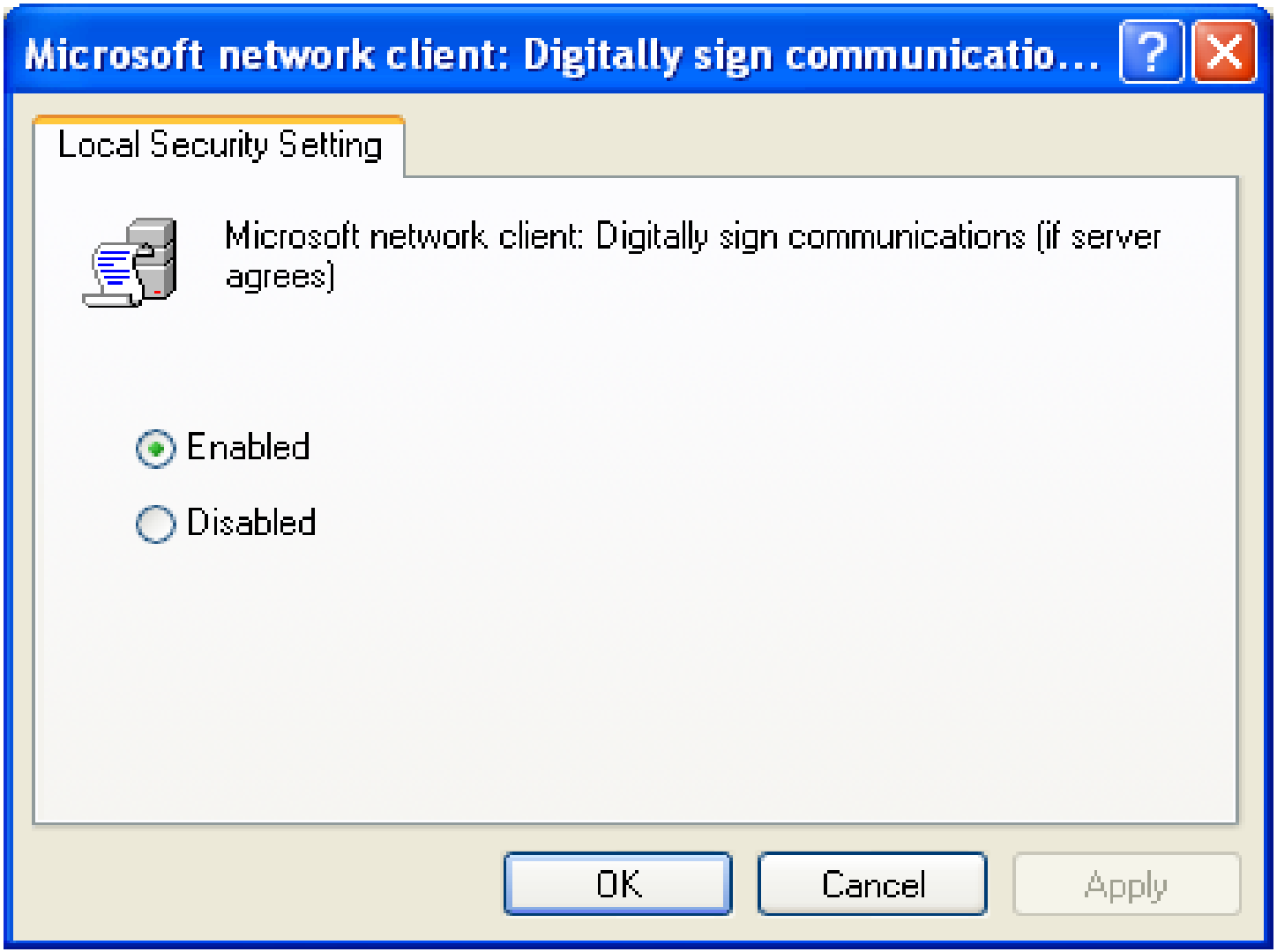
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Client and Server: Digitally Sign Communications (Four Related Settings)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

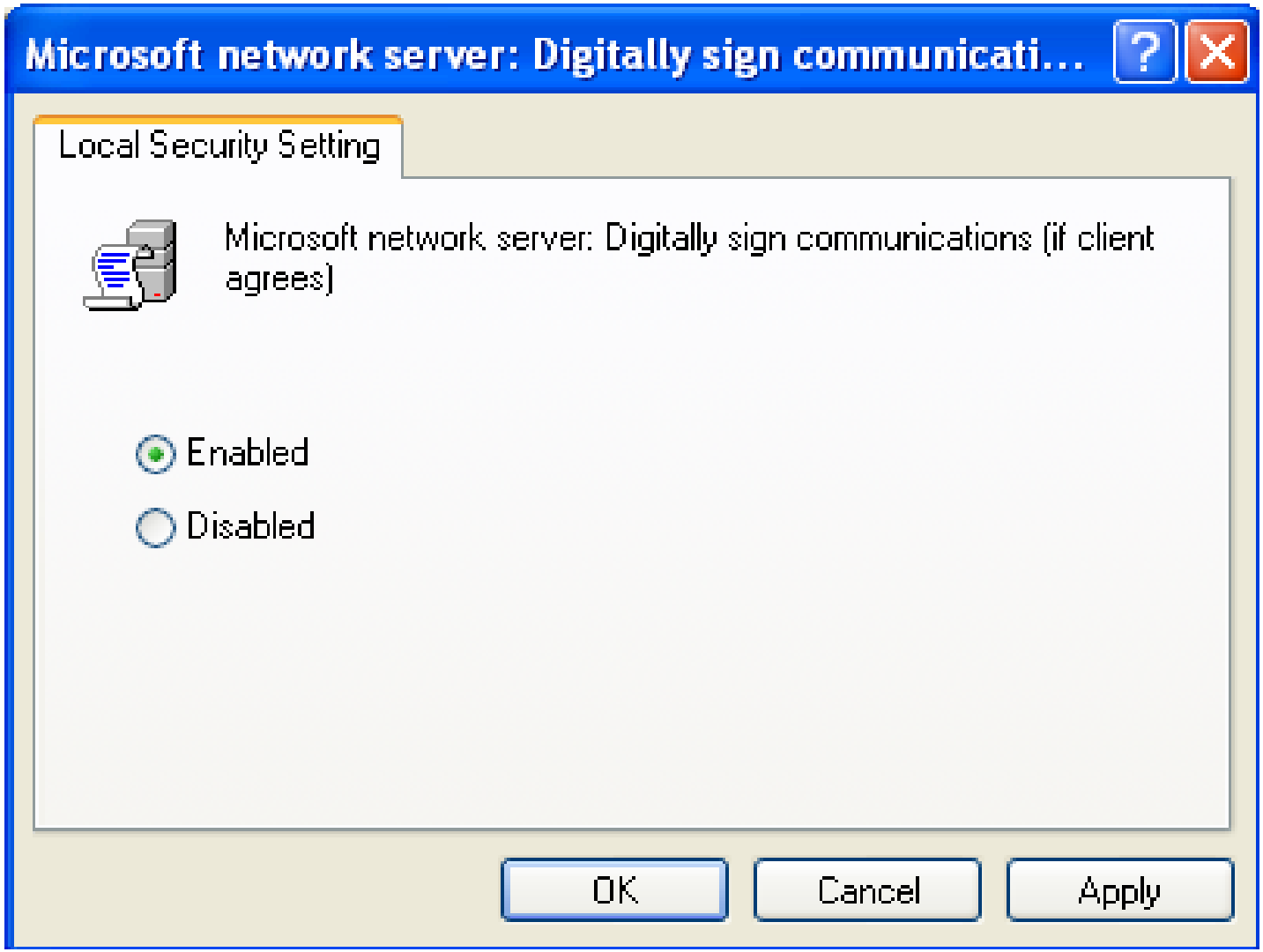
Microsoft Network Client and Server: Digitally Sign Communications (Four Related Settings)



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Client and Server: Digitally Sign Communications (Four Related Settings)



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Client: Send Unencrypted Password to Third-party SMB Servers

This policy allows the SMB redirector to send plaintext passwords to non-Microsoft SMB servers which doesn't support password encryption during authentication

The values for the **Microsoft network client: Send unencrypted password to third-party SMB servers** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Client: Send Unencrypted Password to Third-party SMB Servers

Vulnerability

- By enabling this policy the server can transmit passwords in plaintext across the network to other computers that offer SMB services

Countermeasure

- Configure the policy setting to **Disabled**

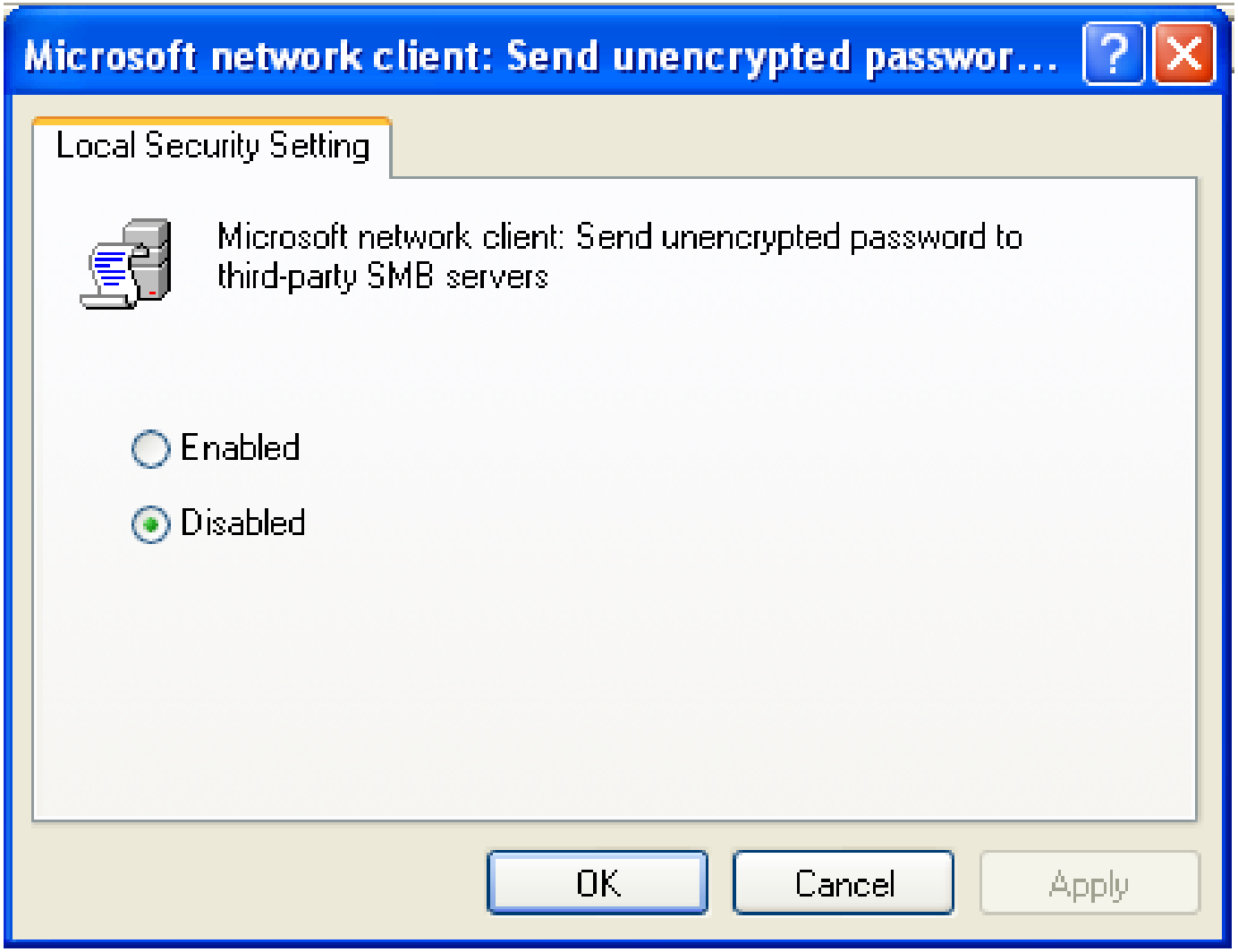
Potential Impact

- MS-DOS, Windows for Workgroups 3.11, and Windows 95a may not communicate through SMB protocol.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Client: Send Unencrypted Password to Third-party SMB Servers



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Server: Amount of Idle Time Required before Suspending Session

This policy sets the amount of idle time that must pass in an SMB session to suspend the session

The values for this policy are:

- Minimum – **0**
- Maximum – **99999** (208 days)

The values for the **Microsoft network server: Amount of idle time required before suspending session** setting is:

- User-defined period of time in minutes
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

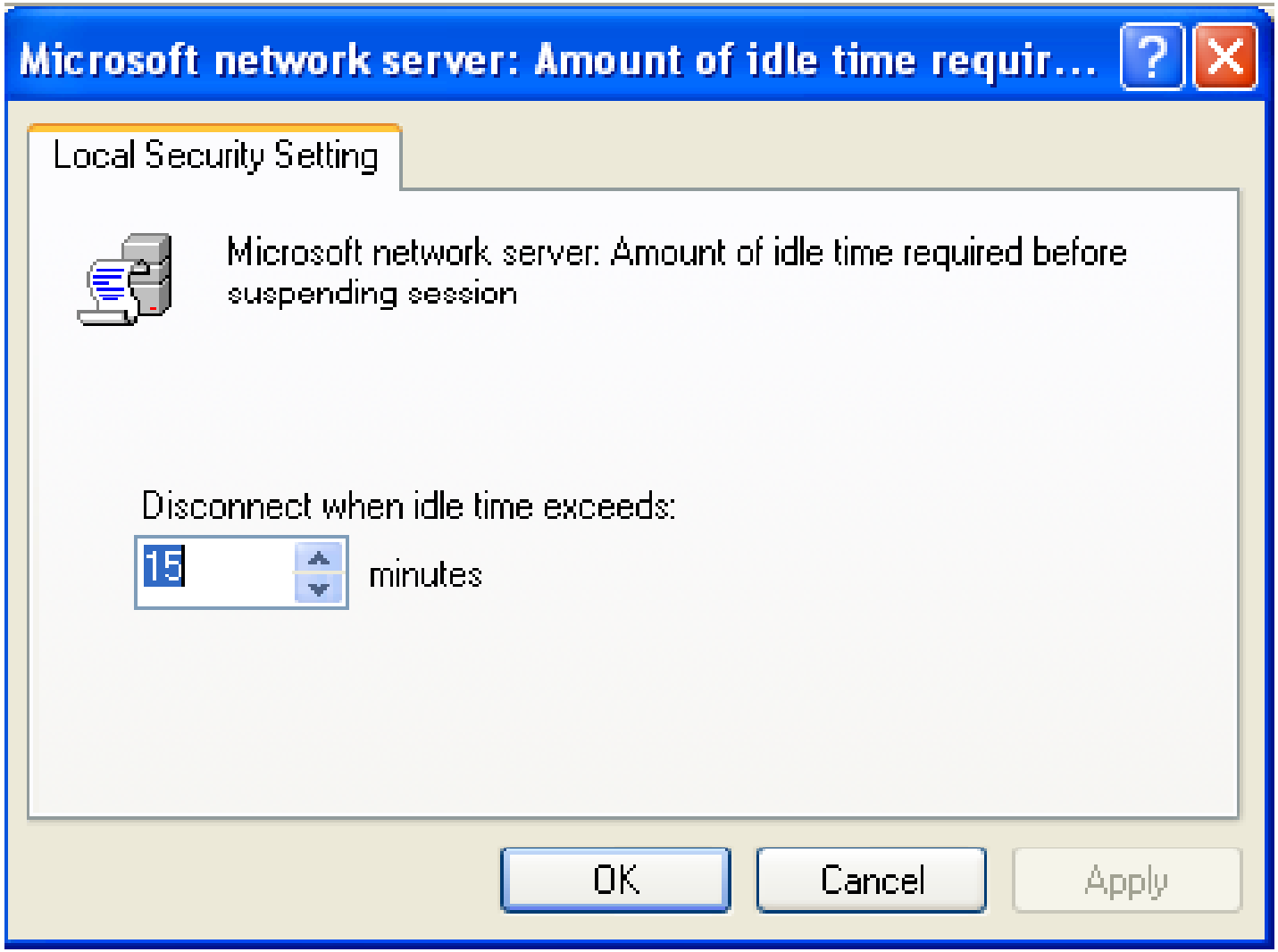
Microsoft Network Server: Amount of Idle Time Required before Suspending Session

Vulnerability	• Each SMB session consumes server resources, and frequent null sessions can slow down or fail the server • An attacker can fill the server with null sessions and affect performance
Countermeasure	• Configure this value to 15 minutes
Potential Impact	• This has a little impact as if the client recommence activity SMB session will be reestablished

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Server: Amount of Idle Time Required before Suspending Session



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Server: Disconnect Clients when Logon Hours Expire

This policy decides whether or not to disconnect users who are connected to the local computer outside their user account's valid logon hours

If this policy is enabled, a client session is disconnected as soon as client logon hours expire

Network security: Force logoff when logon hours expire should be enabled if this policy is enabled

The values for the **Microsoft network server: Disconnect clients when logon hours expire** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Server: Disconnect Clients when Logon Hours Expire

Vulnerability

- If logon hours are decided for the user then enable this policy setting

Countermeasure

- **Enable** this policy setting

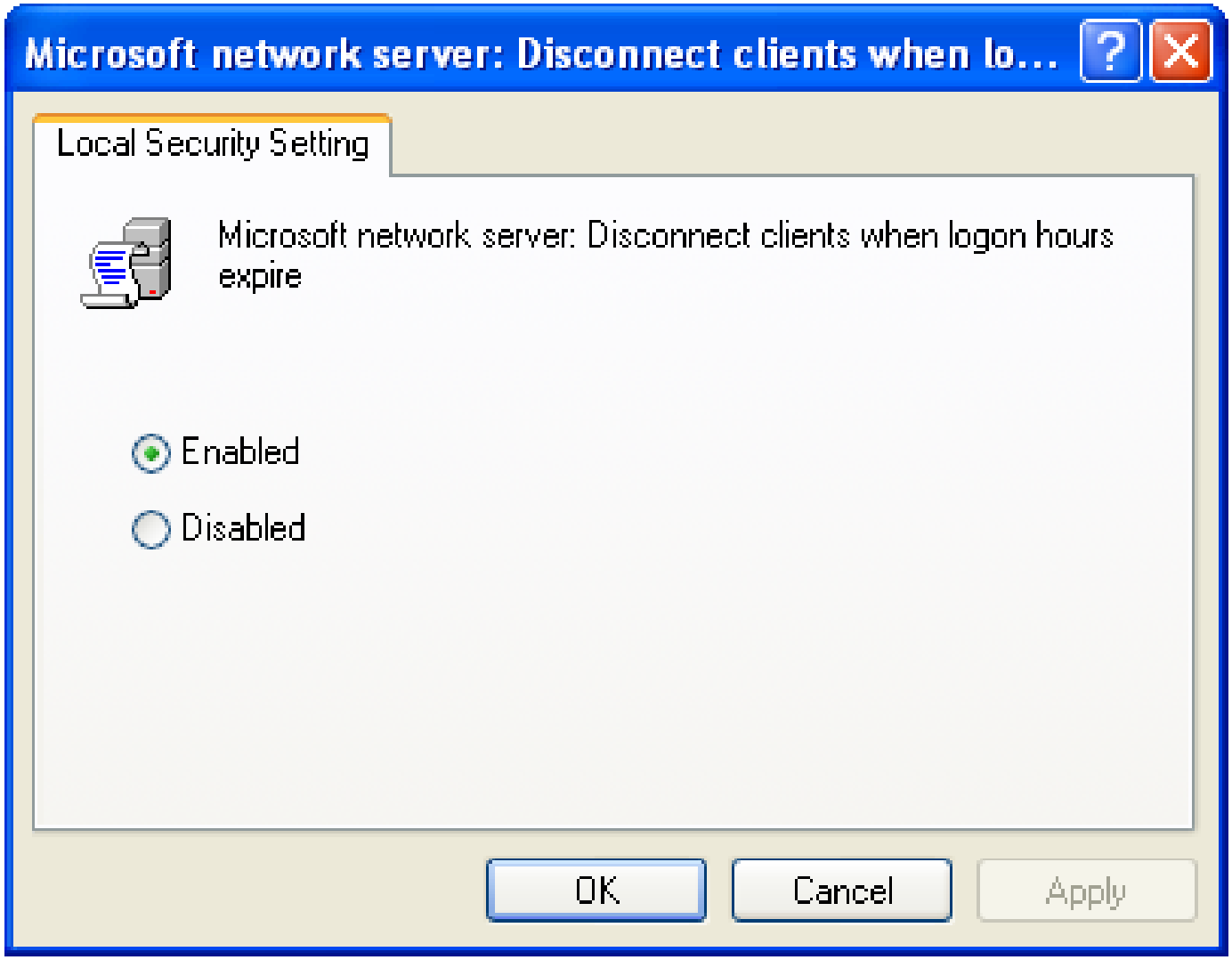
Potential Impact

- If logon hours are availed the client session will forcibly be stopped

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Network Server: Disconnect Clients when Logon Hours Expire



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Allow Anonymous SID/Name Translation

This policy decides that an anonymous user can request SID attributes for another user or not

The values for the **Network access: Allow anonymous SID/Name translation** setting is:

- Enabled
- Disabled
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Allow Anonymous SID/Name Translation

Vulnerability

- By enabling this policy, a local access user can learn the real name of the administrator account with the SID

Countermeasure

- **Disable** this policy setting

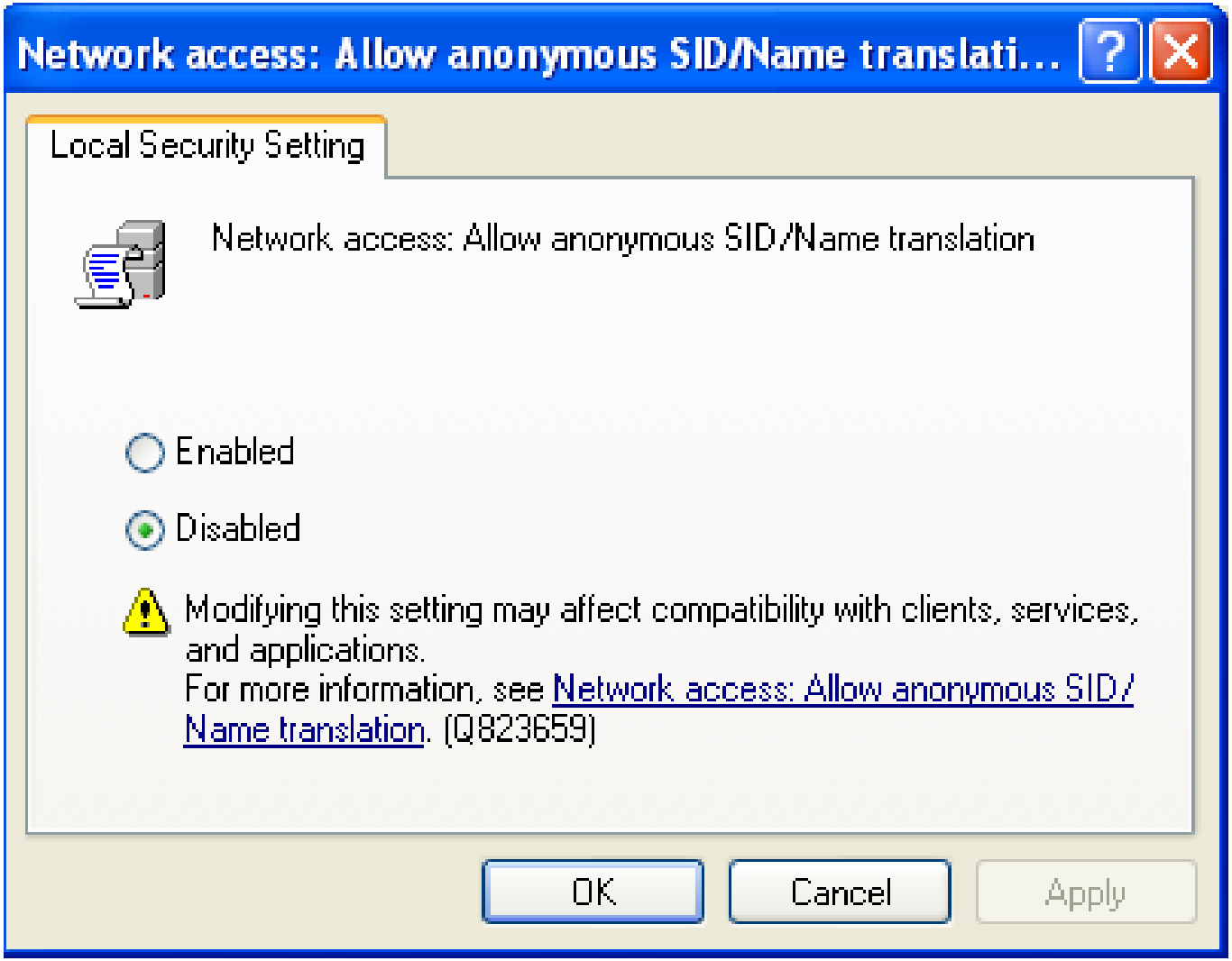
Potential Impact

- **Member machine** – This policy is **Disabled.**
- **Domain controller** – This policy is **Enabled.**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Allow Anonymous SID/Name Translation



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts

This policy determines the additional permissions given to the anonymous connections to the computer

Windows allows anonymous users to perform certain activities

The values for the **Network access: Do not allow anonymous enumeration of SAM accounts** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

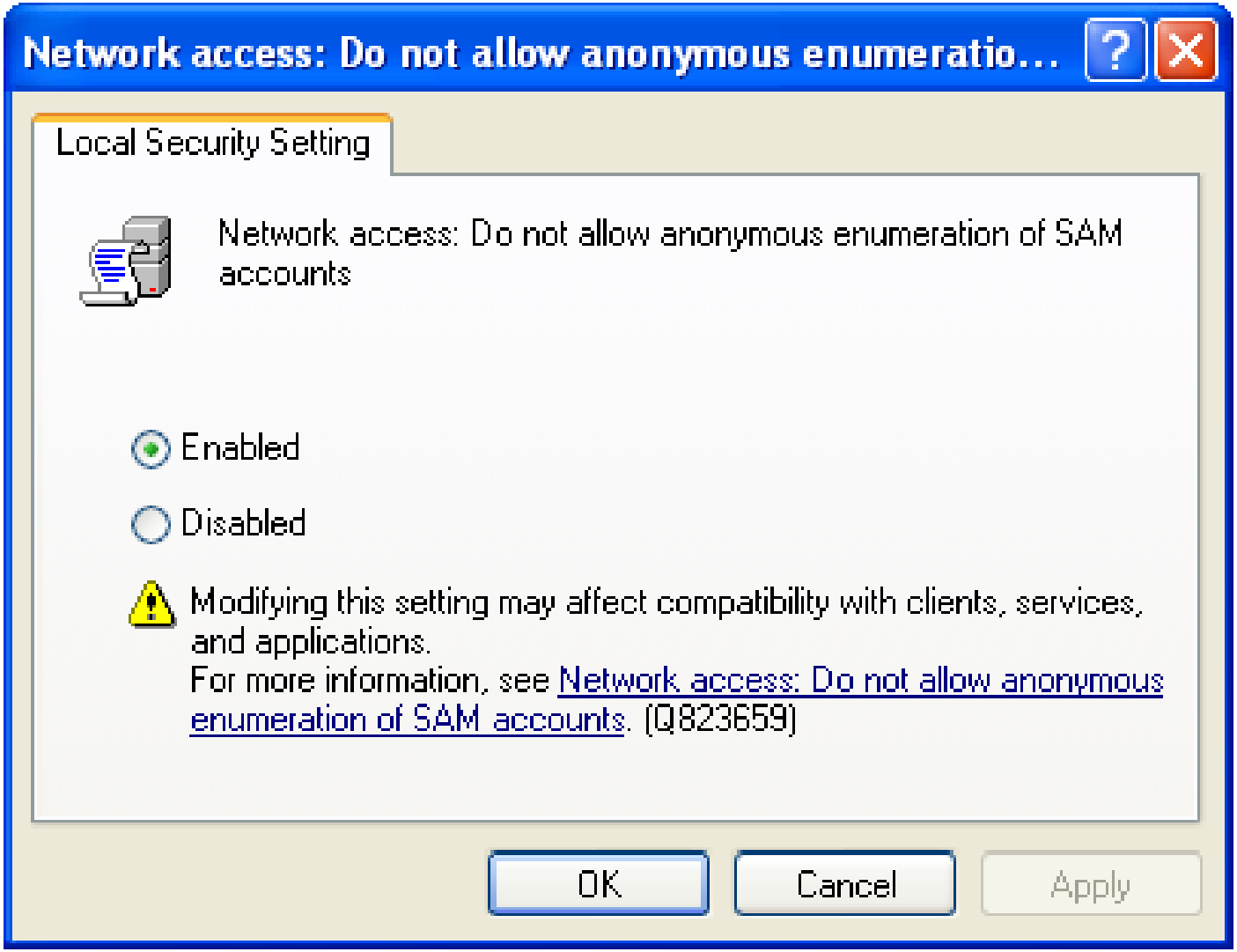
Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts

Vulnerability	• An unauthorized user can find the account names and implement social engineering methods to guess password
Countermeasure	• **Enable** this policy setting
Potential Impact	• It will be impossible to establish trusts with Windows NT 4.0–based domains. As client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts And Shares

This policy finds whether unidentified enumeration of Security Accounts Manager (SAM) accounts and shares is allowed

By enabling this policy, you cannot allow anonymous enumeration of SAM accounts and shares

The values for the Network access: Do not allow anonymous enumeration of SAM accounts and shares setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts And Shares

Vulnerability

- An unauthorized user can make a list of account names and use the information to guess password or perform social engineering attacks

Countermeasure

- Configure this policy setting to **Enabled**

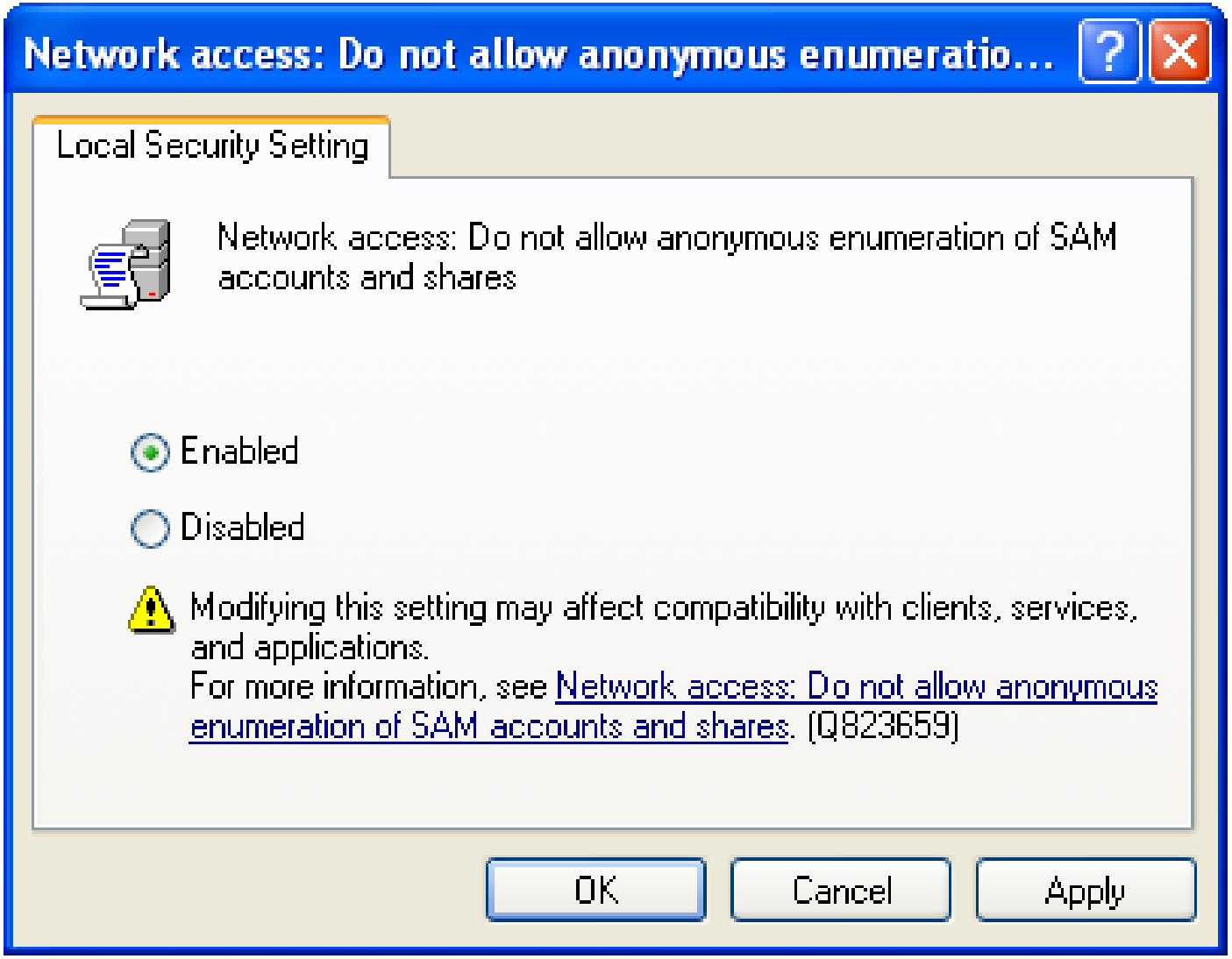
Potential Impact

- Granting access to users of another domain is not possible as administrators can not list the accounts on the other domain
- Users should authenticate before accessing the lists of shared folders and printers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts And Shares



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

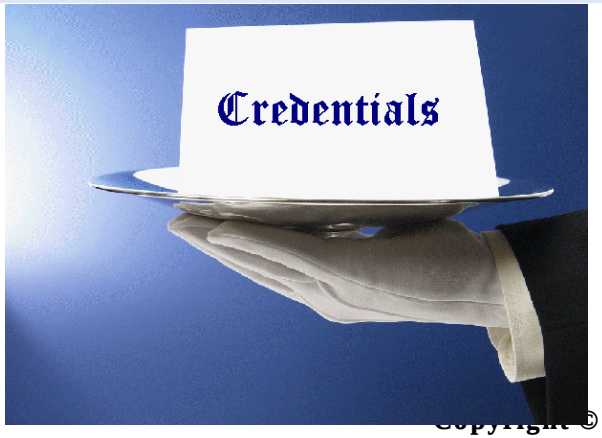
Network Access: Do Not Allow Storage of Credentials or .NET Passports for Network Authentication

This policy decides that the stored User Name and Passwords should be stored for the later use or not

By enabling the policy, the Stored User Names and Passwords feature of Windows does not store passwords and credentials

The values for the **Network access: Do not allow storage of credentials or.NET Passports for network authentication** setting are:

- Enabled
- Disabled
- Not Defined



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Do Not Allow Storage of Credentials or .NET Passports for Network Authentication

Vulnerability

- The cached passwords can be accessed by the user when he logs on to the computer

Countermeasure

- Configure the policy to **Enabled**

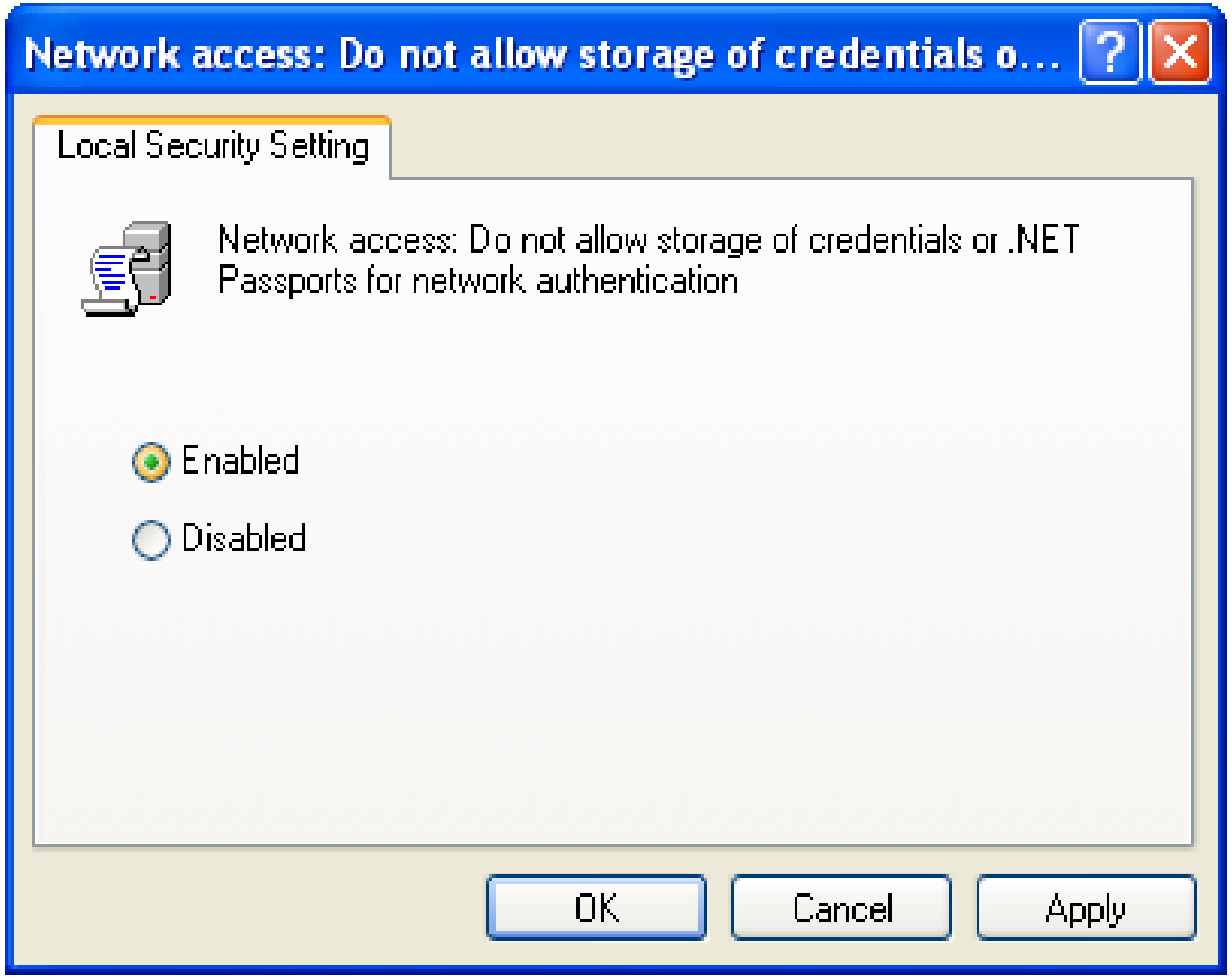
Potential Impact

- Users with no access to the network resources are always prompted for the password
- This policy setting should have no impact on user who can access with there Active Directory–based domain account

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Do Not Allow Storage of Credentials or .NET Passports for Network Authentication



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Let Everyone Permissions Apply to Anonymous Users

By this policy, the additional permissions given to anonymous connections to the computer are determined

By default, the token created for the anonymous connections does not include the Everyone SID

Permissions given to the **Everyone** group do not apply to anonymous users

The values for the Network access: Let Everyone permissions apply to anonymous users setting are:

- **Enabled**
- **Disabled**
- **Not Defined**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Let Everyone Permissions Apply to Anonymous Users

Vulnerability

- An unauthorized can list account names and use the information to attempt to guess password, perform social engineering attacks, or launch DoS attacks

Countermeasure

- Configure this policy setting to **Disabled**

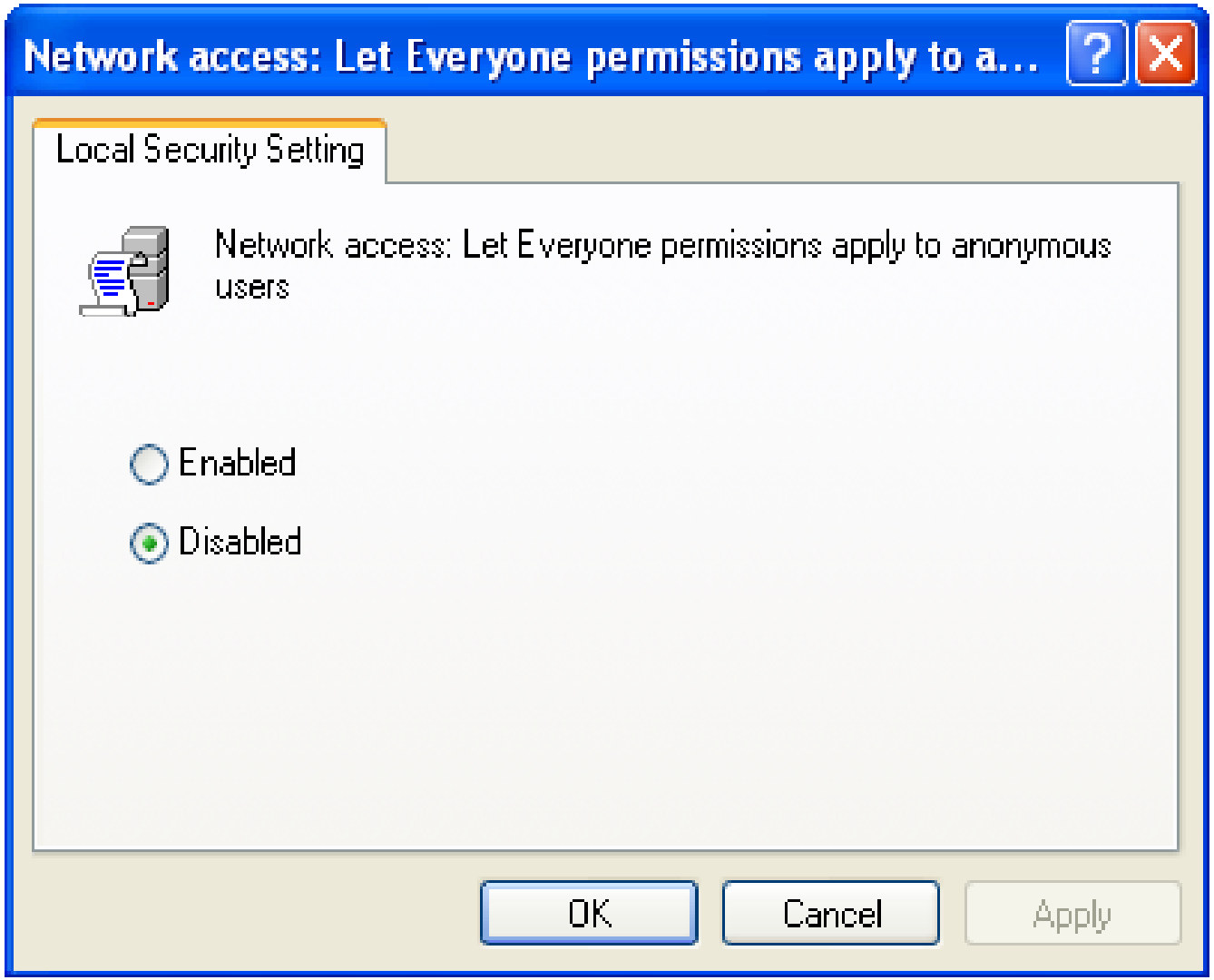
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Let Everyone Permissions Apply To Anonymous Users



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Named Pipes that can be Accessed Anonymously

This policy concludes which communication sessions, or pipes, will have attributes and permissions that allow anonymous access

The values for the **Network access: Named Pipes that can be accessed anonymously** setting are:

- A user-defined list of shares
- Not Defined

Enable the **Network access: Restrict anonymous access to named pipes and shares** setting for this policy setting to take affect

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Named Pipes that can be Accessed Anonymously

Vulnerability

- Access can be restricted to pipes as COMNAP and LOCATOR to help in preventing unauthorized access to the network
- **Default Named Pipes That Are Accessible Anonymously**

Named pipe	Purpose
COMNAP	SNABase named pipe. Systems Network Architecture (SNA) is a collection of network protocols that were originally developed for IBM mainframe computers.
COMNODE	SNA Server named pipe.
SQL\QUERY	Default named pipe for SQL Server.
SPOOLSS	Named pipe for the Print Spooler service.
EPMAPPER	End Point Mapper named pipe.
LOCATOR	Remote Procedure Call Locator service named pipe.
TrkWks	Distributed Link Tracking Client named pipe.
TrkSvr	Distributed Link Tracking Server named pipe.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Named Pipes that can be Accessed Anonymously

Countermeasure

- Configure this policy setting to a null value (enable the setting but do not enter named pipes in the text box)

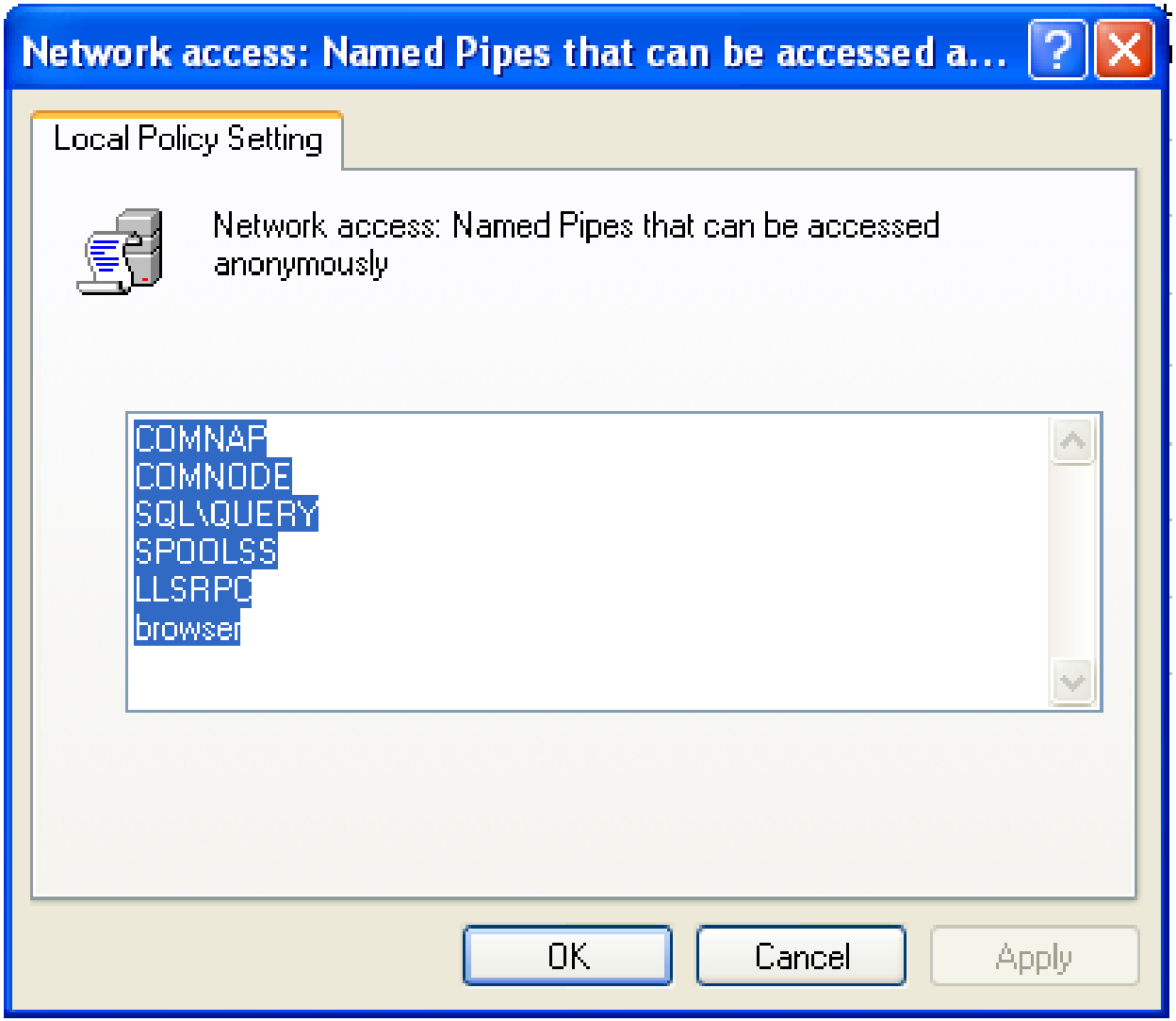
Potential Impact

- On configuring this policy the null session access over named pipes will be disabled
- Applications relaying on unauthenticated access to named pipes will no longer function

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Named Pipes that can be Accessed Anonymously



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Remotely Accessible Registry Paths

This policy helps to decide which paths will be accessible when an application or process references the **WinReg** key to determine access permissions

The values for the **Network access: Remotely accessible registry paths** setting are:

- A user-defined list of paths
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

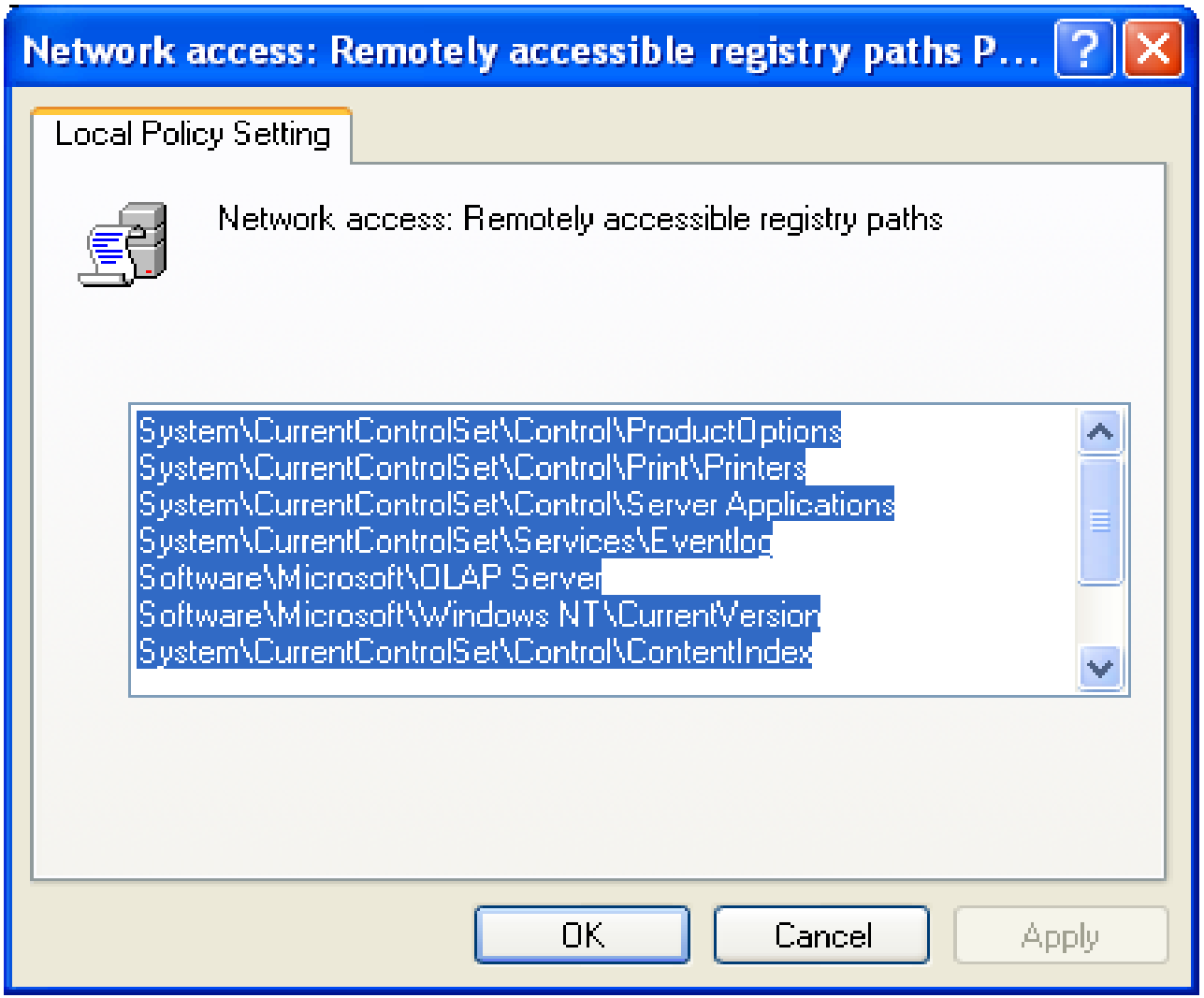
Network Access: Remotely Accessible Registry Paths

Vulnerability	• An attacker can use the information in a registry (holds computer configuration information) for unauthorized activities • To protect the registry from unauthorized access ACLs are assigned
Countermeasure	• Configure this policy setting to a null value (enable the setting but do not enter any paths in the text box)
Potential Impact	• Remote management tools as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server, require remote access to the registry to properly monitor and manage those computers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Remotely Accessible Registry Paths



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Remotely Accessible Registry Paths and Sub-paths

This policy gets the registry path and sub-path to be accessible when an application or process references the **WinReg** key

The values for the Network access: Remotely accessible registry paths and sub-paths setting are:

- A user-defined list of paths
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Remotely Accessible Registry Paths and Sub-paths

Vulnerability

- The default ACL of the registry will restrict unauthorized access and protect its access, it reduces the risk of attack

Countermeasure

- Configure this policy setting to a null value (enable the setting but do not enter any paths in the text box)

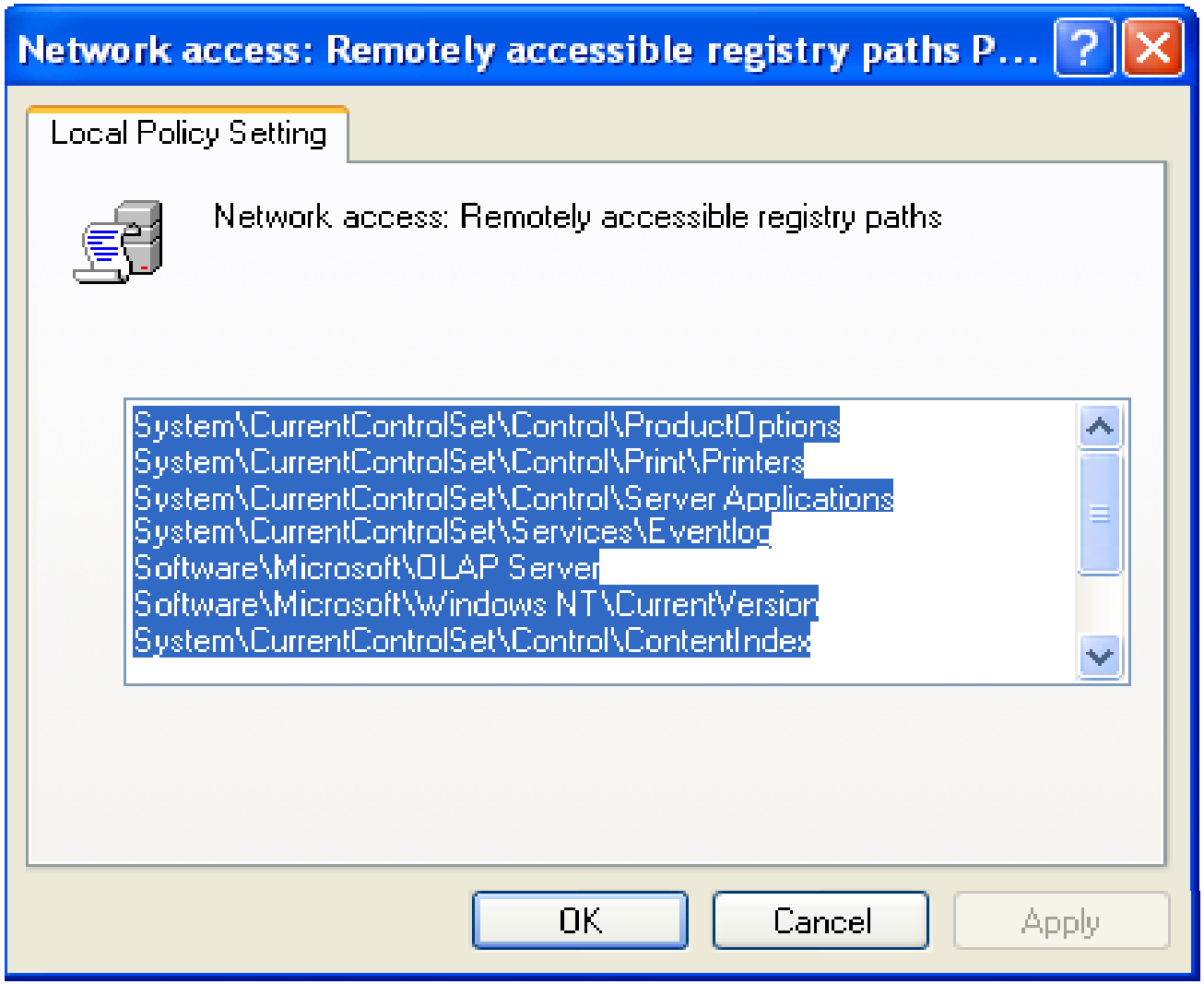
Potential Impact

- If the default registry paths are removed the Remote management tools like the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server may fail

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Remotely Accessible Registry Paths and Sub-paths



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Restrict Anonymous Access to Named Pipes and Shares

If this policy is enabled, only those files (shares and pipes) are accessed which are named in **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously** settings

With a value of 1 to **RestrictNullSessAccess** you can restrict null session access

The values for the Network access: Restrict anonymous access to Named Pipes and Shares setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Restrict Anonymous Access to Named Pipes and Shares

Vulnerability	• Null sessions can be exploited through shares on the computers
Countermeasure	• Configure this policy setting to **Enabled**
Potential Impact	• By enabling this policy null sessions are restricted for unauthorized access to all server pipes and shares except the names listed in **NullSessionPipes** and **NullSessionShares** entries

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Shares that can be Accessed Anonymously

This policy lists the network shares those can be accessed by anonymous users

The values for the **Network access: Shares that can be accessed anonymously** setting are:

- A user-defined list of shares
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Shares that can be Accessed Anonymously

Vulnerability

- Any share can be accessed by a user on that network. Sensitive information can be revealed

Countermeasure

- Configure the policy setting to a null value

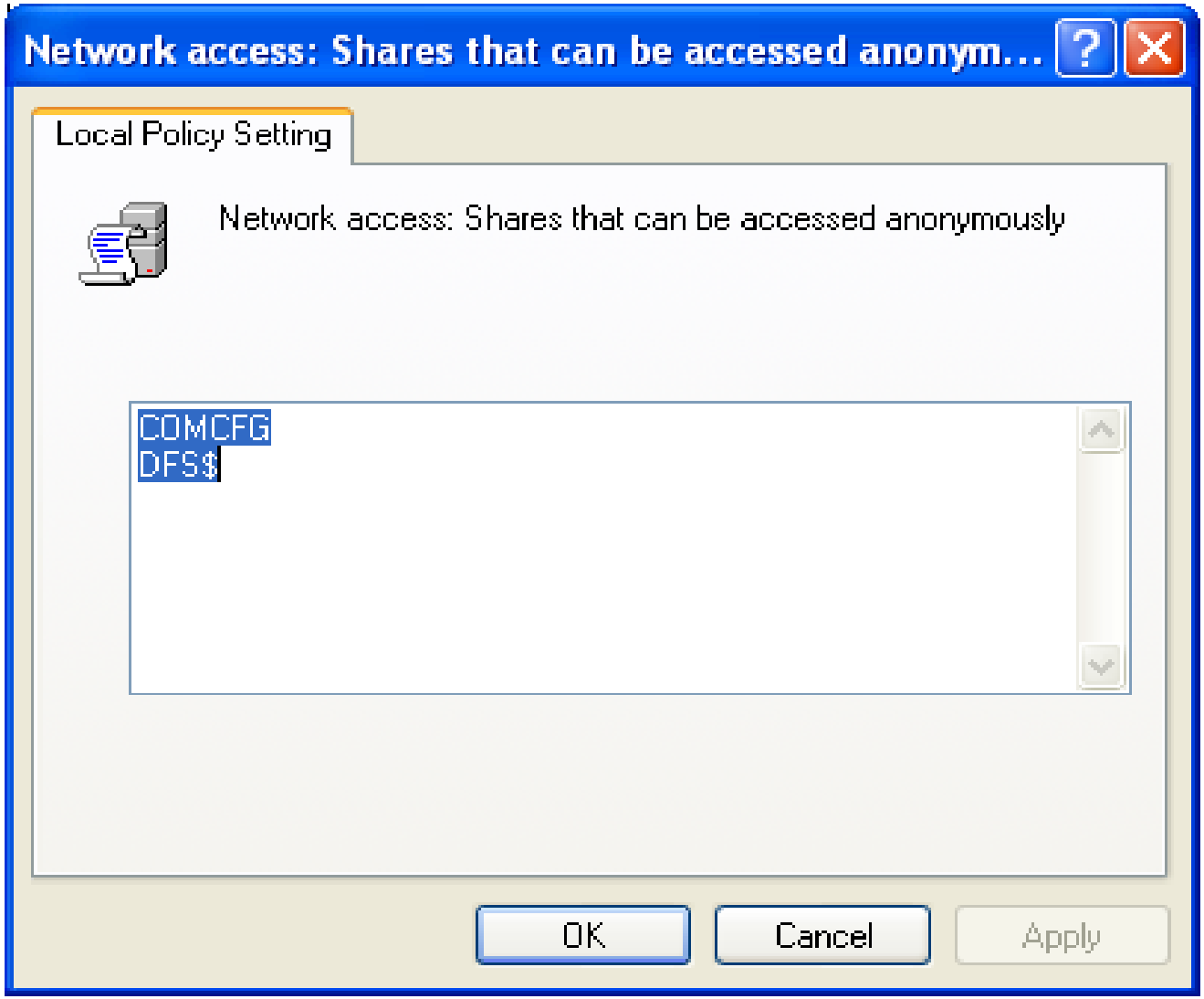
Potential Impact

- A little impact can be present as it is the default configuration, only authorized users can access to shared resources

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Shares that can be Accessed Anonymously



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Sharing and Security Model for Local Accounts

This policy shows how network logons that use local accounts are authenticated

If the policy is configured to:

- **Classic**
  - Network logons authenticate with those credentials
  - Provides precise control over access to resources
  - Default configuration for Windows XP Professional
- **Guest only**
  - Network logons are automatically mapped to the Guest account.
  - This account receives the same level of access to a resource
  - Default configuration for Windows XP computers joined to a domain and Windows Server 2003 computers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Sharing and Security Model for Local Accounts

This setting has no effect on Windows 2000 computers.

The values for the **Network access: Sharing and security model for local accounts** setting are:

- Classic. Local users authenticate as themselves.
- Guest only. Local users authenticate as Guest.
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Sharing and Security Model for Local Accounts

Vulnerability	• With Guest account privileges the data is more secured as the shared resources cannot be accessed by the unauthorized users • With classic privileges the files are accessed by only authorized users with a password
Countermeasure	• Configure the **Network access: Sharing and security model for local accounts** setting to **Classic – local users authenticate as themselves** • On end-user computers, configure this policy setting to **Guest only – local users authenticate as guest**
Potential Impact	• None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Access: Sharing and Security Model for Local Accounts

EC-Council

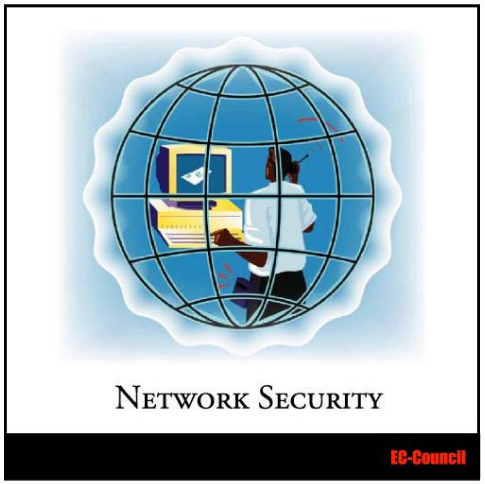
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: Do Not Store LAN Manager Hash Value on Next Password Change

This policy decides on storing hash values for the new password (when changed) by the LAN manager

The values for the **Network security: Do not store LAN Manager hash value on next password change** setting are:

- Enabled
- Disabled
- Not Defined



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: Do Not Store LAN Manager Hash Value on Next Password Change

Vulnerability

- If this policy setting is enabled, attackers cannot succeed in accessing in SAM file for username and password hashes

Countermeasure

- Configure this policy setting to **Enabled**
- This makes it necessary for the users to change the password when they next login as to remove the hashes

Potential Impact

- Some Third-party vendors and some operating systems as Windows 95, Windows 98, and Windows ME may fail

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: Do Not Store LAN Manager Hash Value on Next Password Change

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: Force Logoff when Logon Hours Expire

This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. It affects the SMB component

If you enable this policy setting, client sessions with the SMB server will be disconnected when the client's logon hours expire

If you disable this policy setting, established client sessions will be maintained after the client's logon hours expire

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: Force Logoff when Logon Hours Expire

This policy decides on disconnecting the user connected out side his logon hours

- **Enable** – Disconnects the session when client logged on out side the login hours
- **Disable** – Maintains the session even the client is exceeds his login hours

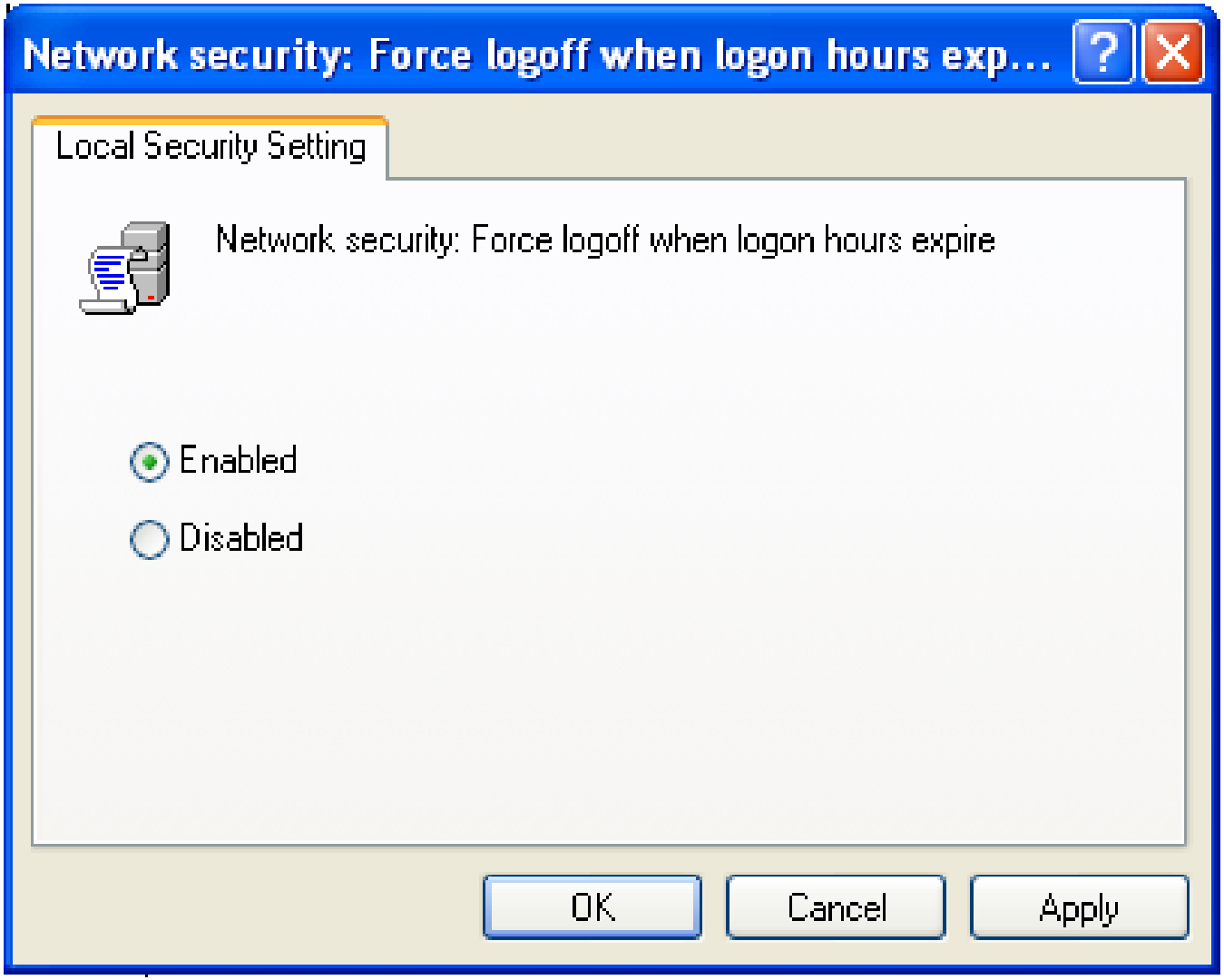
The values for the **Network security: Force logoff when logon hours expire** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: Force Logoff when Logon Hours Expire



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LAN Manager Authentication Level

LAN Manager (LM) is a member of Microsoft client/server software's

LM allows users to connect personnel computers with each other on a single network

In Active Directory domains, the Kerberos protocol is the default authentication protocol, if it is not negotiated LM, NTLM, or NTLMv2 will be used by Active Directory

LAN Manager authentication includes the) variants

LM, NTLM, and NTLMv2 authentication's are used to do the following operations:

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LAN Manager Authentication Level

- Join a domain
- Authenticate between Active Directory forests
- Authenticate to down-level domains
- Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP)
- Authenticate to computers that are not in the domain

The values for the Network security: LAN Manager authentication level setting are:

- Send LM & NTLM responses
- Send LM & NTLM — use NTLMv2 session security if negotiated

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LAN Manager Authentication Level

- Send NTLM responses only
- Send NTLMv2 responses only
- Send NTLMv2 responses only\refuse LM
- Send NTLMv2 responses only\refuse LM & NTLM
- Not Defined

The policy setting finds the challenge/response authentication protocol is used for network logons.

The session security level that the computers negotiate as follows:

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LAN Manager Authentication Level

Send LM & NTLM responses. Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication

Send LM & NTLM – use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication

Send NTLM response only. Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LAN Manager Authentication Level

Send NTLMv2 response only. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.

Send NTLMv2 response only\refuse LM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).

Send NTLMv2 response only\refuse LM & NTLM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM (accept only NTLMv2 authentication).

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LAN Manager Authentication Level

Level 0

- **Send LM and NTLM response; never use NTLMv2 session security**. Clients use LM and NTLM authentication, and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication

Level 1

- **Use NTLMv2 session security if negotiated**. Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication

Level 2

- **Send NTLM response only**. Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LAN Manager Authentication Level

Level 3

- **Send NTLMv2 response only**. Clients use NTLMv2 authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication

Level 4

- **Domain controllers refuse LM responses**. Clients use NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers refuse LM authentication, that is, they accept NTLM and NTLMv2

Level 5

- **Domain controllers refuse LM and NTLM responses (accept only NTLMv2)**. Clients use NTLMv2 authentication, use and NTLMv2 session security if the server supports it. Domain controllers refuse NTLM and LM authentication (they accept only NTLMv2)

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LAN Manager Authentication Level

Vulnerability

- Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 9x clients only send LM)
- The response sent by LM is the weakest form of authentication response sent on the network, which will provide3 a way to the attackers to sniff the traffic for user passwords

Countermeasure

- Configure the policy setting to **Send NTLMv2 responses only**

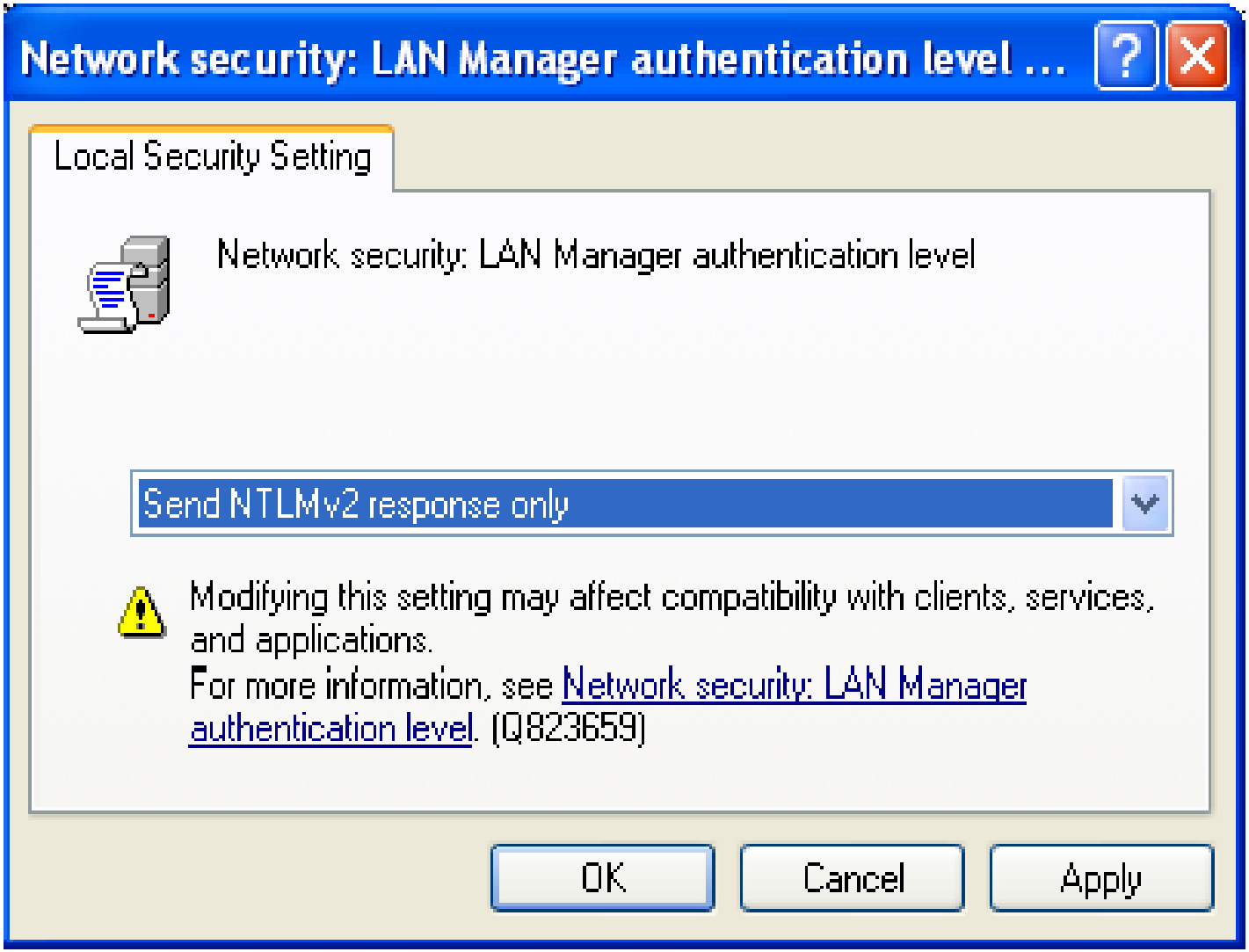
Potential Impact

- If NTLMv2 authentication is not supported the client can not access domain resources by using LM and NTLM.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LAN Manager Authentication Level



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LDAP Client Signing Requirements

The level of data signing requested is decided by the policy representing the client, who makes LDAP BIND request. As follows:

None. Request is carried with the caller-specified options.

Negotiate signing

- The LDAP BIND request is initiated with the LDAP data signing option, if Transport Layer Security/Secure Sockets Layer (TLS/SSL) has not been started
- If TLS/SSL has been started, the LDAP BIND request is initiated with the caller-specified options

Require signature. If the LDAP server's intermediate saslBindInProgress response does not indicate that LDAP traffic signing is required, request command will be failed

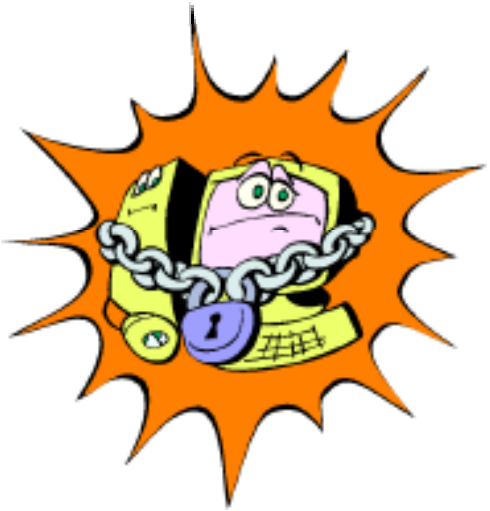
EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LDAP Client Signing Requirements

The values for the **Network security: LDAP client signing requirements** setting are:

- None
- Negotiate signing
- Require signature
- Not Defined



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LDAP Client Signing Requirements

Vulnerability

- In an LADP server an attacker can act as a man-in-middle and captures the packets between the server and client and try to modify it and forwards wrong data to the receiver
- A strong physical security measures can protect the network infrastructure

Countermeasure

- Configure the policy setting to **Require signature**.

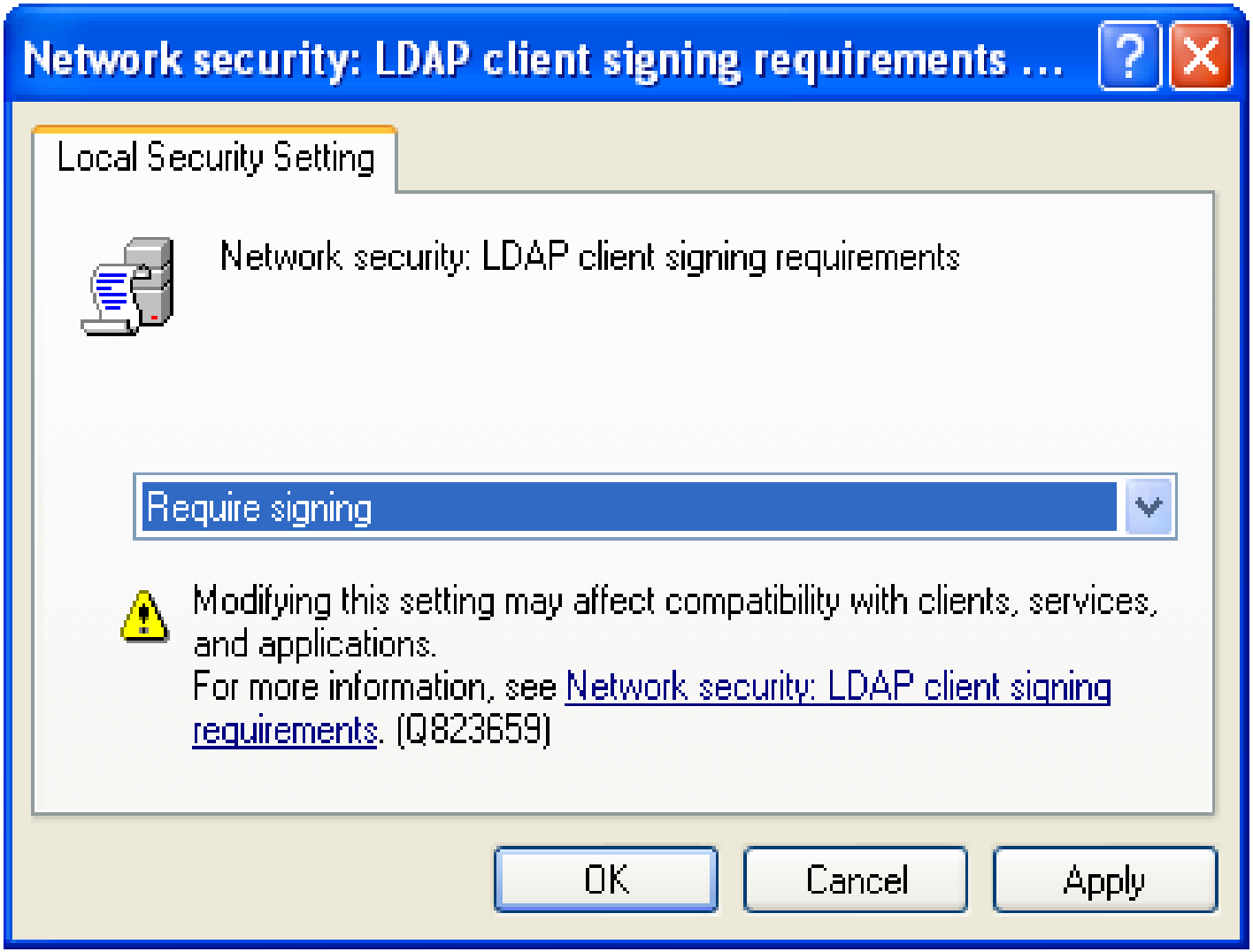
Potential Impact

- If server is configured to LDAP signature, the client should also be configured as to communicate with the server

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: LDAP Client Signing Requirements



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: Minimum Session Security for NTLM SSP based (Including Secure RPC) Clients/Servers

By this setting a client require the negotiation of message encryption, integrity 128-bit encryption or NTLMv2 session security. This policy values are dependent on **LAN Manager Authentication Level** policy setting values

The values for the **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients** setting are:

- **Require message confidentiality**. If no negotiation is done the connection will fail.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: Minimum Session Security for NTLM SSP based (Including Secure RPC) Clients

Require message integrity. Lack of message integrity will fail the connection, which is assessed through message signing

Require 128-bit encryption. If 128-bit strong encryption is not negotiated the connection will fail

Require NTLMv2 session security. If the NTLMv2 protocol is not negotiated the connection will fail

Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: Minimum Session Security for NTLM SSP based (Including Secure RPC) Clients

Vulnerability

- Enable all the options for this setting

Countermeasure

- Enable all four options that are available for the policy setting

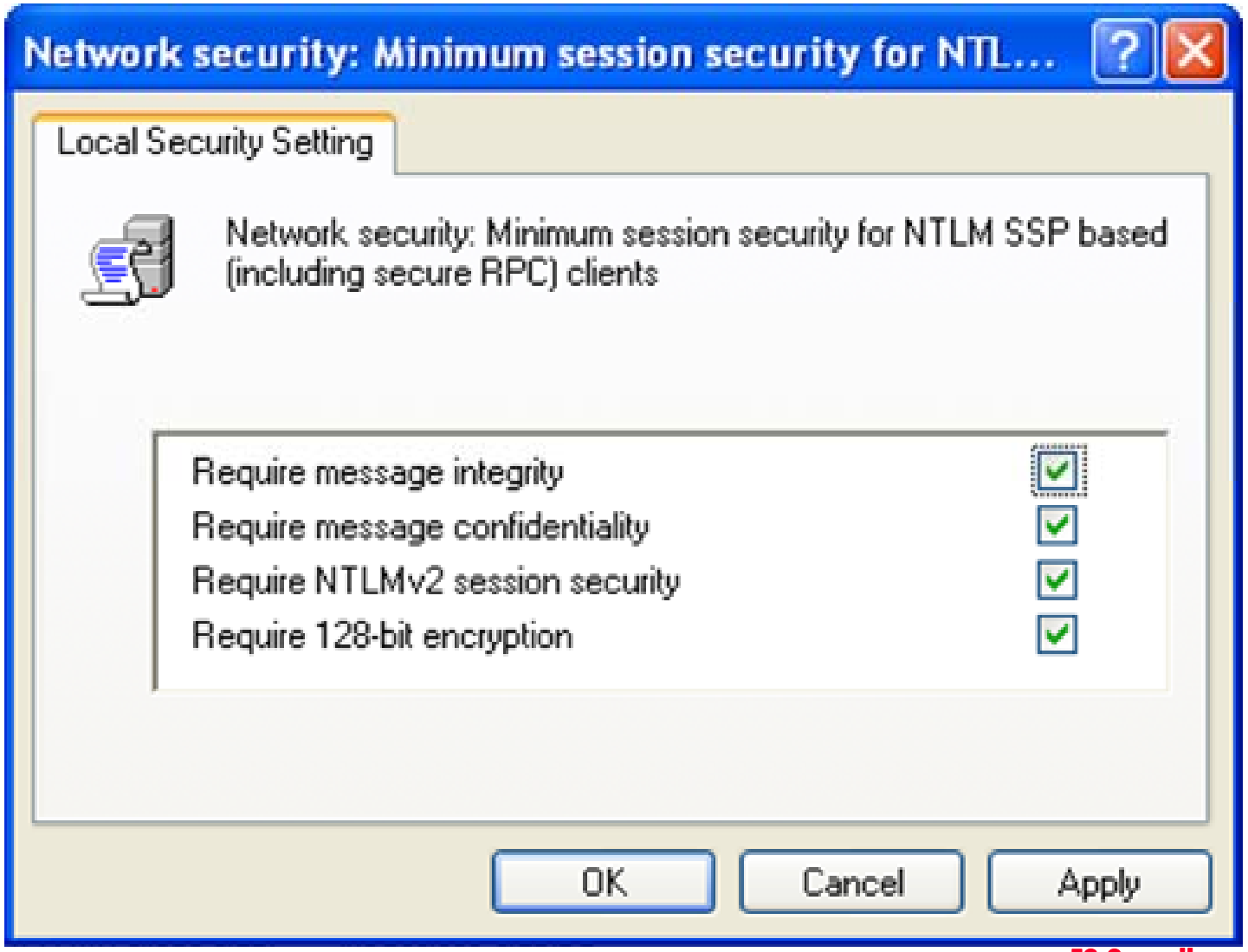
Potential Impact

- Client computers with old servers can not support these settings

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Security: Minimum Session Security for NTLM SSP based (Including Secure RPC) Clients



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Recovery Console: Allow Automatic Administrative Logon

This policy decides whether the administrator password has to be given before granting permission to the computer

Enable – No password is necessary for to logon to the administrator account at the recovery console

The values for the Recovery console: Allow automatic administrative logon setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Recovery Console: Allow Automatic Administrative Logon

Vulnerability

- The recovery console is helpful for troubleshooting and repairing computers. It is even unsafe to automatically logon to the console, as any one can walk on to the console and logon to it

Countermeasure

- Configure this policy setting to **Disabled**

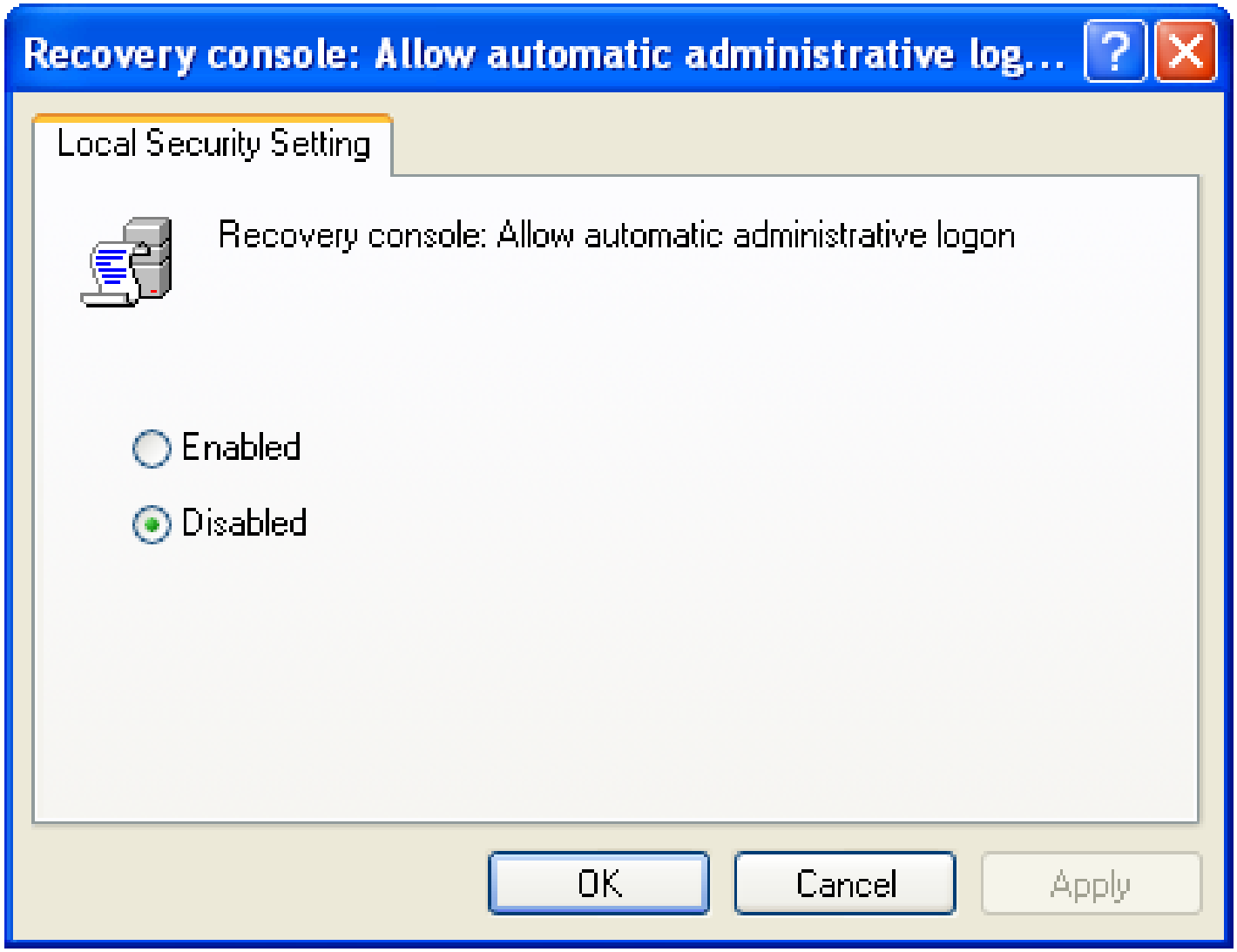
Potential Impact

- The Recovery Console needs a user name and password

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Recovery Console: Allow Automatic Administrative Logon



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Recovery Console: Allow Floppy Copy and Access to all Drives and all Folders

Recovery Console SET command, which sets the recovery console variables is made available when this policy is enabled.

- **AllowWildCards**. Enables wildcard support for some commands (such as the DEL command)
- **AllowAllPaths**. Allows access to all files and folders on the computer
- **AllowRemovableMedia**. Allows files to be copied to removable media, such as a floppy disk
- **NoCopyPrompt**. Suppresses the prompt that typically displays before an existing file is overwritten

The values for the **Recovery console: Allow floppy copy and access to all drives and all folders** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Recovery Console: Allow Floppy Copy and Access to all Drives and all Folders

Vulnerability

- If an attacker is able to re-start the server in Recovery Console mode he can access private data and can clear the audit log

Countermeasure

- Configure this policy setting to **Disabled**

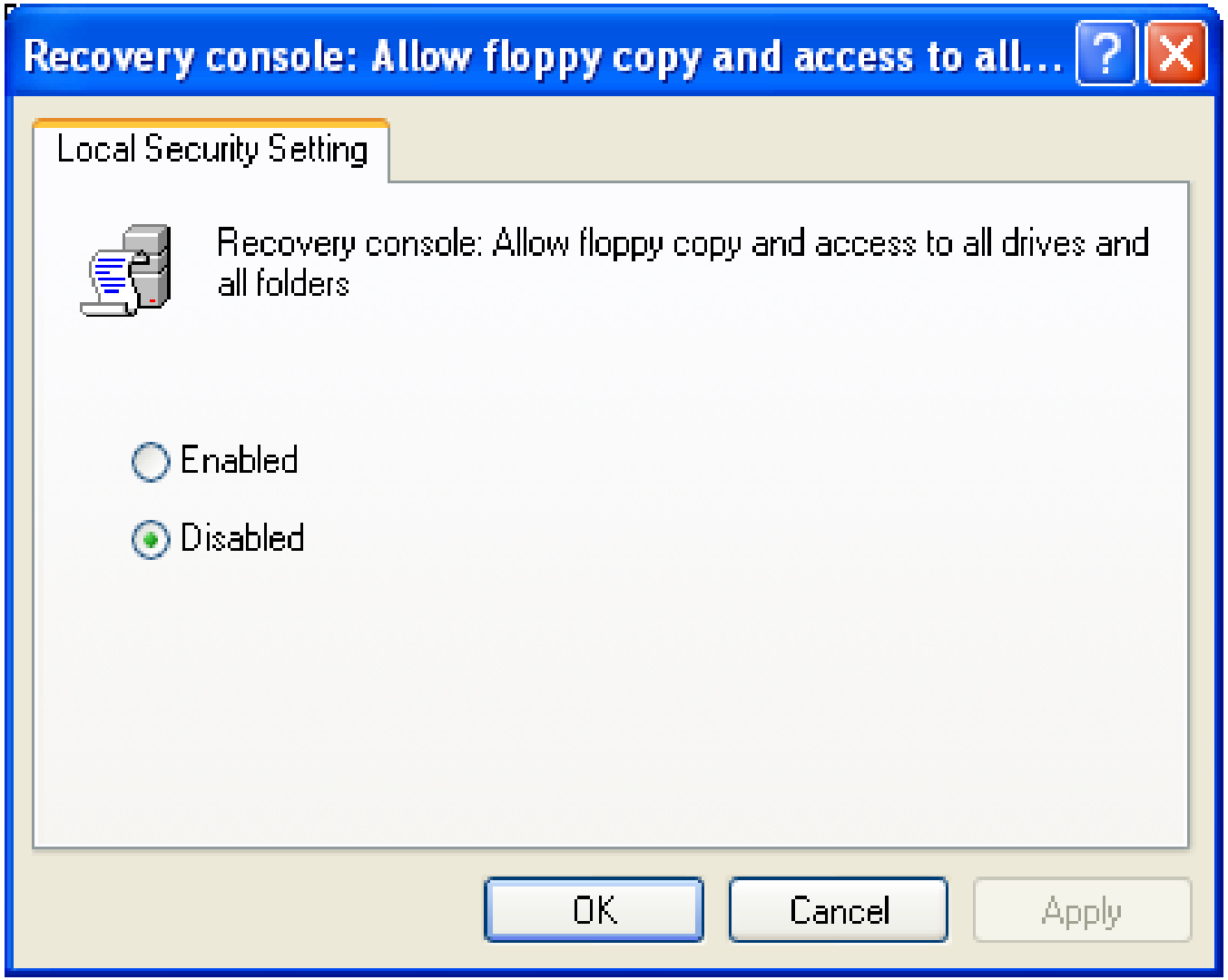
Potential Impact

- Any personnel able to logon to Recovery Console will be able to copy the data

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Recovery Console: Allow Floppy Copy and Access to all Drives and all Folders



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shutdown: Allow System to be Shut Down Without Having to Log On

This policy decides whether the computer can shut down with out logging to windows.

- Enable – The **Shut Down** command is available on the Windows logon screen
- Disable – The **Shut Down** option is removed from the Windows logon screen

The values for the **Shutdown: Allow system to be shut down without having to log on** setting are:

- Enabled
- Disabled
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

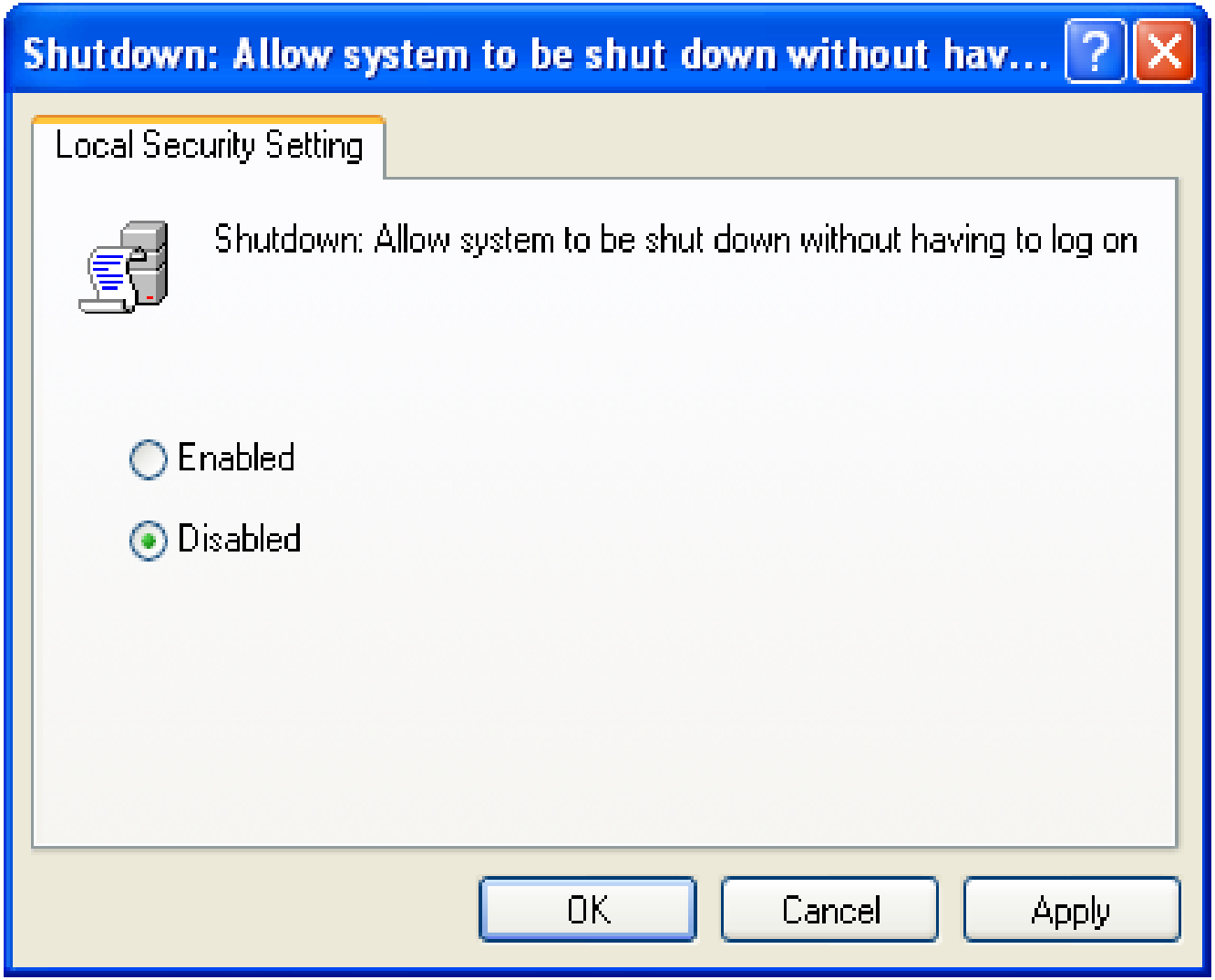
Shutdown: Allow System to be Shut Down Without Having to Log On

Vulnerability	• Attacker can shutdown the server manually and can cause a DoS condition
Countermeasure	• Configure this policy setting to **Disabled**
Potential Impact	• It is necessary for the admin to logon to the console and shut it down or restart it

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shutdown: Allow System to be Shut Down Without Having to Log On



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shutdown: Clear Virtual Memory Page File

This policy decides whether the computer will clear the virtual memory page when the system shuts down

If a computer is allowing any other operating system to start, it should be made sure that the system page file should be wiped completely

Enable this setting to clean the virtual memory page and hibernate file Hiberfil.sys

The values for the Shutdown: Clear virtual memory page file settings are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shutdown: Clear Virtual Memory Page File

Vulnerability

- An attacker can move the system volume to a different location and analyze the contents of the paging file
- The data from RAM to Page file can be accessed

Countermeasure

- Configure the setting to **Enabled**.

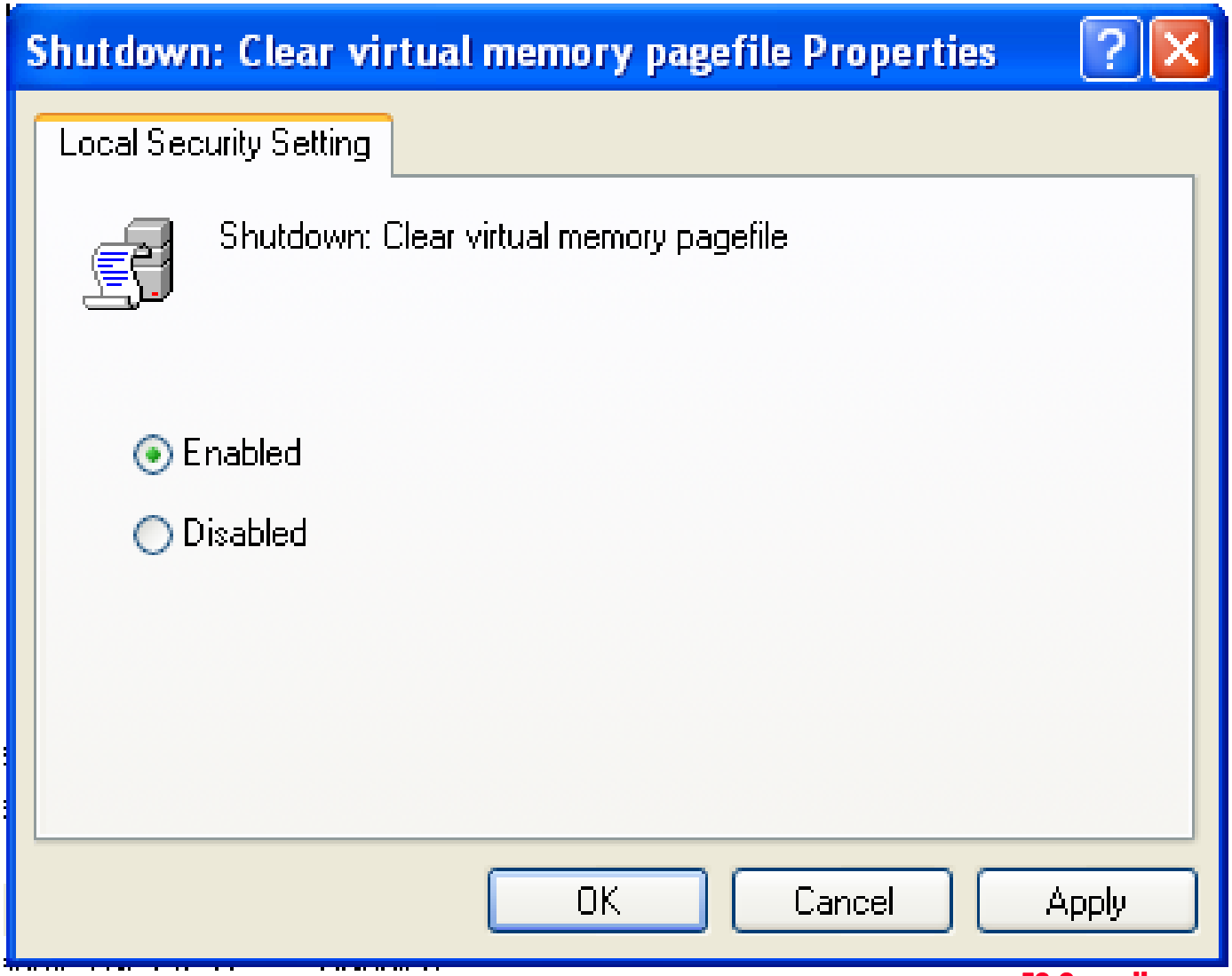
Potential Impact

- The shut down and restart time of a server will increase
- A warning message should be given before implementing this policy

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shutdown: Clear Virtual Memory Page File



EC-Council
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Cryptography: Force Strong Key Protection for User Keys Stored on the Computer

This policy checks whether user can use private keys, as S/MIME key, without a password

The values for the **System cryptography: Force strong key protection for user keys stored on the computer** setting are:

- User input is not required when new keys are stored and used
- User is prompted when the key is first used
- User must enter a password each time they use a key
- Not Defined

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Cryptography: Force Strong Key Protection for User Keys Stored on the Computer

Vulnerability	• In this configure a password must be provided which is distinct from the domain password, when ever they use a key
Countermeasure	• Configure the setting to **User must enter a password each time they use a key**
Potential Impact	• The password has to be entered every time the key is accessed

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Cryptography: Use FIPS Compliant Algorithms for Encryption, Hashing, and Signing

The TLS/SSL Security Provider only support the cipher suite TLS_RSA_WITH_3DES_EDE_CBC_SHA

Only Triple Data Encryption Standard (DES) encryption algorithm for TLS traffic encryption is used

Enable – File System Service (EFS) supports only Triple DES encryption algorithm for encrypting file data

The values for the System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Cryptography: Use FIPS Compliant Algorithms for Encryption, Hashing, and Signing

Vulnerability

- By enabling this policy, computer will use most powerful algorithm. available for digital encryption, hashing and signing

Countermeasure

- Configure the policy setting to **Enabled**

Potential Impact

- If the servers do not support the algorithm, the client computers may not be able to interact with it
- Networks with out the use of this algorithm might not communicate with the server
- If this policy is enabled you have to configure Internet Explorer to use TLS

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Cryptography: Use FIPS Compliant Algorithms for Encryption, Hashing, and Signing

To enable Internet Explore to use TLS

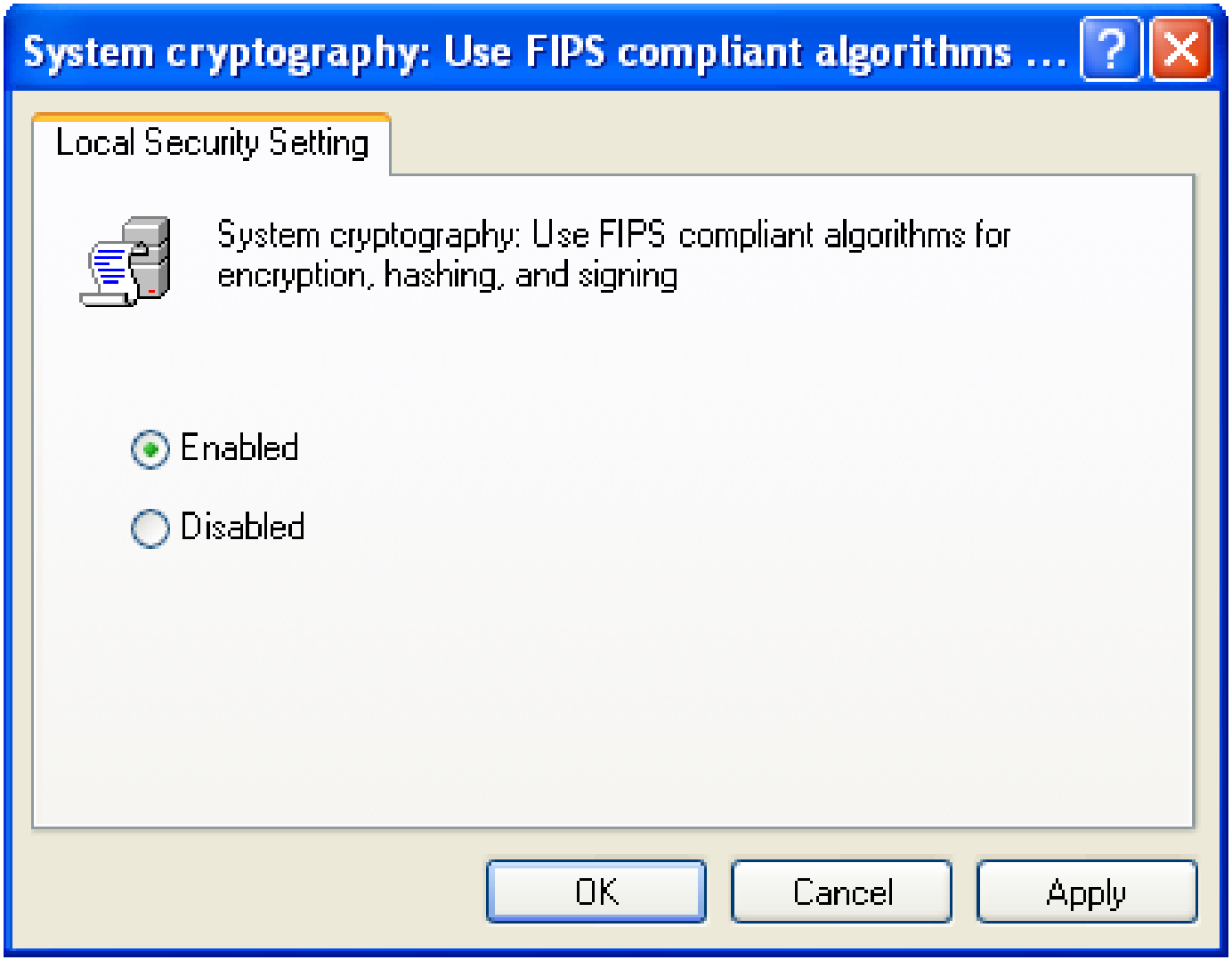
- On the Internet Explorer **Tools** menu, open the **Internet Options** dialog box
- Click the **Advanced** tab
- Select the **Use TLS 1.0** checkbox

IE can also be configured by Group Policy or by using the Internet Explorer Administrators Kit

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Cryptography: Use FIPS Compliant Algorithms for Encryption, Hashing, and Signing



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Objects: Default Owner for Objects Created by Members of the Administrators Group

This policy is used to find that **Administrators** group or an object creator is a default owner of any system objects

The values for the **System objects: Default owner for objects created by members of the Administrators group** setting are:

- Administrators group
- Object creator
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Objects: Default Owner for Objects Created by Members of the Administrators Group

Vulnerability

- If configuration is done for **Administrators group** it won't be possible to create system objects

Countermeasure

- Configure the policy to **Object creator**

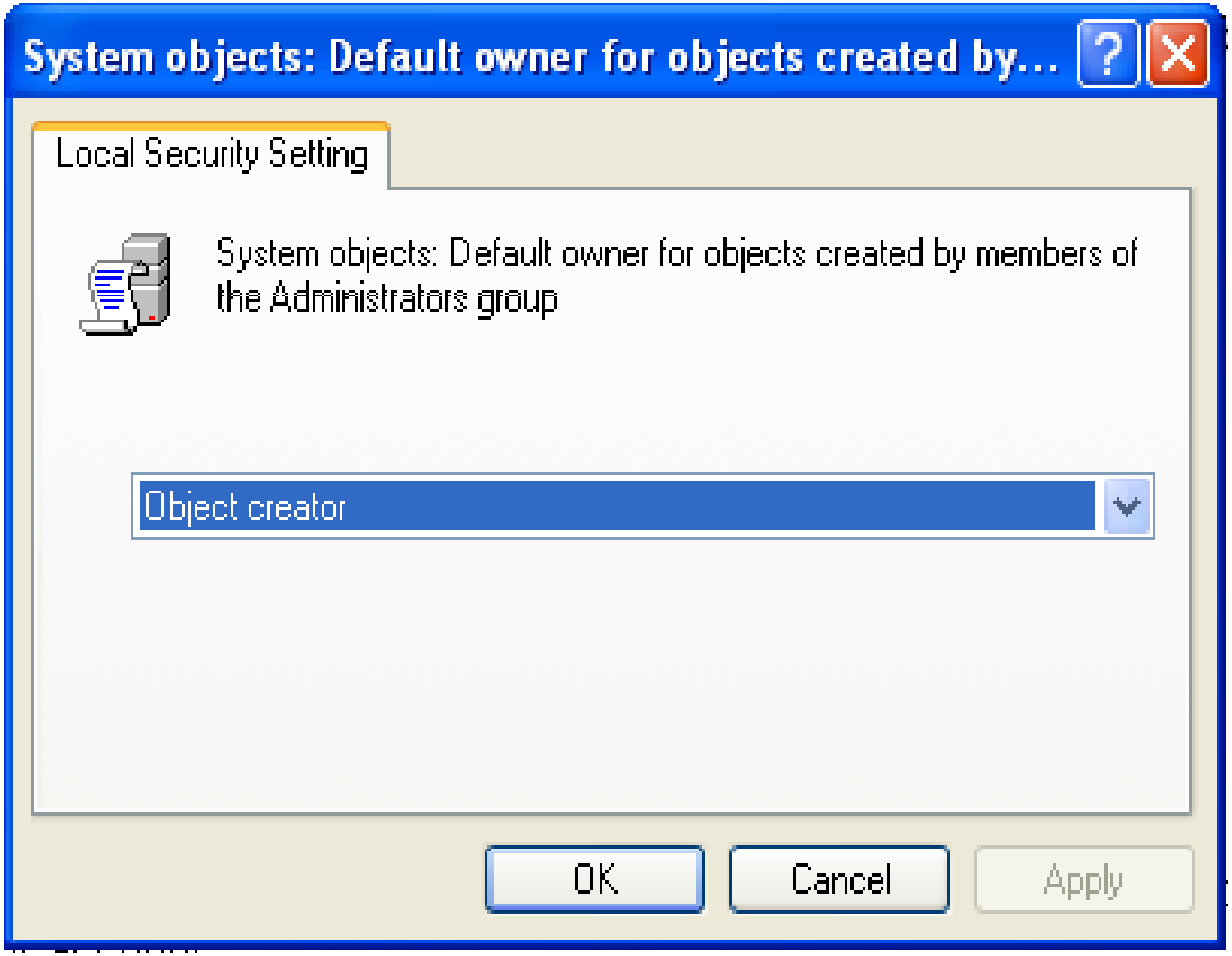
Potential Impact

- If an object is created the ownership is given to the created account but not to the general Administrator account

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Objects: Default Owner for Objects Created by Members of the Administrators Group



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Objects: Require Case Insensitivity for Non-Windows Subsystems

This policy checks whether it can set case insensitive for all sub systems

Kernel supports case sensitive for other subsystems

Enable – Case insensitivity is enforced for all directory objects, symbolic links, and IO as well as file objects

Disable – The Win32 subsystem does not become case-sensitive

The values for the System objects: Require case insensitivity for non-Windows subsystems setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Objects: Require Case Insensitivity for Non-Windows Subsystems

Vulnerability

- If this policy is not enabled a user can create a subsystem with a same file name with a mix of Upper and lower case letters to confuse the users

Countermeasure

- Configure the policy setting to **Enabled**

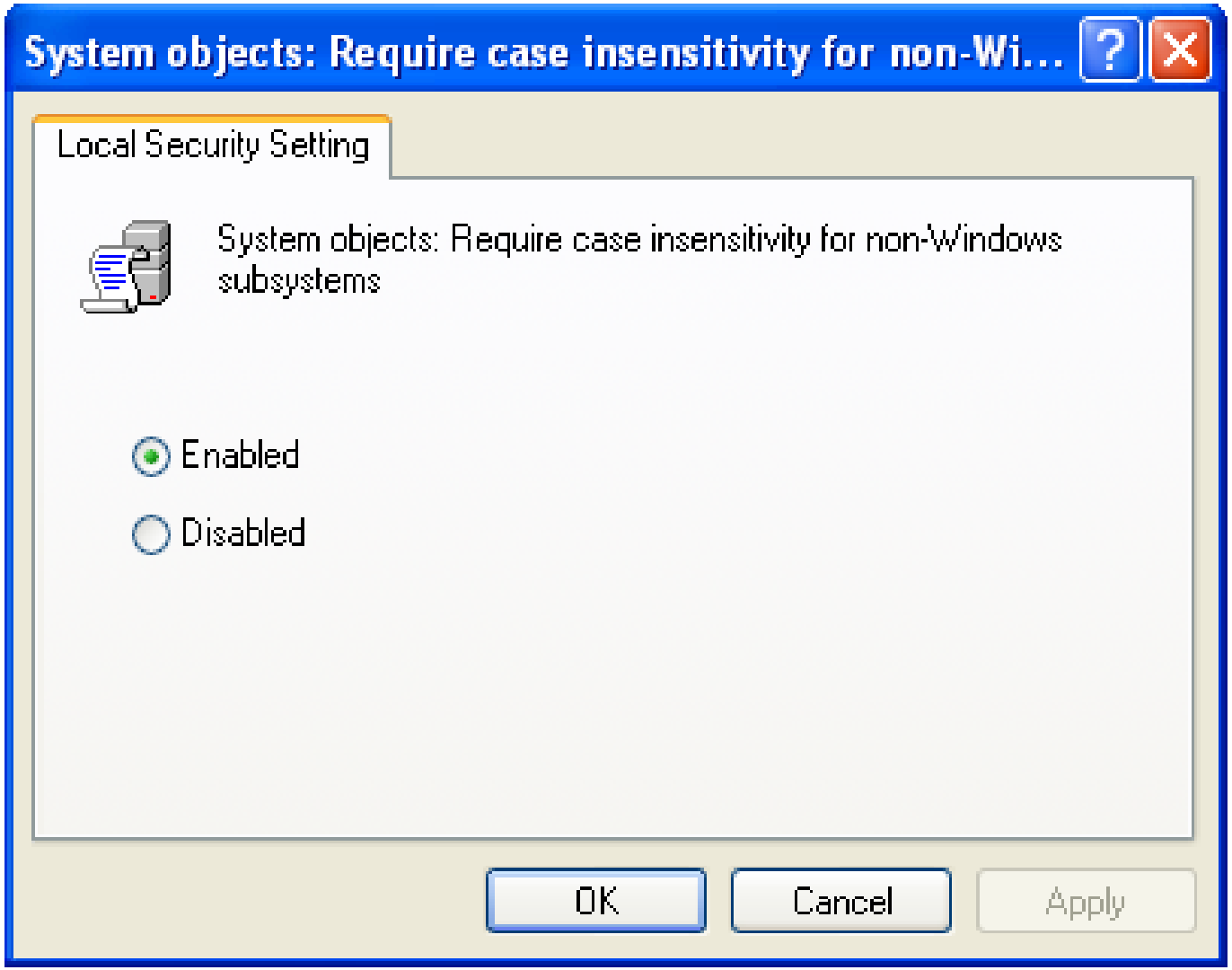
Potential Impact

- This configuration may confuse users familiar with UNIX-based case-sensitive operating systems

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Objects: Require Case Insensitivity for Non-Windows Subsystems



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Objects: Strengthen Default Permissions of Internal System Objects

The strength of the default DACL for objects is obtained by this policy

Object are located and shared according to the windows shared list

The values for the **System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Objects: Strengthen Default Permissions of Internal System Objects

Vulnerability

- Enable – The default DACL is strengthened as non-administrators can access the object created but cannot modify them

Countermeasure

- Configure the policy setting to **Enabled**

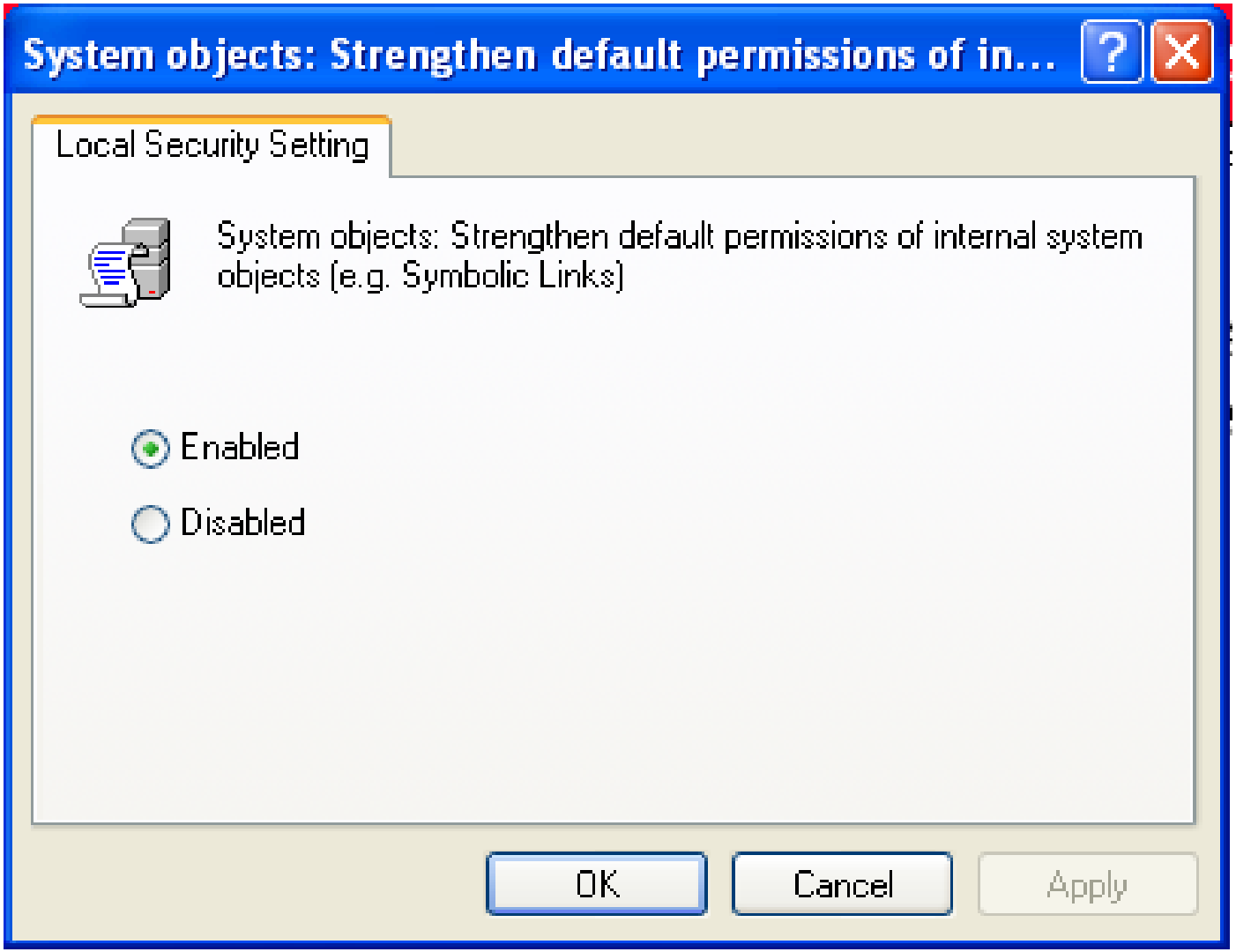
Potential Impact

- None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Objects: Strengthen Default Permissions of Internal System Objects



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Settings: Use Certificate Rules on Windows Executables for Software Restriction Policies

This policy decides on the digital certificates are processed or not when software restriction policies are enabled

Certification rules are enabled or disabled by the policy

The values for the **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies** setting are:

- Enabled
- Disabled
- Not Defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Settings: Use Certificate Rules on Windows Executables for Software Restriction Policies

Vulnerability

- Software restriction can stop the execution of viruses and Trojan horse

Countermeasure

Configure the policy setting to Enabled

Potential Impact

Software restriction policies check a certificate revocation list (CRL) to ensure that the software's certificate and signature are valid

Edit the software restriction policies in the desired GPO to disable this feature

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Event Log

Event log records events happen on the computer. The log container defines attributes as maximum log size, access rights for each log, and retention settings and methods

Event Log Settings

- You can configure the event log settings in the following location within the Group Policy Object Editor:
  - **Computer Configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Event Log Size

This policy estimates the maximum size of the event log

The event log file runs as a service in Services.exe file and processes as EventLog.dll. All the processes in Services.exe run on 1 GB of memory space. If no extra memory is assigned to the process problem may arise

If the allocated memory is not sufficient, no error message will be displayed and the event will not appear in the log

As per Microsoft the practical limit is approximately 300 MB combining all *event logs* on most of the servers

The values for the Maximum event log size setting are:

- A value in kilobytes between 64 and 4,194,240. It must be a multiple of 64

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Maximum Event Log Size (Cont'd)

Vulnerability	• Enable – If there is an increase on the number of objects to audit, the events will exceed the log capacity and force the system to shutdown • Disable – Prevents abnormal shut down
Countermeasure	• Sensible log size policies should be availed as to detect and track unauthorized actions
Potential Impact	• Configuring the retention method helps when the event log is full it will overwrite the older entries rather that the newer one • An attacker can generate and fill the log to force it to overwrite the log and clear the older data

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Prevent Local Guests Group from Accessing Event Logs

This policy decides on accessing rights for guest user on the Application, Security, and System event logs

The values for the **Prevent local guests group from accessing event logs** setting are:

- Enabled
- Disabled
- Not Defined

These setting will only be supported on Windows 2000 and later versions

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Prevent Local Guests Group from Accessing Event Logs (Cont'd)

Vulnerability

- An attacker can logon as a guest and know lot of information

Countermeasure

- Enable the setting for the policies of all three event logs

Potential Impact

- None

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Retain Event Logs

This policy gets the number of days for retaining the event log data, if the retention method is specified by days

Make sure that the available log size will be enough to capture all logs

The values for the **Retain event logs** setting are:

- A user-defined number in days between 1 and 365
- Not Defined

A user with **Manage auditing and security log** user right can access the Security log

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Retain Event Logs (Cont'd)

Vulnerability

- Archive the log at scheduled intervals:
- Open the **Properties** dialog box for this policy
- Specify the appropriate number of days in the **Retain application log** setting
- Select **Overwrite events by days** for the event log retention method

Countermeasure

- Configure the setting for the policies of all three event logs to **Not Defined**

Potential Impact

- None

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Retention Method for Event Log

Wrapping method for the Application, Security, and System logs is selected by this policy

Do not archive the Application log:

- Open the **Properties** dialog box for this policy
- Select the **Define this policy setting** check box
- Click **Overwrite events as needed**

Want to archive the log at scheduled intervals:

- Open the **Properties** dialog box for this policy
- Select the **Define this policy setting** check box
- Click **Overwrite events by days**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Retention Method for Event Log (Cont'd)

Specify the appropriate number of days in the **Retain application log** setting. Ensure that the maximum log size is large enough to accommodate the interval

If you must retain all the events in the log:

- Open the **Properties** dialog box for this policy
- Select the **Define this policy setting** check box
- Click **Do not overwrite events (clear log manually)**

It needs that the log should be cleared manually

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Retention Method for Event Log (Cont'd)

The values for the **Retention method for event log** setting are:

- Overwrite events by days
- Overwrite events as needed
- Do not overwrite events (clear log manually)
- Not defined

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Retention Method for Event Log (Cont'd)

Vulnerability

- If **Event log retention method** is set to **Manual** or **Overwrite events by days**, important information might be cleared when the log is full or a DoS attack may occur.

Countermeasure

- Configure the retention method for all three event logs to the option **Overwrite events as needed**.
- Configure this setting to **Manual**

Potential Impact

- Once the log is full it stops recording the events until it is cleared. Or Retention method is set to overwrite old entries

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Delegating Access to the Event Logs

In Microsoft Windows Server™ 2003, there is a possibility to customize the permissions on each event log on a computer

The access control list (ACL) is stored as a Security Descriptor Definition Language (SDDL) string, in a REG_SZ value called "CustomSD" for each event log in the registry

Edit the value and restart the computer to make the setting effect

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Services

Services Overview

- To access the resources and objects a service must logon and most services can not change there logon account
- The service will fail if you change the default account.
- Microsoft Management Console (MMC) Service can grant permissions to an account to logon as a service
- Windows Server 2003 includes three built-in local accounts that are used as the logon accounts for various system services:
  - **Local System account**
    - This account has full access to the computer, in this account a local system account can logon to a domain controller
    - A local system will not have a user accessible password

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Services (Cont'd)

- **Local Service account.**
  - This account is same as a local built in account. It has a same level of rights as a user group
  - The account is represented as NT AUTHORITY\Local Service, with out a user accessible password
- **Network Service account**
  - This account is same as a local built in account. It has a same level of rights as a user group
  - The account is represented as NT AUTHORITY\Network Service, with out a user accessible password

- You can configure the system services settings in the following location within the Group Policy Object Editor:
  - **Computer Configuration\Windows Settings\Security Settings\System Services**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Services Overview

Vulnerability

- An unneeded application or a service can raise an attack at any point. As a measure these files should be removed

Countermeasure

- Disable all unnecessary services.
- The possible values for these Group Policy settings are:
  - Automatic
  - Manual
  - Disabled
  - Not Defined
- Configure an access control list to manage service security for each service

Potential Impact

- If any of the system services are to be changed, you should make a pre check on a separate computer before applying it to the productive computer

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Set Permissions on Service Objects

Graphical user based (GUI) based tools can be used to modify services

Tools as the Group Policy Object Editor and the MMC Security Templates use the Security Configuration Editor DLL to apply these permissions

In Windows XP the MMC Security Templates used to configure the startup state of a service

Regardless of whether you click **OK** or **Cancel**, these permissions will be applied to the configured services

EC-Council

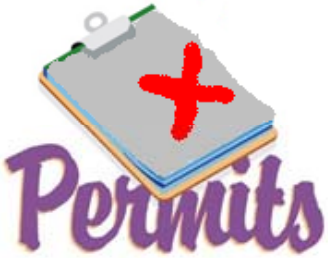
Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Set Permissions on Service Objects (Cont'd)

Microsoft recommends do not alter the permissions on services that are included with Windows XP or Windows Server 2003

There several different options to deal with this challenging situation:

- Use the Security Configuration Wizard, an optional Windows component that is included with Windows Server 2003 Service Pack 1 (SP1). Microsoft recommends this approach when you need to configure services and network port filters for various Windows Server 2003 server roles



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Set Permissions on Service Objects (Cont'd)

Run the MMC Security Template snap-in and Group Policy Object Editor on a server that runs Windows Server 2003 with SP1. Microsoft recommends this approach when you need to configure services for security templates or Group Policies that will be applied to Windows XP

Use a text editor such as Notepad to edit the security templates or Group Policies on a computer that runs Windows XP Professional. This method is the least desirable, but some customers may have no choice. Detailed instructions are provided in the following section

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Manually Editing Security Templates

A computer can be unbootable if security templates are created with incorrect template definition

When GUI based tools are configured the information is stored in "Service General Setting" section of the file

The format for each entry includes three comma-separated fields

- First Field – service name.
- Second Field – startup state
  - 4 specifies Disabled
  - 3 specifies Manual
  - 2 specifies Automatic

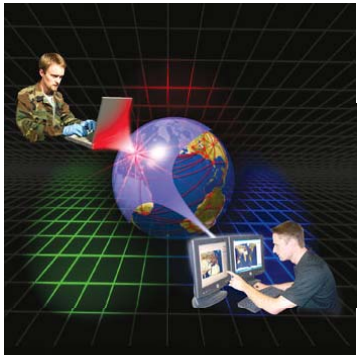
EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Manually Editing Security Templates (Cont'd)

Third Field – Permissions for the service object, in Security Descriptor Definition Language (SDDL)

To solve problems with permissions on the service objects, remove the SDDL string in the third field but leave the pair of double-quotation marks



Test security templates thoroughly before they are applied to production computers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

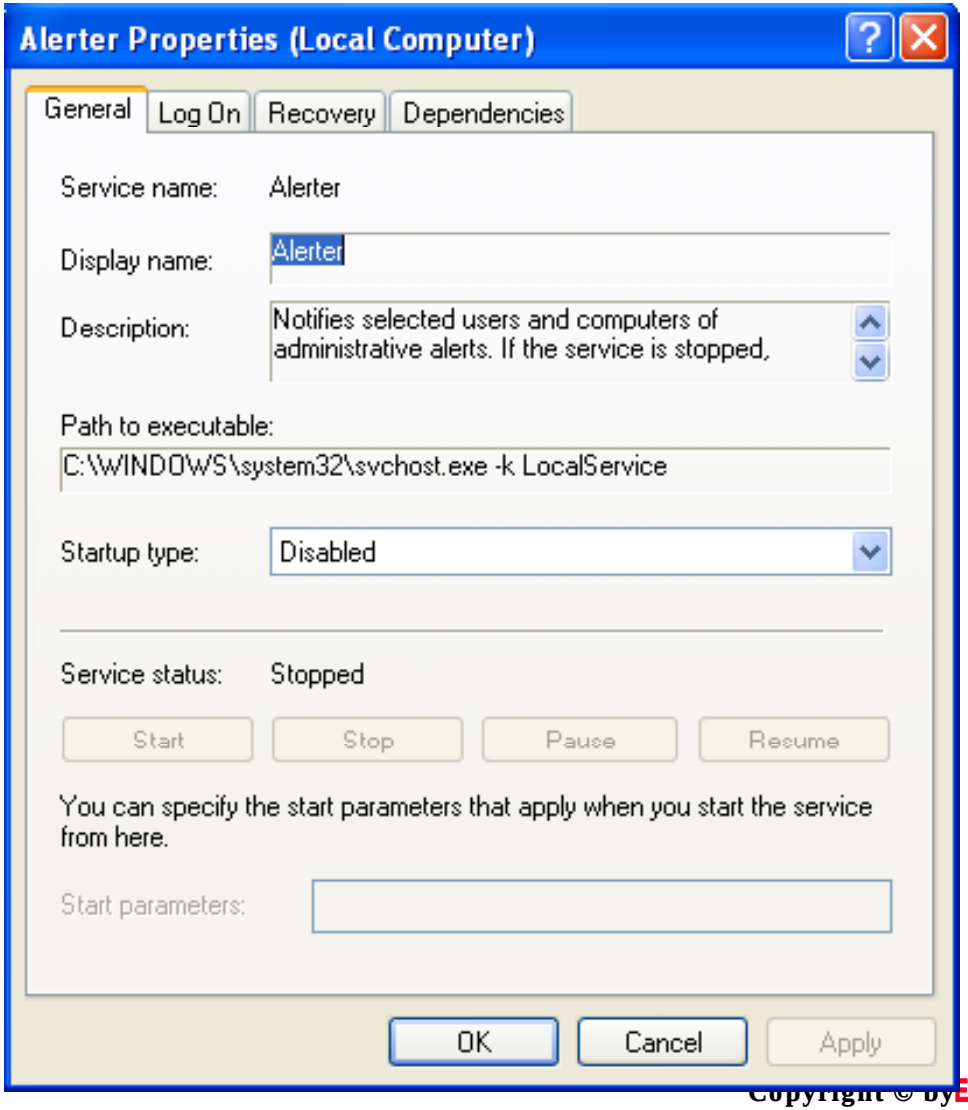
System Services - *Alerter*

- This service alerts users on administrative alerts
- Using this message can be sent to computers on the network
- Alert message warn users about security and access problems
- When an alert message is sent from a server to client, a Messenger service should be running on the client computer
- If Alerter is turned off, applications will be unable to notify a user

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Services - *Alerter*



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Application Experience Lookup Service

- The service is a part of the Application Compatibility Administrator
- When applications are launched it runs application compatibility lookup request
- To apply application compatibility software updates this service should be active
- This service in used internally by the operating system. No network, internet or Active Directory services are used by the service
- If disabled this service will run but no calls are made to it
- You cannot stop the actual process

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Application Layer Gateway Service

This service is a sub component for windows networking subsystem

Support is provided to plug-ins that allows network protocols to pass through firewalls

The Application Layer Gateway (ALG) can change the data in packets by opening the ports

The ALG FTP plug-in support active FTP sessions with the Network Address Translation (NAT) engine included in Windows

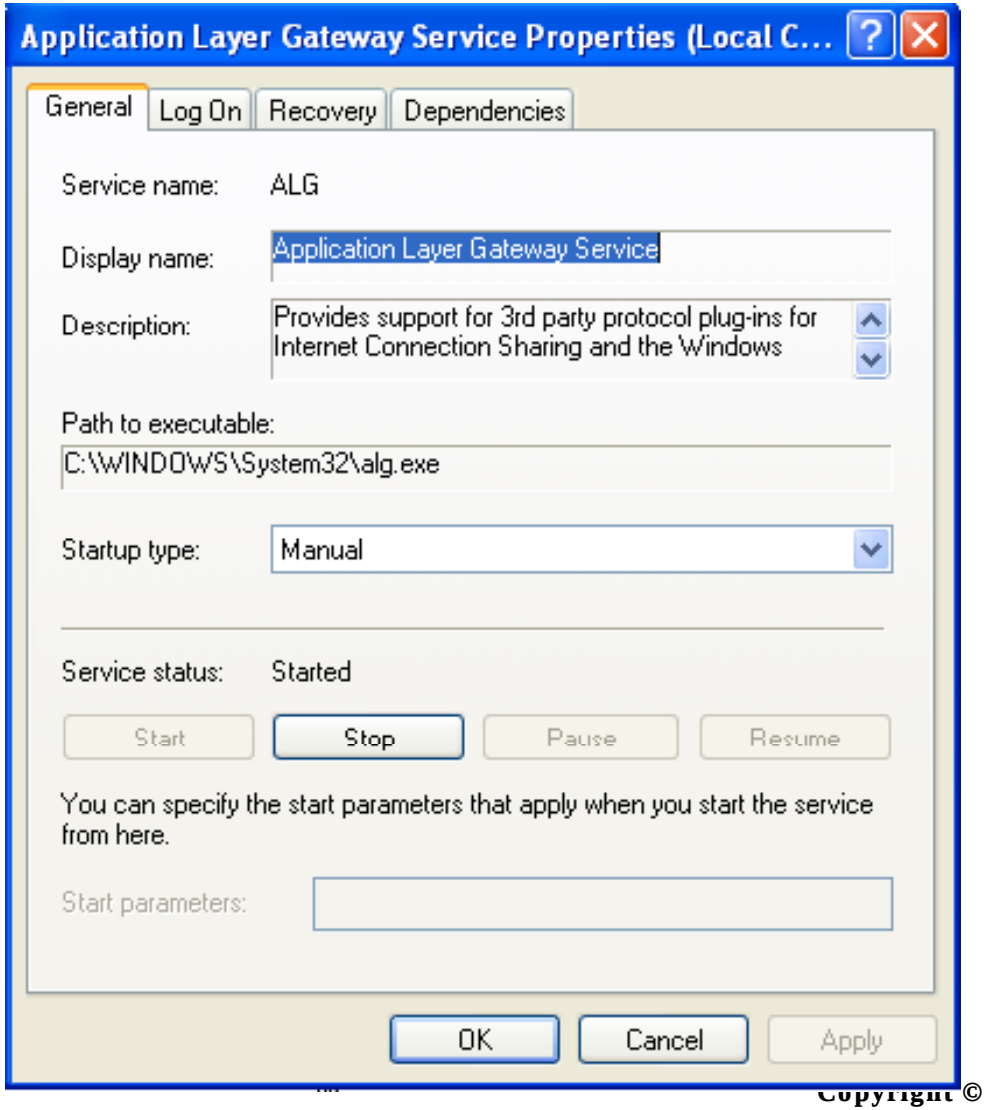
The ALG FTP plug-in can pass the traffic to a private port in range 3000-5000. Then it monitors traffic on the FTP channel. The FTP plug-in will even update ports in the FTP control channel stream

If this service stops, the connectivity for the protocols will be unavailable and will affect the network

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Application Layer Gateway Service



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Application Management

The software installation services are provided by this service and the requests to install, and remove applications are handled

This service is called when **Click Start -> Control panel -> Add/Remove Program -> Add** (or) when installing and removing an application

The service starts at its first call and does not terminate after it starts

If disabled, it's unable to install or remove program, it will not deploy application information

The message displayed in **Add programs from your network** dialog box is as following:

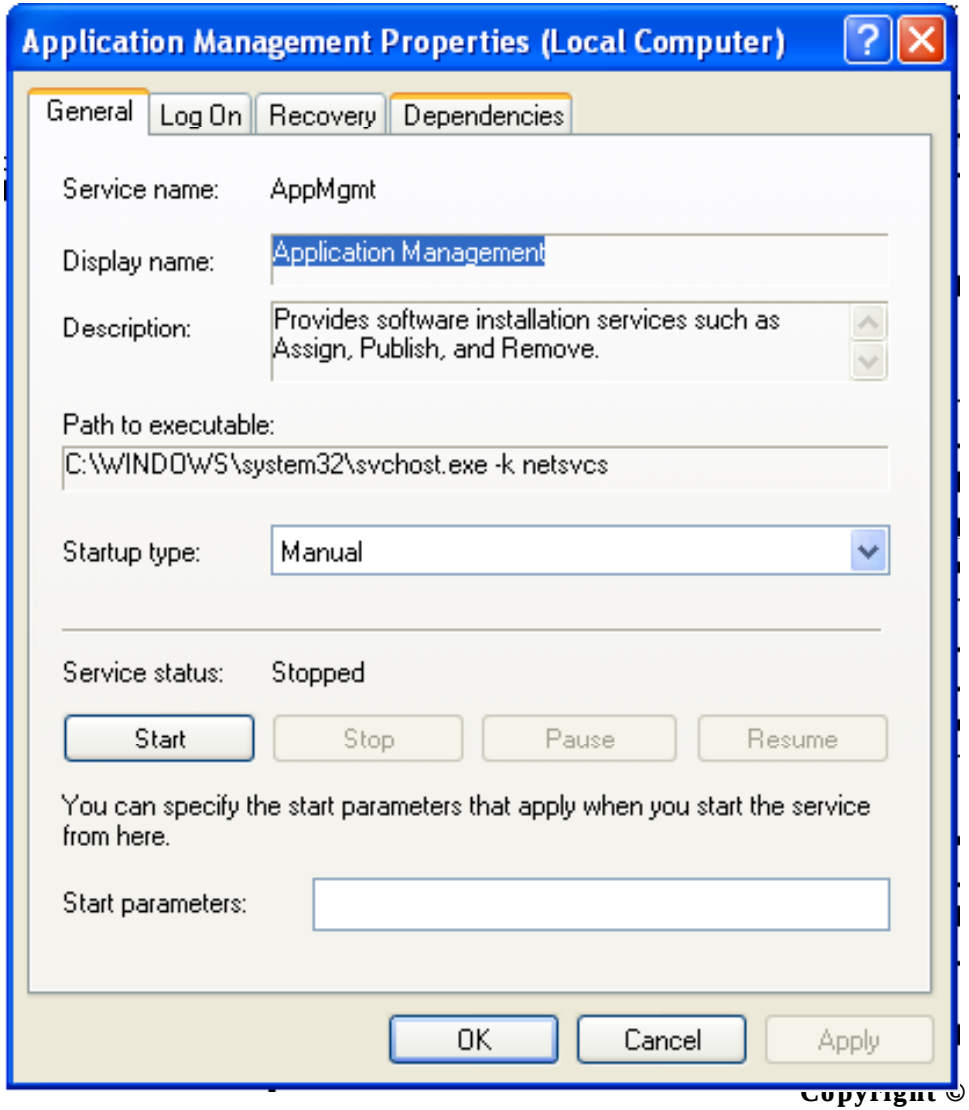
- No programs are available on the network.

This service can only be started after restarting the computer

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Application Management



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

ASP .NET State Service

ASP.NET gets the support for out-of-process session states from this service

ASP.NET supports a process known as session state, which list the values associated with the client session

Session state can be store as

- In process
- Microsoft SQL Server™ database
- out-of-process session state server

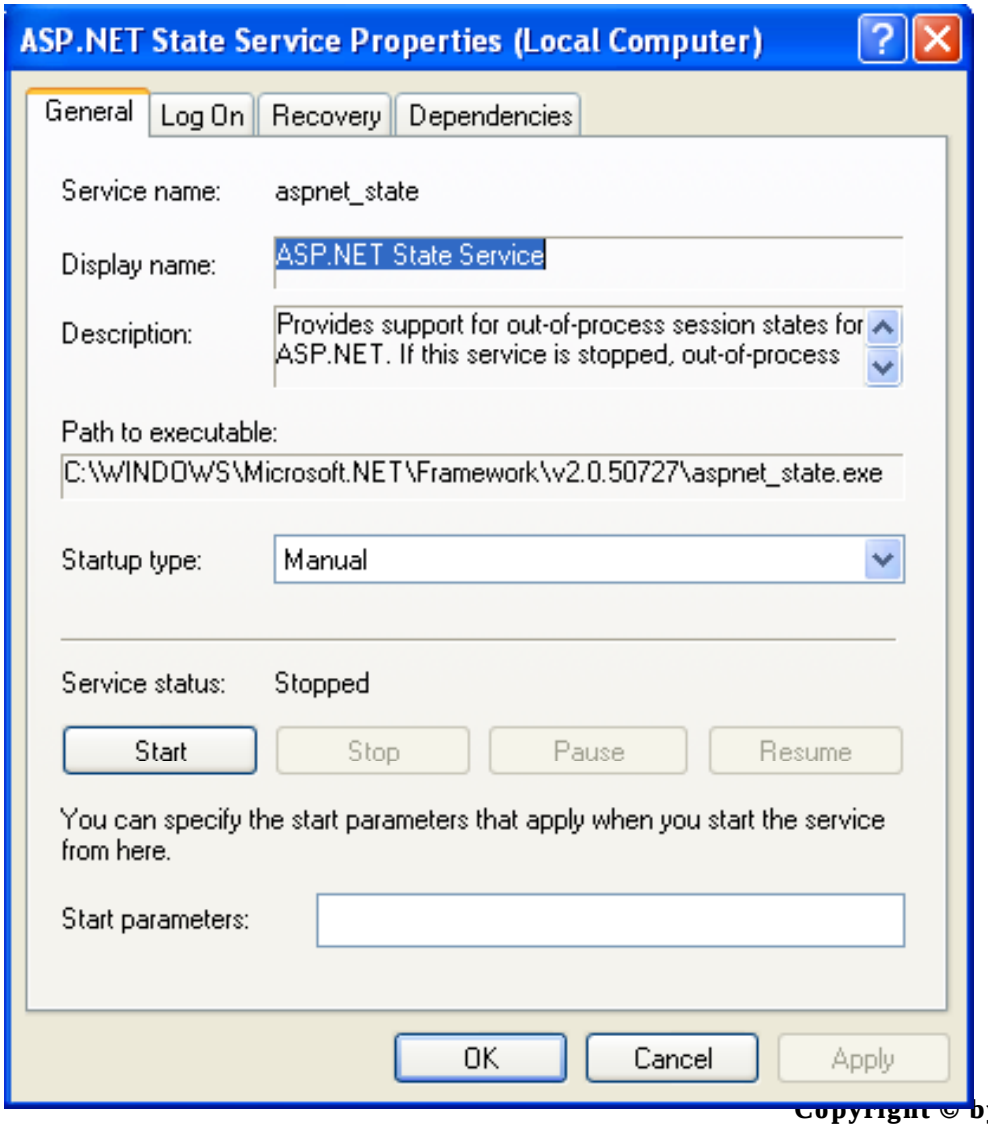
This service stores session data out-of process

The service is disabled until it is changed manually to Automatic or Manual option

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

ASP .NET State Service



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Automatic Updates

The security updates are downloaded and installed by enabling this service

The operating system detects your online state and notify before download, before installation, or the updates are installed automatically

Turn off the automatic updates as **Start -> Control Panel -> System -> Automatic updates**

The MMC Group Policy Object Editor to configure an intranet server that is configured with Windows Server Update Services

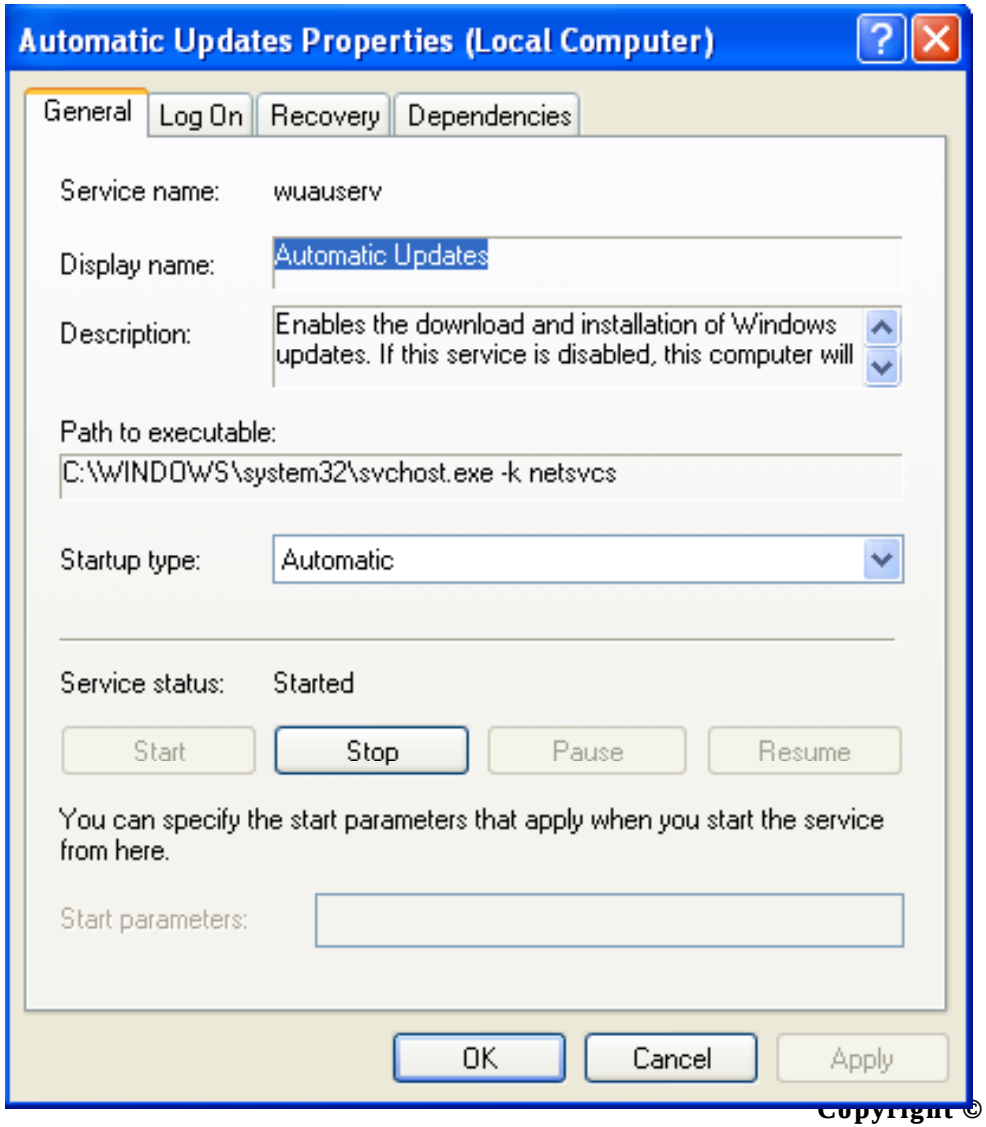
A server on the network can be specified as an internal update service

If disabled, automatic updates are canceled

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Automatic Updates



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Background Intelligent Transfer Service (BITS)

This service is a background file transfer mechanism between a client and HTTP server and a queue manager. The transfer is performed through an idle network as not to disturb other network traffic

BITS have to be start manually.

If the user logoff or connection is lost the service is stopped. Again when the user logs on the transfer starts

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Background Intelligent Transfer Service (BITS) Cont'd

BITS uses a queue to transfer jobs, in which the job priority can be set (one foreground and three background priority levels are used to prioritize the jobs) and you can specify that the file has to be transferred in foreground or background

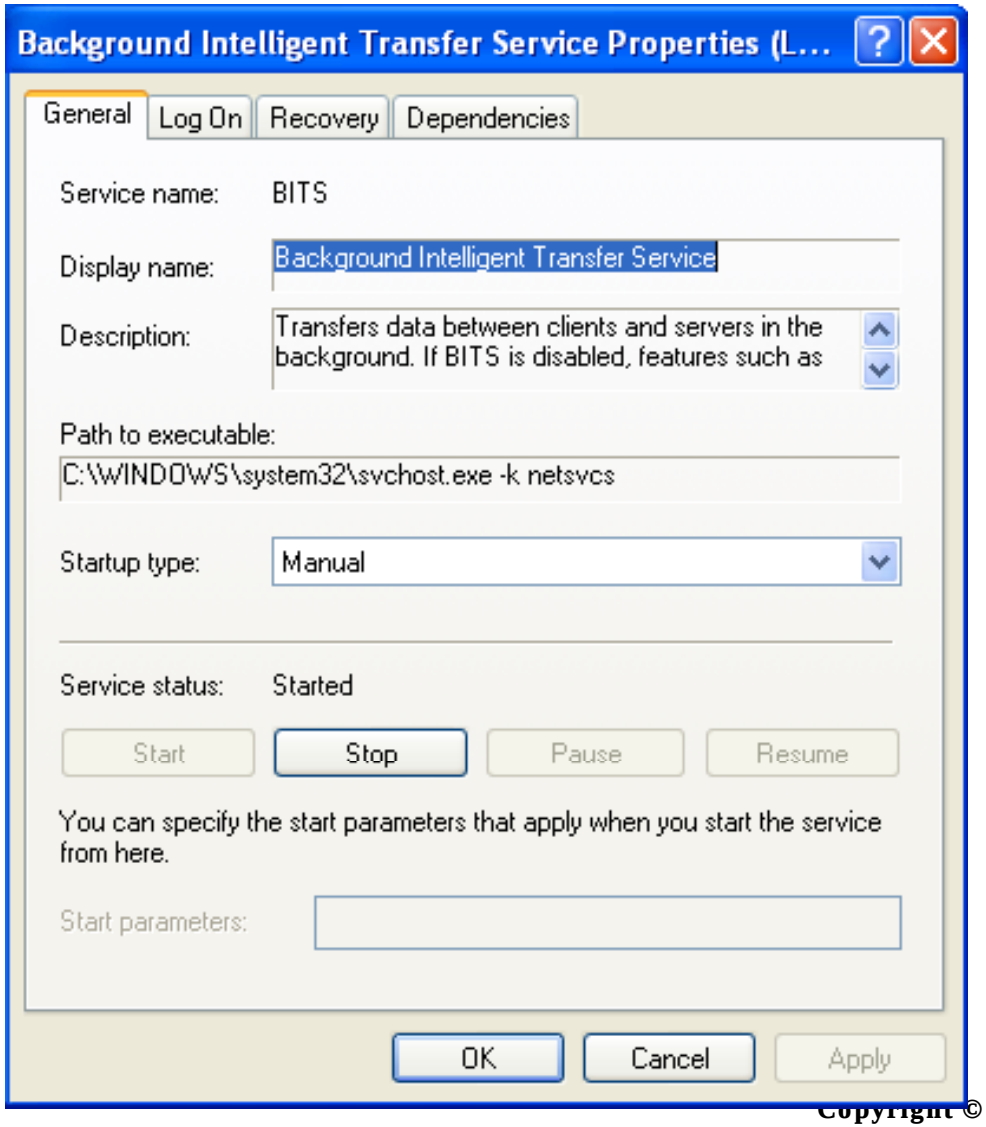
The rate of bandwidth to transfer is decided by BITS depending upon the network traffic

If BITS is disabled the services like Automatic Update will not be able to process

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Background Intelligent Transfer Service (BITS) Cont'd



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Certificate Services

This service enables a business to act as its own certificate authority (CA) and issue and manage digital certificates for applications

Windows Server 2003 supports multiple level of CA hierarchy

This service has to install by Administrators through **Control Panel -> Add/Remove programs**

If it is disabled, certificate request is not accepted

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Client Service for NetWare

For the logon user this service provides access to file print resources on NetWare networks and Netware servers that run Novell Directory Services (NDS) or bindery security (NetWare versions 3.x or 4.x) from your computer

It does not support IP protocol so it can not be linked with NetWare 5.x in an IP-only environment

For this capability, Internetwork Packet Exchange (IPX) protocol should be load on the NetWare 5.x server

If disabled, files and print resources are not accessible

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

ClipBook

This service creates and share pages of data for review by remote users

This service has to depend on the **Network Dynamic Data Exchange (NetDDE)** service to create the actual file shares to connect

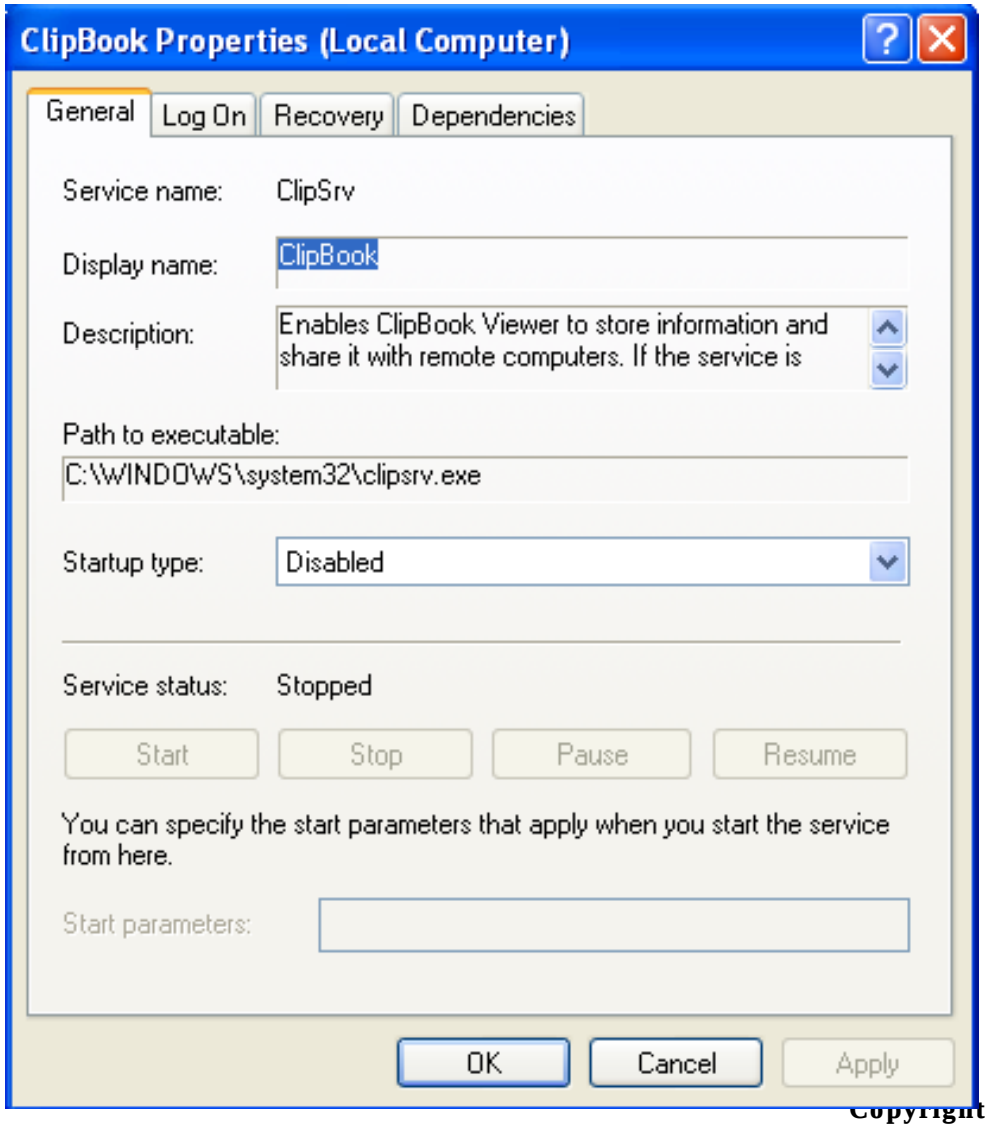
This service is installed by default but is disabled

Clipbrd.exe can used to view the local Clipboard

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

ClipBook



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Cluster Service

This service manages the cluster database by handling server cluster operations

The two different cluster solutions for the Windows platform are:

- Server clusters - Provide a highly available environment for applications that must run reliably for long periods of time

- Network Load Balancing (NLB) clusters - Provide a highly available and highly scalable environment for other types of applications

This service provides support for Server Cluster, it controls all cluster operations and manages its database

Each node in a cluster runs one instance of the Cluster Service

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Cluster Service (Cont'd)

Windows Server 2003 supports up to eight-node server clusters in both the Enterprise Server and Datacenter Server editions of Windows

This service is not installed and by default

Server clusters can have one of three different configurations:

- Single node. These server clusters can be configured with or without external cluster storage devices
- Single quorum device. These server clusters have two or more nodes and are configured so that every node is attached to one or more cluster storage devices
- Majority node set. These server clusters have two or more nodes in which the nodes may or may not be attached to one or more cluster storage devices

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

COM+ Event System

The service sets automatic event distribution to COM component

The late-bound events or method calls between the publisher or subscriber and the event system are supported by COM+ programming model

This handles event semantics for publisher and subscriber

The life cycle of the subscription is separate from that of either the publisher or the subscriber

Subscriptions can be made before activating the publisher or subscriber

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

COM+ Event System (Cont'd)

Publisher	Subscriber
Offer to publish event types	Request event types from specific publishers

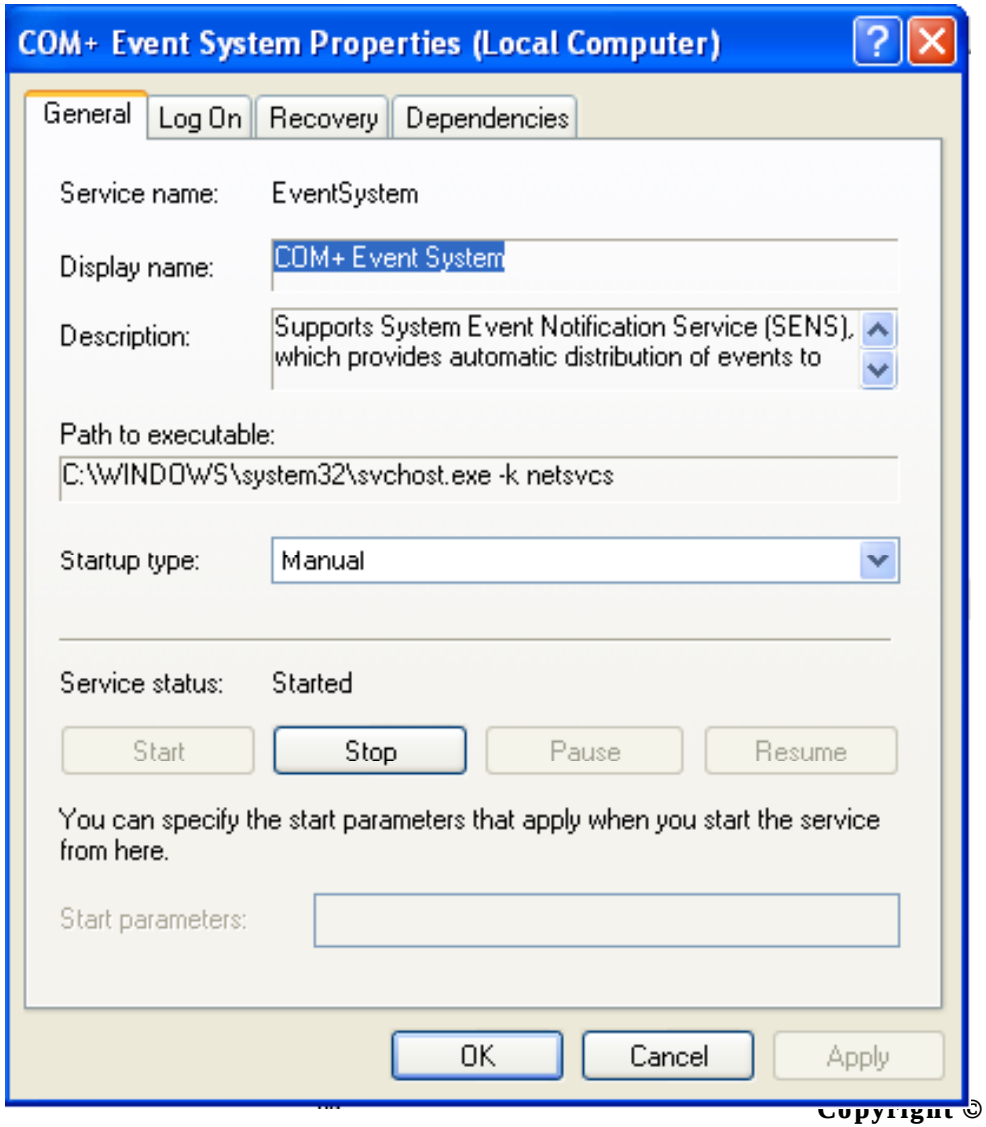
The life cycle of the subscription is separate from that of either the publisher or the subscriber

Subscriptions can be made before activating the publisher or subscriber

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

COM+ Event System (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

COM+ System Application

This service manages the configuration and tracking of COM+-based components

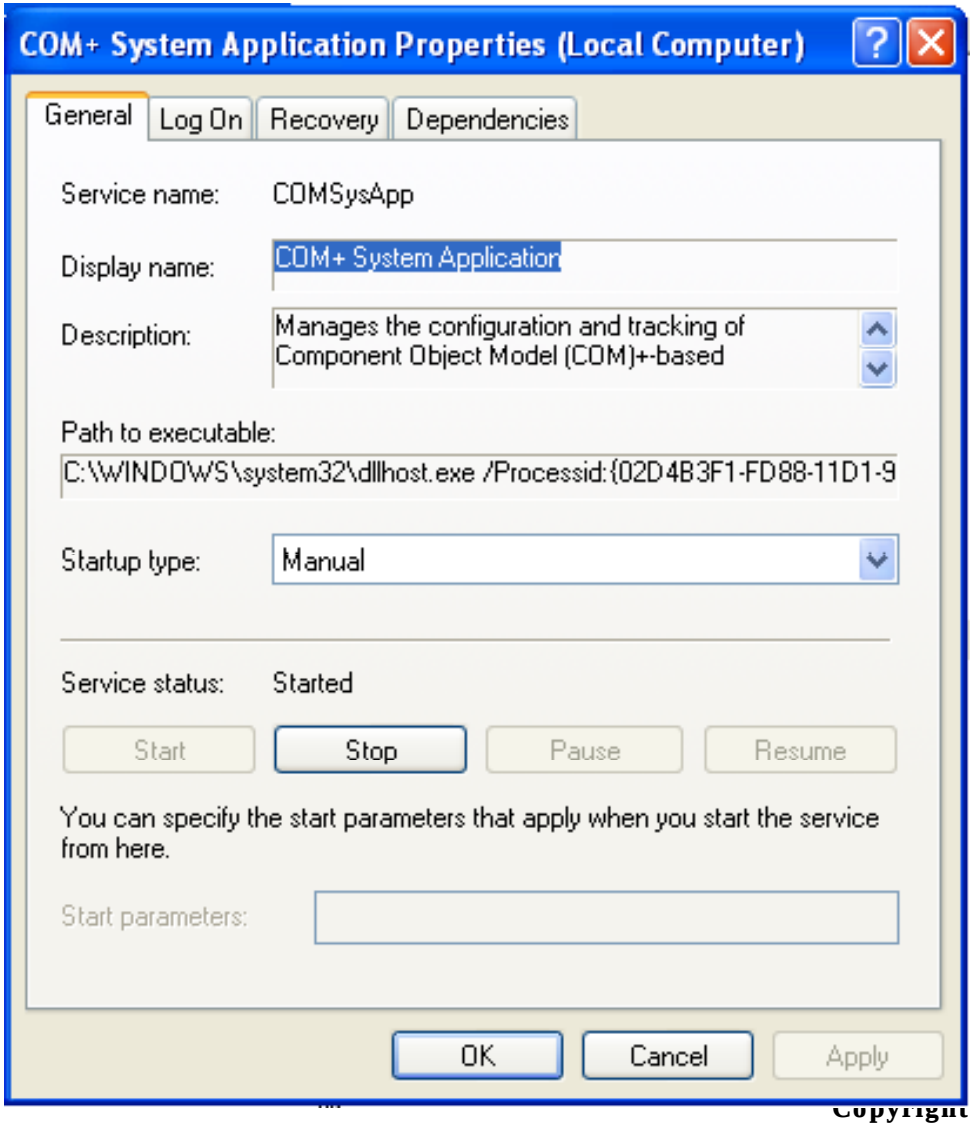
If the service stops most of the COM+-based object will not work properly

This service is necessary to the **Volume Shadow Copy** for Windows Backup and backup applications that rely upon the Windows Backup API

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

COM+ System Application



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

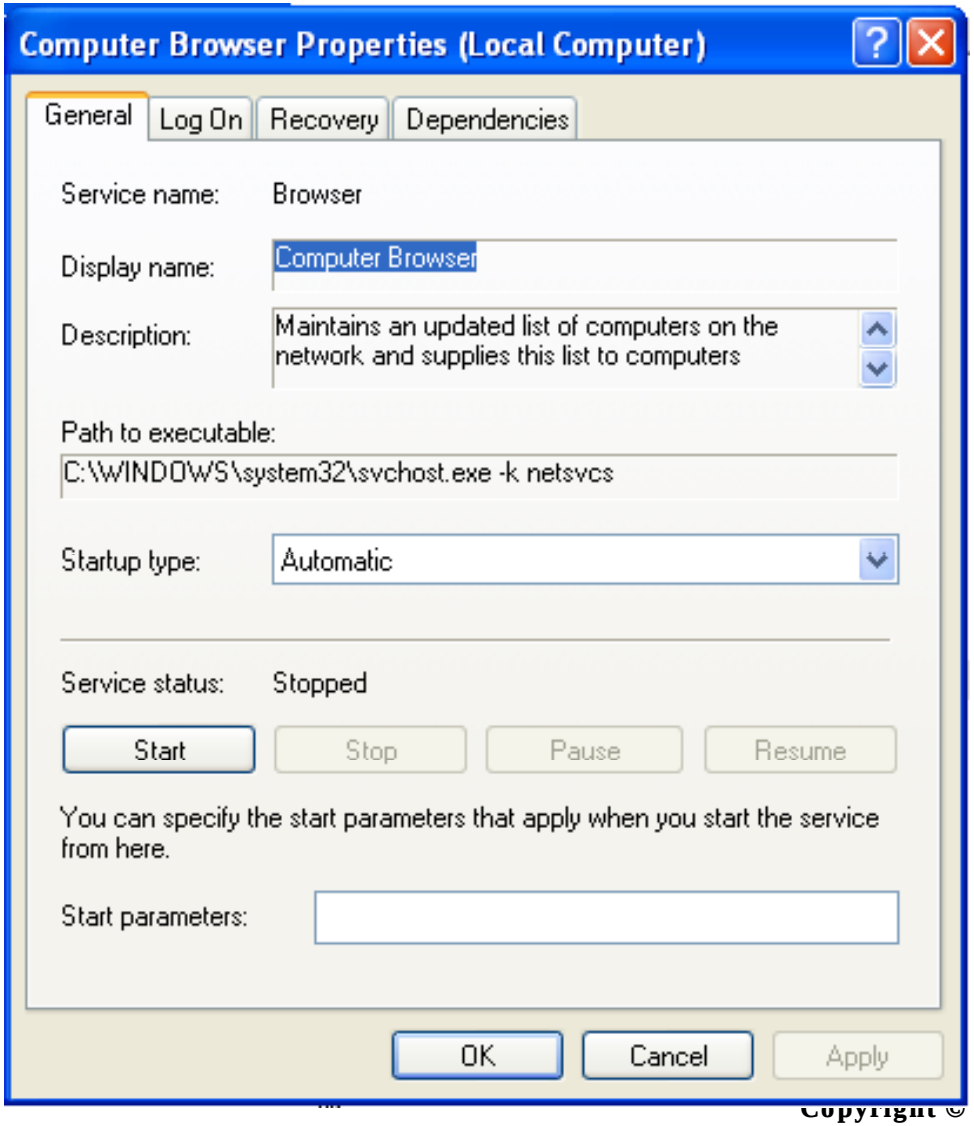
Computer Browser

- This service manages the list of computers on the network and sends the programs requested
- It is used by Windows-based computers to view network domain and resources
- It maintains the browser list for the computers designated as browsers
- Early versions of Windows applications need browsing capabilities
- The **Computer Browser** service is enabled and started by default
- If disabled, the browser list will not be updated or maintained

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Computer Browser



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Cryptographic Services

The service provides key-management service for the computer

This is contain management services:

- Catalog Database Service. Adds, removes, and looks up catalog files. Used to verify signed files in Windows File Protection (WFP), Driver Signing, and setup
- Protected Root Service. Adds and removes Trusted Root Certification Authority certificates. Only Local System accounts have write-access to the list. If disabled, the current user can not add or remove Trusted Root Certificate Authority certificates
- Key Service. Administrators can enroll for certificates on behalf of the local computer account. If disabled, auto enrollment will not be available

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Cryptographic Services (Cont'd)

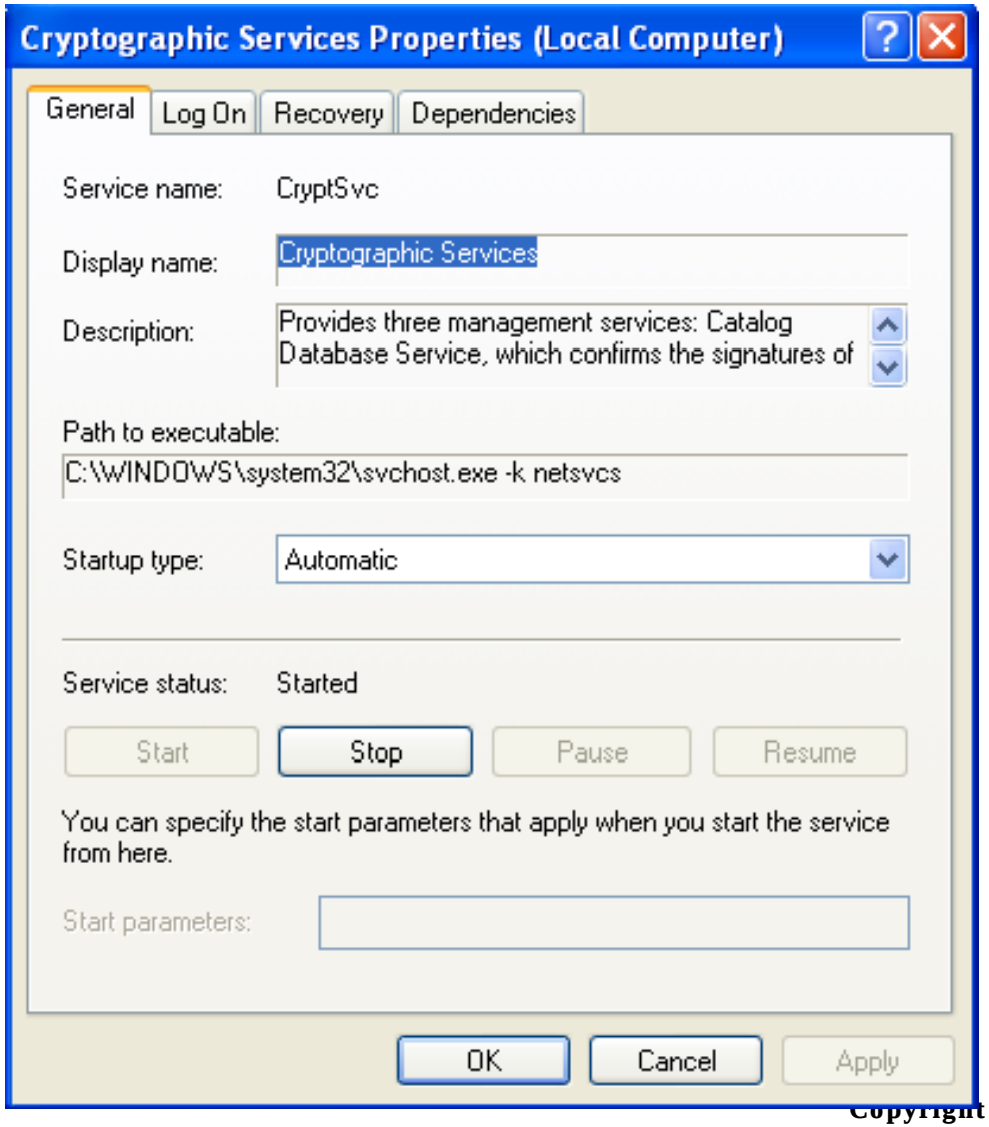
The service is enabled and started automatically by default

If disabled, the management services will not work properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Cryptographic Services (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DCOM Server Process Launcher

The DCOMLaunch service incorporates the functions of the old Remote Procedure Call (RPC) service which required Local System privileges

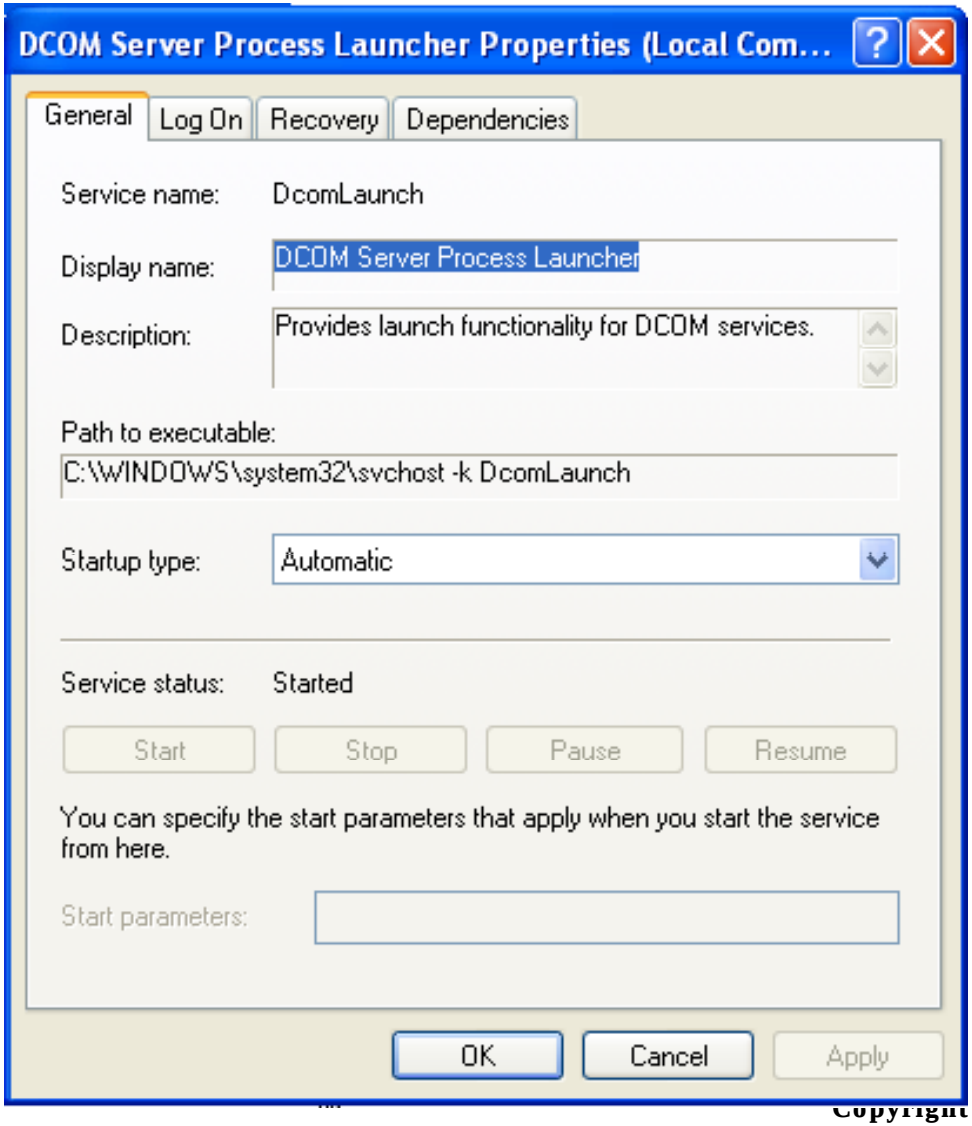
This service is enabled and started by default

If disabled, DCOM requests and RPC's will not work properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DCOM Server Process Launcher



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DHCP Client

Network configuration is managed by this service

IP addresses and DNS names are updated by this service

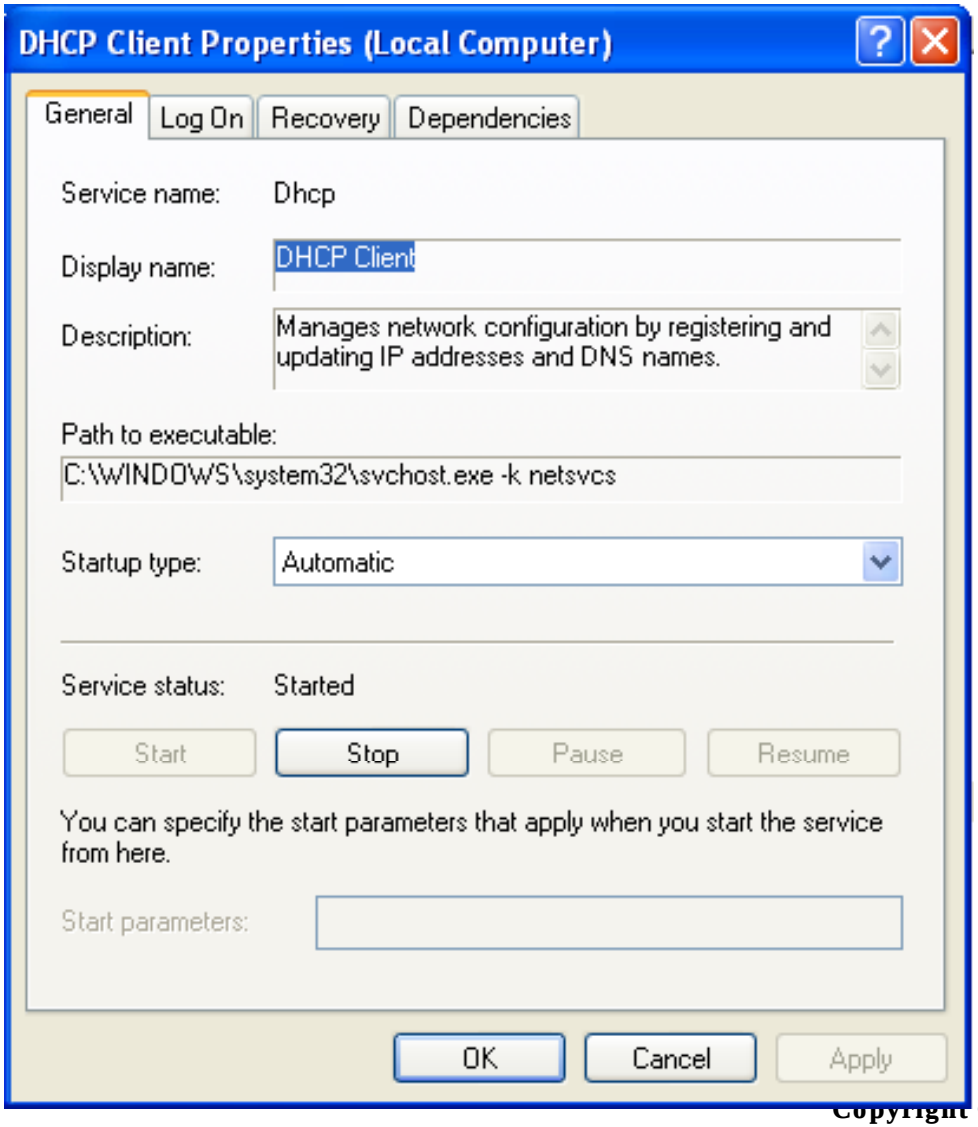
It is not needed to configure settings for DNS or WINS.

- Click Obtain DNS Server Address Automatically option to enable the service

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DHCP Client



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DHCP Server

It allocates IP addresses and enable configuration of network settings. It uses a Client /Server model

In a network there may be one or more DHCP servers to maintain TCP/IP configuration

The server database contains:

- Valid configuration parameters for the client computers
- Valid IP addresses that are maintained in a pool for assignment to client computers, and reserved addresses for manual assignment
- Duration of the lease offered by the server. The lease defines the length of time the assigned IP address is valid

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DHCP Server (Cont'd)

The complexity over the address configuration administration is minimized by DHCP and IP standards

Multicast address allocation is performed using the Multicast Address Dynamic Client Assignment Protocol (MADCAP), while registered IP addresses are dynamically given to the client computers

DHCP server gives configuration in the form of address-lease to the client computer

If disabled, the IP addresses cannot be issues automatically

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

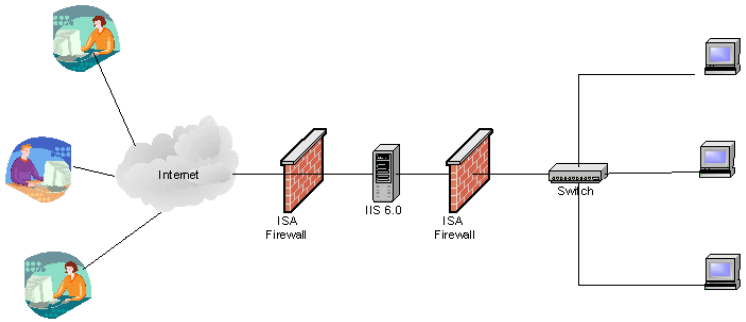
Distributed File System

This service manages logical volumes distributed across a local or wide area network (WAN)

DFS is a distributed service integrating disparate file shared into a single logical namespace

If disabled, it is unable to access the file sharing and logical data through name space

To access the data when disabled, the names of services and shares of namespace should be known



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Distributed Link Tracking Client

The service maintains links between NTFS file system

The service makes sure that shortcuts and Object Linking and Embedding (OLE) links continue working after the target file is renamed or moved

The distributed link tracking stamps a unique object identifier (ID) in the target file, when a shortcut is created known as link source

A file Link Client which refers to the target file also stores information about the object ID internally

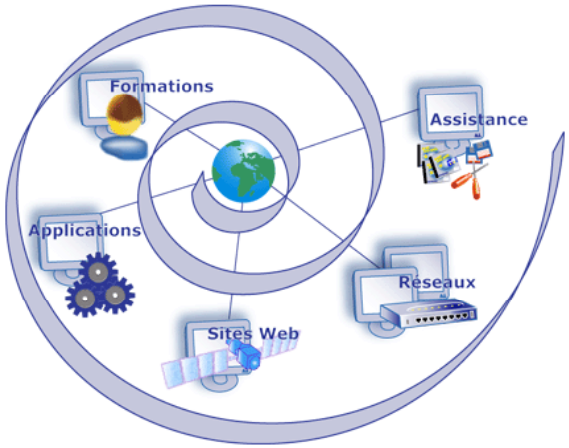
EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Distributed Link Tracking Client (Cont'd)

Distributed link tracking uses an object ID to locate the link source file when:

- Link source file is renamed
- Link source file is moved to another folder on the same volume or a different volume of the same computer
- Link source file is moved to another computer in the network
- Shared network folder that contains the link source file is renamed



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Distributed Link Tracking Client (Cont'd)

In a Windows 2000 or Windows Server 2003 domain the service, the link source file is in the following additional scenarios:

- Computer that contains the link source file is renamed.
- Volume that contains the link source file is moved to another computer within the same domain

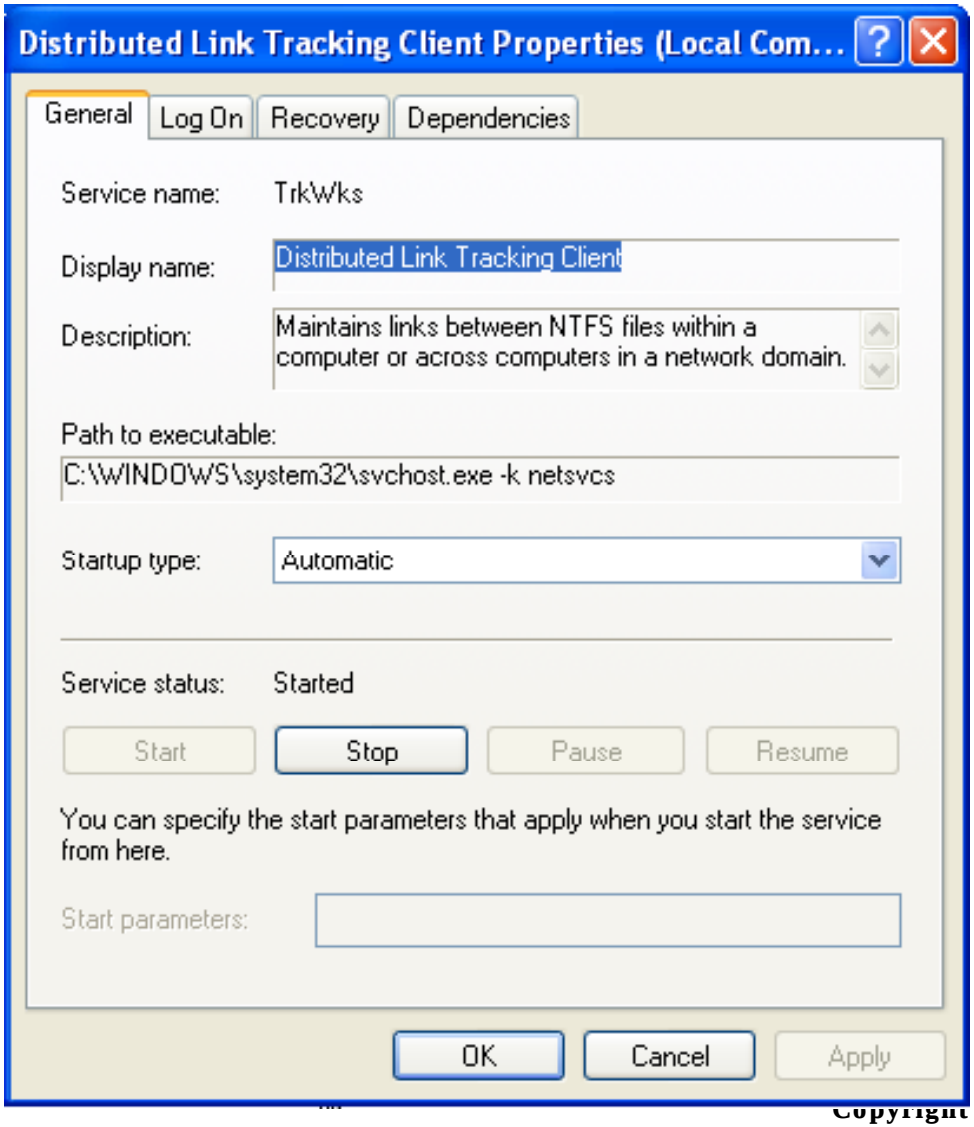
Scenarios involving the **Distributed Link Tracking Server** service require that the client computer have the **DLT_AllowDomainMode** system policy configured for clients that run Windows XP with SP1 or SP2

If the service is disabled, links are not maintained or tracked

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Distributed Link Tracking Client (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Distributed Link Tracking Server

The service store information on the files moved between volumes is tracked

Enabled

- The service runs on every domain controller.
- Enable the **DLT_AllowDomainMode** system policy for Windows XP

Disabled

- The links maintained by the **Distributed Link Tracking Client** service will slowly become less reliable
- This service is disabled by default in Windows 2003

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

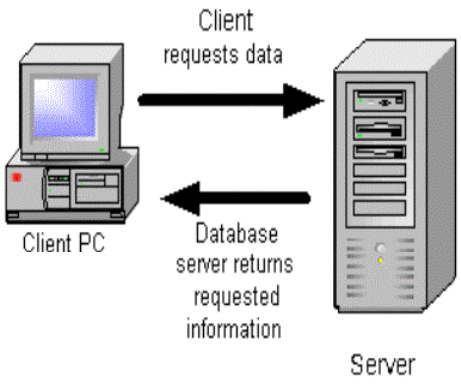
Distributed Link Tracking Server (Cont'd)

This service enables **Distributed Link Tracking Client** service which tracks linked documents in the same domain

This service is disabled by default

This service should be enabled on all the domain controllers

When ever Windows is upgraded this service must be enabled manually



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Distributed Transaction Coordinator

Transactions distributed across many computers and/or resource managers should coordinate with this service

If COM+ has to be used to configure transactional components then this service is useful

It is by default installed and active

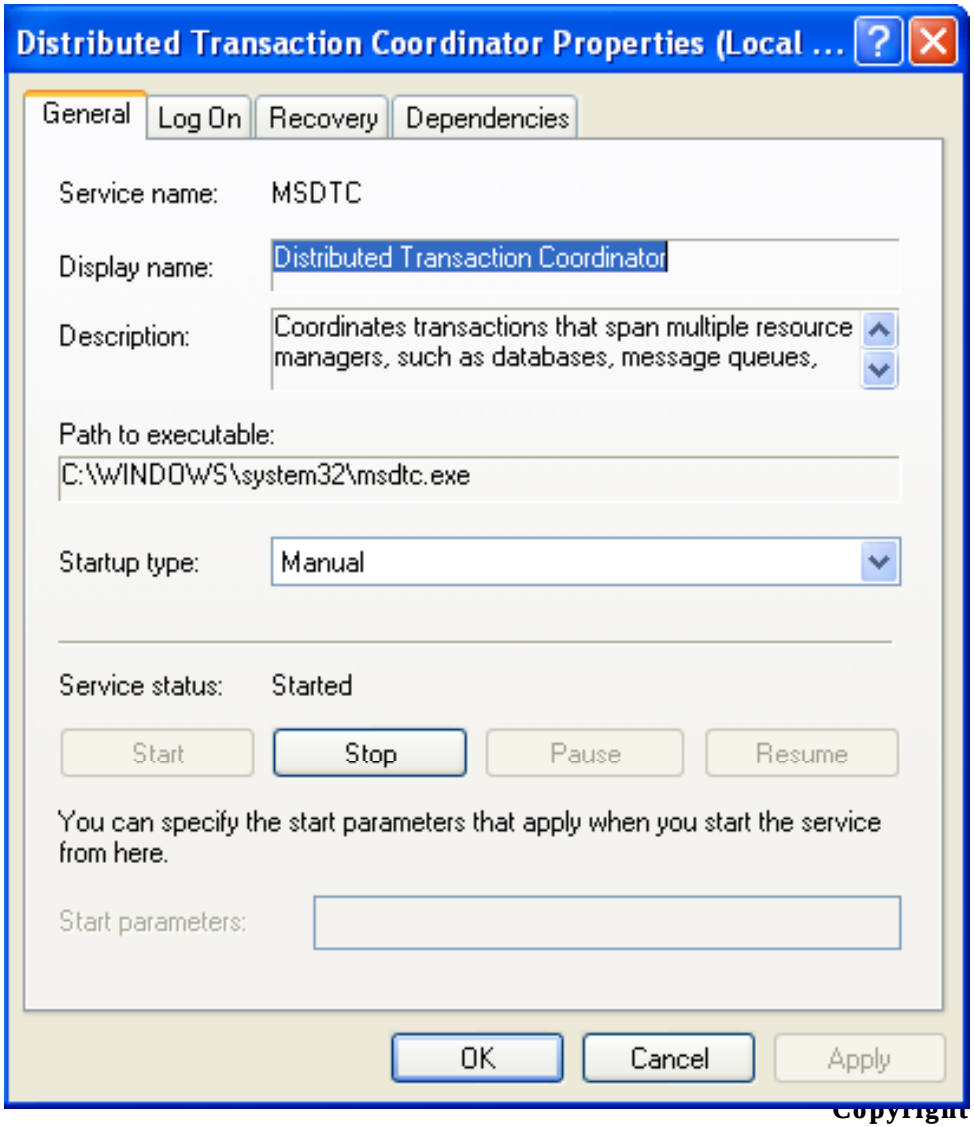
Transaction uses this service will stop if this service is stopped

Applications making use of these transaction services may affect by disabling this service

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Distributed Transaction Coordinator



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DNS Client

This service resolves and caches the DNS names for a computer

This service should be present in every computer performing DNS name resolution, used for locating domain controllers in Active Directory Domain and to locate identified devices using DNS name resolution

The below features are kept into practice by DNS Client:

- System-wide caching. The resources are recorded to the client cache when applications query DNS server. This is used to answer specific queries

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DNS Client (Cont'd)

RFC-compliant negative caching support. Both positive and negative query responses are recorded.

Avoidance of unresponsive DNS servers. The **DNS Client** uses a server search list ordered by preference. The list contains preferred and alternate DNS servers configured for each active network computer. Windows Server 2003 re-order the list as per:

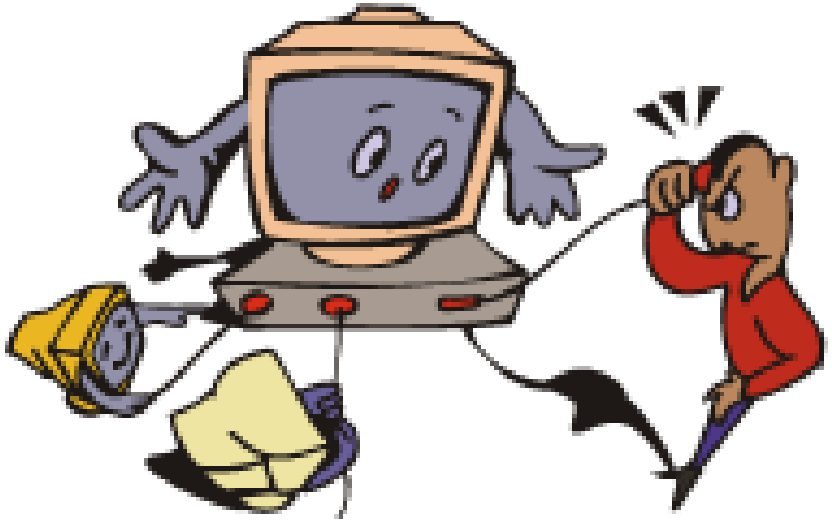
- Preferred DNS servers are given first priority.
- If no preferred DNS servers are available, then alternate DNS servers are used.
- Unresponsive servers are removed temporarily from these lists.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DNS Client (Cont'd)

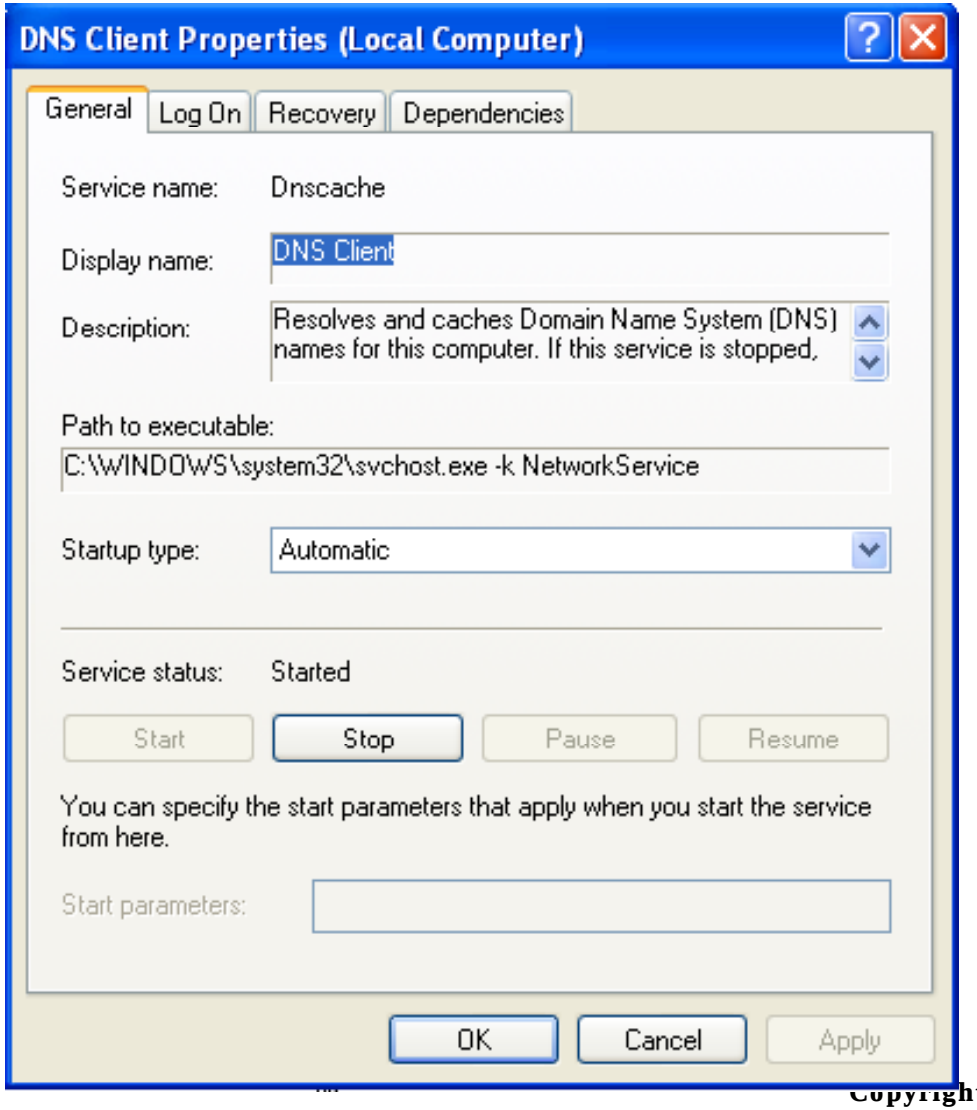
If the service is disabled, DNS names can not be resolved or might not be able to locate Active Directory domain controllers and users may not be able to logon



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DNS Client (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DNS Server

Enabling DNS name resolution is done by this service. It responsibility is to answer questions and update DNS name requests

This service is used to find domain controllers in Active Directory and devices identified by there DNS names

If disabled the DNS updates will not take place

If there is no authoritative DNS server, it is unable to locate domain controllers

This service is installed and activated if Windows server 2003 is made a DNS server

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Error Reporting Service

This service will collect, store and send any unexpected application errors to Microsoft

Error reporting is authorized to applications which run in non-standard environment, for giving useful information to Microsoft for debugging the errors

This feature can be configured on deciding the type of errors to send

If an error occurs a display message is given with error codes and stops the running application

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Error Reporting Service (Cont'd)

Configure the reporting service as:

- When an error occurs it can send the report to Microsoft
- It can prompt the administrator to send the report to Microsoft

Program errors and abnormal shutdown errors are different

This service is to check the Quality control process of an application, and rectify the generated errors in next version

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

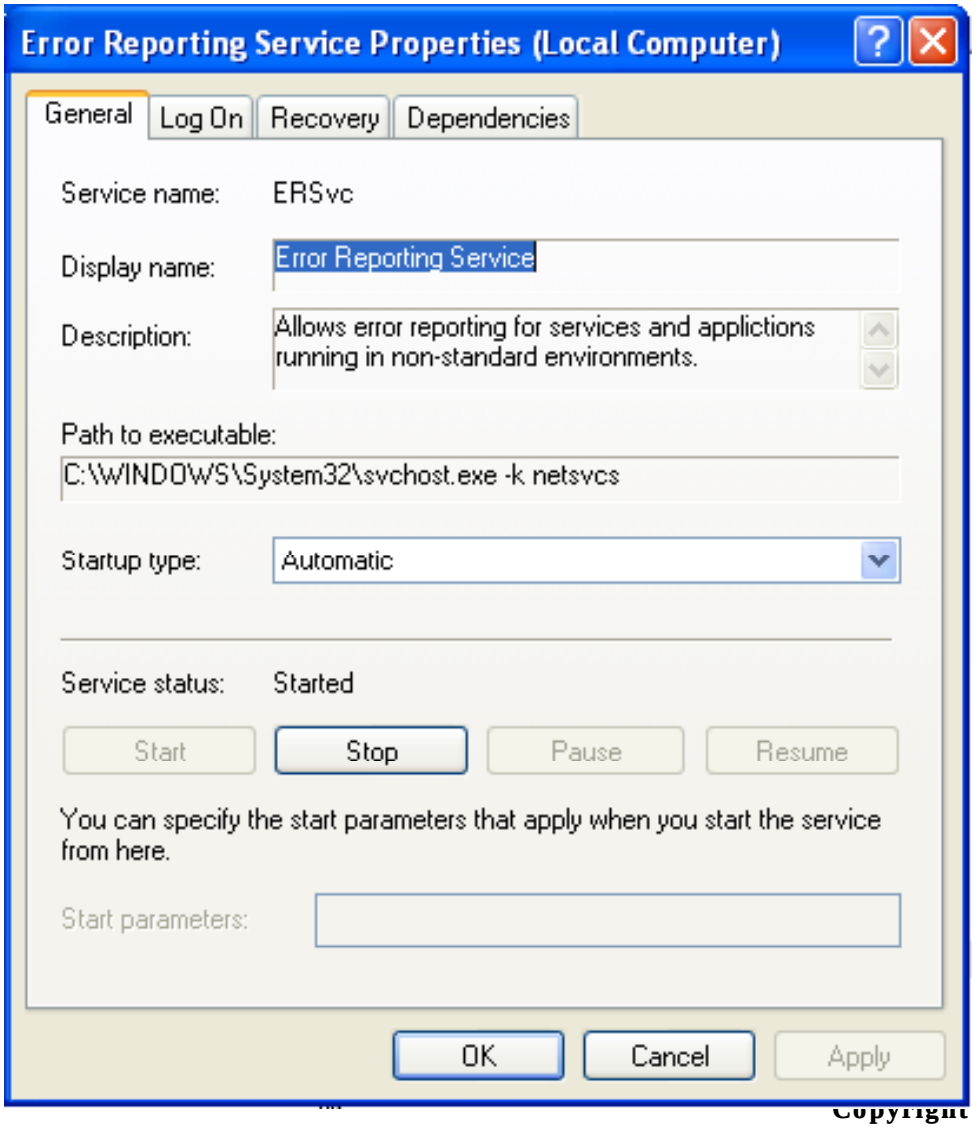
Error Reporting Service (Cont'd)

If disabled, the error reports are not sent to Microsoft

This service is installed and run by default

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Error Reporting Service (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Event Log

The service start event log messages initiated by Windows based programs and components in Event Viewer

These messages enclose information which helps to solve any problem

You can view the log with the help off Event Log APIs or MMC Event Viewer snap-in

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Event Log (Cont'd)

Computers with Windows Server 2003 generate event as:

- Application log. Records application program events
- Security log. Records events related to valid and invalid logon attempts and resources
- System log. Records events that for Windows components

A domain controller in Windows Server 2003 records events as:

- Directory service log. Records events related to Active Directory
- File Replication service log. Records Windows File Replication service events

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Event Log (Cont'd)

Computer in Windows configured as DNS Server an additional log:

- DNS Server log. Contains events logged by Windows DNS service

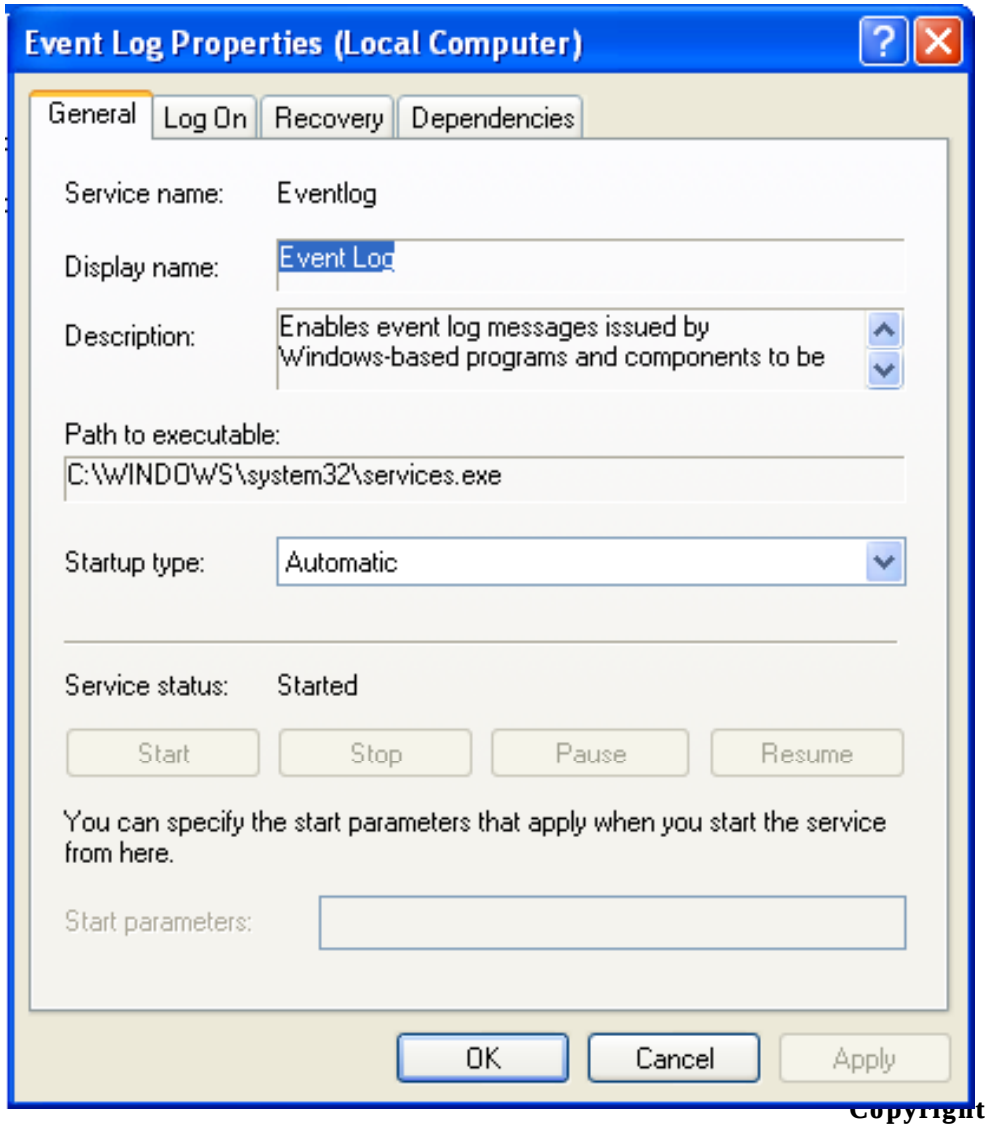
If disabled, it is impractical to track events, which may minimize the possibility to solve the computer problem

Neither security events are audited and nor previous event logs are viewable

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Event Log (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Fast User Switching Compatibility

For the applications requiring assistance in multiple user environments, the management process is provided by this service

This feature allows multiple users to change the session easily without logging off

This service performs one of four different actions when a specific problematic program when the service is activated:

- With Type1 programs - A first instance of a program is closed when second is launched, for this you need administrator privileges

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Fast User Switching Compatibility (Cont'd)

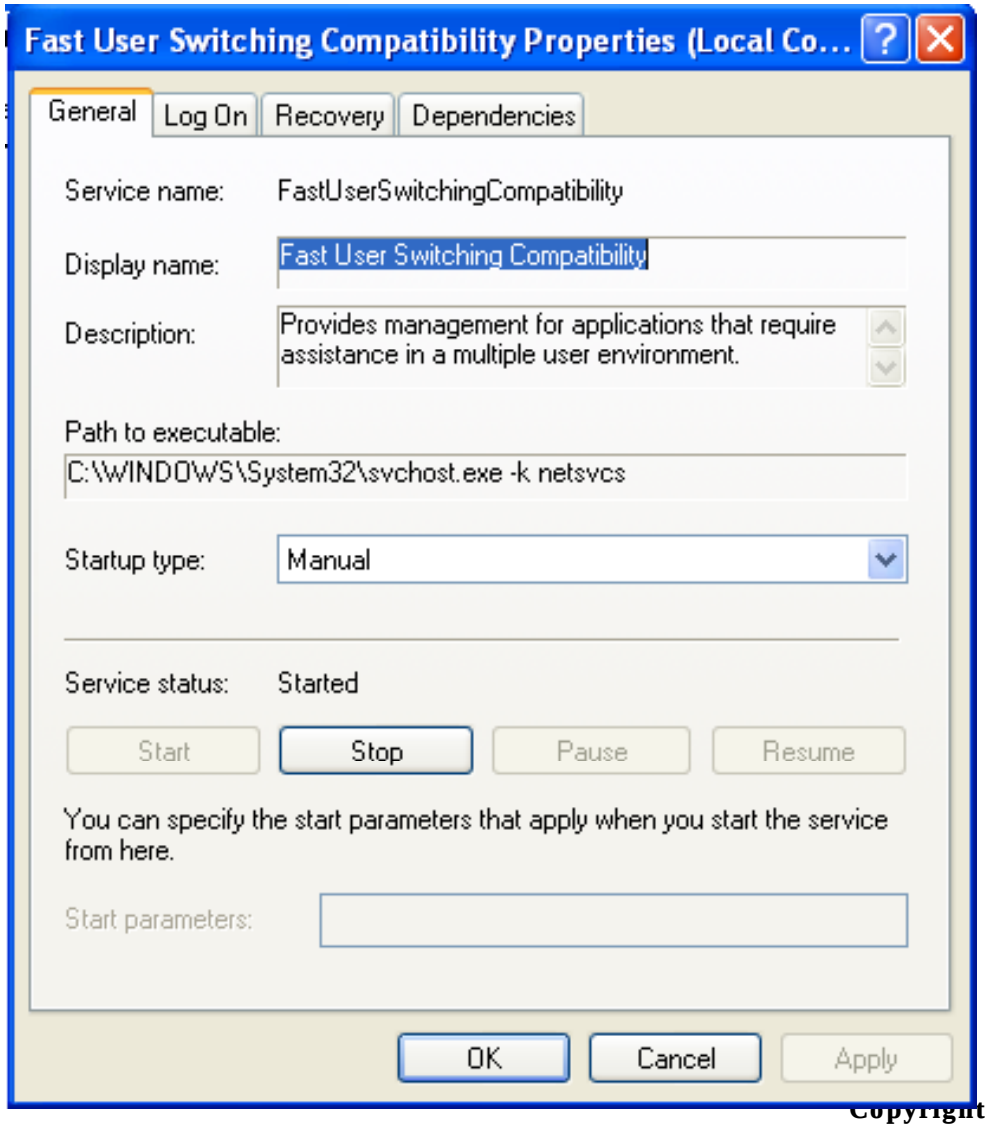
With Type 2 programs – Service closes the programs when the session is disconnected

With Type 3 programs –Closes the programs on disconnecting the session and restarts them when the user logs on to the session

With Type 4 programs – Closes the programs when any other user logs on

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Fast User Switching Compatibility (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Fax Service

This service a Telephony Application Programming Interface (TAPI) gives fax capabilities to user computers. Users can send fax using it

The below features are offered by this service:

- Send and receive faxes
- Track and monitor fax activity
- Inbound fax routing
- Server and device configuration management
- Archiving of sent faxes

If the print spooler or telephony service is disabled this service will not start successfully

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

File Replication

This service allows files to be copied and maintained at the same time on various servers automatically

The FRS is automatic replication service in Windows 2000 and the Windows Server 2003 family and it replicates the contents of the System Volume (SYSVOL) between all domain controllers in a domain

If disabled, neither replication nor synchronization of data will occur

The service is by default installed but the startup state is configured as **Manual**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

File Server for Macintosh

The service allows storing the access files in Macintosh computers running on Windows Server 2003

This service is by default not installed or started

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

FTP Publishing Service

- This service gives FTP connectivity and administration through Microsoft Internet Information Server (IIS) snap-in
- It contains capability to throttle bandwidth, security accounts, and extensible logging
- It allows users to access only their files on an FTP site
- If disabled, the server losses the capability of an FTP server
- This service is not installed automatically

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Help and Support

Running the help & support centre applications to run, supporting the application, enabling communication between client application and help data are allowed by this service

Data about help topic and access to database in provided

If it is configured to manual, the service is started when Help and Support Centre is accessed from the desktop

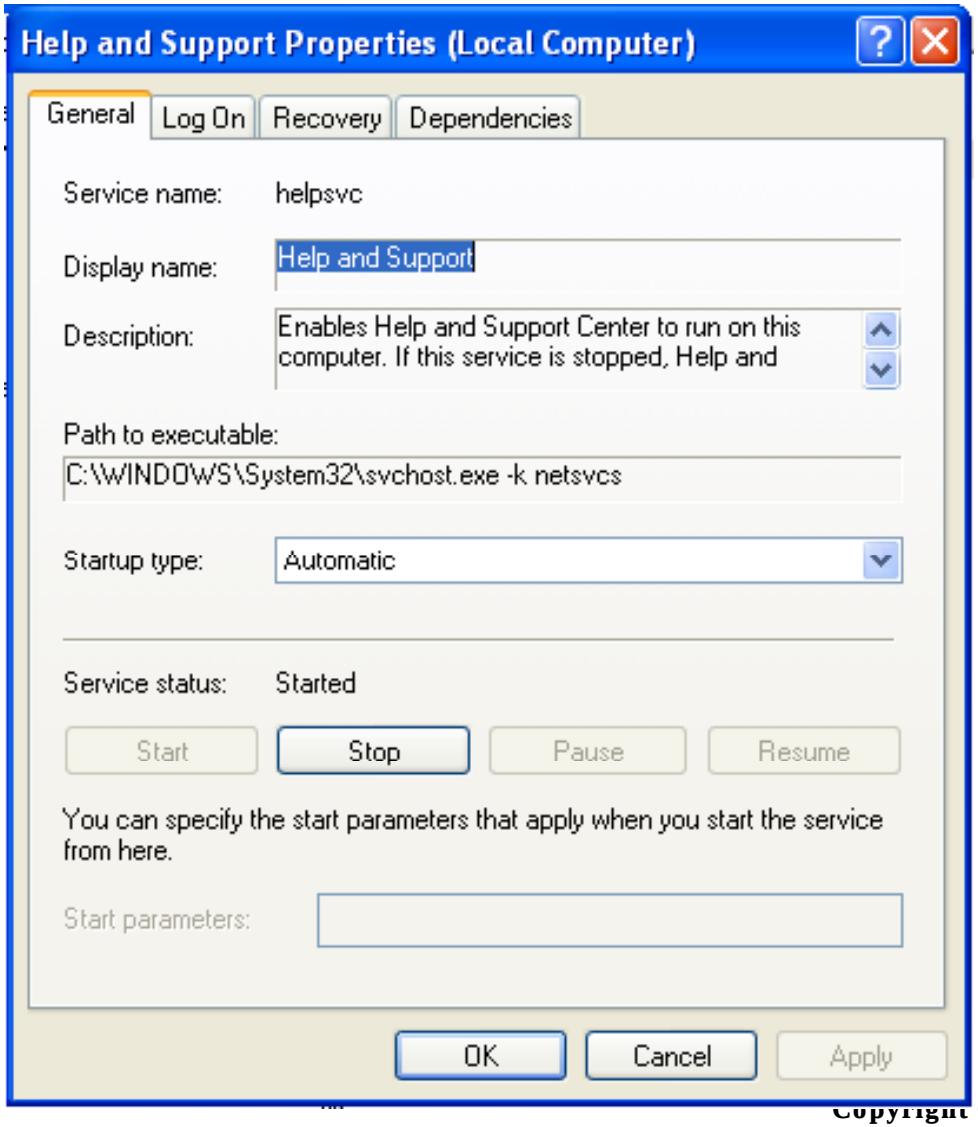
If disabled, a message will be displayed as: **Windows cannot open Help and Support because a system service is not running**

On the other hand, users can see *.HLP and *.CHM files located in Windows\Help folder

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Help and Support

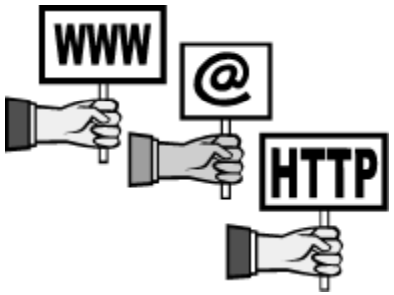


Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

HTTP SSL

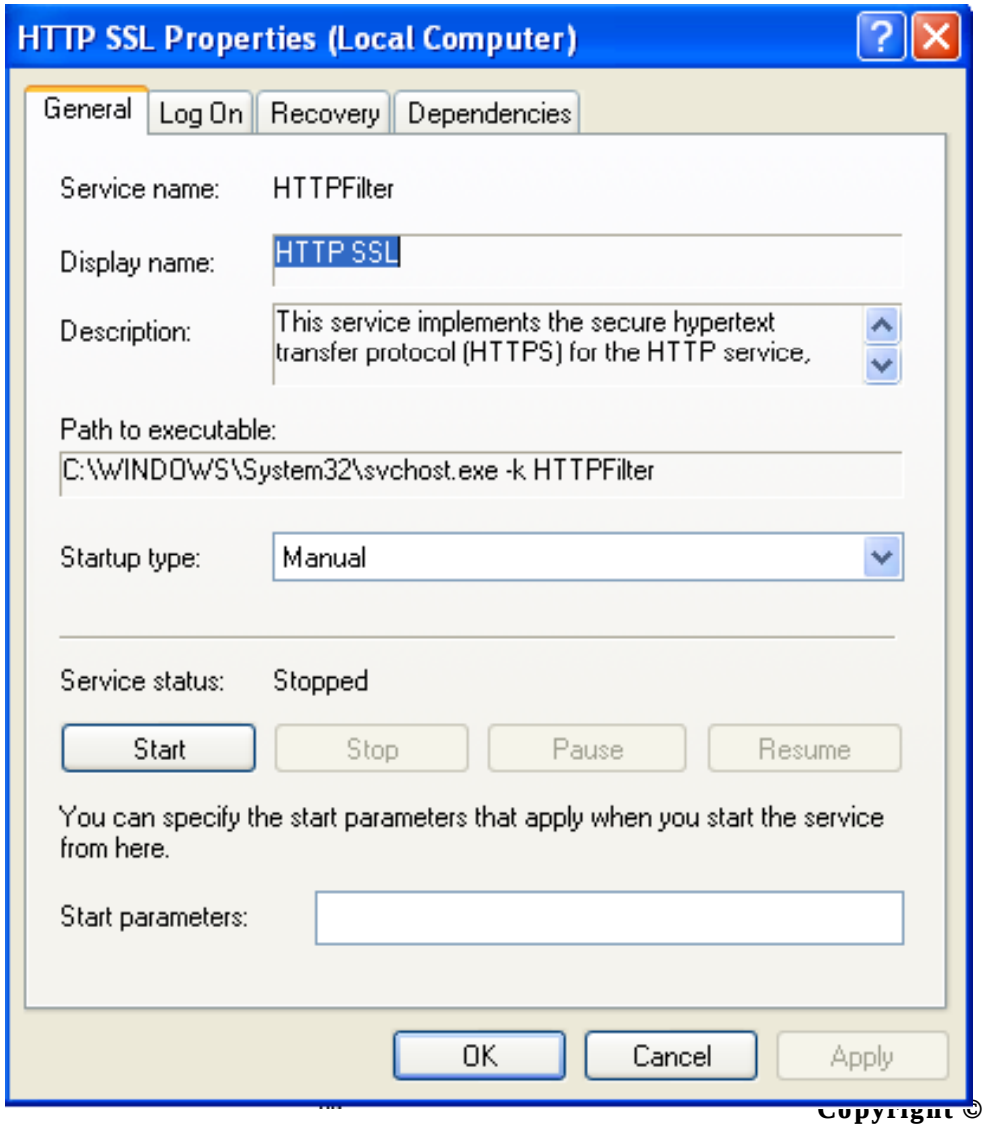
HTTP SSL:

- This service is starts IIS for Secure Socket Layer (SSL) functions; it is an open standard which sets a secure channel for preventing interception of vital information
- If disabled, SSL functions are not performed by IIS
- The service is installed with IIS



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

HTTP SSL



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Human Interface Device Access

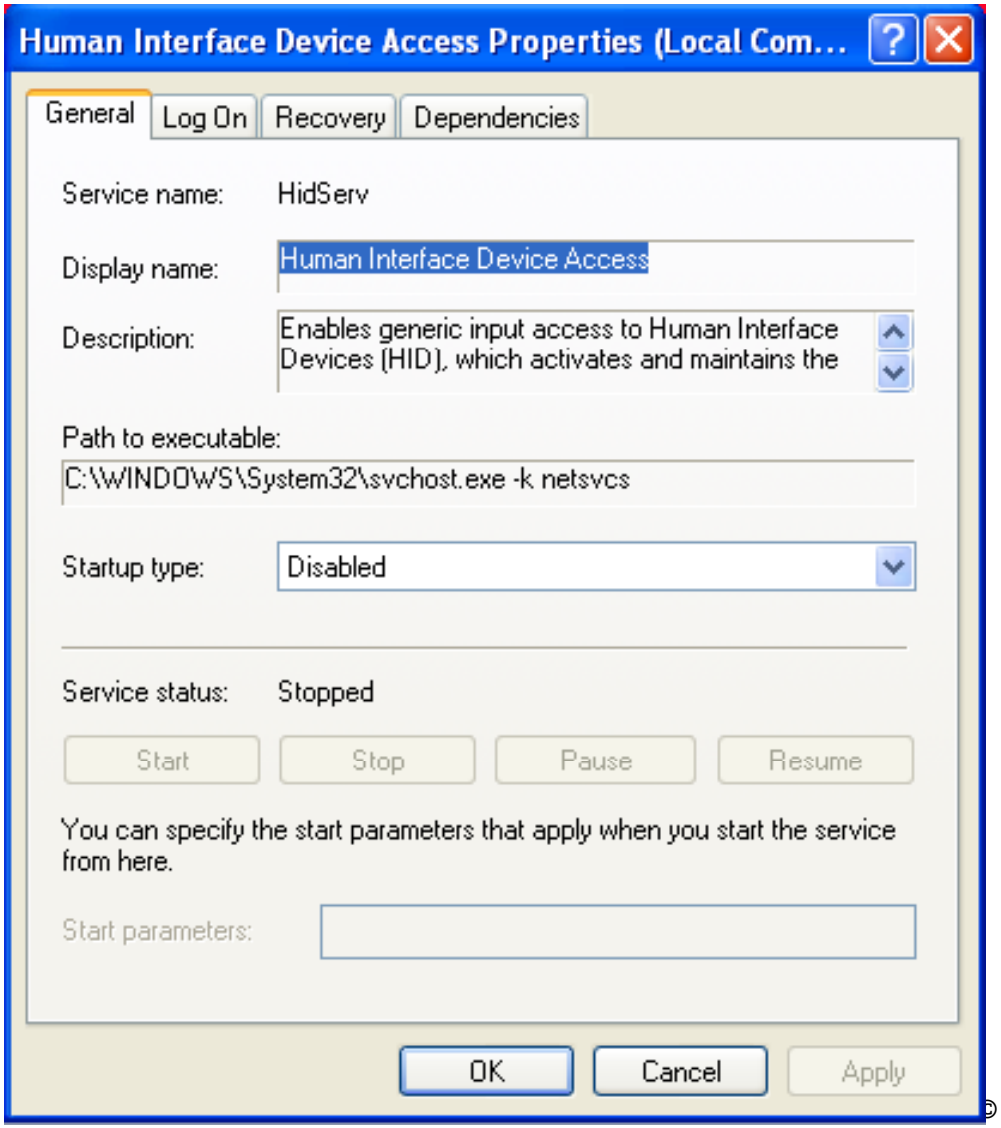
This service input access to Universal Serial Bus (USB) devices

This is installed and started by default in Windows XP and Windows Server 2003

If disabled, the hot buttons controlled by it will not work

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Human Interface Device Access



© by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IAS Jet Database Access

The service provides authentication, authorization and accounting assistance through Remote Authentication Dial-in User Service (RADIUS) protocol

The above service can also be obtained by Internet Authentication Services (IAS)

IAS is used as a RADIUS proxy used for routing RADIUS messages between its clients and servers. IAS acts as a switch or router through which the accounting messages flow

It exists only in 64-bit version of Windows

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IAS Jet Database Access (Cont'd)

A RADIUS infrastructure has following components:

- Two IAS jet databases
- las.mdb – Configure IAS
- Dnary.mdb – To validate dictionary used by RADIUS for vendor specific attributes

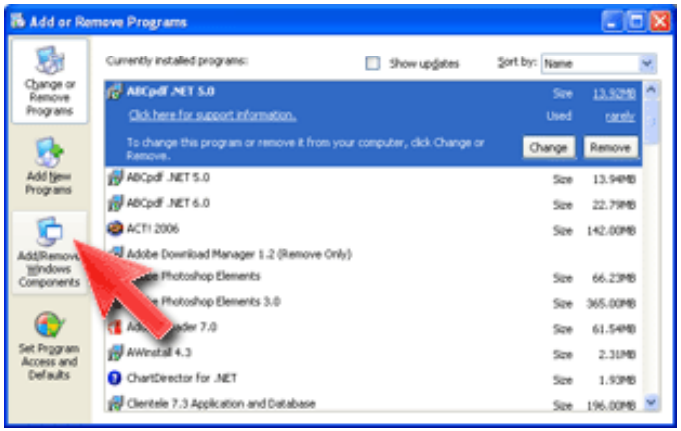
If disabled, remote network access needed for user authentication is not available, Service is not installed by default

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IIS Admin Service

- Administration of IIS components is allowed by this service
- If disabled, it is not possible to run Web, FTP, NNTP, or SMTP sites
- This service is installed by default in Windows 2000
- IIS components are installed Control Panel -> Add/Remove or Configure Your Server



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IMAPI CD-Burning COM Service

This service manages CD creation and CD-Recording through the Image Mastering Applications Programming Interface (IMAPI) COM interface when user requests through Internet Explorer (IE)

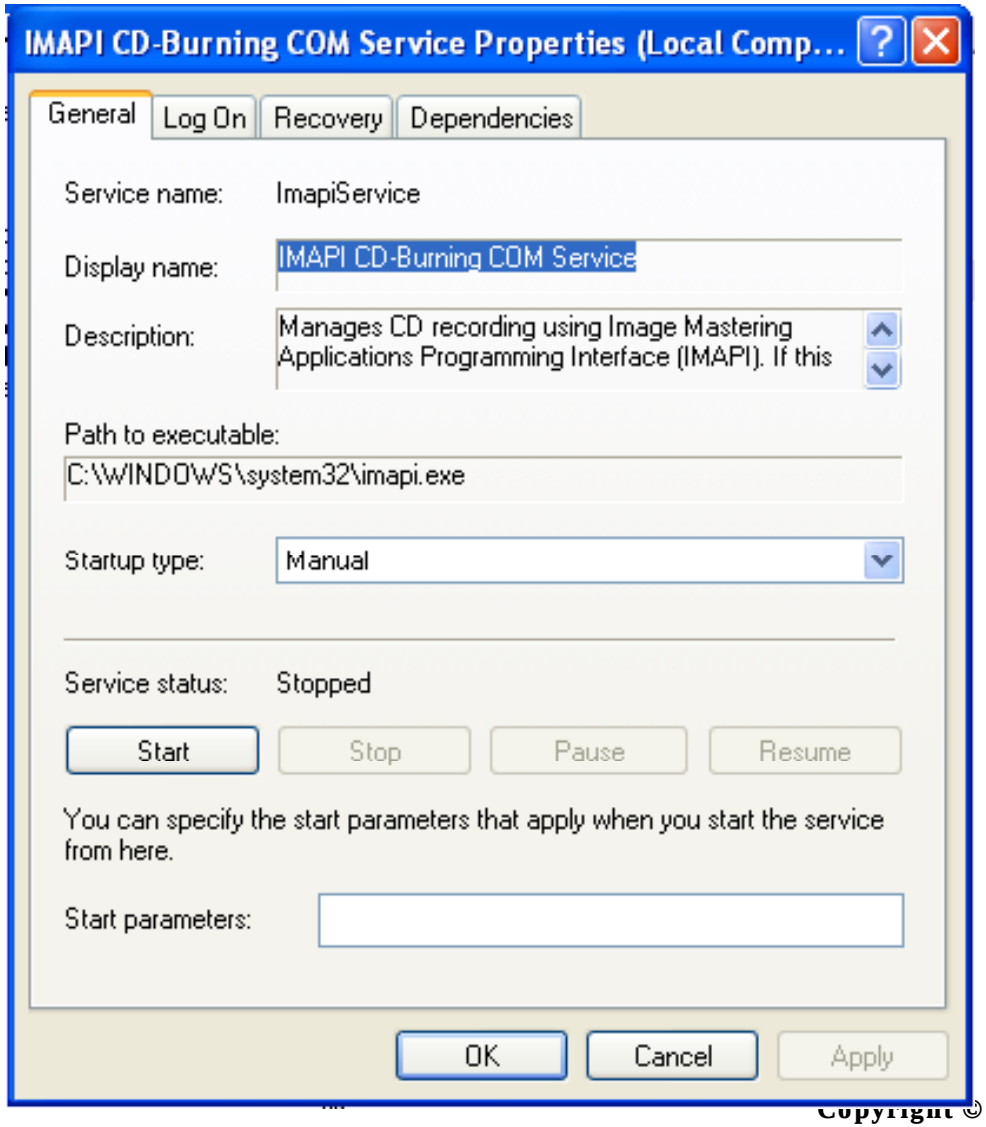
If disabled, CD's can not be recorded in Windows XP and Windows Server 2003. But using a third party application you can write the CD's

The service is installed by default on Windows XP, but only starts when user requests the service

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IMAPI CD-Burning COM Service



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Indexing Service

This service creates a querying language by indexing the files on local and remote computers, and also supports quick document search capability

This service maintains the file indexes every time the file is created, modified or deleted

This service is set to manual, by default

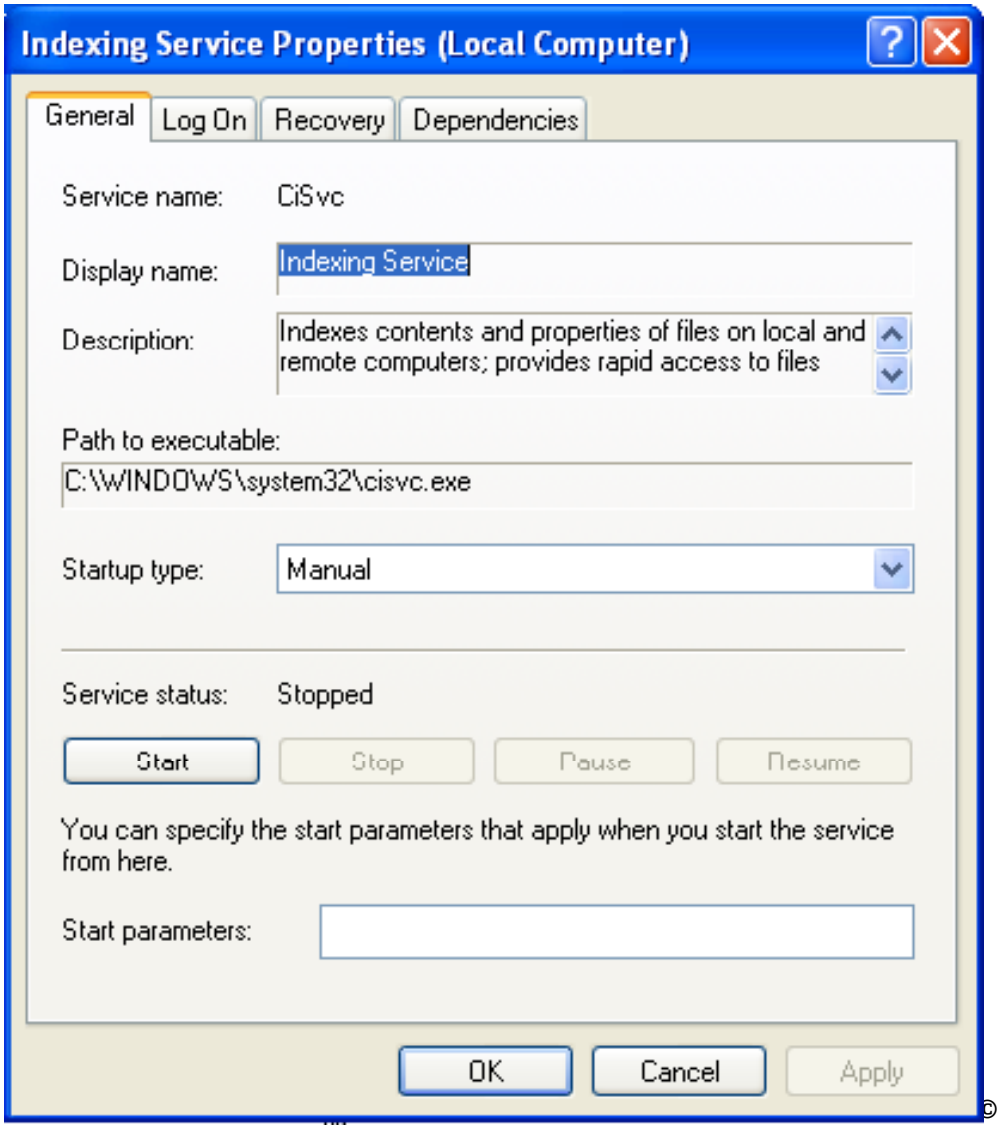
By using MMC index snap-in you can configure the service to index at non-idle times

If disabled, text base services will slow down

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Indexing Service



© by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Infrared Monitor

- Infrared connections are used to share files and images by enabling this service
- Windows XP has it by default, if an infrared device is detected at the time of installation
- This feature is not available Windows Server 2003 Web Enterprise, or Datacenter Server editions
- If disabled, files and images are not shared through infrared connection

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Authentication Service

The IAS service carries out centralized authentication, authorization, audit, and accounting of users connected on to the network

IAS implements the IETF standard RADIUS protocol, for enabling heterogeneous network access equipment

If disabled, the made authentication requests are failed over the back IAS server

This service must installed manually

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Intersite Messaging

Inter site Messaging:

- The service exchanges messages between computers running on Windows Server site. It is used as a mail based replication between sites
- The service sends and receives request to a transport add-in DLL file, then the message is sent to the destination computer
- If disabled, no message is exchanged, replication will not work, and no suite routing data is calculated
- It is installed by default in Windows 2003

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IP Version 6 Helper Service

It gives Internet protocol version 6 (IPv6) connectivity over an Internet Protocol version 4 (IPv4) network

The IPv6 (6to4) protocol is a new network layer protocol. It solves many IPv4 problems with regarding to address depletion, security, auto-configuration, and extensibility

6to4 is a tunneling technique in RFC 3056. It uses a global address prefix of 2002

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IP Version 6 Helper Service (Cont'd)

This service also provides 6over4, also known as multicast tunneling

If disabled, the computer will only have IPV6 connectivity

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IPSec Policy Agent (IPSec Service)

The service gives end-to-end security on TCP/IP network between client and server

It manages IPsec policy, starts the Internet Key Exchange (IKE) and coordinates IPsec policy settings with the IP security driver

The service is controlled through the commands NET START or NET STOP

IPsec operates on IP layer transparent to other operating system services. It also contains packet filtering and negotiate security

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IPSec Policy Agent (IPSec Service) (Cont'd)

Configure IPsec to:

- Packet filtering with actions to permit, blocks, or negotiate security
- Negotiated trust and secure IP communication. The IKE protocol authenticates sending and receiving of data packetsover this policy setting
- Protect IP packets with IPsec secure formats that provide cryptographic integrity, authenticity, and (optionally) encryption of IP packets
- Secure end-to-end connections through IPsec transport mode
- Secure IP tunnels through IPsec tunnel mode

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IPSec Policy Agent (IPSec Service) (Cont'd)

IPsec provides security for Layer Two Tunneling Protocol (L2TP) VPN connections

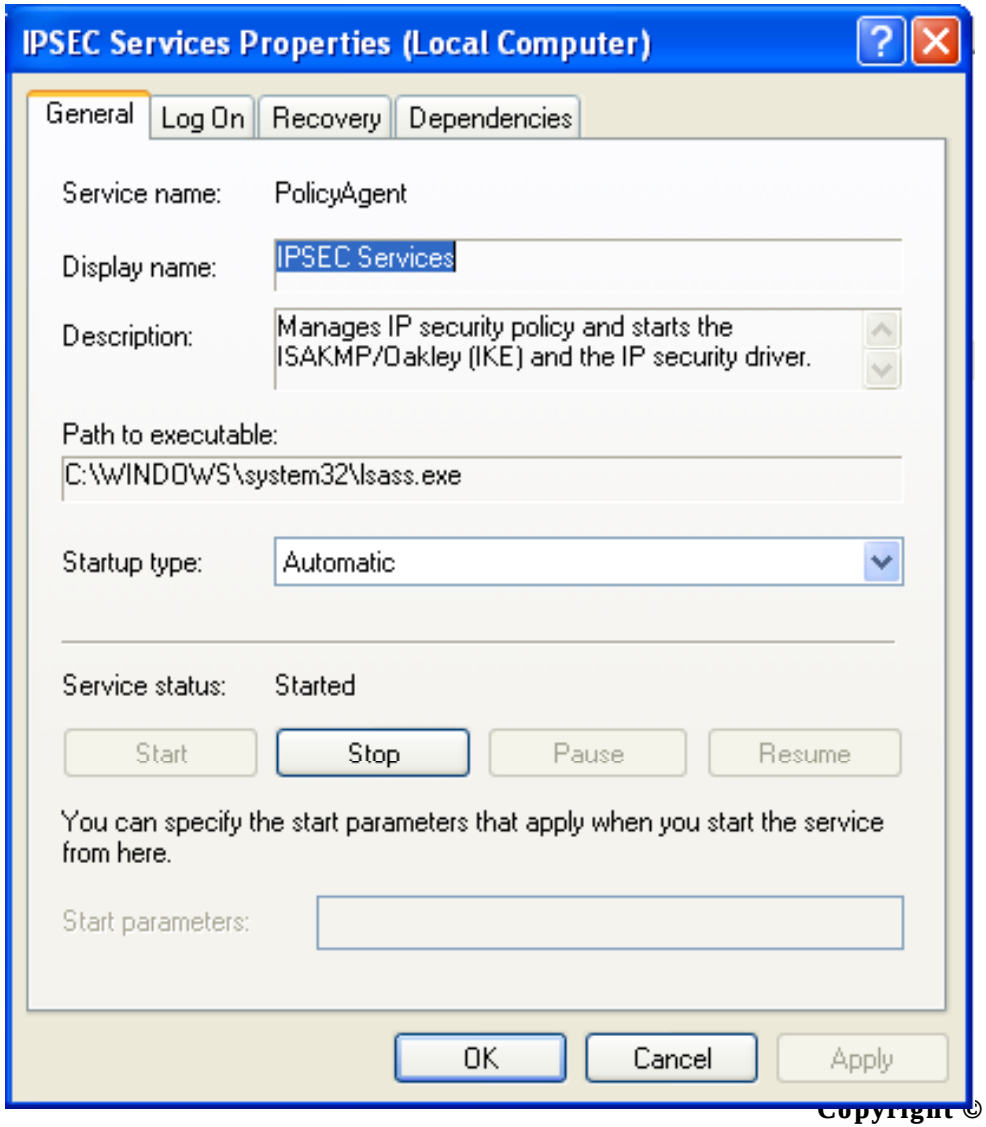
If disabled, it will impair TCP/IP security between clients and servers on the network

This service is installed and activated by default on Windows Server 2003 and Windows XP

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IPSec Services



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Kerberos Key Distribution Center

The service enables users to logon to the network and authenticate with Kerberos v5 authentication protocol

The Kerberos Key Distribution (KDC) provides two services:

- **Authentication Service**. Issues ticket-granting tickets (TGTs) for connection to the ticket-granting service in its own domain or in any trusted domain. The TGT is used by the time it expires
- **Ticket-Granting Service (TGS)**. Issues tickets for connection to computers in its own domain. The ticket can be reused until it expires

If disabled, resources cannot be accessed as users can not logon

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

License Logging Service

The service monitors and records license information of client access

This service works with a part of operating system (Ex: IIS, Terminal Services) and products which are not a part of operating system

If disabled, the licensing will be compulsory but no monitoring is done

This service s disabled by default

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Logical Disk Manager

The service detects and keeps track the new hard disk drives and transfers the disk volume information to **Logical Disk Manager Administrative Service** for configuration

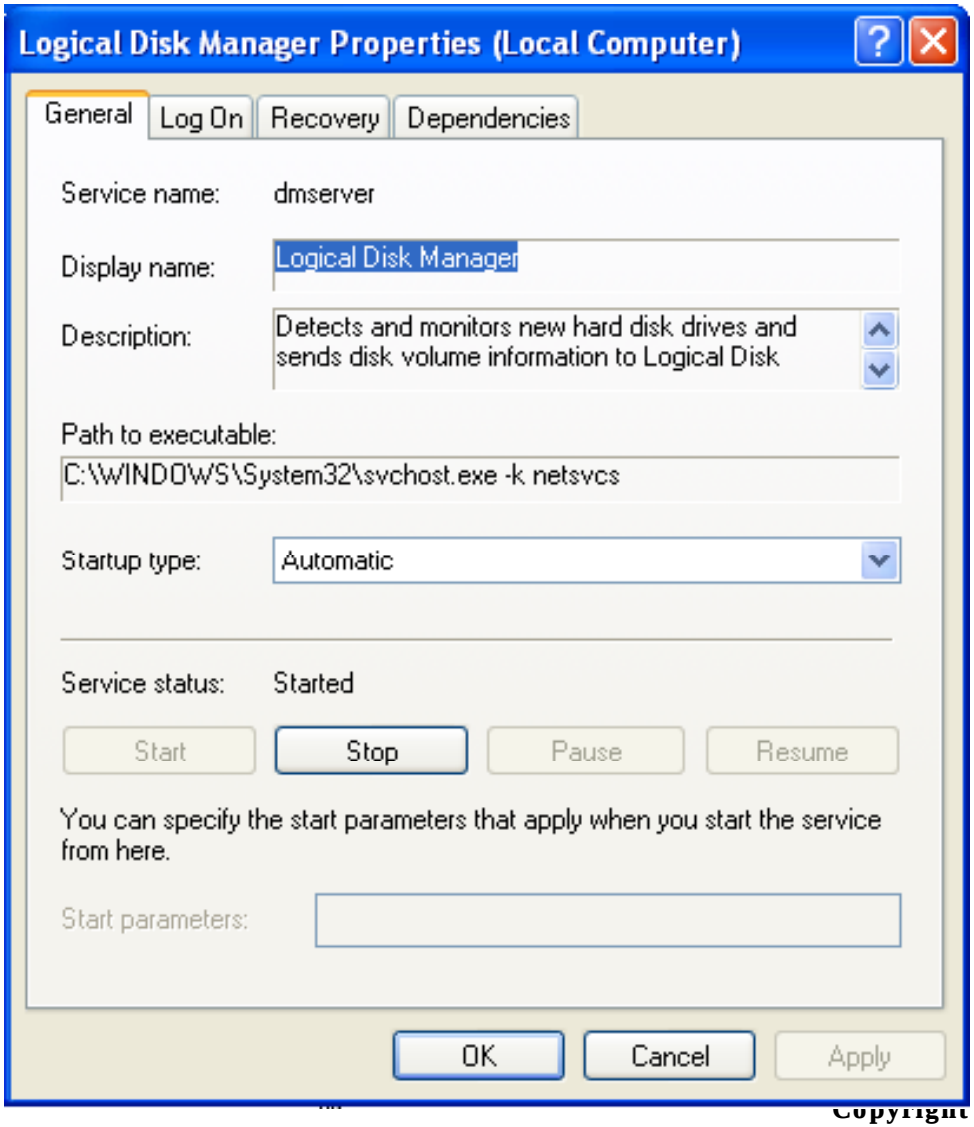
This service is used to tracks plug and play service

If disabled, disk status and configuration information will not be captured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Logical Disk Manager



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Logical Disk Manager Administrative Service

The administration services for disk management request and configuring hard disk drives and volumes is done by this service

The service is started when ever a new hardware is detected or the MMC Disk Management snap-in or the Diskpart.exe tool are opened

The service only runs for configuration processes and stops

If disabled, when ever you try to configure a disk the following error message is displayed,

- Unable to connect to Logical Disk Manager Service

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Machine Debug Manager

Debugging for various applications (local or remote) is handled by this service

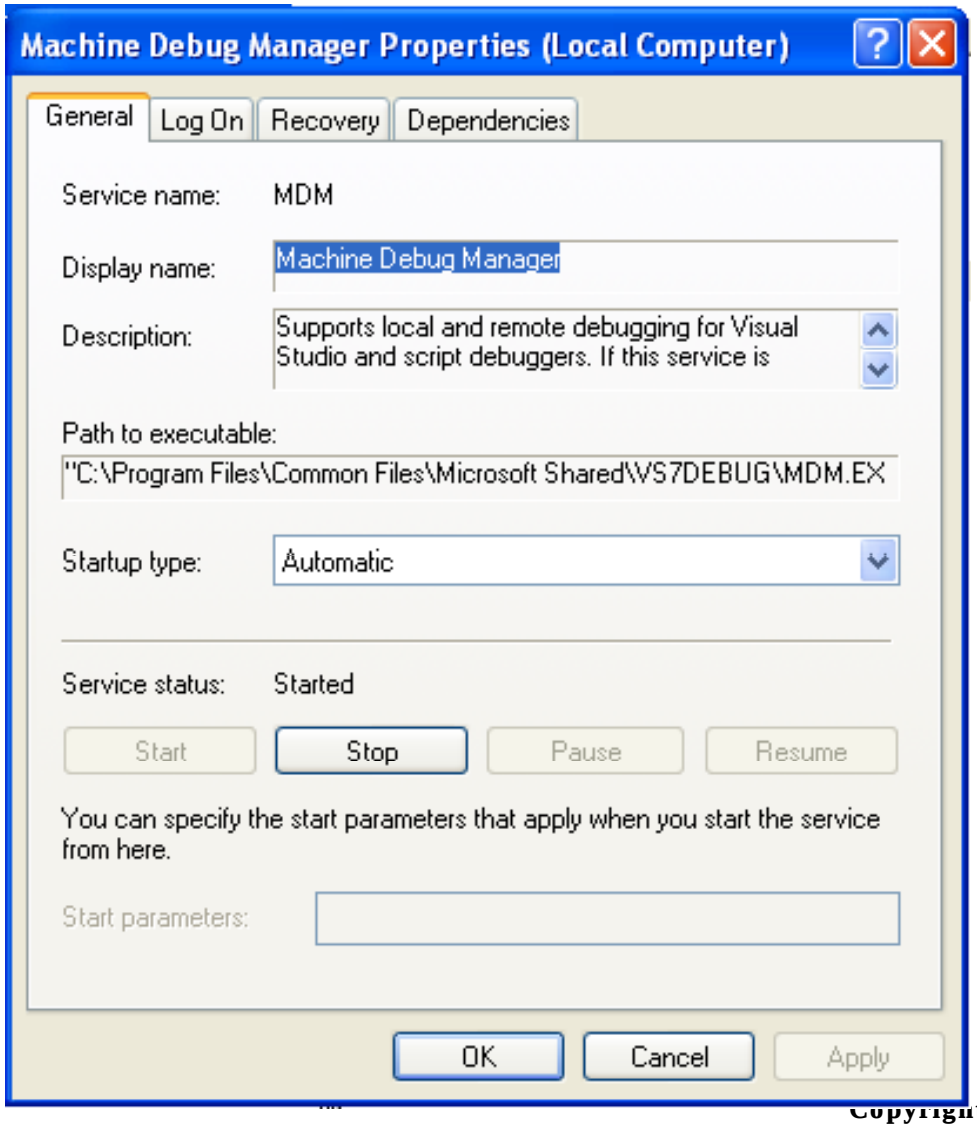
If disabled, any attempts made for debugging are failed and shows an error message as

- Unable to start debugging. The Machine Debug Manager Service is disabled

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Machine Debug Manager



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Message Queuing

The service can be used to create messaging applications in Windows; it acts as a messaging infrastructure and a development tool

The service provides guaranteed message delivery, efficient routing, security, and priority-based messaging

By this reason Microsoft do not recommend this service for Windows XP as an unauthorized user is permitted to connect to the queue in Windows XP version of this service to implement remote read features. By which any user can flush the queue and can create a DoS condition

If disabled, distributed messages will be unviable

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Message Queuing Down Level Clients

This service provides Active Directory access for Windows NT 4.0, Windows 9.x and Windows 2000 clients using Message Queue Service on domain controllers

The routing information in Active Directory is used by this service for security related objects

This service is required in Windows Server 2003 domain controllers which use Message Queuing

If disabled on a domain controller, the Active Directory services for the Microsoft Message Queuing client version 3.0 and earlier are not available

This service has to be installed later in Windows Server 2003

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Message Queuing Triggers

To monitor the messages arrived in Message Queuing service queue; this service offers a rule based system

This service is present in all versions of Windows apart from Windows XP Home Edition. This service is optional

If disabled, applying a rule based monitoring is not carried out automatically

This service has to be installed later in Windows Server 2003 computers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Messenger

This service performs the task of sending/receiving messages from users, admin, Alert services

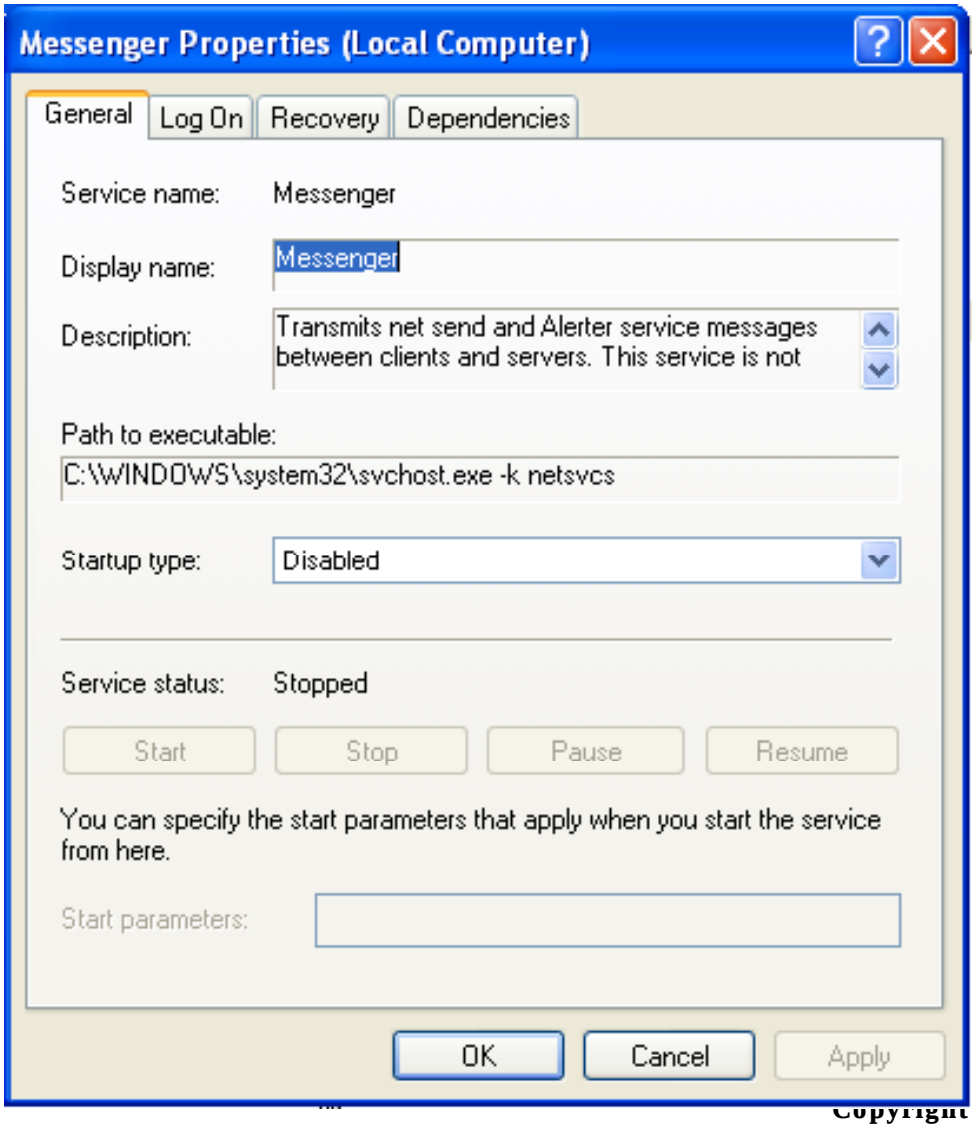
This service is not related to MSN Windows based messenger

If disabled, no messages are transmitted on the network

This service is installed but disabled by default on Windows Server 2003 and Windows XP computers

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Messenger



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft POP3 Service

This service is used for email transfer and retrieval services, to manage email accounts on mail server

When installer the user can connect to the server and get there emails with a email client program with a which supports POP3 protocol

This service works in combination with **SMTP service** to send out going mails

If disabled, email transfer and retrieval service will not work

This service is not installed by default; it has to be done manually

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Software Shadow Copy Provider

The service is used to manage software based shadow copies taken by **Volume Shadow Copy service.**

Two general classes of shadow copies are:

- **Hardware** – A mirror of two or more disks that are split into separate volumes.
- **Software** – Uses a copy-on-write scheme for copying all sectors of a volume that change over time into a differential area on disk.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Software Shadow Copy Provider (Cont'd)

Shadow copies can resolve three classic data backup challenges:

- Back up files opened for exclusive access
- Maintain a computer's availability during the shadow copy.
- Use of the same communications channels as snapshots to facilitate information transfer between application and backup tools

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Software Shadow Copy Provider (Cont'd)

The platform for shadow copies consists of the following:

- A set of shadow copy APIs, which handle application synchronization
- A shadow copy device driver that copies old sectors to a "difference file" when they are first replaced
- Support in the software development communities for the sync and provider APIs

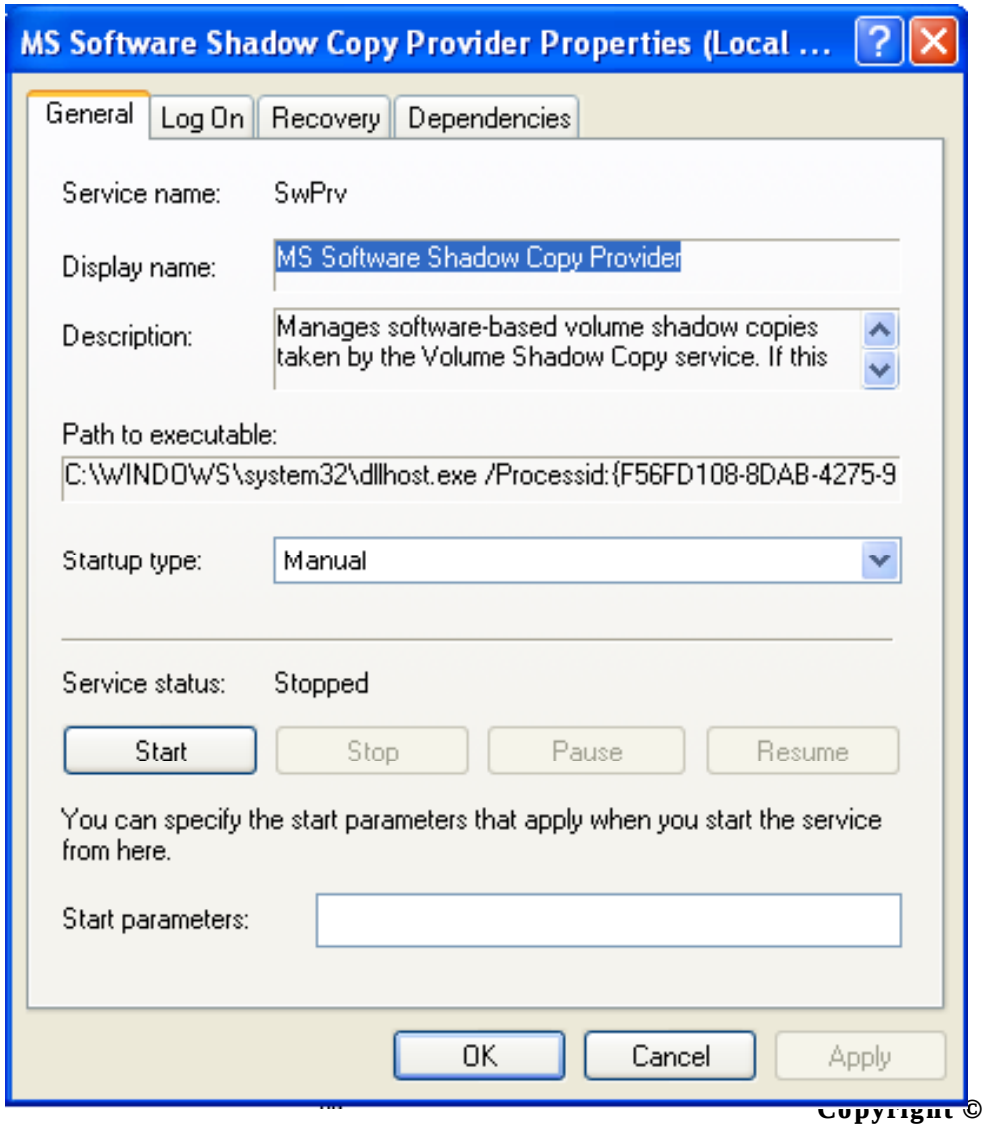
If disabled, shadow copies cannot be managed; by this the back can fail

This service is installed by default but runs when requested in Windows Server 2003

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Microsoft Software Shadow Copy Provider (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

MSSQL$UDDI

- When the Universal Description, Discovery, and Integration (UDDI) feature of the Windows Server 2003 family is installed including this service
- The service allocates resources between multiple users concurrently
- It implements the business rules from stored procedures and triggers for consistency of data
- UDDI is an industry specification for the description and discovery of Web services
- The service has to be installed manually on Windows Server 2003
- If disabled, the UDDI SQL Server database will no longer be available, for querying or accessing data

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

MSSQLServerADHelper

If Microsoft SQL Server and Microsoft SQL Server Analysis Services to publish information in Active Directory are not invoked by the local system account, this service enables them

Only one instance of this service should be there on a computer

This service is not a server based service; it will not handle client requests

This service cannot be disabled, it starts and stops automatically

This service has to be installed manually on Windows Server 2003

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

.NET Framework Support Service

When a process initializes a Client Running Service, this service will inform the subscriber client

This service provides a run-time environment known as the Common Language Runtime (CLR), which manages code execution by providing services

If disabled, there will be no notification given to the user if a .NET application accesses a CLR

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Net Logon

A secure channel is maintained by this service between your computer and domain controller to validate users and services

It passes through the authentication, by transmitting user credentials and receives domain security identifiers and user rights by a secure channel

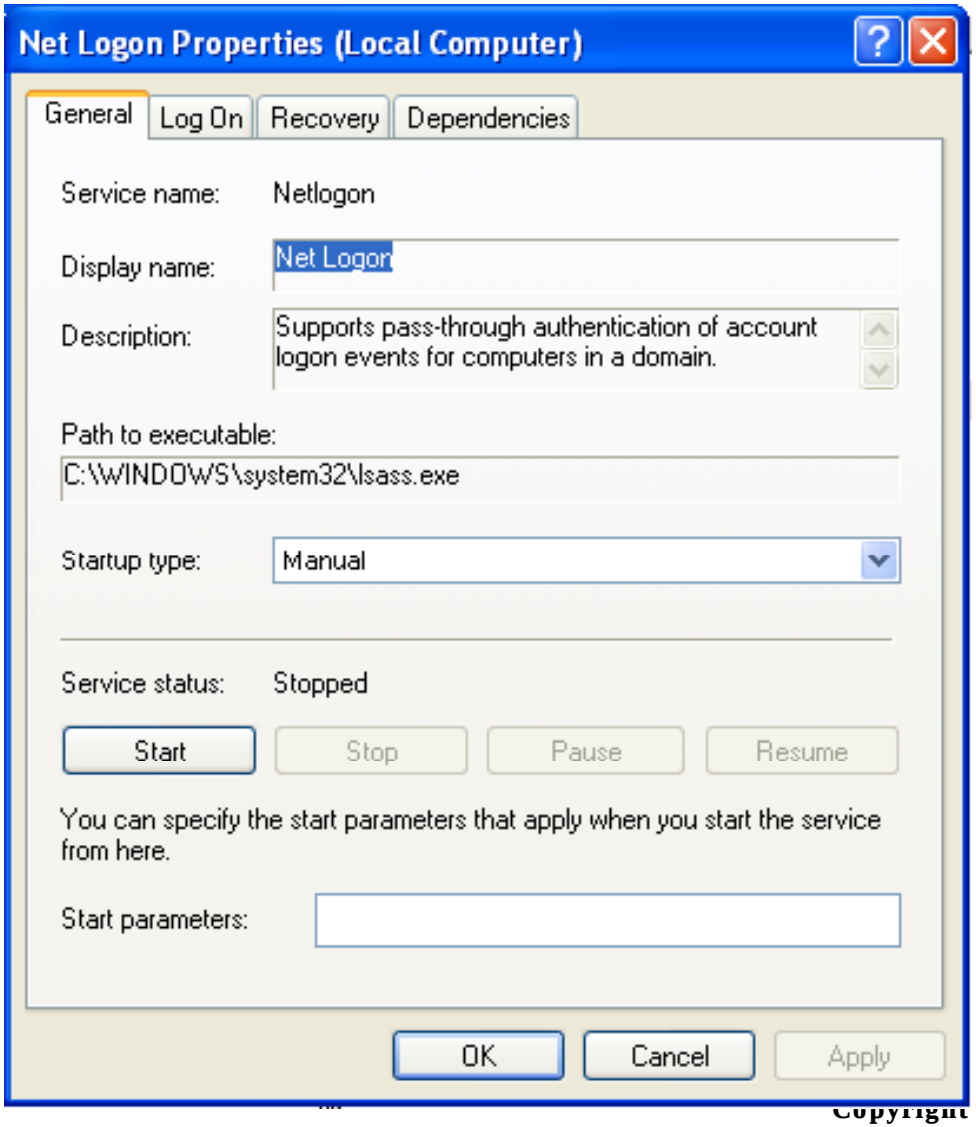
It is installed in Windows Server 2003 and Windows XP computers; it has to be started manually

If disabled, the computer users may not be authenticate and services and the domain controller cannot register DNS records

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Net Logon



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

NetMeeting Remote Desktop Sharing

The service allows authorized users to access your desktop remotely.

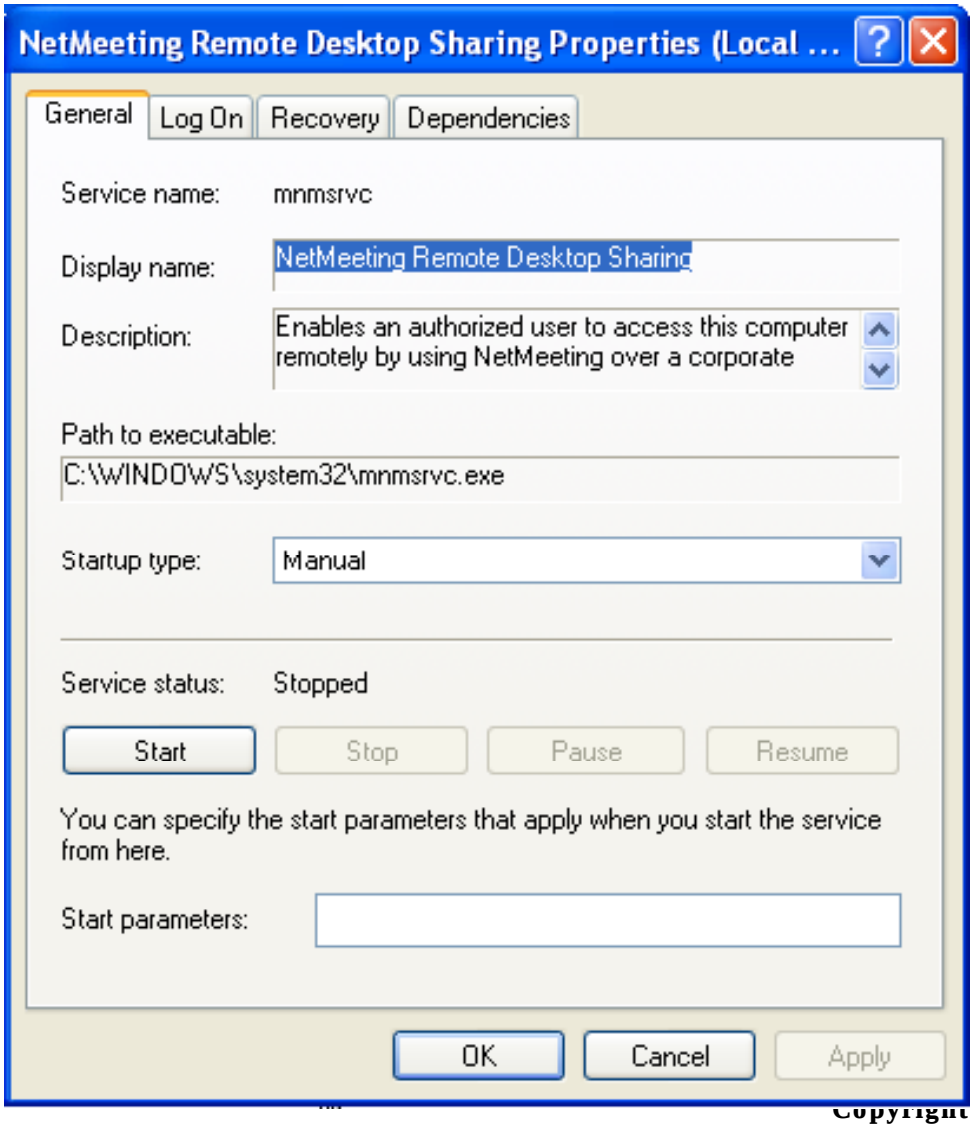
The service is installed and disabled by default, and has to be enabled by the user.

If disabled, the right to access the user desktop remotely may not be provided.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

NetMeeting Remote Desktop Sharing



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Connections

The service is used to manage objects in network connection folder, to view network and remote connections

This service will start automatically, and when stopped the client side configuration of LAN, dial-up and VPN will be not available

If disabled:

- Connections will not display in the Network Connections folder
- Check for Network Location-aware Group Policies will not function properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Connections (Cont'd)

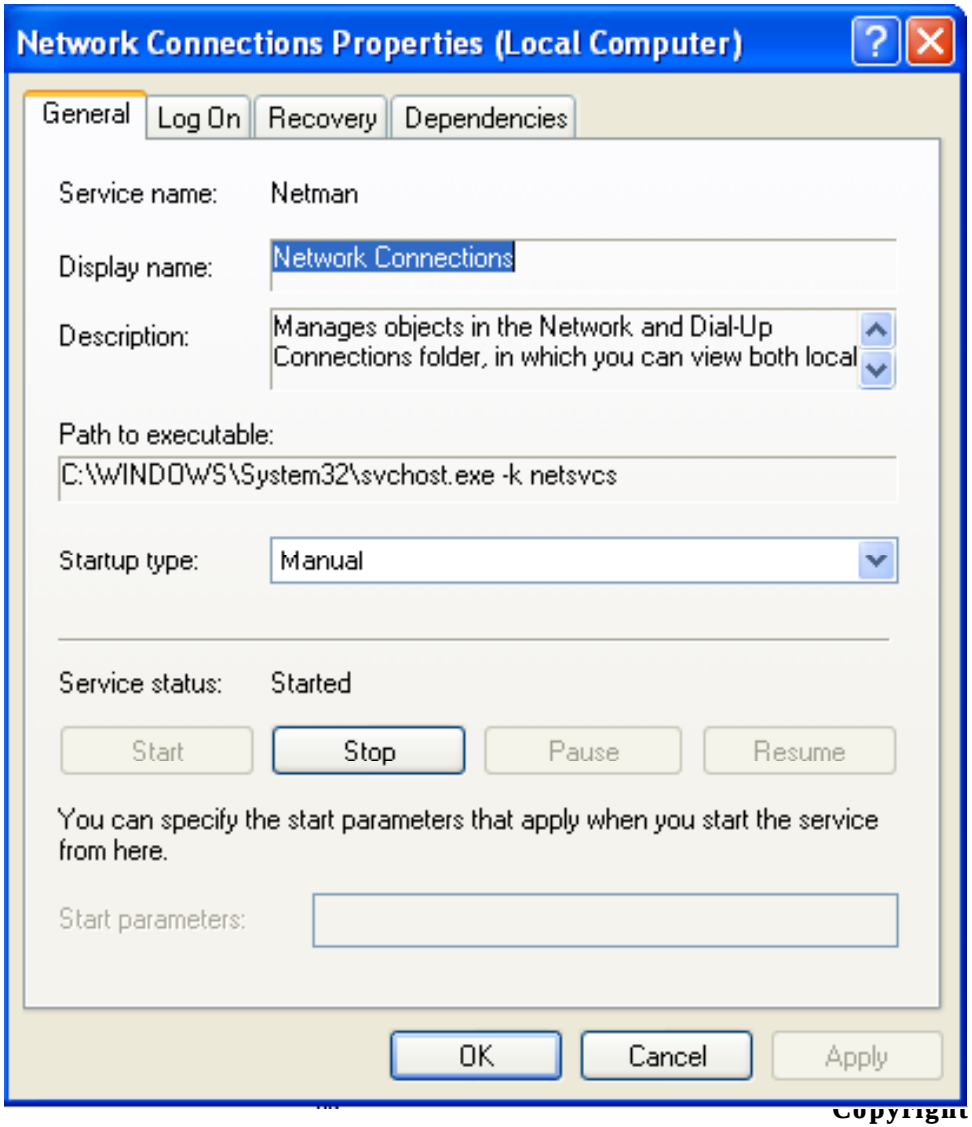
If Disabled:

- Events that pertain to media connects and disconnects will not be received
- Internet connection sharing will not function
- The ability to configure incoming connections, wireless settings, or your home network will be unavailable
- New connections will not be created
- Any services that explicitly depend on this service will not start

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Connections (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network DDE

The service provides network transport and security for Dynamic Data Exchange (DDE) for programs that run on the same computer or on different computers

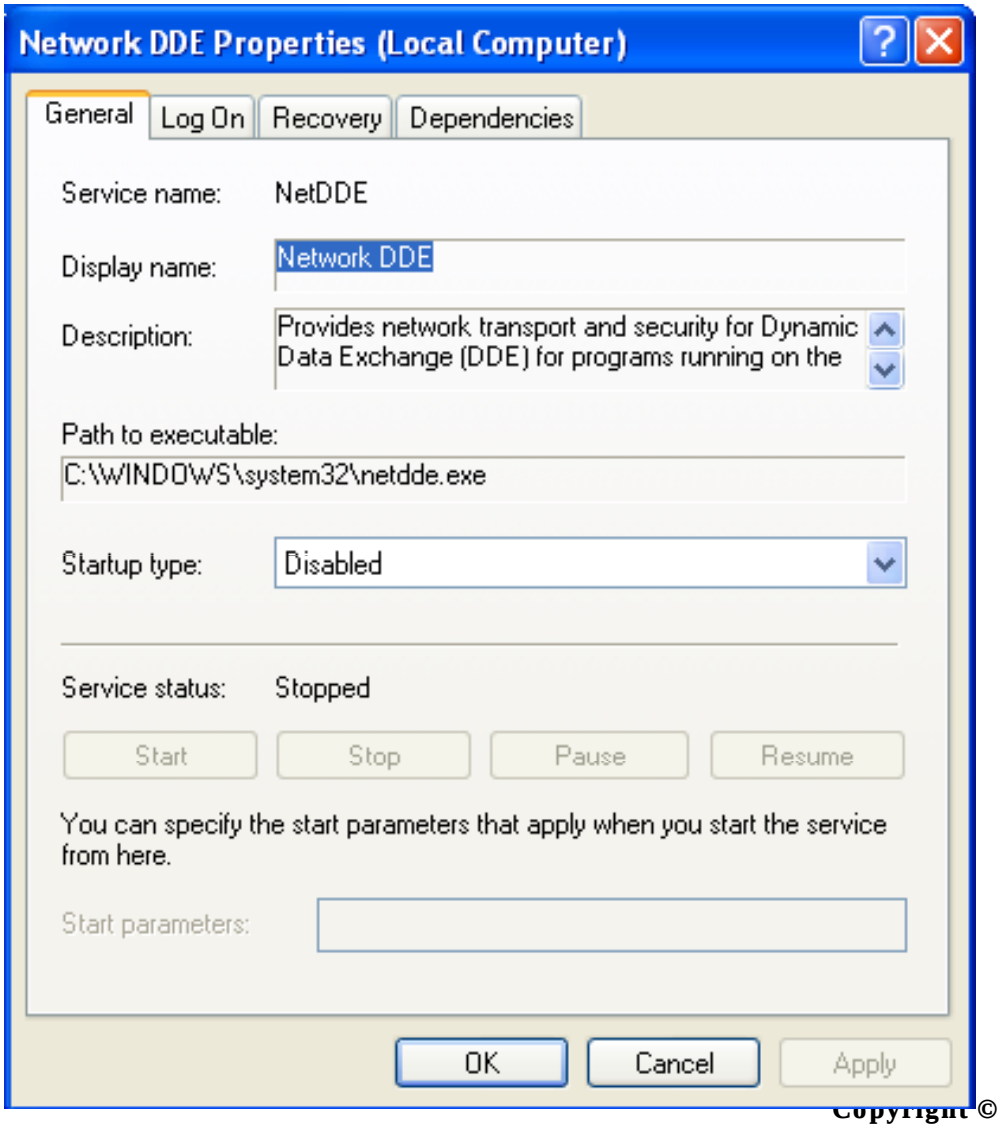
This service is disabled after installation by default. The start up type has to be manual to use network DDE functionality

If disabled, DDE transport and security will not be available

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network DDE



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network DDE DSDM

It manages DDE network shares. It is only used by Network DDE service

It maintains a database DDE shares for information about trusted shares

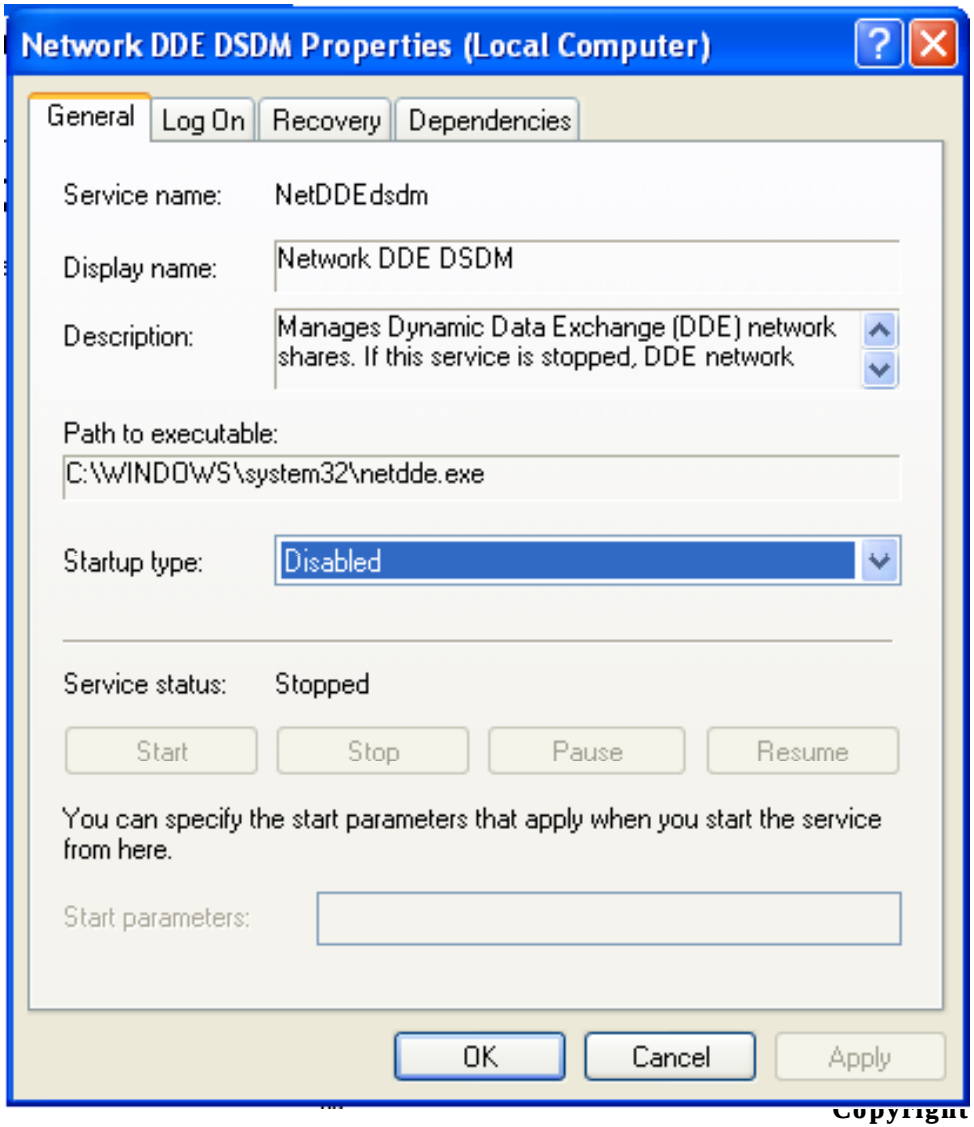
This service is disabled after installation by default. The start up type has to be manual

If disabled, the dependent applications will be stopped as DDE network shares will be unavailable

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network DDE DSDM



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Location Awareness (NLA)

The network configuration is collected and stored by this service

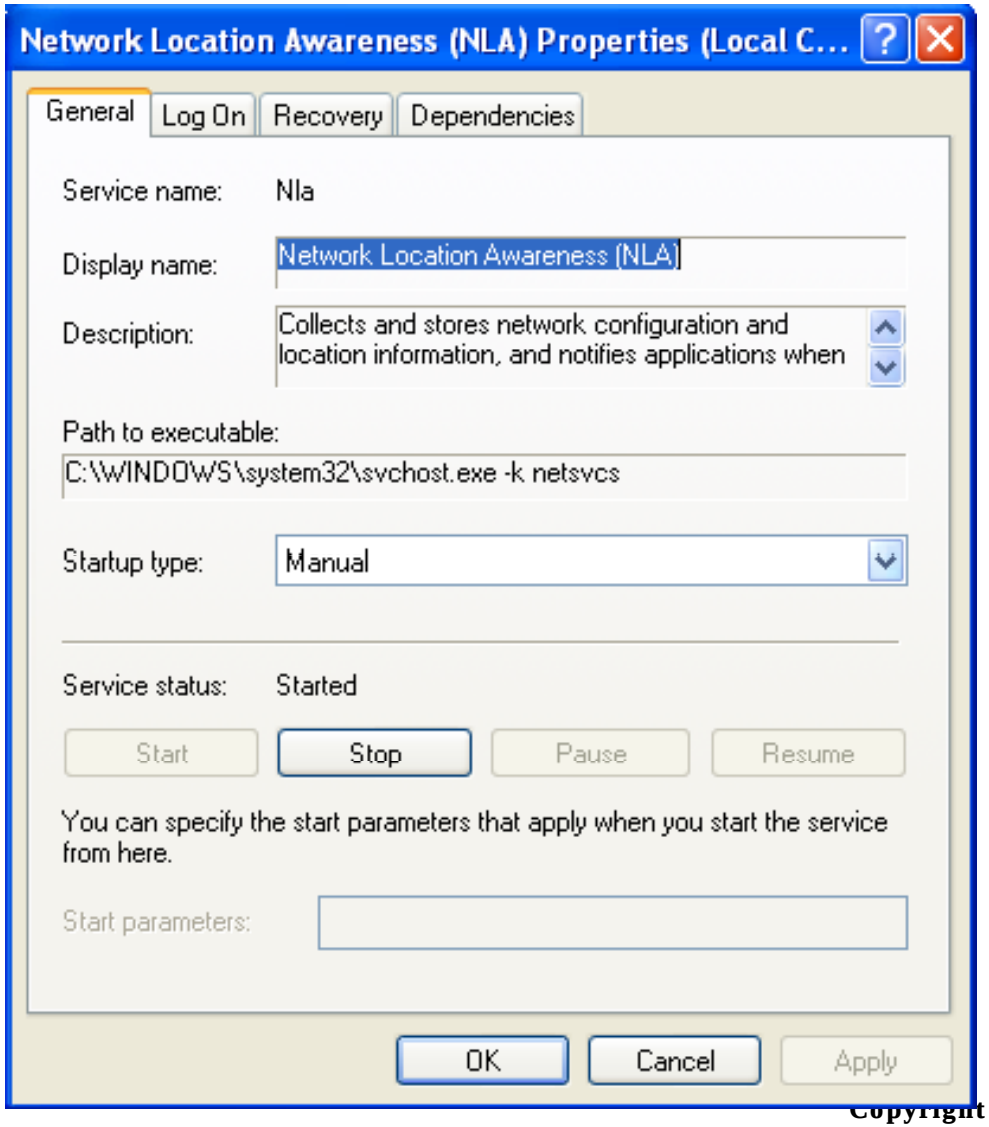
It is a default service in Windows XP; this service is started by the dependent services

If disabled, network location functionality will not be available

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Location Awareness (NLA)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Provisioning Service

The service has the ability to download and manage XML configuration files, which has automatic network provisions for Internet service providers and private networks

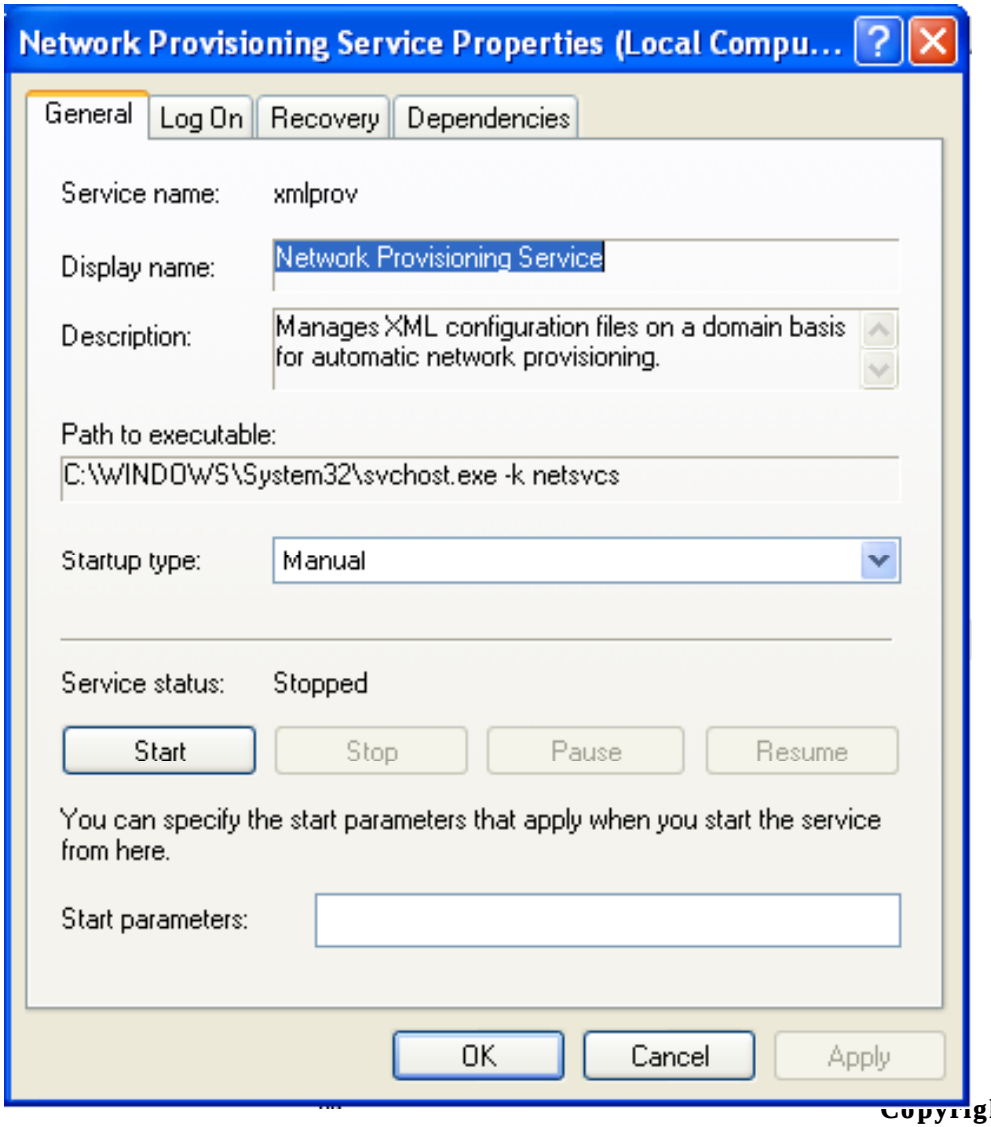
This service works with the **Wireless Zero Configuration** service to provide support for the latest wireless security standards

If disabled, the configuration and operations of wireless network interface will no longer be successful

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Provisioning Service



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network News Transfer Protocol (NNTP)

- The servers using Windows Server 2003 can behave as news servers, with the help of this service
- It is an internet standard
- This service has to be installed later with conjunction to IIS
- If disabled, reading or retrieving posts will not be possible for the client computers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

NTLM Security Support Provider

- RPC programs using transport other than named pipes, gets security from this service
- Using this user can logon and authenticate by NTLM authentication protocol
- Windows 2000 has Kerberos v5 which provides more security than NTLM (Windows NT LAN Manager)
- Using NTLM a user is authenticated using an encrypted challenge/response protocol
- This is installed and run by default on all Windows XP and Windows Server 2003 computers
- If disabled, the clients using this authentication protocol can not logon

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Performance Logs and Alerts

The service lets you to collect performance data based on configuration done from local and remote computers then writes the data to a log and triggers an alert

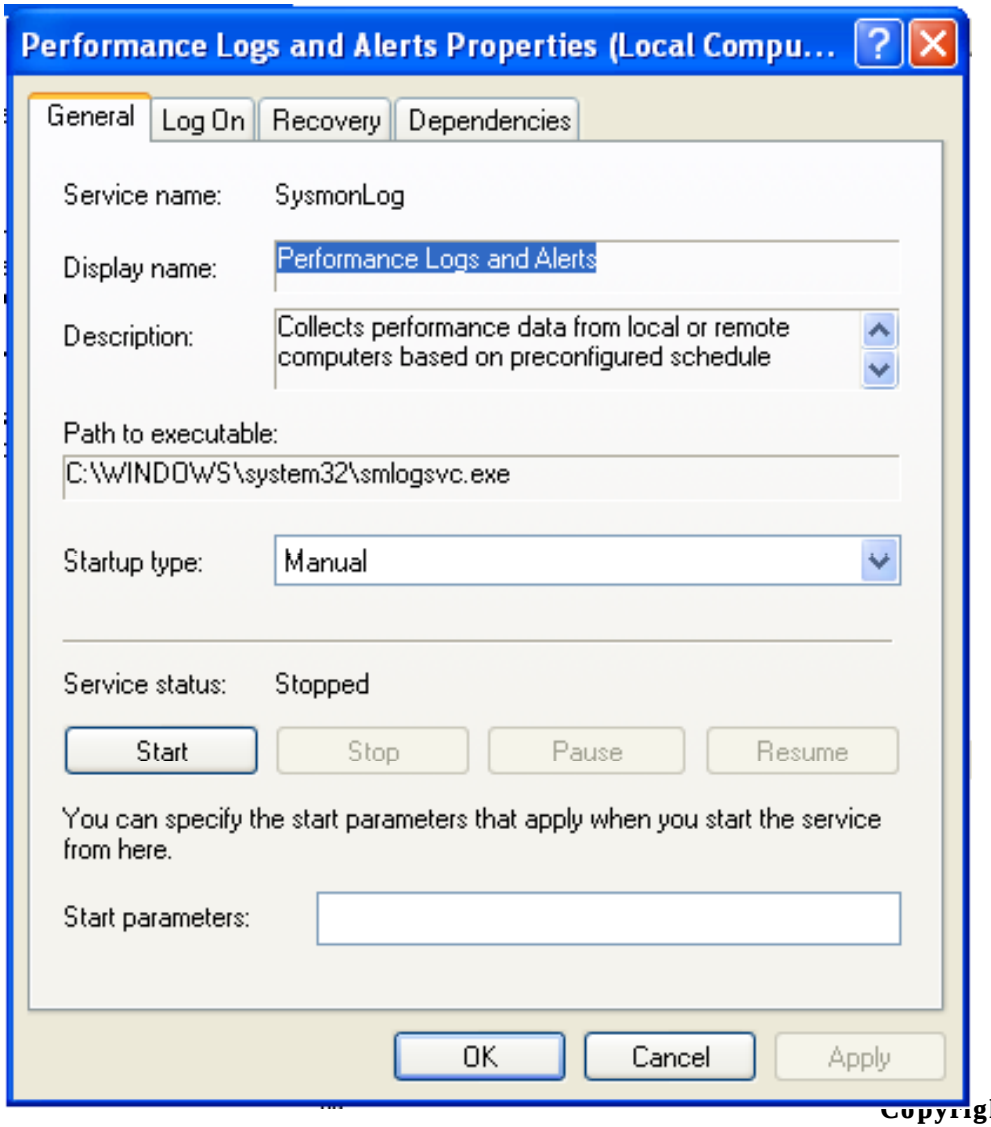
This service runs only if there is a minimum of one schedule

If disabled, no data is gathered on the performance

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Performance Logs and Alerts



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Plug and Play

This service lets the computer to identify and adapt hardware changes with minimum input

This will let you add/remove hardware with out any information about it

This service is configured to perform functions automatically

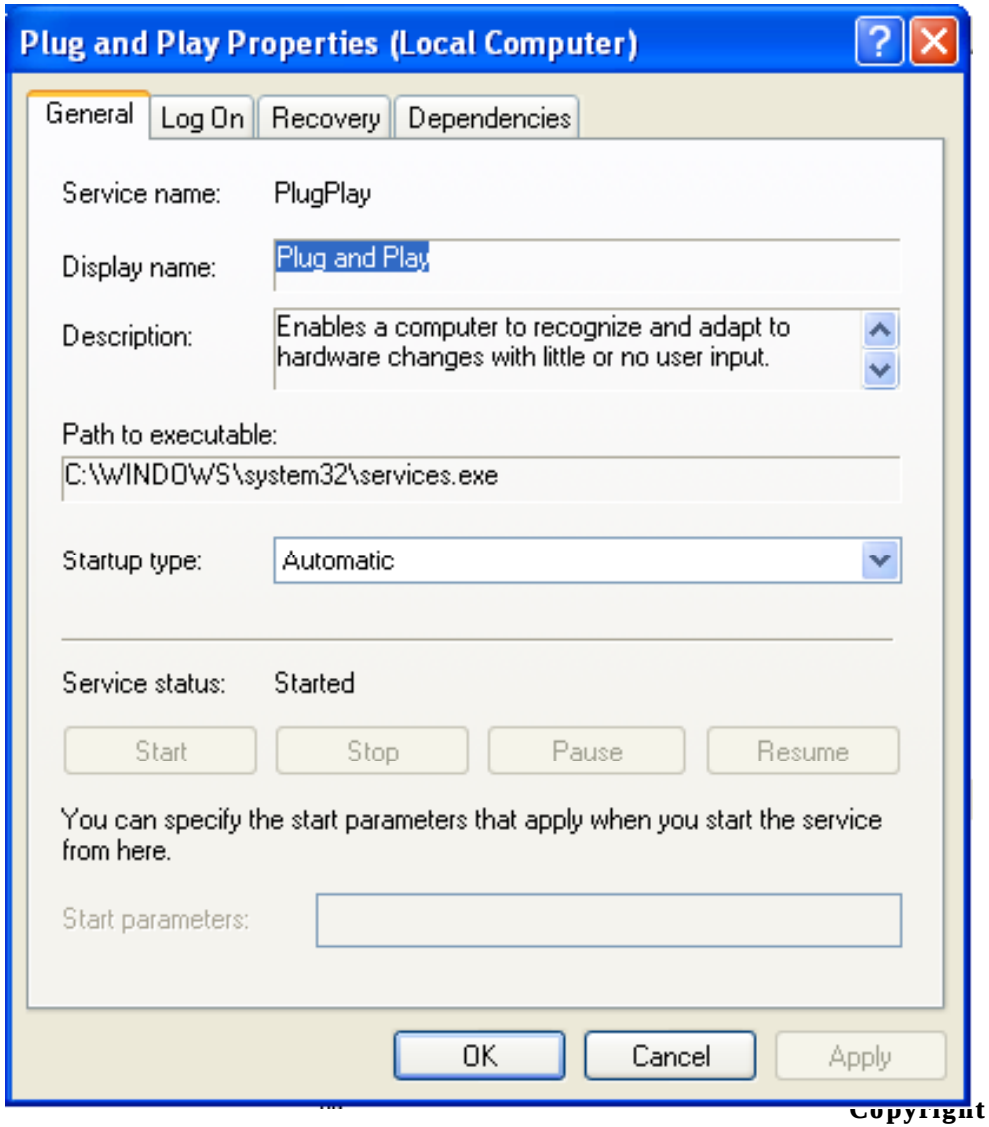
This service cannot be stopped using MCC, rather it can be done using MSCONFIG troubleshooting tool

The device manager will be blank without any hardware

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Plug and Play



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

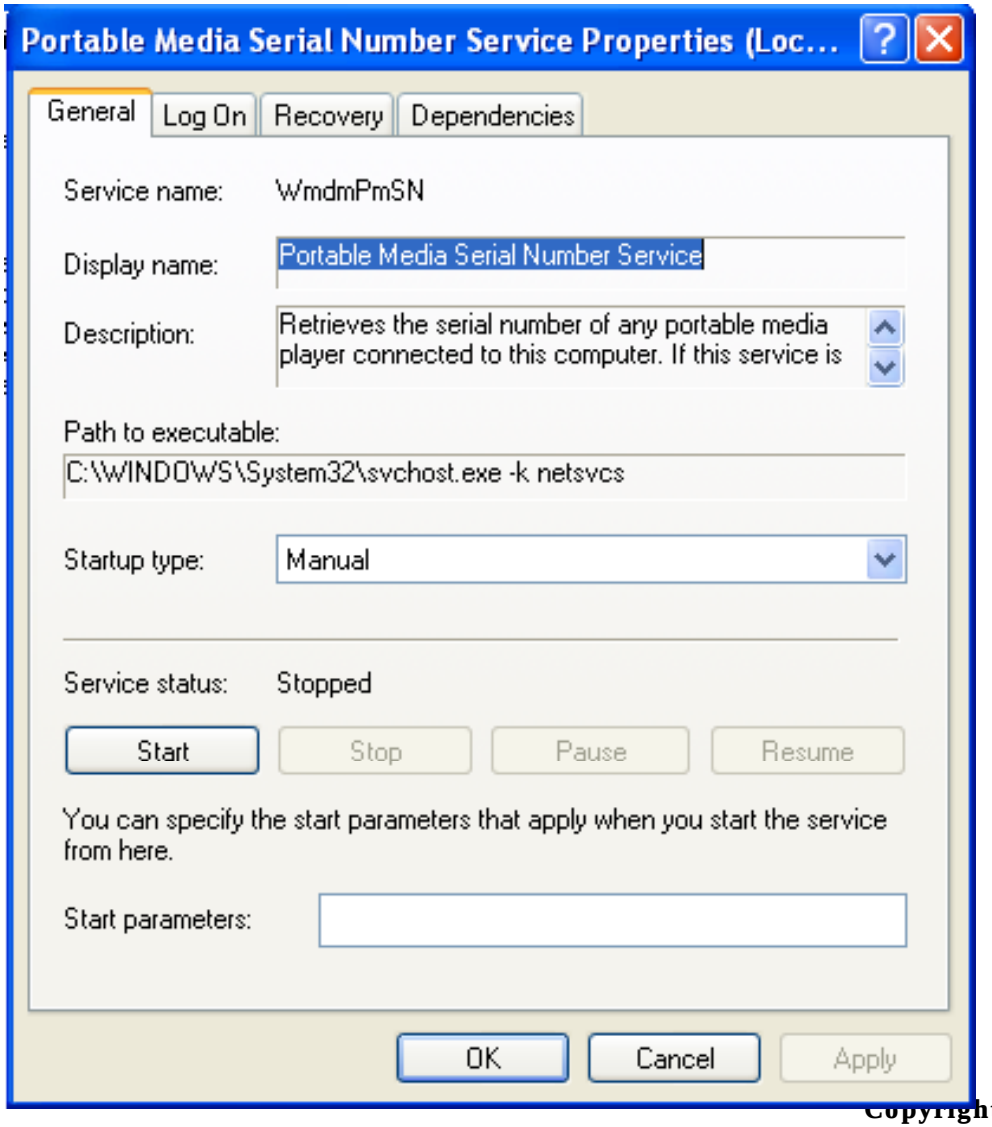
Portable Media Serial Number

- IT retrieves the serial number of any music player connected to the computer
- Windows Media Device Manager (WMDM) can use this service and find the number so that the files can be copied directly to that device
- It is installed in Windows XP and Windows 2003 by default
- It is started manually, and is launched by the request made by WMDM
- If disabled, the serial number can not be accessed from the device

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Portable Media Serial Number



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Print Server for Macintosh

By using this service Apple Macintosh client can send print jobs to print spooler on a Windows Server 2003 computer.

This service has to be installed manually.

If disabled, the print operations can not be carried.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Print Spooler

The service manages local and network print queues to control the print jobs. It communicates with printer I/O components

If disabled, print and fax operations are not carried

This service deletes each record when the operation is carried out

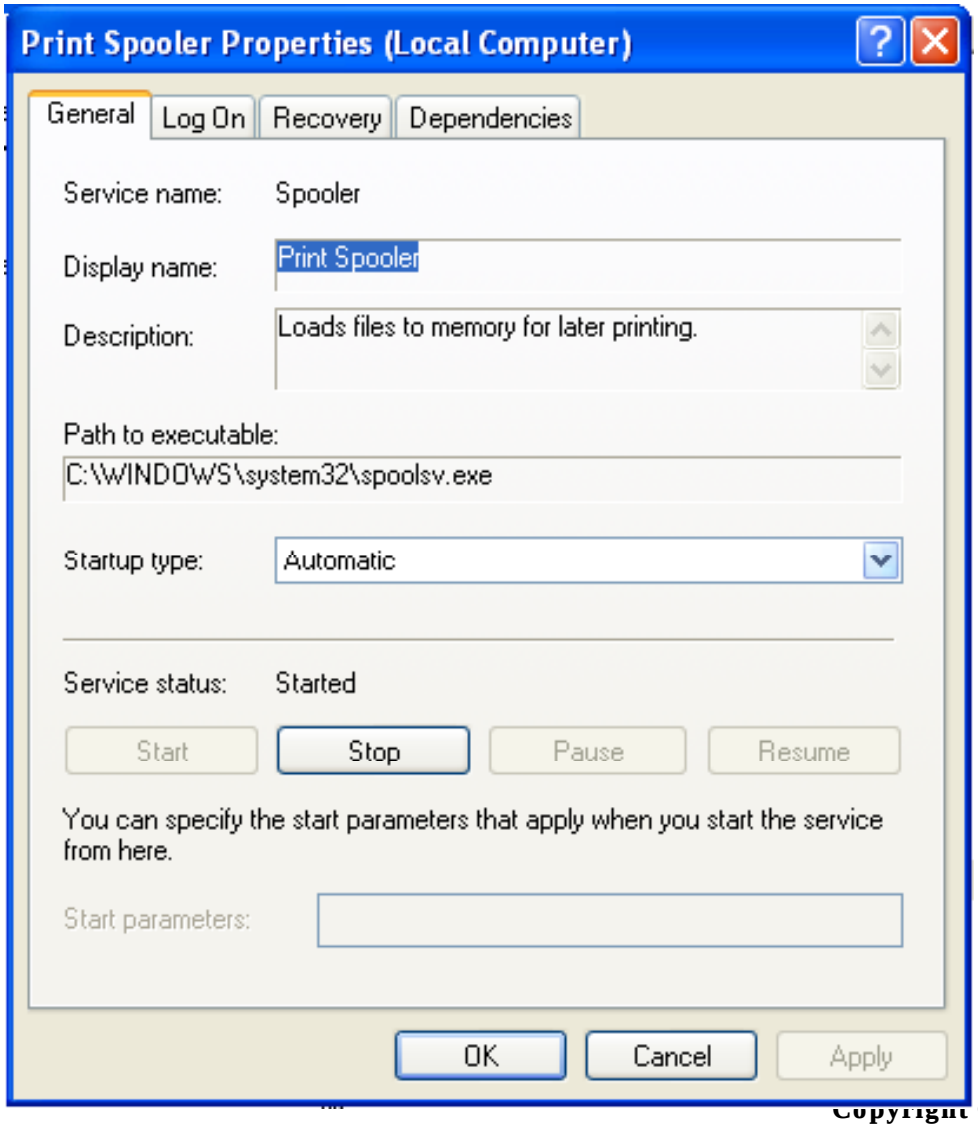
If the service is disable the unused records are not deleted, which may cause the server to crash

This service has to be configured to Disable or manual

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Print Spooler



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Protected Storage

The sensitive information is stored using this service to protect it

A set of libraries are given to store information, and details of storage itself

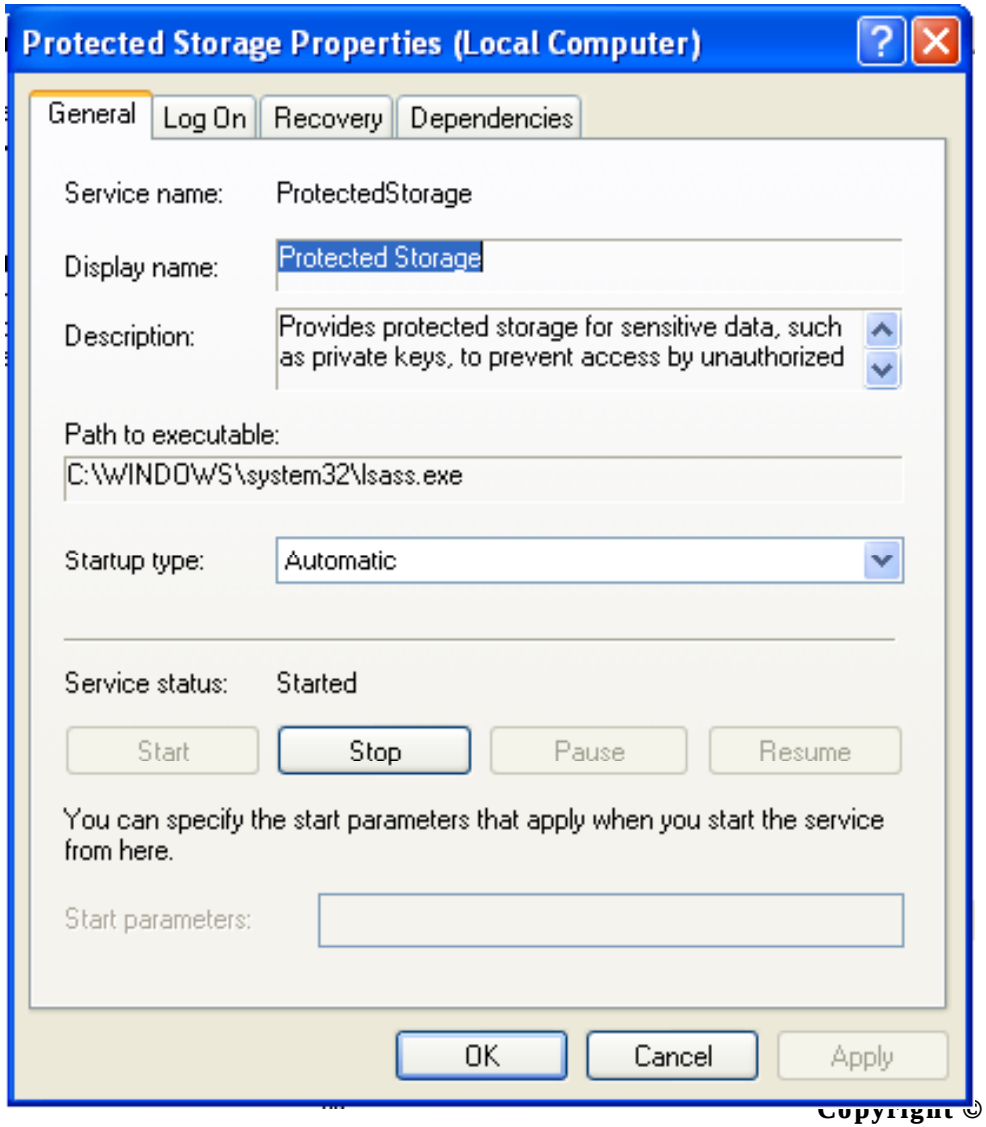
The service uses a Hash-Based Message Authentication Code (HMAC) and the Secure Hash Algorithm 1 (SHA1) cryptographic hash functions to encrypt the user's master key

If disabled, private keys will be inaccessible, the **Windows Certificate Services** service will not operate, Secure Multipurpose Internet Mail Extensions (S/MIME) and SSL will not work, and smart card logon will fail

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Protected Storage



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

QoS RSVP Service

This service is a standard, developed to obtain more effective use of network resources

Using this service the client and server can differentiate between data types and manage end-to-end network traffic

QoS can achieve the end-to-end transfer with the help of IETF (Internet Engineering Task Force)

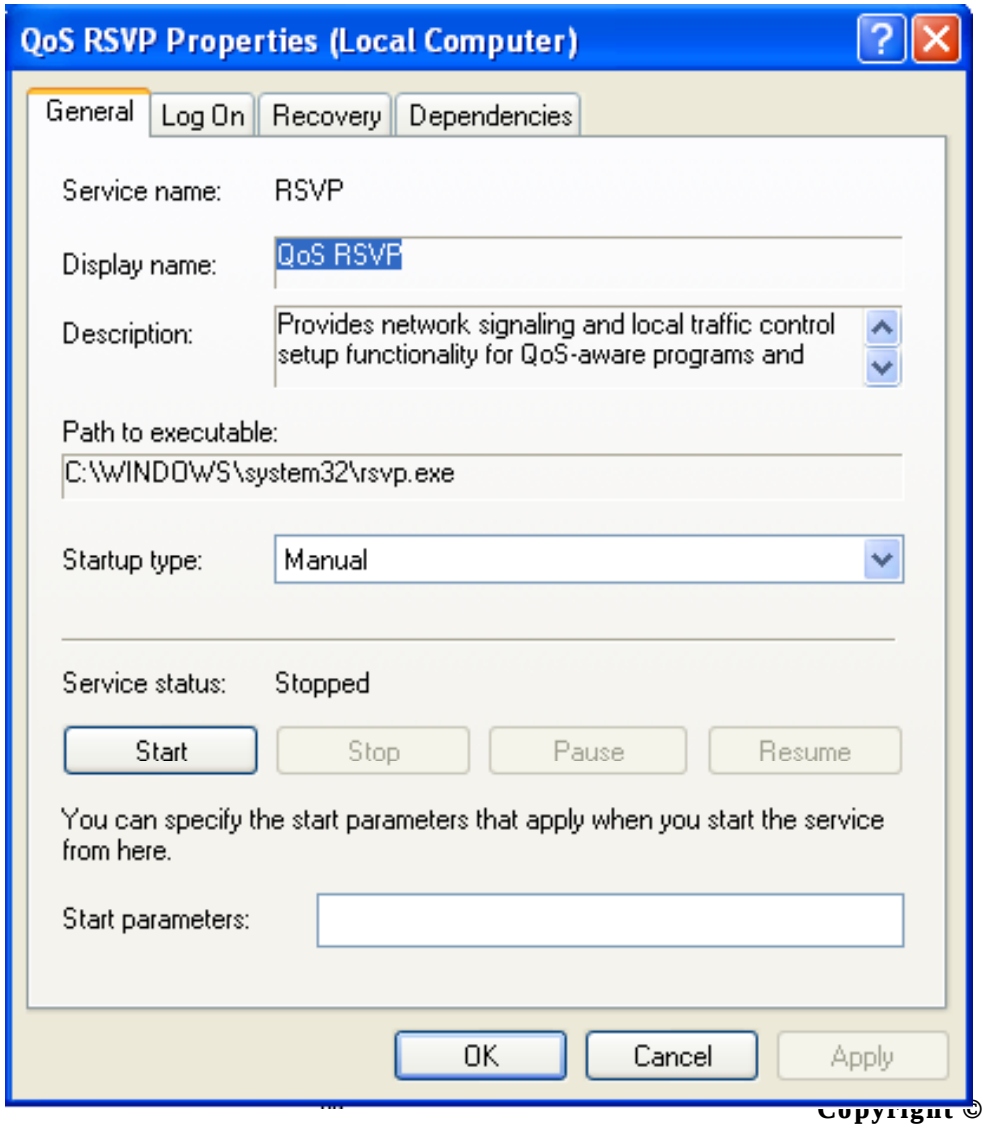
It is installed on Windows XP by default

If disabled, the computer can not perform QoS connection

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

QoS RSVP Service



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Access Auto Connection Manager

The service finds out the attempt in which a remote network can not be accessed, and gives another way to perform the operation

For a better performance the service manages a database with the information to connect to a particular location from the successful attempts

This service is installed by default in Windows XP and Windows Server 2003, and configured to manual

If disabled, manual establishment of connections have to be performed

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Access Connection Manager

The system service manages a dial-up and VPN connection between computer to internet or computer to remote computer.

By sending a request of the service a VPN connection is sent to setup a connection.

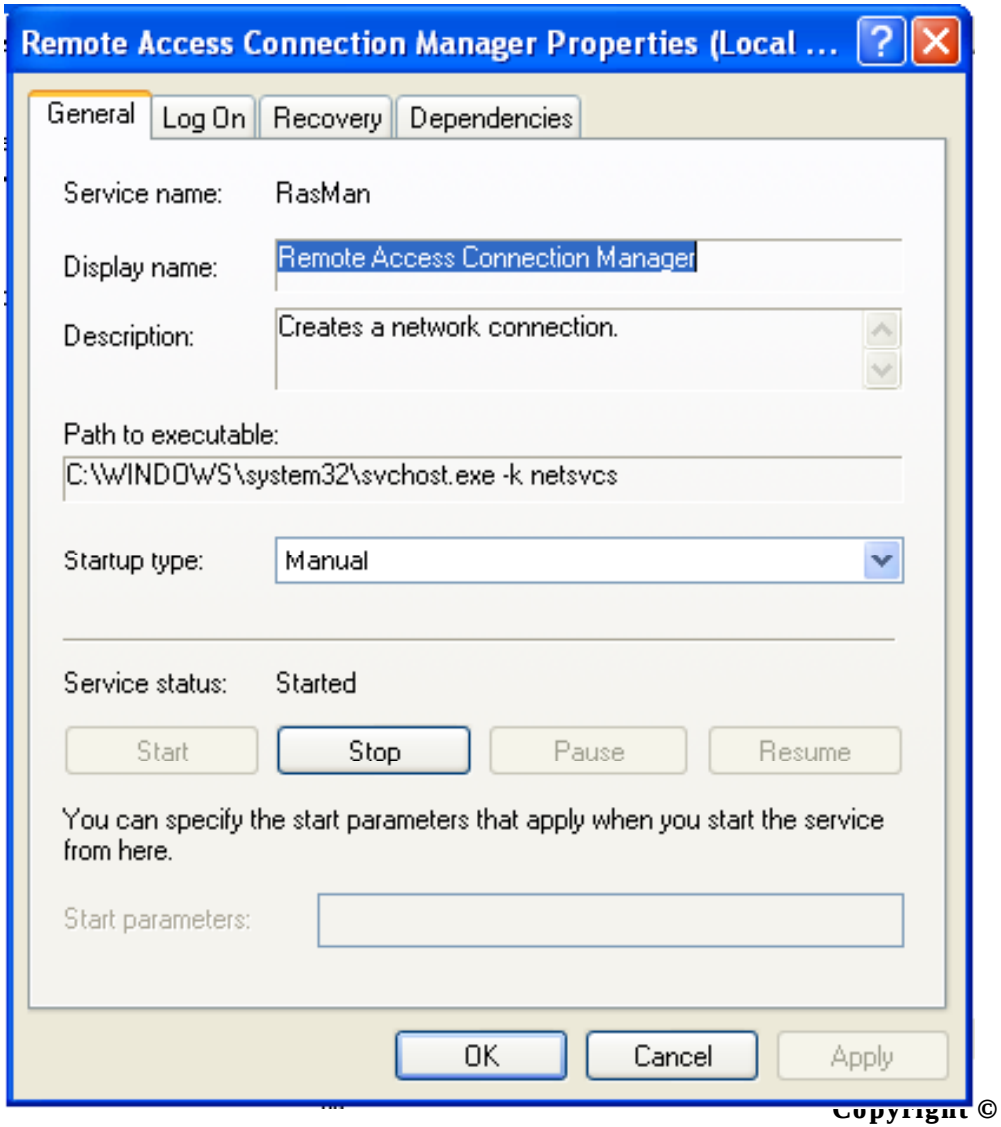
This service is configured to manual, it is started only when at least one or more VPN or dial up connections.

If disabled, making dial-up or VPN connections is not possible.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Access Connection Manager



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Administration Service

When the restarts the below tasks are performed to support remote administration:

- Increments the server boot count
- Generates a self-signed certificate
- Raises an alert if the date and time has not been set on the server.
- Raises an alert if the Alert E-mail functionality has not been configured.

When a Remote Server Manager asks to execute a task, this service starts the process through a COM interface

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Administration Service (Cont'd)

COM interface accepts the requests made by Administrator or Local System accounts

This is configured to automatic by default

If disabled, Remote Administration Tools features may not function properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Desktop Help Session Manager

The Remote Assistance feature in the Help and Support Center application (Helpctr.exe) are managed by this feature.

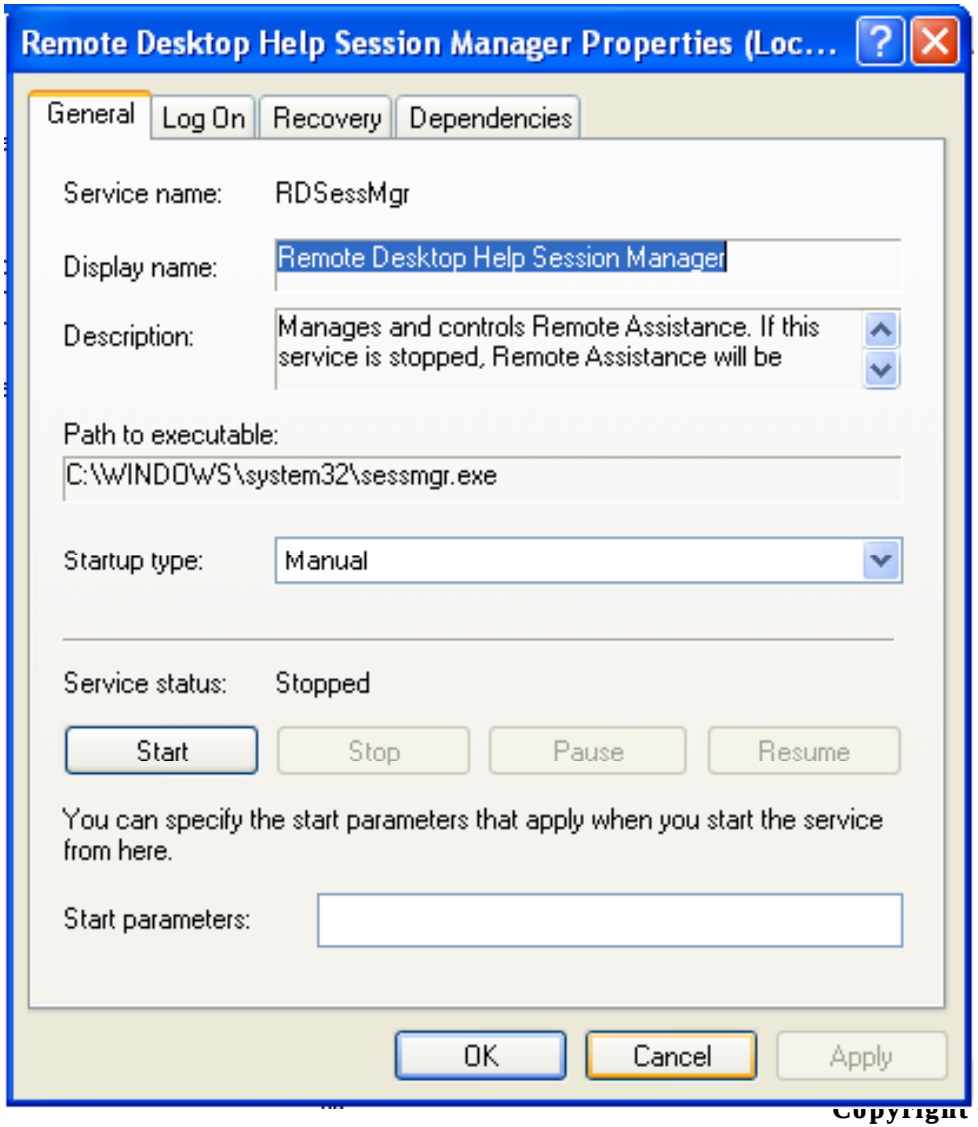
This service is installed by default but starts when Remote Assistance is making/receiving a request.

If disabled, Remote Assistance is unavailable.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Desktop Help Session Manager



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Installation

The service has the ability to install Windows 2000, Windows XP, and Windows Server 2003 on Pre-Boot Execution Environment (PXE) remote boot-enabled client computers

RIS is a windows deployment feature in Windows Server 2003, support on-demand image-based or script-based operating system installations on a network connection

RIS is implemented for simplifying the operating system development process

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Installation (Cont'd)

RIS can be used as:

- Provide an operating system to users on demand.
- Image of an operating system can be given to a group of users.

This service has to be installed later.

If disabled, user cannot use RIS tools from the computer.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Procedure Call (RPC)

It is a secure IPC (Internet process communication) mechanism used for data swapping and starting a process in remote location

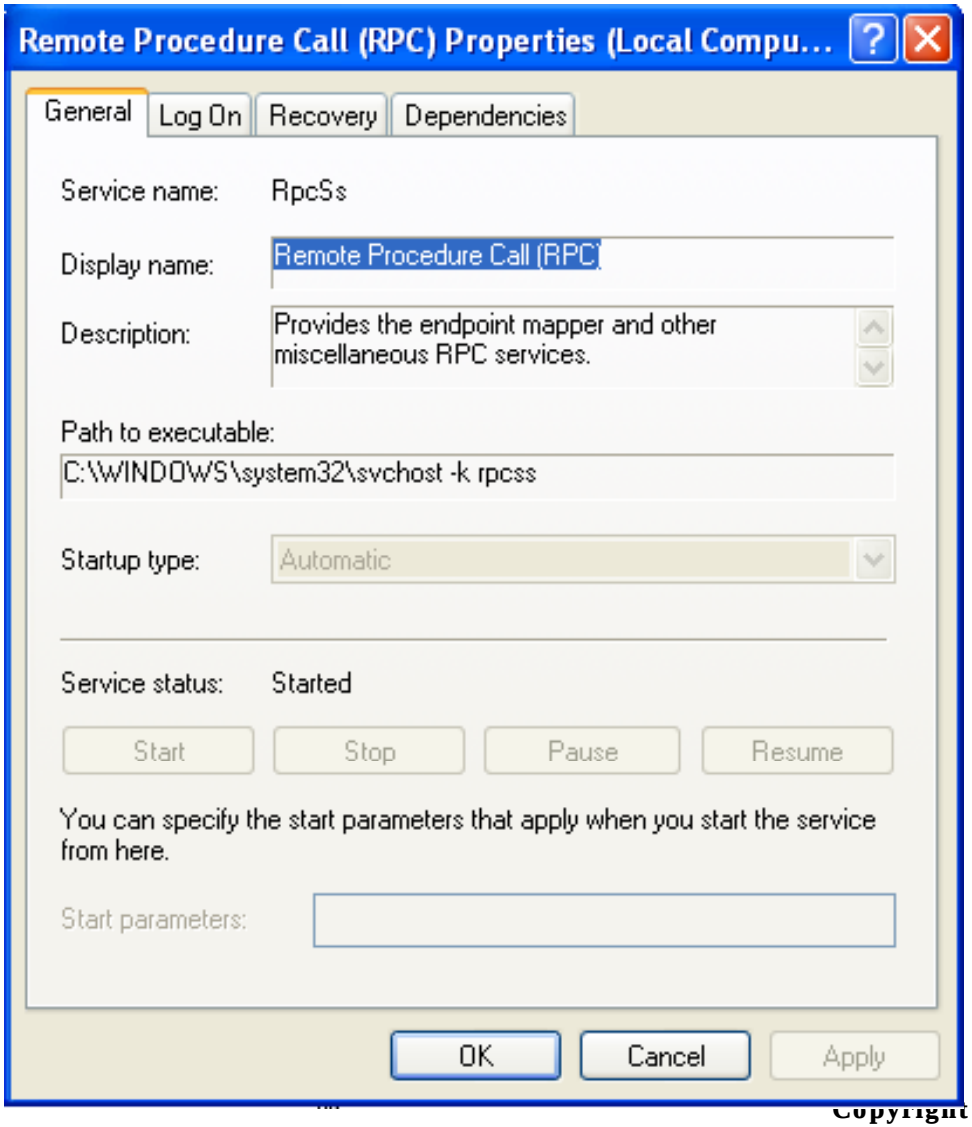
This service acts as RPC endpoint mapper and COM Service Control Manager (SCM)

This service can not be disabled or stopped as the operating system will not load with out it

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Procedure Call (RPC)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Procedure Call (RPC) Locator

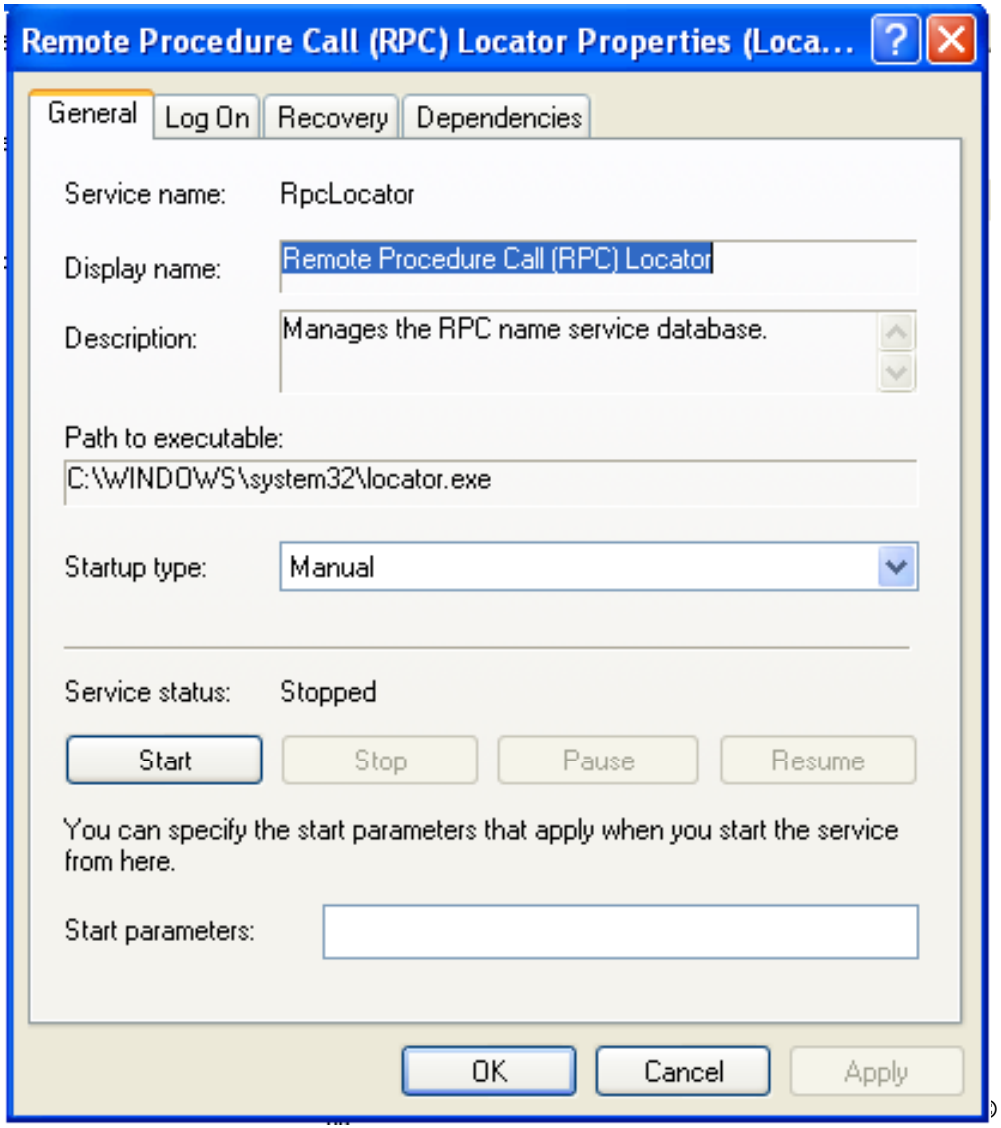
The service enables RPC client using RpcNs* family of APIs to locate RPC servers. It even manages RPC name service and name server database.

If disabled, RPC clients that need to locate RPC services on other computers mat not find it.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Procedure Call (RPC) Locator



EC-Council

© by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Registry Service

The service enables remote users having the ability to modify registry settings on the domain controller

This service is installed and run automatically Windows XP and Windows Server 2003

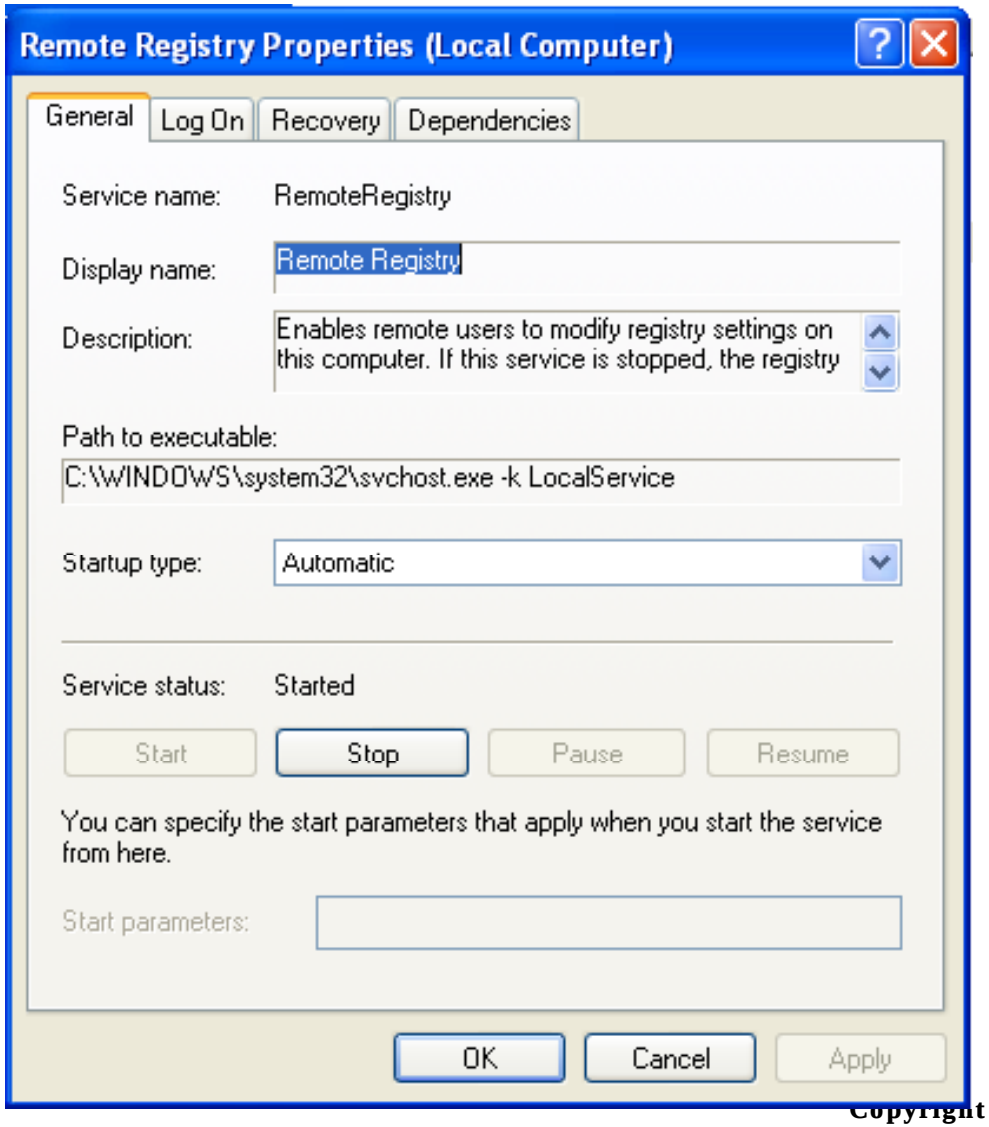
Only Administrators and Back operators can modify the registry remotely

If disabled, only local computer registry can be modified and no application depending on the service can work

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Registry Service



EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Server Manager

The service provides:

- Holds the Remote Administration alert information
- Provides an interface to raise, clear, and enumerate Remote Administration alerts
- Provides an interface to execute Remote Administration tasks

In Windows Server 2003 the service is installed and set to automatic

If configured to Manual, the service is started with request to Remote Administration Tasks or Remote Administration Alerts

If disabled, the service depending on this service will not start

EC-Council
ved.
Reproduction is Strictly Prohibited

Remote Server Monitor

Critical computer resources are monitored and mange watchdogs timers hardware on remotely managed servers

If disabled, the timers will stop and no monitoring is done

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Storage Notification

If the files are accessed from a secondary storage media to read/write, this service will notify the user

This service allows the user to cancel the process

It is not installed by default on Windows XP and Windows Server 2003

If disabled, neither notification on files is given and nor a user can cancel a operation

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remote Storage Server

The service stores rarely used files in secondary storage device. It allows Remote Storage subsystem in Windows to tell users if an offline file is used

Remote storage is hierarchical storage management (upper level storage to lower level storage)

This service is installed as part of a Remote Storage Windows component which has to be installed manually

If disabled, file cannot be retrieved or moved from a secondary storage media

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Removable Storage

The service operates automated removable media devices and manages the catalog removable media

This service automates mounting, dismounting and eject media functions and provides drive cleaning mechanism

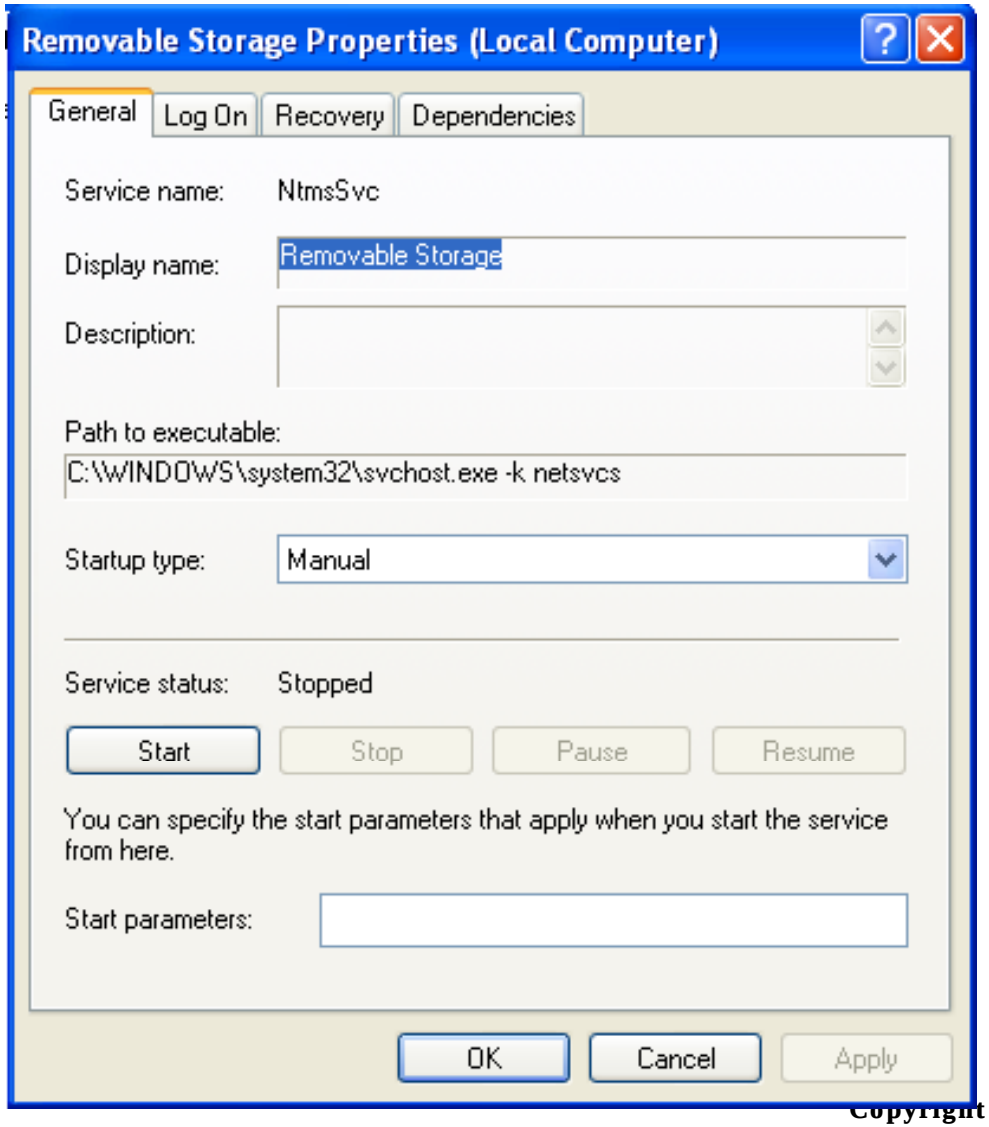
This is installed by default, and configured to run when requested

The service is inactive when there is no process

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Removable Storage



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Resultant Set of Policy Provider

You can connect to Windows Server 2003 domain controller and simulate Resultant Set of Policy (RSoP) for Group Policy settings. The simulation is referred to as planning mode

This service is installed by default but configured to start manually

If disabled, RSop planning mode simulation will not be available

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Routing and Remote Access

The service provides multi protocol LAN-to-LAN, LAN-to-WAN, VPN and NAT routing services and provides dial-up and VPN remote access services

The service replaces the Routing and Remote Access Service (RRAS) and Remote Access Service (RAS) features in Windows NT 4.0

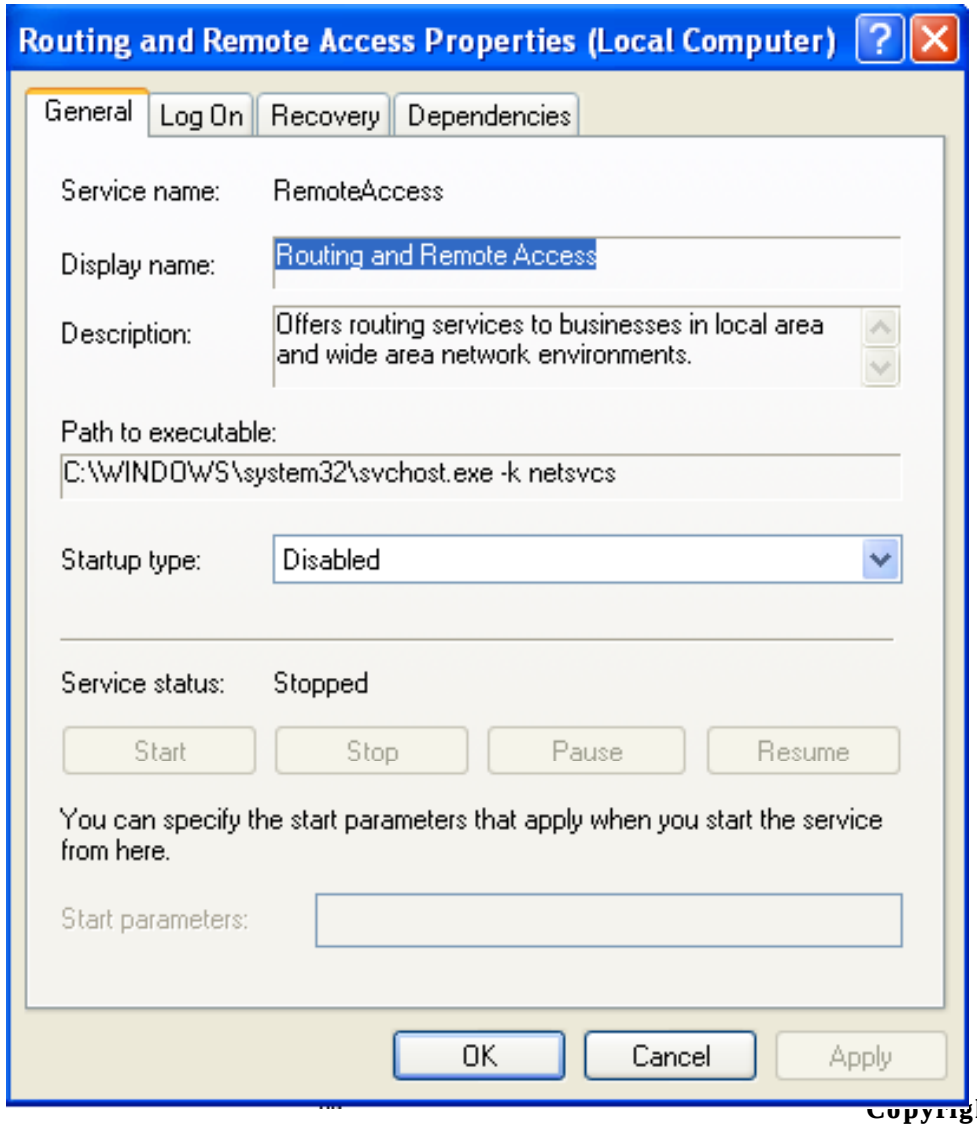
The service is installed and disabled by default

If disabled the incoming RAS, VPN or dial-on-demand connections, and routing protocols will not be received or transmitted

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Routing and Remote Access



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

SAP Agent

The service advertises network services on an IPX network through the IPX Service Advertising Protocol (SAP).

Features as file and print services depend this service.

It requires NWLINK IPX/SPX Compatible Transport protocol, and not installed by default.

If disabled, the reference features may not work properly.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

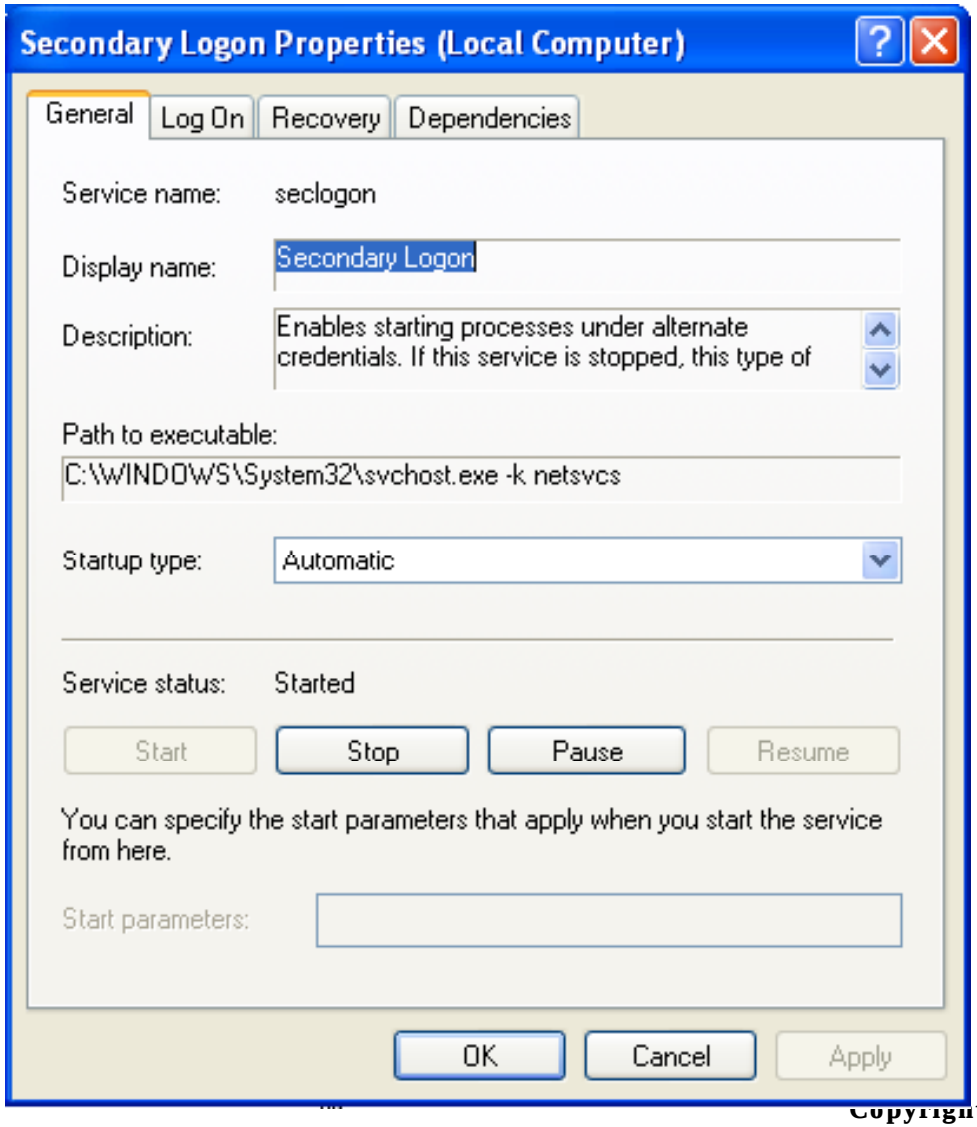
Secondary Logon

- Users can create processes with different security principals with the help of this service
- A restricted user can use this service to temporarily run an application
- This service contain RunAs.exe allowing to run *.exe file and MMC consoles
- This service is also called as **RunAs Service**
- Installed and run automatically by default
- If disabled, this type of logon will be unavailable

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Secondary Logon



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Accounts Manager

User and group information is protected by this service

The startup of this service signals other services that it is ready to accept requests

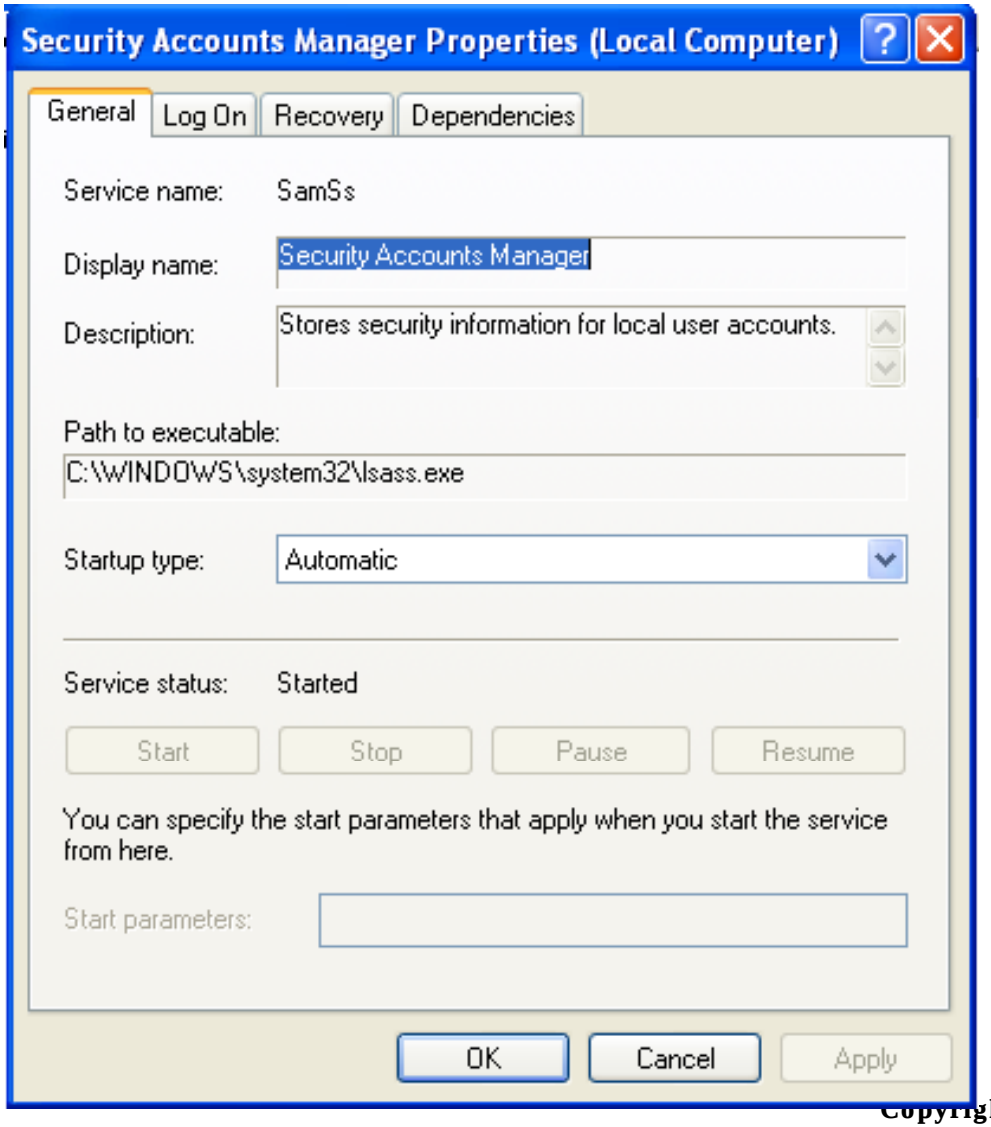
If disabled, other processes can not start

Do not disable this service

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Accounts Manager



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Center

The service manages security setting by giving a central location for Windows XP with SP2 computers

This service performs the tasks such as:

- Checks whether the Windows Firewall service is running
- Queries specific third-party WMI providers to see if compatible antivirus software is installed, whether the software is up-to-date, and whether real-time scanning is turned on

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Center (Cont'd)

Checks the configuration of the **Automatic Updates** service.

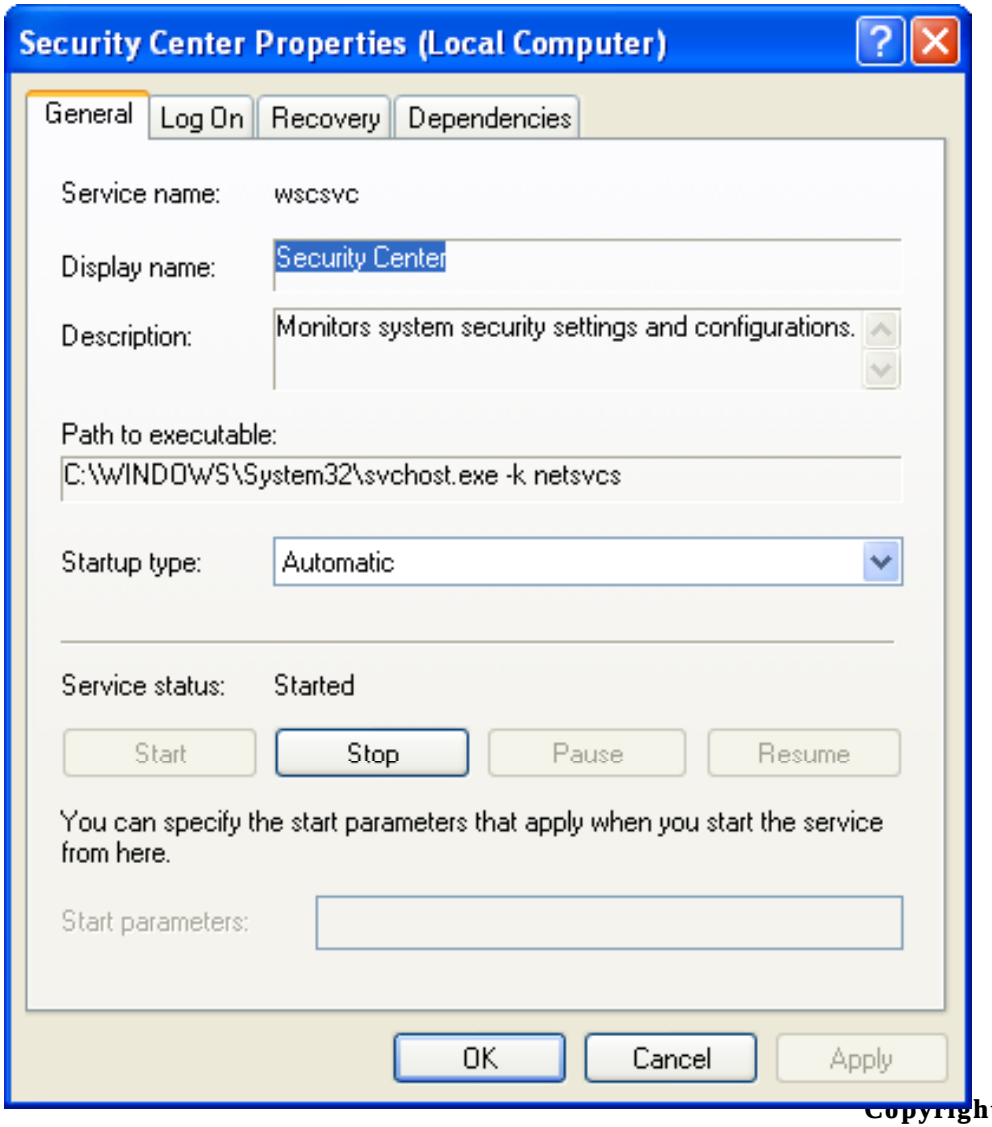
If any service is not up to date a alert message is given to the user.

If disabled, the components will work as per the setting but no centralized service is provided.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Center (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Server

This service provides RPC support, file, print, and named pipe sharing over the network

This service is installed and runs automatically by default on Windows XP and Windows Server 2003

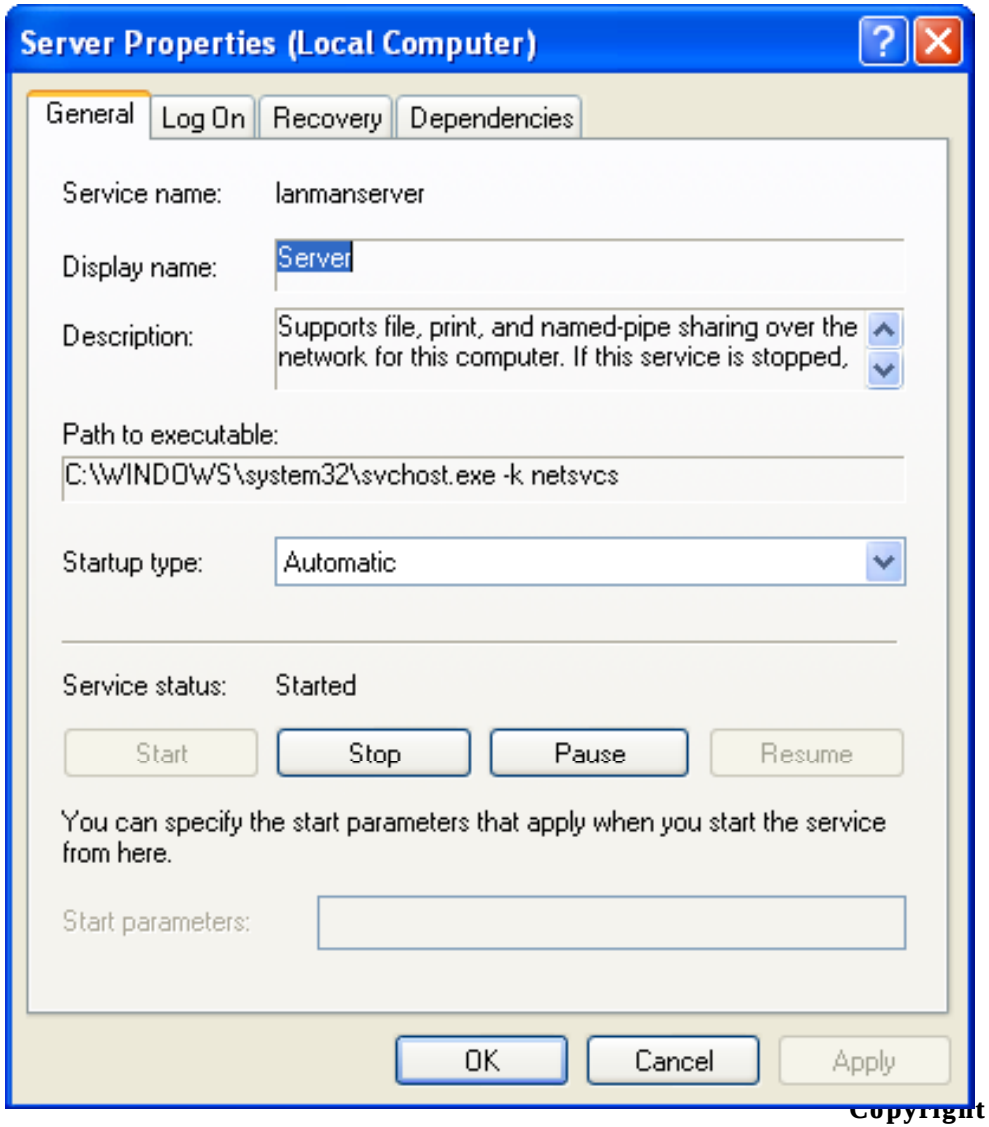
If disabled, local files and printers cannot be shared

It is not able to satisfy remote RPC request

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Server



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shell Hardware Detection

Notification for Auto play hardware events is provided and monitored by this service

Independent hardware vendors (IHVs) and independent software vendors (ISVs) can extend the support to include their hardware devices and applications

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shell Hardware Detection (Cont'd)

Media and device types that are supported by AutoPlay include:

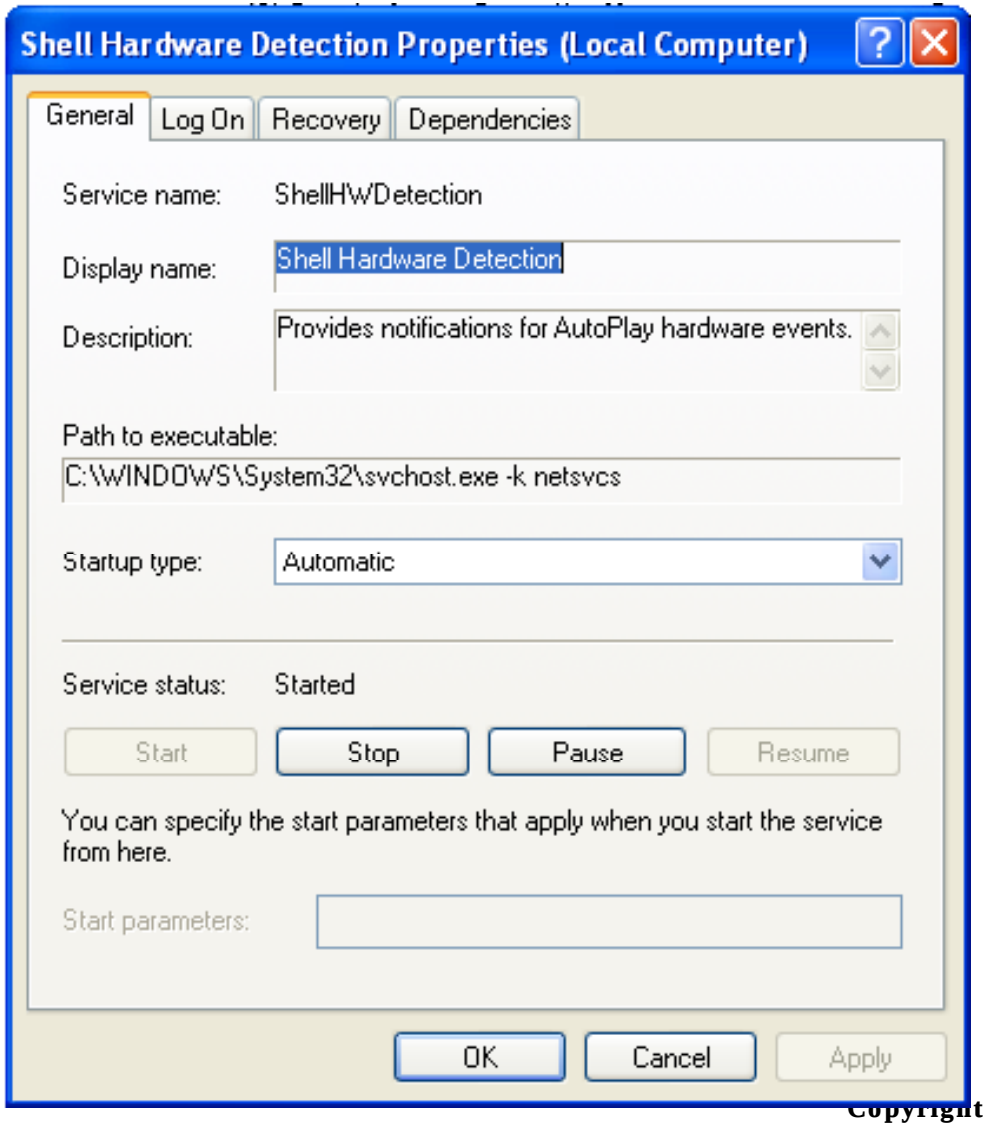
- Removable storage media
- Flash media
- PC cards
- External hot-plug USB or 1394 fixed drives
- Supported content types, which include:
  - Pictures (.jpg, .bmp, .gif, and .tif files)
  - Music Files (.mp3 and .wma files)
  - Video (.mpg and .asf files)

This service is installed and run automatically by default

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Shell Hardware Detection (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Simple Mail Transport Protocol (SMTP)

This is an e-mail submission and relay agent

This service is used for inter-site email based replication in Windows domain controller

This service is installed and run by default on Windows Server 2003, Web Edition

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Simple TCP/IP Services

The service supports the following protocols and ports:

- Echo, port 7, RFC 862
- Discard, port 9, RFC 863
- Character Generator, port 19, RFC 864
- Daytime, port 13, RFC 867
- Quote of the Day, port 17, RFC 865

If enabled, all the above protocols are enabled

If disabled, the operating system is not affected

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Simple TCP/IP Services (Cont'd)

This service has to be installed manually

Install the service only if it is necessary to support communication with other computers that use the referenced protocol

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Smart Card

The service controls access to a smart card that is inserted into smart card reader

The Resource Manager performs functions:

- Identifies and tracks resources
- Allocates readers and resources across multiple applications
- Supports transaction primitives to access services that are available on a given card

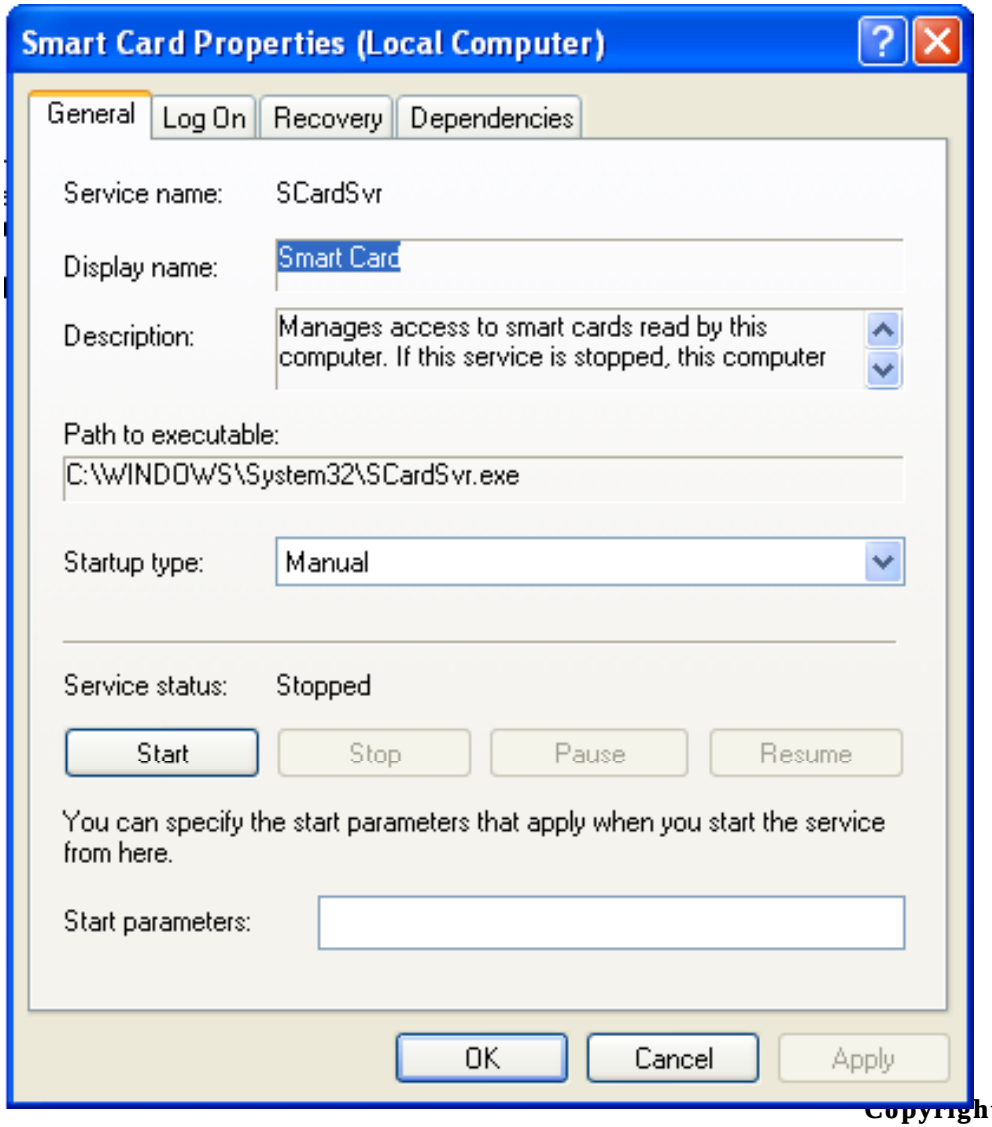
This service is automatically installed on Windows XP and Windows Server 2003 by default, but is configured to start manually

If disabled, smart cards can not be read

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Smart Card



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Special Administration Console Helper

This service performs remote management tasks if a function is stopped by an error message

The Windows Emergency Management Services component supports two out-of-band console interfaces:

- The Special Administration Console (SAC)
- !SAC, a subset of SAC commands

Both interfaces support input/output operations

Using command prompt a inbound communication channel by this service

If disabled, SAC service will not be available

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Event Notification

This service monitors events

This service is installed and run automatically by default

If disabled, no event notifications are sent:

- Win32 APIs IsNetworkAlive() and IsDestinationReachable() will not work.
- ISens* interfaces will not work. SENS logon/logoff notifications will fail.
- SyncMgr (Mobsync.exe) will not work properly.
- The COM+ EventSystem will fail when it tries to notify SENS of some events.
- The **Volume Shadow Copy** service will not load properly.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System Restore Service

Windows XP users can take snap shots of there computer and save them as restore point

This service is enabled by default to make point, before any critical modification

If disabled, no restore points will be created

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Task Scheduler

The service allows the computer to start a task on the computer

The following tasks can be performed by this service:

- Create work items (currently the only type of work item that is available is tasks)
- Schedule tasks to run at specific times or when a specific event occurs
- Change the schedule for a task
- Customize how tasks are run
- Stop a scheduled task

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Task Scheduler (Cont'd)

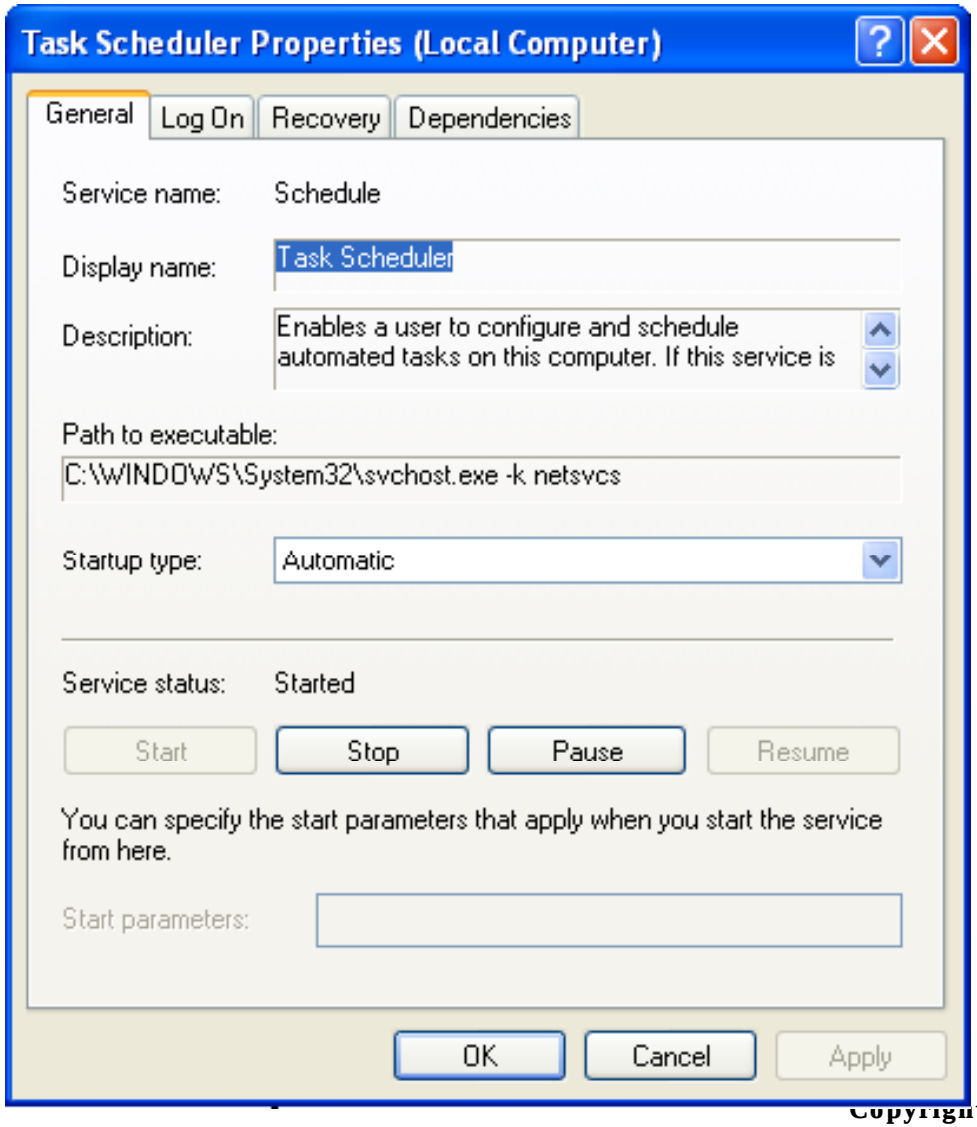
This service is present by default in the computer

If disabled, no tasks will run automatically. This service is generally used to perform backup operations

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Task Scheduler (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

TCP/IP NetBIOS Helper Service

The service provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients on your network

It is enabled to share files, print and logon to the network

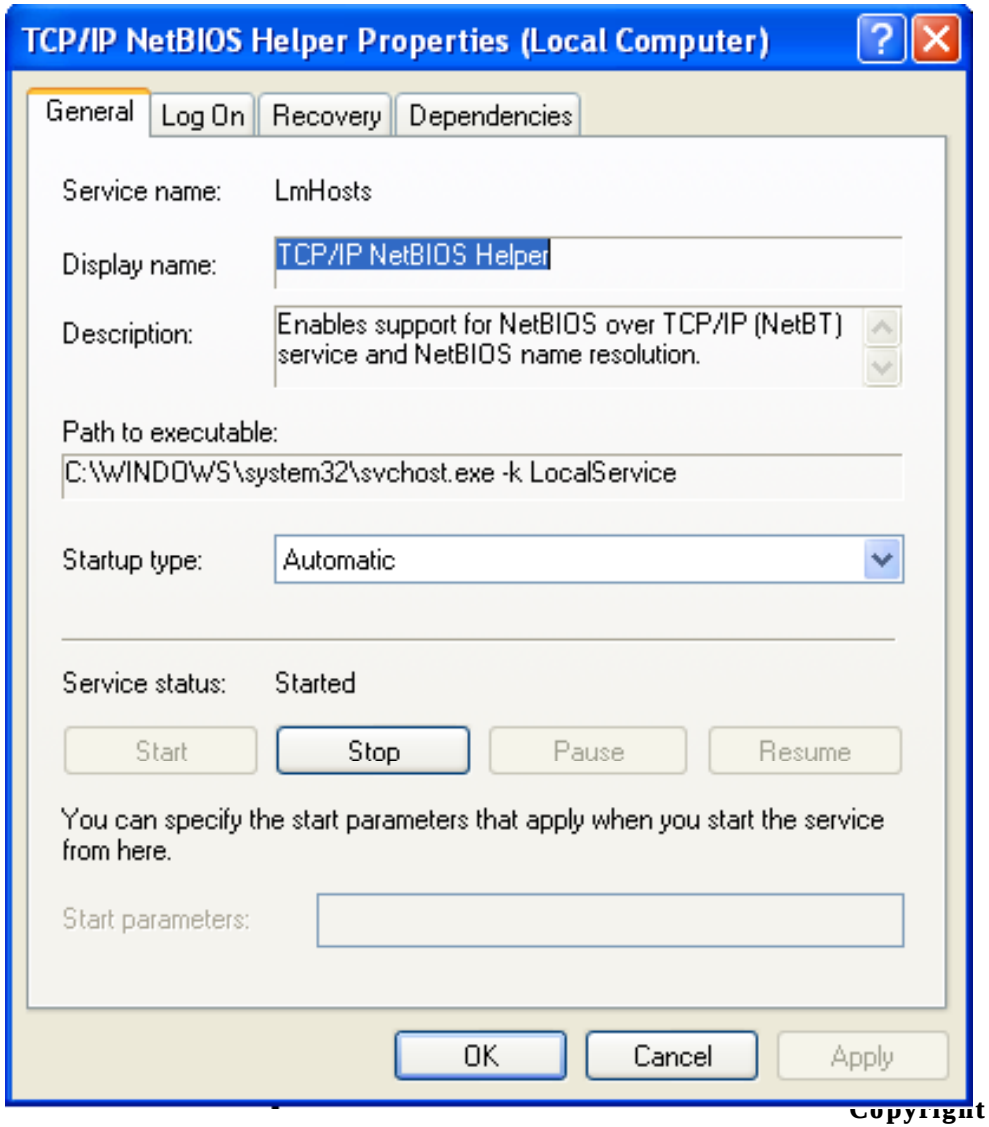
This is installed and started automatically

If disabled, NetBT, Redirector (RDR), Server (SRV), **Net Logon** and **Messenger** service clients might not be able to share files, printers and log on to computers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

TCP/IP NetBIOS Helper Service



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

TCP/IP Print Server

TCP/IP-based printing through the Line Printer Daemon protocol is enabled by this service

This is an optional component and has to be installed separately

If disabled, TCP/IP-based printing will not be supported

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Telnet

This provides ASCII terminals to ASCII telnet clients

It supports four types of terminals:

- American National Standards Institute (ANSI)
- VT-100
- VT-52
- VTNT.

This allows logon and running a program from command line

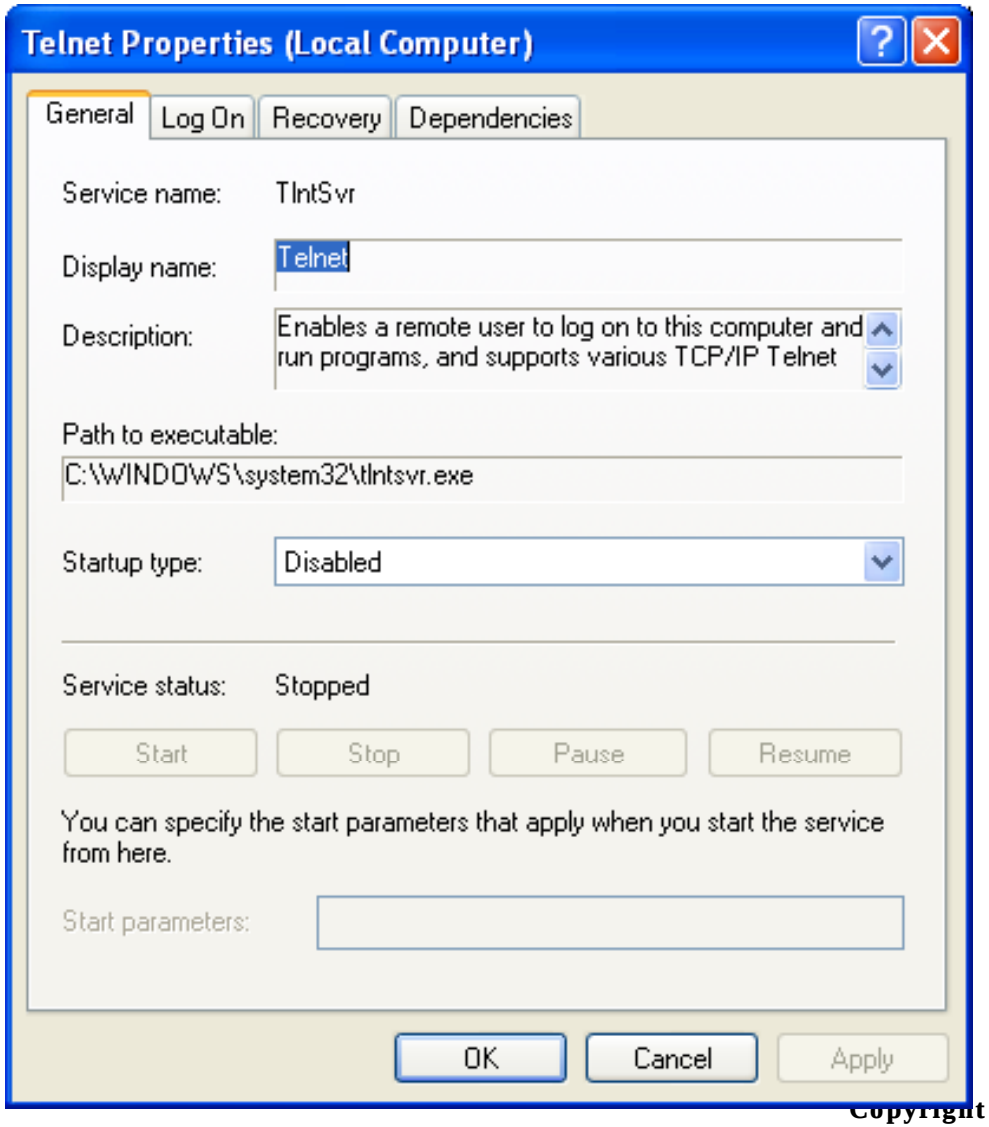
This service is installed by default but disabled

If disabled, remote user access to programs will be unavailable through the Telnet client

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Telnet



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Terminal Services

The service provides a multi session environment allowing client devices to interact with virtual Windows desktop session

This is installed by default, Configure the server or Add/Remove Windows Components to change the **Terminal Services** mode, with a startup type to manual

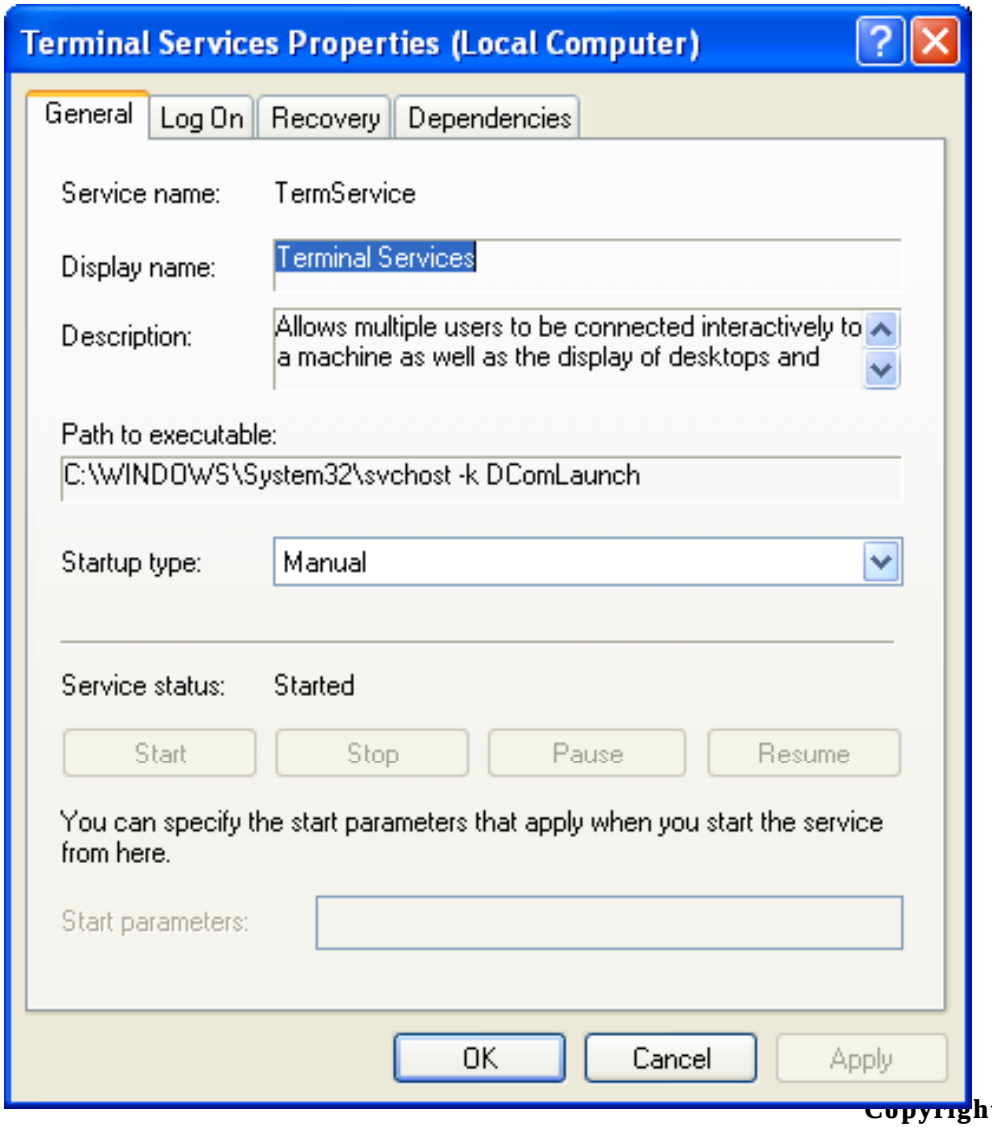
If disabled, Remote Assistance will not work

To prevent remote use clear the **Allow Remote Assistance** and **Allow Remote Desktop** checkboxes on the **Remote** tab of the **System Properties** property sheet

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Terminal Services



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Terminal Services Licensing

When a terminal server is connected this service installs a license server and offer registered client licenses

This service stores the client license and searches for the appropriate terminal

This service is needed by the servers where the service is installed in application mode

If disabled, the licenses are unable to issue

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Terminal Services Session Directory

TSSD:

- This service manages a multi session environment to allow a client to access a virtual windows desktop session and windows based programs
- This service uses clusters to route a connection between the user and the server where already a session is active
- This service monitors the disconnected sessions and resets the session
- If disabled, the made request will be sent to one of the active servers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Trivial FTP Daemon

The service is a part of RIS and do not need any authentication for Windows Server 2003

The following RFCs define TFTP protocol:

- RFC 1350 – TFTP
- RFC 2347 – Option extension
- RFC 2348 – Block size option
- RFC 2349 – Timeout interval, and transfer size options

By using this service the initial files necessary to begin remote installation process are been downloaded

This service is not installed by default

If disabled, the client computer requiring RIS will fail to install

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Uninterruptible Power Supply

This service is to connect a UPS to your computer as not to interrupt the work

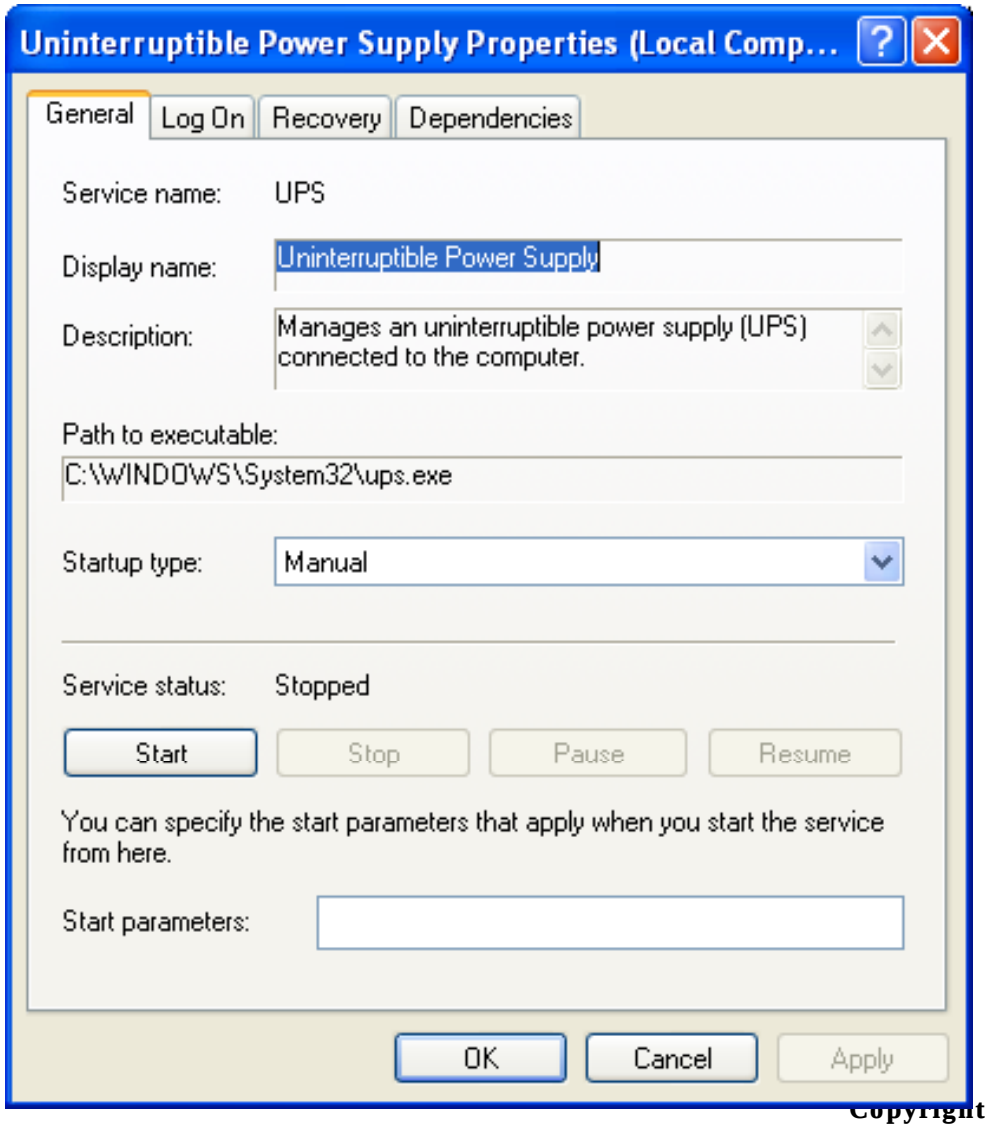
This is a default service, and is configured to manual

If stopped, the UPS will not be there to provide power backup

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Uninterruptible Power Supply



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Upload Manager

The file transfer (synchronous and asynchronous) between client and server is managed by this service

This service is helped to upload drivers and other needed updates when ever available

The service is installed by default but configured to manual

If disabled, the file transfer will not occur

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Virtual Disk Service

The service provides a single interface to manage block storage virtualization

Using this service, you can manage bind operations, performance monitoring, topology discovery and tracking, volume status, and fault tracking

The service is installed and configured to manual

If disabled, this service will no longer be available

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

WebClient

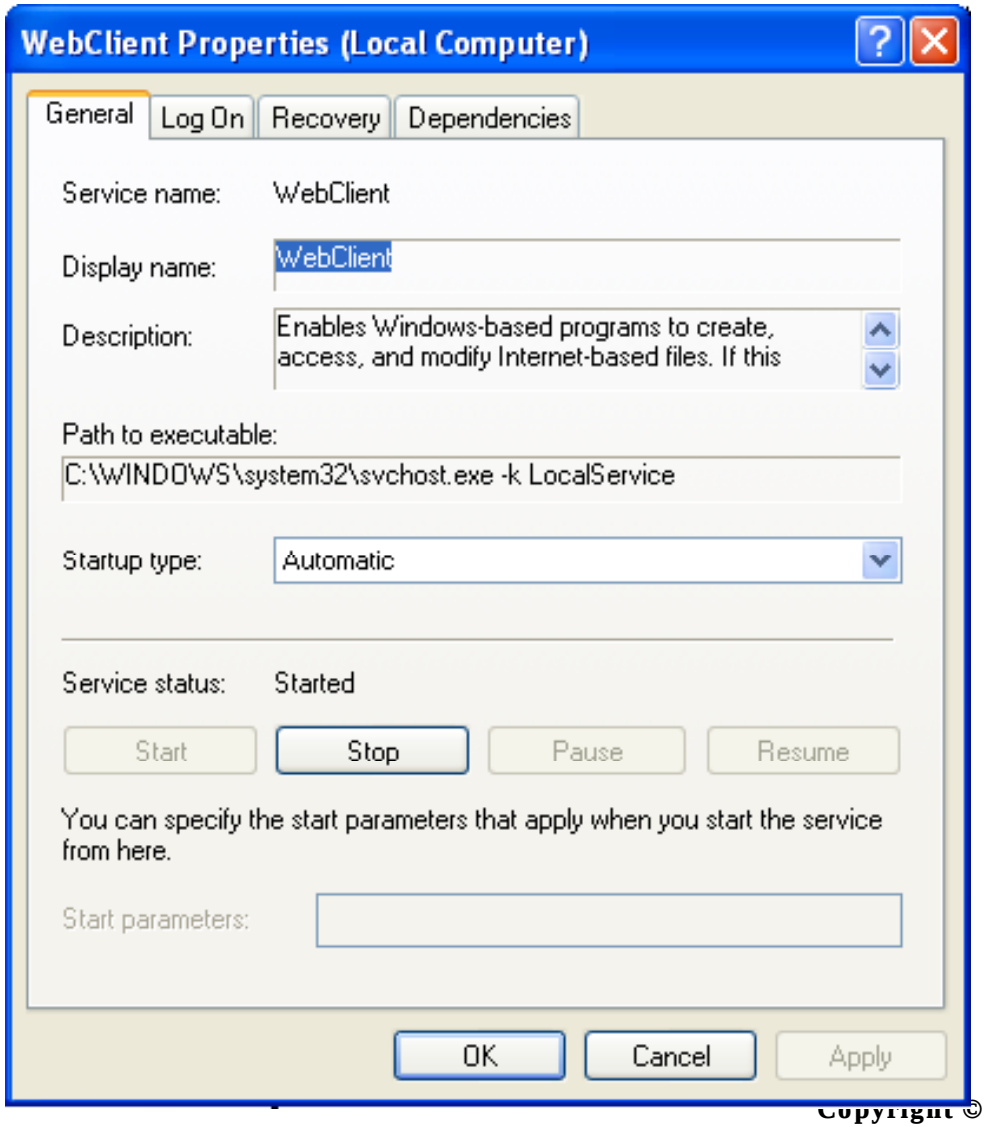
This service allows Win32 applications to access documents on internet

This service is installed and started automatically on Windows XP, but on Windows Server 2003 this service is disabled

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

WebClient



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Web Element Manager

This service is installed on Windows Server 2003, web edition

The administrator can connect to website on port 8098 to get the information on:

- Tabs to display on the Administration Web site
- Remote administration tasks that are available to the Administrator
- Table of contents
- Help topics
- Remote administration alerts that can be displayed

This service will start when ever a request is sent and stops after it operations are performed

If disabled, a service dependent on this service will not start

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows Firewall /Internet Connection Sharing

This service uses a dial up or broadband connection to provide network address translation (NAT), address and name resolution, and/or intrusion-prevention services

- Enabled - Computer becomes integrated gateway

This service has a location-aware Group Policy

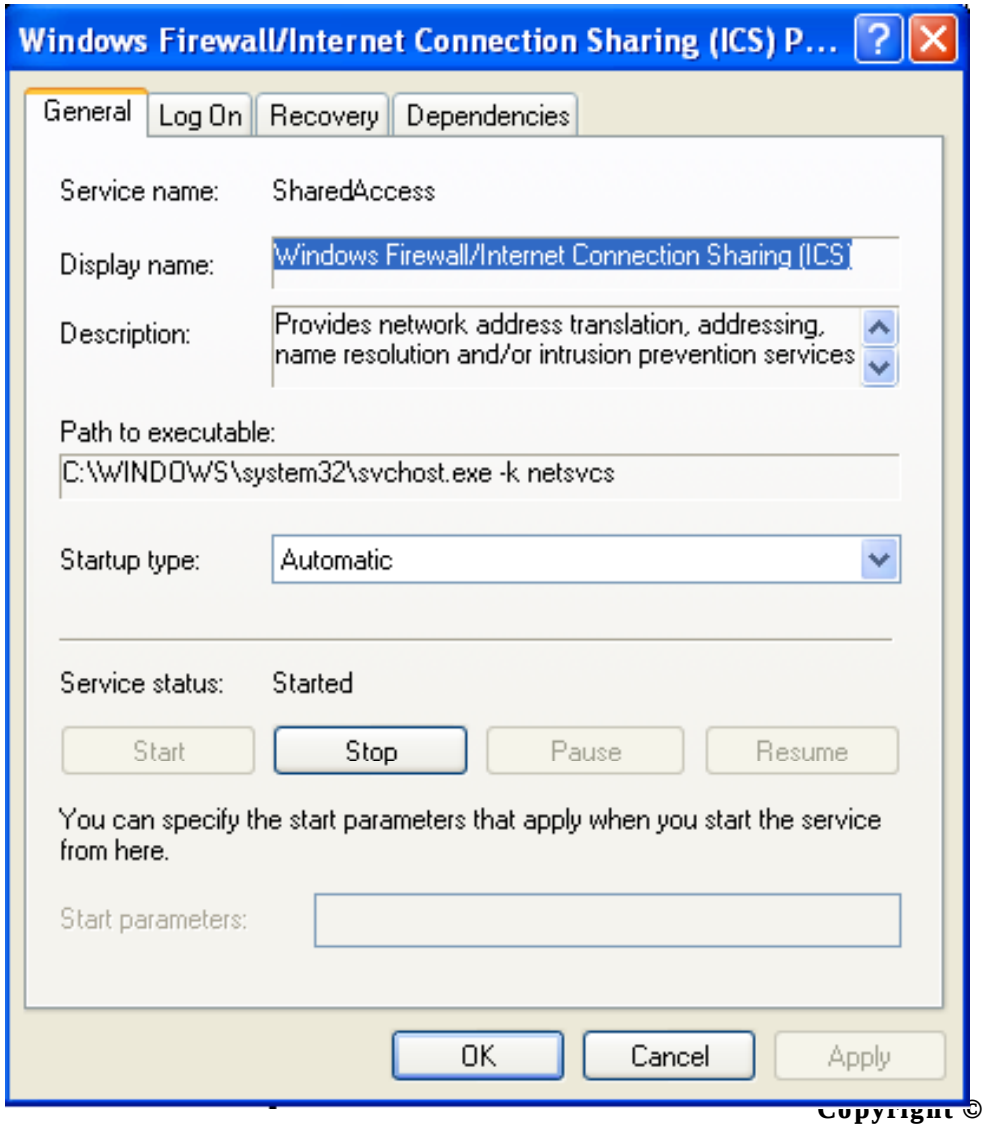
In windows XP and Windows Server 2003 this service is automatically started by default, but disabled in Windows Server 2003

If disabled, network services will be unavailable

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows Firewall /Internet Connection Sharing



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

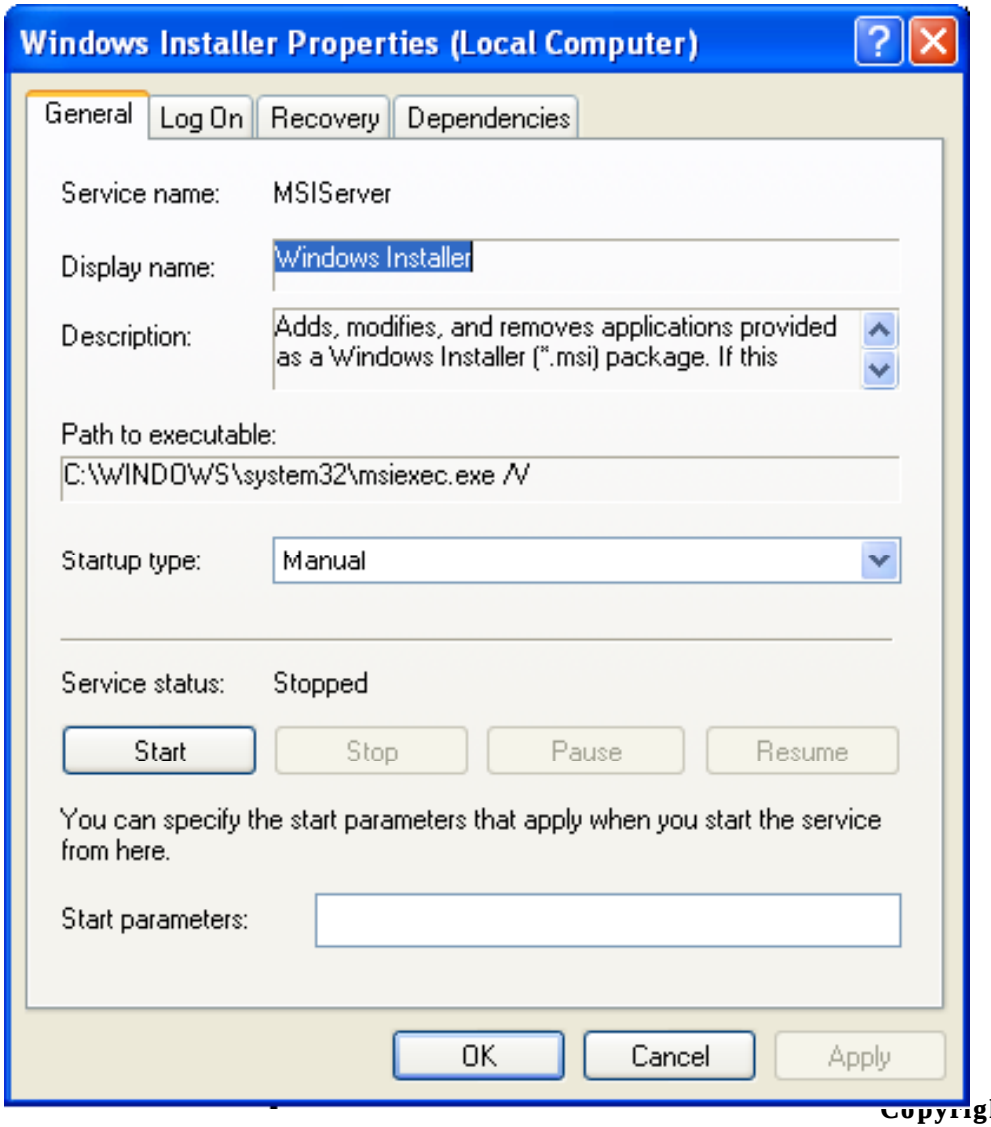
Windows Installer

- This service manages the process of installing and removing of applications
- This service can be used to modify, repair, or remove existing applications
- This service has a package of .msi files containing information on application setup and installation
- This service also acts as extensible software management system
- This is installed by default but configured to manual
- If disabled, application can not be installed if they need this service to do so

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows Installer



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows System Resource Manager

This service is an optional tool to help customers deploy applications into consolidation scenarios

The **WSRM** service is optional and runs on Windows 2000 service Pack 3

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows Time

This service manages the synchronization of date and time on the whole network

A NTP (Network Time Protocol) is used to synchronize the clock of the client and the server

Using this service the time can be synchronized from an external time server

If disabled, the local computer will not be synchronized with the external network

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows Time (Cont'd)

There are two possible scenarios:

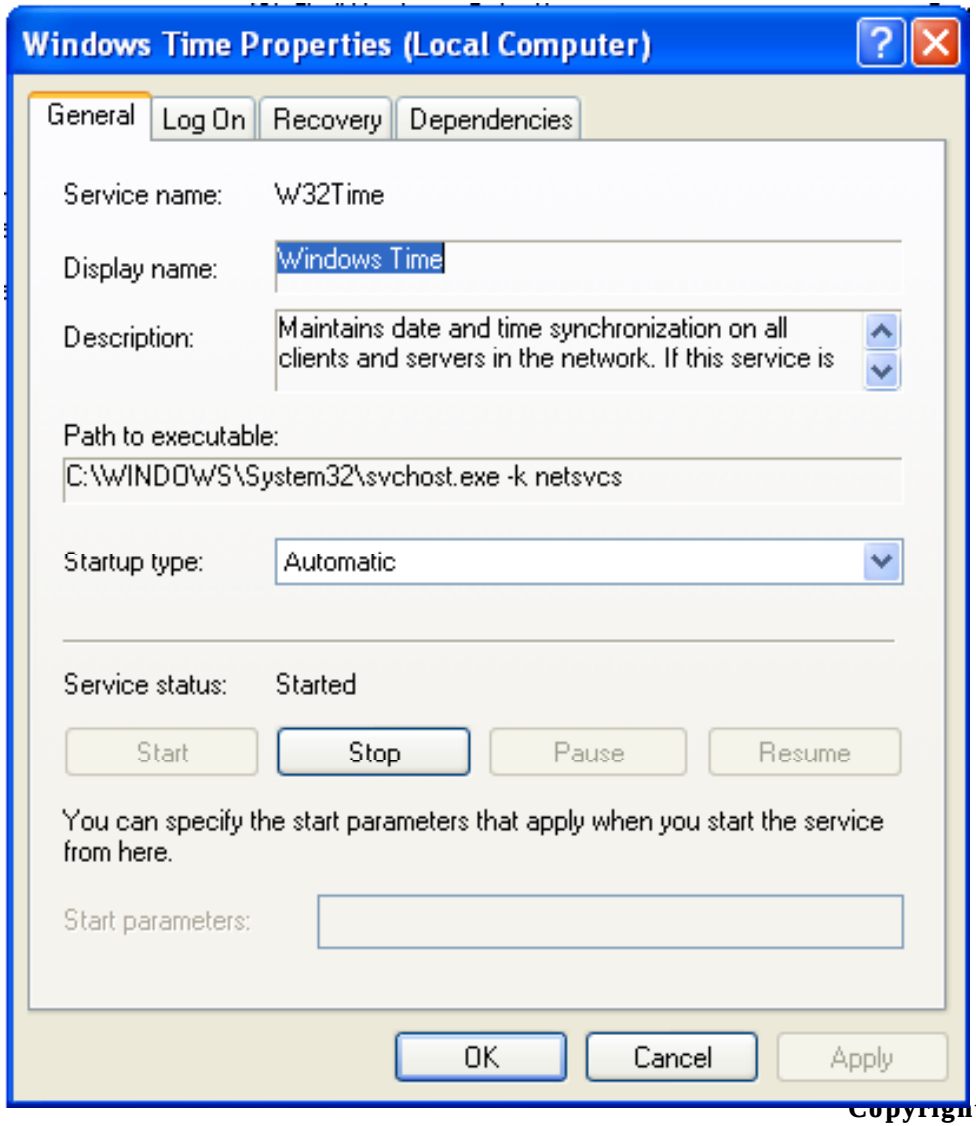
- If you stop the service on a workstation, the workstation will not be able to synchronize its time with another source but no other external server will be affected
- If you stop the service on a domain controller, the same effect as in the previous scenario will apply but domain members will also be unable to synchronize time with it

By default, the service is installed and run automatically on Windows XP and Windows Server 2003 computers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows Time (Cont'd)



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

WinHTTP Web Proxy Auto-Discovery Service

This service process the Web Proxy Auto-Discovery (WPAD) protocol for Windows HTTP Services (WinHTTP)

WPAD is a protocol enabling an HTTP client to automatically discover a proxy configuration

If disabled, A WAPD protocol is executed with in the HTTP client, but not in an external service process and there will be no functionality loss

This service is installed by default and configured to manual

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Wireless Configuration

The service starts automatic configuration for IEEE 802.11 wireless adapter for wireless communication

This service is installs and starts automatically on Windows Server 2003 and Windows XP

If disabled, automatic wireless configuration will not be provided

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Workstation

The service creates and maintains network connection and communication

It is installed and run automatically on Windows XP and Windows Server 2003

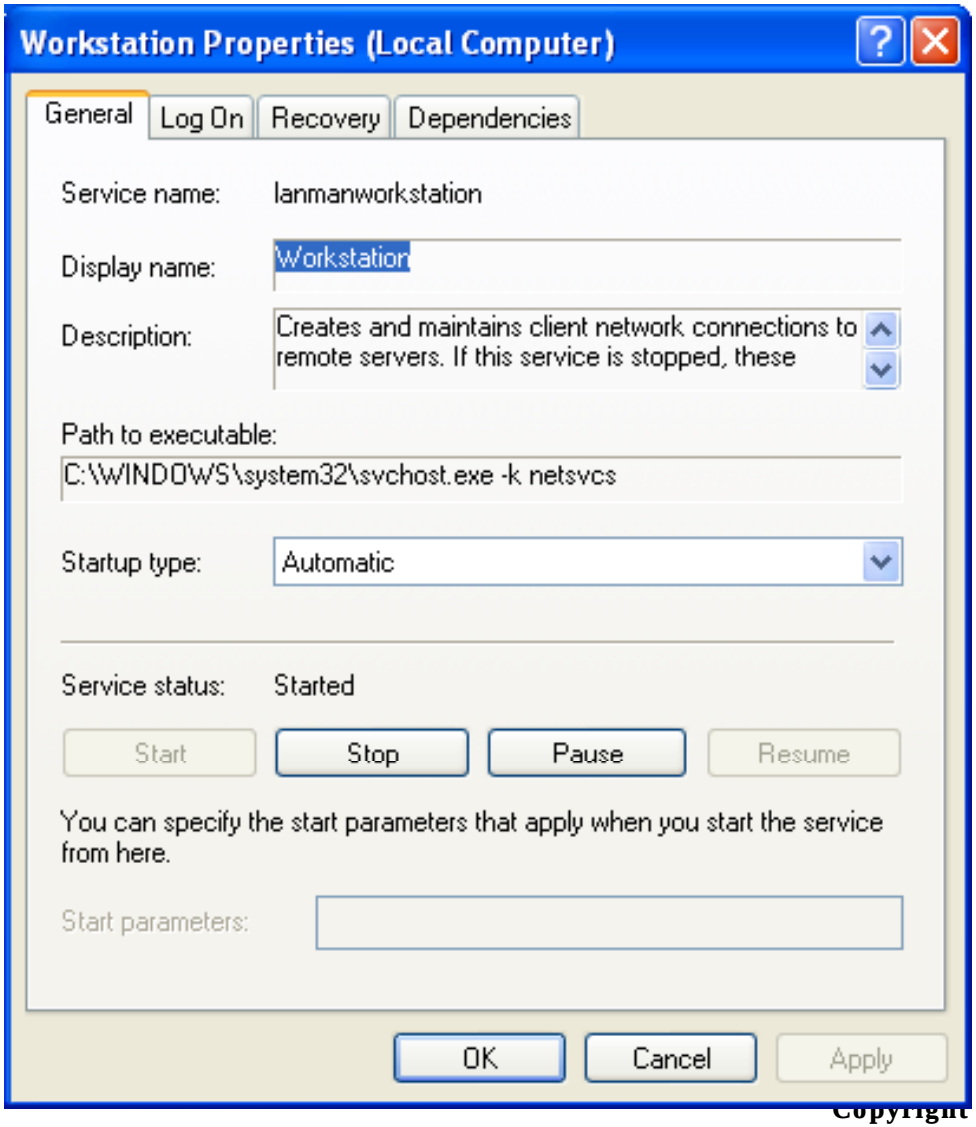
If disabled, remote servers can not be connected and can not access files through named pipes

Internet browsing and web client will work properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Workstation



Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

World Wide Web Publishing Service

The service provides web connectivity and administration of sites through MMC IIS snap-in

This service is an optional component installed on Windows Server 2003 or Windows XP as part of the IIS package

If stopped, the Windows Server 2003 operating system can not serve a Web request

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Software Restriction Policies

Software restriction policies provide a policy-driven system to specify which programs are allowed to execute and which are not

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

The Threat of Malicious Software

The daily increase usage of network in business computing is more likely than an organization's users which encounter malware (malicious software)

These policies can help organizations protect themselves through another layer of defense against viruses, Trojans, and other types of malicious code

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

The Threat of Malicious Software (Cont'd)

Vulnerability

- Networks are collaborated increasingly in use of communication, instant messaging and peer-to-peer applications, and this may increase risk from viruses, worms and other forms of malware
- E-mail and instant messaging can transport unwanted hostile code which can take many forms from native Windows executable (.exe) files, to macros in word processing (.doc) documents, to script (.vbs) files
- E-mail messages are often transmitted with viruses and worms which include techniques to trick users for activating the malicious code

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

The Threat of Malicious Software (Cont'd)

Vulnerability

- Various forms of code can be difficult for users to know which is safe and which is not
- Activate malicious code may damage hard disk, flood a network, confidential information or compromise security of computer

Countermeasure

- To test the policies a sound design can be created in organization before deploying them into production environment

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

The Threat of Malicious Software (Cont'd)

Potential Impact

- A hostile application and other disable applications are allowed through flawed software restriction policy.
- Sufficient resources are given to manage and trouble shoots the implementation of policies.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows XP and Windows Server 2003 Administrative Templates

This section of the group policy gives the settings for appearance of the computer in the environment

This section has many settings available to configure and import .adm files to make other settings available

Administrative template settings are shown in this section

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Computer Configuration Settings

This settings made in this section are available only to the members of Active Directory® directory service domain

NetMeeting

- This feature allows user to conduct vital meeting on the network
- They can be configured from the following location:
  - **Computer Configuration\Administrative Templates\Windows Components\NetMeeting**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

NetMeeting

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Remote Desktop Sharing

By using the policy, the remote desktop sharing features can be stopped

Enable – The policy cannot be configured to automatically answer calls and remote control of the local desktop

The values for the Disable remote Desktop Sharing setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Remote Desktop Sharing (Cont'd)

Vulnerability

- Enabled, the remote desktop sharing feature is not accessible

Countermeasure

- Configure the policy setting to **Enabled**

Potential Impact

- User cannot configure remote desktop sharing but can make use of features like Windows Remote Assistance and Remote Desktop if enabled

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Explorer Computer Settings

Internet Explorer (IE) a Web browser in Windows XP and Windows Server 2003 can be managed through group policies

Configure this policy setting at:

- **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer**

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Automatic Install of Internet Explorer Components

This setting stops the automatic download of components through IE, when ever the user browses a site

If disabled or not configured, the user may be stopped to install the necessary software

By this setting the admin can set conditions on what kind of components can be installed

The values for the **Disable Automatic Install of Internet Explorer components** setting are:

- **Enabled**
- **Disable**
- **Not Configured**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Automatic Install of Internet Explorer Components (Cont'd)

Vulnerability	• Some Web sites may have malicious code in their components and if a user trying to access this component the code can be executed and data may loss
Countermeasure	• Configure the setting to Enabled
Potential Impact	• IE will not allow downloading of components automatically

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Periodic Check for Internet Explorer Software Updates

This policy disables the automatic update option on IE, and user will not know what newer versions are updated for the software

If disabled, IE will check on updates every 30 days

By this policy setting admin can keep track on the version control of IE

The values for the Disable Periodic Check for Internet Explorer software updates setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Periodic Check for Internet Explorer Software Updates (Cont'd)

Vulnerability

- This policy can be enabled to stop automatic periodic checks for updates

Countermeasure

- Configure the policy setting to **Enabled**

Potential Impact

- This will not allow IE to automatically download and install and component
- But the admin should have any other program that can run updates for necessary software

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Software Update Shell Notifications on Program Launch

This policy will not display a message to the user if any Microsoft Software Distribution Channel installs a new component

If disabled, a message is sent to inform the users about the new installation

The values for the **Disable software update shell notifications on program launch** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Software Update Shell Notifications on Program Launch (Cont'd)

Vulnerability

- By enabling this policy, the administrator may not want the users to have any kind of intimation on the installation of components and service packs

Countermeasure

- Configure the setting to Enabled

Potential Impact

- Users will not receive any message to notify the about any installation

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Make Proxy Settings Per-Machine (Rather than Per-User)

If enabled, the user cannot change user defined proxy settings

The values for the Make proxy settings per-machine (rather than per-user) setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Make Proxy Settings Per-Machine (Rather than Per-User) (Cont'd)

Vulnerability

- If disabled, users can set there own proxy settings

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- The users have to use the settings defined for the computer

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Zones: Do Not Allow Users to Add/Delete Sites

The policy disables site management settings for security zones

If disabled, users can Add/Remove site zones

The values for the Security Zones: Do not allow users to add/delete sites setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Zones: Do Not Allow Users to Add/Delete Sites (Cont'd)

Vulnerability

- If the policy is not configured, the users can add/remove sites which may contain malicious data

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- An administrator has to configure to add any remote site

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Zones: Do Not Allow Users to Change Policies

This policy setting permit you to effectively disable the Custom Level button and Security level for the zone slider on the Security tab in the Internet Options dialog box

If disabled, users may modify the security zone settings. The values for the Security Zones: Do not allow users to change policies settings are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Zones: Do Not Allow Users to Change Policies (Cont'd)

Vulnerability	• If users can change the security setting malicious data codes can be available
Countermeasure	• Configure the setting to **Enabled**
Potential Impact	• For IE zone, users are not able to configure security setting

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Turn off Crash Detection

The crash detection feature in IE is managed by this policy

If enable, A crash in IE will start Windows Error Reporting

If disabled, crash detection feature will be functional

The values for the **Turn off Crash Detection** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Turn off Crash Detection (Cont'd)

Vulnerability	• This report may contain important information from the computer memory
Countermeasure	• Configure the policy setting to **Enabled**
Potential Impact	• The information gathered by the crashes on the add-ons is not reported to Microsoft • Disabling this option will allow to report the problem

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow Users to Enable or Disable Add-ons

By configuring this policy, user cannot operate through Manage Add-ons

If enabled, it is not possible to Manage Add-ons

If disabled, the user will be able to Manage Add-ons

The values for the **Do not allow users to enable or disable add-ons** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow Users to Enable or Disable Add-ons (Cont'd)

Vulnerability

- The add-ons not allowed by the organization security policy will relatively cause some problem

Countermeasure

- Configure the value of the setting to **Enabled**

Potential Impact

- If enabled, Add-ons cannot be managed

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Explorer\Internet Control Panel\Security Page

Configure Internet Explorer Security Page Group Policy settings within the Group Policy Object Editor at the location:

- **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page**

Follow the general security guidelines

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Explorer\Internet Control Panel\Security Page (Cont'd)

Vulnerability

- If users are allowed to any security setting in IE, they may install applications with malicious code

Countermeasure

- Use the settings in the **Internet Explorer\Internet Control Panel\Security Page** node to configure values for security zone-related behavior

Potential Impact

- The default values for these policy settings provide enhanced security over earlier versions of Windows

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Explorer\Internet Control Panel\Advanced Page

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Software to Run or Install Even if the Signature is Invalid

This policy settings concludes on the usage of a software with an invalid signature

Enable – Install and run software with invalid file signature

Disable – Cannot install software with invalid file signature

The values for the **Allow software to run or install even if the signature is invalid** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Software to Run or Install Even if the Signature is Invalid (Cont'd)

Vulnerability	• All software download have digital signatures attached to it, to recognize its validity • The validity of unsigned code cannot be ascertained
Countermeasure	• Configure the setting to **Disabled**
Potential Impact	• The software signatures may have invalid signatures. A proper check has to be performed before using the software

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Active Content from CDs to Run on User Machines

This policy concludes whether active contents on CDs can run on user computers.

The values for the **Allow active content from CDs to run on user machines** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Active Content from CDs to Run on User Machines (Cont'd)

Vulnerability

- The installing software from a CD rather than the network can crack an organization security policy

Countermeasure

- Configure the setting to **Disabled**

Potential Impact

- When enabled, applications to be installed form the CD might not work properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Third-party Browser Extensions

(This policy setting is only available in Windows Server 2003.)

A third-party browser extension known as Browser Helper Objects (BHOs) can be used

The values for the **Allow third-party browser extensions** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Third-party Browser Extensions (Cont'd)

Vulnerability

- The Third-party browser extensions may not be safe, and may violate security policy

Countermeasure

- Configure the setting to **Disabled**

Potential Impact

- If disabled, user can install third-party browser extensions

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Check for Server Certificate Revocation

(This policy setting is only available in Windows Server 2003.)

A Secure Socket Layer connection between browser and remote server gives a certificate to be used for initial negotiation

If enabled, it determines that the certificate is on the issuing authority's certificate revocation list

The values for the Check for server certificate revocation setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Check for Server Certificate Revocation (Cont'd)

Vulnerability

- User may communicate with server with an invalid certificate. This may lead to information disclosure or even active attacks

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- If enabled, warning messages can be given

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Check for Signatures On Downloaded Programs

(This policy setting is only available in Windows Server 2003.)

This policy will check for a digital signature on the downloaded software

If enabled, this policy will check for the signature and can display information before downloading

The values for the **Check for signatures on downloaded programs** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Check for Signatures on Downloaded Programs (Cont'd)

Vulnerability	• Any virus can be downloaded unknowingly
Countermeasure	• Configure the setting to **Enabled**
Potential Impact	• When enabled, user can view the information about software

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Save Encrypted Pages to Disk

(This policy setting is only available in Windows Server 2003.)

When IE accesses any pages from the remote server, the pages are stored in a temporary folder as IE can access the pages easily next time with out a reconnection

The values for the Do not save encrypted pages to disk setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Save Encrypted Pages to Disk (Cont'd)

Vulnerability

- These pages may contain sensitive information like password and credit card numbers

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- If disabled, the pages will not be saved to the disk

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Empty Temporary Internet Files Folder when Browser is Closed

(This policy setting is only available in Windows Server 2003.)

When files are downloaded from the Internet the temporary files are cached in a temporary folder

These temporary folders have to be cleaned by IE

The values for the **Empty Temporary Internet Files folder when browser is closed** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Empty Temporary Internet Files Folder when Browser is Closed (Cont'd)

Vulnerability

- The file in the temporary folder may contain sensitive information, which may be accessed by any other user

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- IE uses the temp folders to increase browser performance
- If disabled, the time and bandwidth may increase

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Explorer\Security Features

The **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features**

- portion of the Windows Administrative Templates has many settings

Each of these policy settings has their subordinate settings:

Internet Explorer Processes.

- Possible values:
  - **Enable** – the behavior is stopped for IE and Windows Explorer process
  - **Disable** – Default settings are considered
  - **Not Configured** – Default settings are considered

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Explorer\Security Features (Cont'd)

Process List

- This gives individual processes with security features to be enabled or disabled
- A list known, as process list will contain the process applied by the feature
- The value 1 disabled the feature and 0 enables it

All Processes

- Possible values:
  - Enable – the behavior is stopped for IE and Windows Explorer process
  - Disable – Default settings are considered
  - Not Configured – Default settings are considered

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Binary Behavior Security Restriction

IE has components with dynamic binary behavior for HTML elements on to which they where attached

IE security options do not control these dynamic binary behaviors

This policy setting allows some behaviors with admin permission

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Binary Behavior Security Restriction (Cont'd)

Vulnerability	• Some behaviors that are written bad and malicious behaviors can be accessed and compromised
Countermeasure	• Disable binary behaviors and allow only a set of admin-approved behaviors
Potential Impact	• Some applications dependent on binary behavior may not work properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

MK Protocol Security Restriction

This policy blocks MK protocol to reduce attack possibility

The MK protocols have been used to extract data from compressed files

Vulnerability

- Vulnerabilities may be in the MK protocol handler, or in applications calling it

Countermeasure

- The MK protocol must be blocked when it is not necessary

Potential Impact

- The applications needing MK protocol will fail

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Local Machine Zone Lockdown Security

A web browser when access a web page in IE, it places some restrictions as per the security zone

Each zone will be having a set of restrictions

The security zone is decided on basis of the location of access. (Example: An open network may have more restrictions than an intranet work in an organization)

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Local Machine Zone Lockdown Security (Cont'd)

Vulnerability

- Generally attackers try to get privileges to access a computer in a local machine zone

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- If this settings are enabled, IE application which use local HTML may not work properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Consistent MIME Handling

The MIME (Multipurpose Internet Mail Extensions) data is used to handle files downloaded from web server

This setting concludes that Internet Explorer requires that all file-type information that is provided by Web servers be consistent

Enable – IE checks all received files and enforces consistent MIME data

Disable – IE do not need consistent MIME data

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Consistent MIME Handling (Cont'd)

Vulnerability

- An attacker can send executable content by using a non-executable MIME type

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Applications dependent on MIME download objects will be failed

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

MIME Sniffing Safety Features

The process of inspecting the MIME file (Data file, Executable file) is known as MIME sniffing

If enabled, MIME sniffing will not send a file of one type to another

If disabled, MIME sniff that promotes a file

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

MIME Sniffing Safety Features (Cont'd)

Vulnerability	• A malicious web site sends one MIME type with a false indication
Countermeasure	• Configure the setting for **All Processes** to **Enabled**
Potential Impact	• MIME files with wrong functionality will not work

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Scripted Window Security Restrictions

IE allows scripting for opening, resizing and repositioning the windows programmatically like, restricting pop-up windows

If enabled, these restrictions are applied to IE or Windows Explorer

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Scripted Window Security Restrictions (Cont'd)

Vulnerability	• Some websites will resize windows to make the user to use a window with some malicious code
Countermeasure	• Configure the setting for **Internet Explorer Processes** to **Enabled**
Potential Impact	• The malicious website may not work properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Restrict ActiveX Install

This policy is used to block ActiveX control installation

If enabled, users will not be prompted ActiveX control installation, which has to be done manually

If disabled, ActiveX control installation prompts will not be blocked

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Restrict ActiveX Install (Cont'd)

Vulnerability

- User may choose some ActiveX controls which are not permitted to use

Countermeasure

- Configure the setting for **Internet Explorer Processes** to **Enabled**

Potential Impact

- If enable, users cannot be able to install authorized legitimate ActiveX controls

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Restrict File Download

If the policy is enabled, file download prompts that are not user-initiated are blocked

Vulnerability	• Some website start a file download with out users idea
Countermeasure	• Configure the policy value for **Internet Explorer Processes** to **Enabled**
Potential Impact	• None

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Network Protocol Lockdown

Administrators can specify individual protocols (including HTTP and HTTPS) in this policy setting to control which protocols may be used to obtain active content

Vulnerability

- Users may download the malicious data to be executed

Countermeasure

- Configure the policy setting for Internet Explorer Processes to Enabled

Potential Impact

- If zone controls are set, users cannot run pages with active controls

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Information Services

Microsoft Internet Information Service (IIS) 6.0 the built-in web server, allows to share the file easily

Configure the IIS setting:

- **Computer Configuration\Administrative Templates\Windows Components\Internet Information Services**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Prevent IIS Installation

IIS 6.0 is not installed on the computer by default. So, by setting this option to enable you can restrict the installation in future

The values for the **Prevent IIS installation** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Prevent IIS Installation (Cont'd)

Vulnerability

- The older versions of IIS have serious security problem related with it
- IIS 6.0 is secure than its previous versions
- IIS 6.0 should be installed only on web servers

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Applications that need IIS may not be installed
- This policy setting will have no effect if it is enabled on a computer on which IIS is already installed

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Terminal Services

This component is builds on a solid foundation by the application server mode; it is extended with new capabilities in Windows XP

This policy allows Windows based applications to any computing device

When an application runs on TS, the execution is carried on the server, and only display information is transmitted on the network

Configure the Policy settings at the location:

- **Computer Configuration\Administrative Templates\Windows Components\Terminal Services**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log Off of an Administrator Logged in to the Console Session

This policy determines whether an administrator can log off an admin form a remote server where he is logged on

The console session is also known as Session 0

The values for the **Deny log off of an administrator logged in to the console session** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log Off of an Administrator Logged in to the Console Session (Cont'd)

If enable, Logging off an admin connected to the computer is not possible

If disabled, an admin can logoff another admin from a computer

If the current administrator is logged off, unsaved data will be lost

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Deny Log Off of an Administrator Logged in to the Console Session (Cont'd)

Vulnerability	• An attacker can make a Terminal Server session and get access to the console • The attacker will have a complete control on the computer
Countermeasure	• Configure the setting to **Enabled**
Potential Impact	• An administrator cannot log off another admin from a session o console

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow Local Administrators to Customize Permissions

This policy controls the admin rights for permissions in Terminal Services Configuration (TSCC) tool

If enabled, the admin will not be able to change the security description. The security descriptions are Read Only

If disabled, the server admin will have full right for read and write to the security descriptions in TSCC permission tab

The values for the **Do not allow local administrators to customize permissions** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow Local Administrators to Customize Permissions (Cont'd)

Vulnerability

- An attacker who gained permission on a server can change them using TSCC tool to stop other user connections to server and generate a DoS connection

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- The TSCC **Permissions** tab cannot customize per-connection security descriptors or change the default security descriptors

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Sets Rules for Remote Control of Terminal Services User Sessions

This policy gives the control level in a Terminal Server session

There are two types of remote control permissions:

- **View Session** – Permits the remote control user to watch a session
- **Full Control** – Permits the remote control user to interact with the session

If enabled, the admin can interact with the Terminal server session

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Sets Rules for Remote Control of Terminal Services User Sessions (Cont'd)

To disable, set the option to No remote control allowed

If disabled, the admin cannot get the level of permission using TSCC tool

The values for the **Sets rules for remote control of Terminal Services user sessions** setting are:

- Enabled with options for:
  - No remote control allowed
  - Full Control with user's permission
  - Full Control without user's permission
  - View Session with user's permission
  - View Session without user's permission
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Sets Rules for Remote Control of Terminal Services User Sessions (Cont'd)

Vulnerability	• At attacker can gain access as an admin and view the actions of other users
Countermeasure	• Configure the setting to **Enabled** and select the **No remote control allowed** option
Potential Impact	• Administrators will not be able to use the remote control feature to assist other Terminal Services users

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Client/Server Data Redirection

Terminal Services allows data and resources from the client and server to be redirected

This section allows you to customize the redirection type

Configure the Terminal service setting at:

- **Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client\Server data redirection**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Time Zone Redirection

This policy decides on redirecting the time zone to Terminal server session

If enabled, clients can send their time zone information to the server

The computer's time and time zone can be changed by connecting to, Session 0

If disabled, time zone cannot be sent to the server

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Time Zone Redirection (Cont'd)

The values for the Allow Time Zone Redirection setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability	• The time zone can be transmitted between server and the local machine
Countermeasure	• Configure the policy setting to **Disabled**
Potential Impact	• Time zone redirection will not be possible

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow COM Port Redirection

By using this policy redirecting the data to the client port from the remote computer can be stopped

If enabled, data cannot be redirected to COM port computers. And server data cannot be sent to the local computer

If disabled, redirection of Terminal Service COM port is possible

An admin can stop the redirection using TSCC tool

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow COM Port Redirection (Cont'd)

The values for the **Do not allow COM port redirection** setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

- No direct user interaction is needed to forward data from Terminal server session to local computer

Countermeasure

- Configure the policy setting to **Enabled**

Potential Impact

- COM port redirection will not be possible

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow Client Printer Redirection

This policy decides on using the client printers on the Terminal server session

Bt default client printer is mapped to Terminal server session

If enabled, the print job cannot be redirected in the Terminal server session

The redirection is possible when this policy is disabled

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow Client Printer Redirection (Cont'd)

The values for the **Do not allow client printer redirection** setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

- No user interaction is necessary to forward data

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Printer redirection will not be possible

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow LPT Port Redirection

This policy tells to stop the redirection of data to client parallel port or not during a Terminal Server session

If enabled, users cannot redirect server data to their local LPT port

If disabled, LPT port redirection is allowed

The values for the **Do not allow LPT port redirection** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow LPT Port Redirection (Cont'd)

Vulnerability	• No user interaction is necessary to forward data
Countermeasure	• Configure the setting to Enabled
Potential Impact	• LPT port redirection will not be possible

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow Drive Redirection

Using this policy, mapping client drives upon connection to the Terminal service automatically; this behavior can be over ridden

If enabled, client drive redirection is prevented

If disabled, client drive redirection is always allowed

The values for the **Do not allow drive redirection** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Allow Drive Redirection (Cont'd)

Vulnerability	• No user interaction is necessary to forward data
Countermeasure	• Configure the setting to **Enabled**
Potential Impact	• Drive redirection will not be possible

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Encryption and Security

Configure the Terminal Server Encryption and Security settings in the following location:

- **Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Set Client Connection Encryption Level

This policy decides on enforcing an encryption level for the data sent between client and remote computer during the terminal server session

If enabled, a level of encryption can be given for connections on the server. By default the level is high

If disabled, no encryption level is given

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Set Client Connection Encryption Level (Cont'd)

The values for the **Set Client Connection Encryption Level** setting are:

Enabled with encryption options:

- **Client Compatible**. The level encrypts data to maximum key strength. This is used for remote computers running in mixed or legacy client environment.
- **High Level**. This level encrypts the data to 128-bit. Clients that do not support this level of encryption cannot connect.
- **Low Level**. The level encrypts the data to 56-bit. In this data between server and client is not encrypted.

Disabled

Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Set Client Connection Encryption Level (Cont'd)

Vulnerability

- If Terminal Server client will use low level encryption, an attacker can decrypt after capturing the traffic

Countermeasure

- Configure the setting to High Level

Potential Impact

- Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Always Prompt Client For A Password On Connection

- This policy decides on prompting the client for password ever time he is connected
- This policy will ask for password to the client at Terminal service even after connecting to Remote Desktop connection
- If enabled, automatic logon is not accepted
- If disabled, user can logon automatically
- An administrator can still enforce password prompting by using the TSCC tool

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Always Prompt Client For A Password On Connection (Cont'd)

The values for the **Always prompt client for a password on connection** setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

- Users are generally allowed to store their username and password while creating Remote Desktop connection.
- If an attacker accesses a Remote computer and gains access then by using the stored password he can gain access to the Terminal Server.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Always Prompt Client For A Password On Connection (Cont'd)

Countermeasure	• Configure the setting to **Enabled**.
Potential Impact	• Users will always have to enter their password when they establish new Terminal Server sessions

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

RPC Security Policy

Configure the Terminal Server RPC Security setting in the following location:

- **Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security\RPC Security Policy**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Secure Server (Require Security)

This setting decide that a Terminal Server needs secure remote procedure call (RPC) communication with all clients or allows unsecured communication

Using RPC the communication can be made more secure

If enabled, the request from a RPC clients are only accepted which has a secure request

If disabled, the requests are accepted at any level of security for all RPC traffic

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Secure Server (Require Security) (Cont'd)

The values for the **Secure Server (Require Security)** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Secure Server (Require Security) (Cont'd)

Vulnerability	• By the un-secure RPC communication the server is exposed to the man-in-the-middle attack and data disclosure attack
Countermeasure	• Configure the setting to **Enabled**
Potential Impact	• Clients that do not support secure RPC will be unable to remotely manage the server

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Sessions

Configure additional Terminal Server RPC Security settings in the following location:

- **Computer Configuration\Administrative Templates\Windows Components\Terminal Services Encryption and Security\Sessions**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Set Time Limit For Disconnected Sessions

A time limit can be set to the Terminal Server session, which is decided by this policy

The specified time is the maximum time that a disconnected session will remain active

If enabled, the session will be deleted after the specified time limit

If disabled, no time limit is specified for disconnected sessions.

The values for the **Set time limit for disconnected sessions** setting are:

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Set Time Limit For Disconnected Sessions (Cont'd)

The values for the **Set time limit for disconnected sessions setting** are:

Enabled with time specification options for:

- Never
- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes
- 30 minutes
- 1 hour
- 2 hours
- 3 hours
- 1 day
- 2 days

Disabled

Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Set Time Limit For Disconnected Sessions (Cont'd)

Vulnerability	• Every Terminal Server session will use system resources.
Countermeasure	• Configure the setting to **Enabled** and select **1 day** as the option in the **End a disconnected session** list box.
Potential Impact	• The unclosed sessions will be forcibly disconnected after 24 hours of in-activity.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Reconnection From Original Client Only

This policy decides whether the Terminal service will allow a user to connect to his session (disconnected) from a different computer rather than the one used for creating the session

The setting allows the user to do so

If enabled, user can only reconnect form the original client computer. If a user tries from another computer a new session is created

If disabled, user can connect from any computer

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Reconnection From Original Client Only (Cont'd)

The values for the **Allow reconnection from original client only** setting are:

- Enabled
- Disabled
- Not Configured

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Allow Reconnection From Original Client Only (Cont'd)

Vulnerability

- By default, user can connect from any computer
- If enabled, user has to connect from the same computer used before

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Users will connect to re-establish disconnected sessions with the computer that they used to establish the session

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows Explorer

Configure the following Windows Explorer setting in the following location:

- **Computer Configuration\Administrative Templates\Windows Components\Windows Explorer**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Turn Off Shell Protocol Protected Mode

This configures the amount of functionality for the shell protocol to open folders and launch files

In protected mode the functionality will not allow to open large set of files

If enabled, any application can open any folder or file

If disabled, it is set to protected mode and only some files and folders are opened

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Turn Off Shell Protocol Protected Mode (Cont'd)

The values for the **Turn off shell protocol protected mode** setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

- This protocol allows application to open files and folders. This can access and file with malicious code, and may create a DoS condition

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- If enabled, Web pages that depend on use of the shell protocol will not function properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows Messenger

Instant message can be sent to users on the network using Windows Messenger

The messages may include files and any attachments:

Configure the prescribed Windows Messenger setting in the following location:

- **Computer Configuration\Administrative Templates\Windows Components\Windows Messenger**

Do not allow Windows Messenger to be run

- The policy setting allows the user to disable Windows Messenger
- Configure this setting to **Enabled** to stop Windows Messenger

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows Update

This is used to download new software update, drivers etc

Configure the Windows Update settings in the following location:

- **Computer Configuration\Administrative Templates\Windows Components**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure Automatic Updates

This policy determines whether new updates are downloaded from Windows automatic update service or not

If enabled, the operating system will check when the computer is online and check for new updates

If disabled, updates will not take place automatically

Administrator can configure Automatic Updates through the Control Panel

The values for the **Configure Automatic Updates** setting are:

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure Automatic Updates (Cont'd)

Enabled, with options in the **Configure automatic updating** list box for:

- **2. Notify before downloading any updates and notify again before installing them.** In this option the windows will alert the user by giving a message in the status bar about the updates availability. When user clicks it will start auto-download and again prompts the user after completion, to install the updates
- **3. Download the updates automatically and notify when they are ready to be installed.** This option will download the updates automatically without any interruption to the user and then asks for installation
- **4. Automatically download updates and install them on the schedule specified below.** The download and installation will be done as per a specific schedule. The computer will start downloading and installing and if necessary it will restart the computer all by itself

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure Automatic Updates (Cont'd)

Disabled

Not Configured

If enabled, select one of the options (2, 3 or 4).

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure Automatic Updates (Cont'd)

Vulnerability

- The setting help you ensure that the computers have most recent critical operating system updates and service packs installed

Countermeasure

- Configure the policy setting to **Enabled** and select **4**

Potential Impact

- Operating system will download and install at 03:00 A.M. daily

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Reschedule Automatic Updates Scheduled Installations

This policy decides the time period to wait by the automatic updates before starting installation which was previously missed

IF enabled, any missed installation as per schedule will start as soon as the computer is started again

If disabled, the missed scheduled installation will take place with the next schedule installation

The values for the **Reschedule Automatic Updates scheduled installations** setting are:

- Enabled, with the option to specify a time between 1 to 60 minutes
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Reschedule Automatic Updates Scheduled Installations (Cont'd)

Vulnerability

- The automatic installations start after a time period when the computer restarts

Countermeasure

- Configure the setting to **Enabled** and specify 10 minutes

Potential Impact

- Automatic Updates will not start until 10 minutes after the computer restarts

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System

Configure the prescribed System computer setting in the following location:

- **Computer Configuration\Administrative Templates\System**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Turn off Autoplay

Autoplay will start reading a drive as soon as a disk is inserted and will start the setup file or start a media player if the disk is audio disk

If enabled, it prevents the Autoplay functionality. Autoplay is disabled by default

Vulnerability

- At attacker can use this feature to execute a malicious program and hurt the computer

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- The setup files should be initialized and launched manually

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Process The Run Once List

This policy ignores the run once list of programs which runs when Windows starts

If enabled, the run once list cannot be executed as it is the common way to attack

The values for the Do not process the run once list setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Process The Run Once List (Cont'd)

Vulnerability

- The programs in run once list can compromise the security of Windows XP client

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- If enabled, the users may loose some functionality
- This configuration may prevent some setup and installation programs

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Logon

Configure the prescribed Logon computer settings in the following location:

Computer Configuration\Administrative Templates\System\Logon

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Don't Display The Getting Started Welcome Screen At Logon

This policy is used to hide the welcome screen that is displayed when the user logs on

This policy is applicable to Windows 2000 Professional and Windows XP Professional

The operating systems Windows 2000 Server or Windows Server 2003 do not support this policy

The values for the **Don't display the Getting Started welcome screen at logon** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Don't Display The Getting Started Welcome Screen At Logon (Cont'd)

Vulnerability

- The welcome screen helps in exploring the system features

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Users will not see the welcome screen when logged on to the computers

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Process The Legacy Run List

Lists of programs are executed when Windows XP starts

This list is stored in registry at the location:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

The values for the Do not process the legacy run list setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Do Not Process The Legacy Run List (Cont'd)

Vulnerability	• An unauthorized user can run a program each time Windows start and can cause harm to the computer
Countermeasure	• Configure the setting to **Enabled**
Potential Impact	• If enabled, programs like antivirus software and software distribution and monitoring software are prevented from execution

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Group Policy

Configure settings in the following location to modify how group policy is processed:

- **Computer Configuration\Administrative Templates\System\Group Policy**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Explorer Maintenance Policy Processing

This policy tells when IE maintenance policies are updated

This setting overrides the present settings followed while installing updates

To enabled, use the check box and change the options

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Explorer Maintenance Policy Processing (Cont'd)

The values for the **Internet Explorer Maintenance policy processing** setting are:

- **Enabled**
  - Allow processing across a slow network connection.
  - Do no apply during periodic background processing.
  - Process even if the Group Policy objects have not changed.
- **Disabled**
- **Not Configured**

Vulnerability

- Enable this policy and select **Process even if the Group Policy objects have not changed** option to make sure policies will be reprocessed even if they have not changed.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Explorer Maintenance Policy Processing (Cont'd)

Countermeasure

- Configure the setting to **Enabled**
- Clear both of the check boxes for **Allow processing across a slow network** and **Do not apply during periodic background processing**
- Select the check box for **Process even if the Group Policy objects have not changed**

Potential Impact

- These policies are reapplied every time they are refreshed

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IP Security Policy Processing

This policy decides when IP security policies are updated

If enabled, the provided check boxes are used to change the options

The values for the **IP security policy processing** setting are:

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IP Security Policy Processing (Cont'd)

Enabled

- Allow processing across a slow network connection – Even the updates are being transmitted over a slow network. The updates process is carried
- Do not apply during periodic background processing – The updates to the effected policies are stopped in the background
- Process even if the Group Policy objects have not changed – Even if the policies have not been changed the updates and reapplies are processed

Disabled

Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

IP Security Policy Processing (Cont'd)

Vulnerability

- Enable and set **Process even if the Group Policy objects have not changed** option to reprocess the policies even if there is not much change

Countermeasure

- Configure the **IP security policy processing** setting to **Enabled**
- Clear the **Do not apply during periodic background processing** check box
- Select the **Process even if the Group Policy objects have not changed** check box

Potential Impact

- The IP security policies are reapplied for every refresh

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Registry Policy Processing

This policy decides when registry policies are updated

Enabled and use the checkbox to set the option

The values for the **Registry policy processing** setting are:

- Enabled with options for:
  - Do not apply during periodic background processing
  - Process even if the Group Policy objects have not changed
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Registry Policy Processing (Cont'd)

Vulnerability

- Enable and select the **Process even if the Group Policy objects have not changed** option for assurance that the policies will be reprocessed even if nothing is changed

Countermeasure

- Configure the setting to **Enabled**.
- Clear the **Do not apply during periodic background processing** check box
- Select the **Process even if the Group Policy objects have not changed** check box

Potential Impact

- For every refresh group policies are re applied

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Policy Processing

This policy setting decides when security policies are updated

If enabled, use the checkbox to change the option

The values for the **Security policy processing** setting are:

- Enabled with options for:
  - Do not apply during periodic background processing
  - Process even if the Group Policy objects have not changed
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Policy Processing (Cont'd)

Vulnerability	• Enable the policy and select **Process even if the Group Policy objects have not changed** option to make sure that the policies will be reprocessed even if there is no change
Countermeasure	• Configure the setting to **Enabled** • Clear the **Do not apply during periodic background processing** check box • Select the **Process even if the Group Policy objects have not changed** check box
Potential Impact	• For every refresh group policies are re applied

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Error Reporting

This policy lets administrators to manage the cabinet files created by DW.exe and redirect stop error reports to a local file server

This policy helps admin to figure the common errors faced by the users

You can configure the Error Reporting settings in the following location:

- **Computer Configuration\Administrative Templates\System\Error Reporting**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Display Error Notification

This policy setting is user to specify whether a user can send an error report or not.

By enabling the policy the user will get a message if an error occurs.

If **Report Errors** setting is enabled, the user can set to report the error or not.

If disabled, user will not get any option the report the error.

The values for the **Display Error Notification** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Display Error Notification (Cont'd)

Vulnerability	• If disabled, the user will not see the error message
Countermeasure	• Configure the setting to **Disabled**
Potential Impact	• Users will not see error report messages when they are generated

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Report Errors

This policy decides on reporting the errors

If enabled, the user can report the error when occurred

The values for the **Report Errors** setting are:

- Enabled
  - Do not display links to any Microsoft provided "more information" Web sites
  - Do not collect additional files
  - Do not collect additional machine data
  - Force queue mode for application error
  - Corporate upload file path
  - Replace instances of the word "Microsoft"

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Report Errors (Cont'd)

The other values for the **Report Errors** setting are:

- Disabled
- Not Configured

The default configuration is Enable in Windows XP and Disable id Windows Server 2003.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Report Errors (Cont'd)

Vulnerability

- In default configuration, when an error occurs the office will send the error to Microsoft
- If disabled, it is difficult to Microsoft to identify and diagnose the bugs in the application
- In an organization an Corporate Error Reporting (CER) server will be maintained as when an error occur it is pointed to the server. The server will generate a report and will send the information to Microsoft

Countermeasure

- Configure the setting to **Enabled**
- Select the **Corporate upload file path** option to point to the UNC path for your organization's CER server

Potential Impact

- Error reporting will be enabled, the reports are sent to CER server

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Internet Communications Management

The products in Windows family include many technologies that communicate with the internet and maximize ease-of-use

These technologies give many benefits, but this involves a risk as these communicate with site which admin needs to control

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Distributed COM

COM gives computer wide access control list (ACLs)

This check is in addition to any access that is run against the server specific ACLs

If access failed, the call, activation, or launch request is denied

Manage the new DCOM security features in Windows XP SP2 and Windows Server 2003 SP1 in the following:

- **Computer Configuration\Administrative Templates\Windows Components\System\Distributed COM\Application Compatibility Settings**

Common Issues

In this section the two settings share common vulnerability, countermeasure, and potential impact information

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Distributed COM (Cont'd)

Vulnerability	• The COM components written improperly can be attacked across the network, by which information can be reveled, DoS or privilege escalation attacks can rise
Countermeasure	• Use the **Allow local activation security check exemptions** and **Define Activation Security Check exemptions** settings in conjunction with the DCOM access control mechanisms to impose access and execution controls on DCOM components.
Potential Impact	• If DCOM access controls are added to existing applications, those applications may not work properly

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Browser Menus

Through these settings individual features in IE can be Enabled or Disabled

Configured the policy settings in the following location:

- **User Configuration\Administrative Templates\Windows Components\Internet Explorer\Browser menus**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Save This Program To Disk Option

Enable this settings user can click **Save This Program to Disk** button to download program files

If disabled, user will be informed the command is not available

The values for the **Browser menus: Disable Save this program to disk option** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Save this program to disk option (Cont'd)

Vulnerability

- Hostile code can be downloaded from Web sites

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Users can not click **Save This Program to Disk** button to download program files

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Attachment Manager

The Attachment Manager gives the behavior for file attachments in emails and web pages

This service categorizes files that are received and downloaded depending upon the file extension

This service defines files as High risk, Medium risk and Low risk

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Attachment Manager (Cont'd)

The Attachment Manager service divides files into three classes:

- **High Risk**. Windows blocks user access to the file
- **Moderate Risk**. Windows prompts the user before it allows access to the file
- **Low Risk**. Windows will not prompt the user before it allows access to the file, regardless of the file's zone information

These policy settings can be configured in the following location:

- **User Configuration\Administrative Templates\Windows Components\Attachment Manager**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Inclusion List For High Risk File Types

This setting allows you to set the high risk file types

If the file is in high risk list, Windows blocks user access to the file

If the file is from Internet, Windows prompts the user before it allows access to the file

If enabled, you can create your own high risk list

If disabled, Windows uses its built-in list of high risk file types

The values for the **Inclusion list for high risk file types** setting are:

- Enabled (allows you to specify a comma-separated list of file extensions)
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Inclusion List For High Risk File Types (Cont'd)

Vulnerability

- If a user accidentally opens high risks file, these files could defect the computer and possibly the network

Countermeasure

- Configure the setting to **Enabled**
- Specify the additional file types that you want to control

Potential Impact

- If the file type is in more than one list then most restricted list will applied as a countermeasure

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Inclusion List For Moderate Risk File Types

This setting allows you to set the moderate risk file types

If the file is in moderate risk list or Internet, Windows prompts the user before it allows access to the file

If enabled, you can create your own moderate risk list

If disabled, Windows uses its default list

The values for the **Inclusion list for moderate risk file types** setting are:

- Enabled (allows you to specify a comma-separated list of file extensions)
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Inclusion List For Moderate Risk File Types (Cont'd)

Vulnerability

- If a user accidentally opens high risks file, these files could defect the computer and possibly the network

Countermeasure

- Configure the setting to **Enabled**
- Specify the additional file types that you want to control

Potential Impact

- If the file type is in more than one list then most restricted list will applied as a countermeasure
- Use caution for moving high risk file types to the moderate risk list, as it will be easier for users to execute potentially risky files

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Inclusion List For Low File Types

This setting allows you to set the low risk file types

If the file is in low risk list or Internet, Windows prompts the user before it allows access to the file

If enabled, you can create your own low risk list

If disabled, Windows uses its default list

The possible values for the **Inclusion list for low file types** setting are:

- Enabled (allows you to specify a comma-separated list of file extensions)
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Inclusion List For Low File Types (Cont'd)

Vulnerability	• If a user accidentally opens high risks file, these files could defect the computer and possibly the network
Countermeasure	• Configure the setting to **Enabled** • Specify the additional file types that you want to control
Potential Impact	• If the file type is in more than one list then most restricted list will applied as a countermeasure • Use caution for moving high risk file types to the low risk list, as it will be easier for users to execute potentially risky files

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Trust Logic For File Attachments

The logic that windows use to find the risk in file attachment is given by this setting.

If enabled, the order in which Windows processes risk assessment data can be chosen.

If disabled, Windows uses its default trust logic.

The values for the **Trust logic for file attachments** setting are:

- Enabled
  - Looking at the file handler and type.
  - Preferring the file handler.
  - Preferring the file type.
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Trust Logic For File Attachments (Cont'd)

Vulnerability

- Attacker may mould a file to exploit vulnerability in a specific file handler

Countermeasure

- Configure the setting to **Enabled: Looking at the file handler and type**

Potential Impact

- Configure the **Trust logic for file attachments** setting to use both the file handler and type

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Hide Mechanisms To Remove Zone Information

This setting allows the user to manually remove the zone information from a saved file attachment

If the zone information can be removed, users could open potentially dangerous file attachments that Windows had previously blocked

If enabled, windows hide the checkbox and unblock button

If disabled, Windows displays the checkbox and **Unblock** button

The values for the **Hide mechanisms to remove zone information** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Hide Mechanisms To Remove Zone Information (Cont'd)

Vulnerability	• User can remove the location information which could be from an un-trusted location
Countermeasure	• Configure the setting to **Enabled**
Potential Impact	• Users can not remove the zone information from the file

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Notify Antivirus Programs When Opening Attachments

This policy manages how registry antivirus programs are notified when attachments are opened

If enabled, Windows calls the registered antivirus programs to scan an opened file

If the antivirus program fails, the attachment is blocked from being opened

If disable, Windows does not call the registered antivirus programs when file attachments are opened

The values for the **Notify antivirus programs when opening attachments** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Notify Antivirus Programs When Opening Attachments (Cont'd)

Vulnerability	• Antivirus programs which may not perform on-access check will not be able to scan download files
Countermeasure	• Configure the setting to **Enabled**
Potential Impact	• If enabled, all files and emails are scanned

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Windows Explorer

This is used to navigate the file system on clients that run Windows XP Professional

Configure the prescribed Windows Explorer user settings in the following location:

- **User Configuration\Administrative Templates\Windows Components\Windows Explorer**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remove Security Tab

The security tab on files and folders are disabled on properties dialog boxes in Windows Explorer

If enabled, users cannot access the **Security** tab

Users will not be able to change settings on the **Security** tab or view the list of users

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Remove Security Tab (Cont'd)

Vulnerability

- Security tabs can be determined the account permission for any file system object
- Attackers can target those accounts to gain greater access

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- When the tab is enabled, users cannot view the security tab for file system objects or review permissions

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

System\Power Management

Configure the prescribed **System\Power Management** user setting in the following location:

- **User Configuration\Administrative Templates\System\Power Management**

Prompt for password on resume from hibernate / suspend

- This policy controls that the client computer is locked when they are resumed from hibernate or suspend state.
- If enabled, the client computers are locked and users must provide passwords to unlock.
- If disabled, a potential for a serious security breach, because the client computers may be accessed by anyone after they resume operation.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Additional Registry Entries

It provides additional information about registry entries for the base line security template file

Customized Security Configuration Editor

- When MMC (Microsoft Management Console) security templates snap-in the entries in the security template cannot be represented
- The entries are added to .inf file using Security Configuration Editor (SCE)
- To automate any changes the entries are embedded in the security templates
- By removing this policy the changes have to be made manually by using the tool such as Regedt32.exe

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

How to Modify the Security Configuration Editor User Interface

This is used to define security templates for any number of computers

These templates can contain:

- Password policies
- Lockout policies
  - Kerberos protocol policies
- Audit policies
- Event log settings
- Registry values
- Service startup modes
- Service permissions
- User rights

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

How to Modify the Security Configuration Editor User Interface (Cont'd)

These templates also can contain:

- Group membership restrictions
- Registry permissions
- File system permissions

SCE appears in MMC snap-ins and administrator tools, used by the Security Templates snap-in and the Security Configuration and Analysis snap-in

Additional entries are added to SCE using Seregvi.inf

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

How to Modify the Security Configuration Editor User Interface (Cont'd)

The original security settings are in Policies\Security in the snap-ins and tools

The file sceregvi.inf should be updated and re-register the file Scecli.dll

Once the file Sceregvl.inf has been modified and registered, the custom registry values are uncovered in the SCE user interfaces on that computer

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

How to Modify the Security Configuration Editor User Interface (Cont'd)

To manually update sceregvl.inf

- Use a text editor (Notepad) to open the Values-sceregvl.txt file from the SCE Update folder of the download for this guide
- Open another window in the text editor and then open the %systemroot%\inf\sceregvl.inf file
- Navigate to the bottom of the "[Register Registry Values]" section in the sceregvl.inf file. Copy and paste the text from the Values-sceregvl.txt file, without any page breaks, into this section of the sceregvl.inf file
- Close the Values-sceregvl.txt file and open the Strings-sceregvl.txt file from the SCE Update folder of the download

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

How to Modify the Security Configuration Editor User Interface (Cont'd)

To manually update sceregvl.inf

- Navigate to the bottom of the "[Strings]" section in the **sceregvl.inf** file. Copy and paste the text from the Strings-sceregvl.txt file, without any page breaks, into this section of the **sceregvl.inf** file.
- Save the **sceregvl.inf** file and close the text editor.
- Open a command prompt and execute the command **regsvr32 scecli.dll** to re-register the DLL file.

The custom registry values are displayed by the subsequent launch of SCE.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

How to Modify the Security Configuration Editor User Interface (Cont'd)

To automatically update sceregvl.inf

- The **Values-sceregvl.txt, Strings-sceregvl.txt,** and **Update_SCE_with_MSS_Regkeys.vbs** files that are located in the **SCE Update** folder of the download for this guide must all be in the same location for the script to function.
- Execute the **Update_SCE_with_MSS_Regkeys.vbs** script on the computer you wish to update.
- Follow the onscreen prompts

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

How to Modify the Security Configuration Editor User Interface (Cont'd)

The below process will remove custom entries, using this the changes made by automatic update script cab be modified:

To reverse the changes made by the Update_SCE_with_MSS_Regkeys.vbs script

- Execute the **Rollback_SCE_for_MSS_Regkeys.vbs** script on the computer you wish to update.
- Follow the onscreen prompts

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

How to Modify the Security Configuration Editor User Interface (Cont'd)

The below process will remove custom entries added to SCE user interface.

To restore the SCE to its default state for Windows XP with SP2 Windows Server 2003 with SP1

- The **sceregvl_W2K3_SP1.inf.txt, sceregvl_XPSP2.inf.txt,** and **Restore_SCE_to_Default.vbs** files that are located in the **SCE Update** folder of the download for this guide must all be in the same location for the script to function.
- Execute the **Restore_SCE_to_Default.vbs** script on the computer you wish to update.
- Follow the onscreen prompts

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

How to Modify the Security Configuration Editor User Interface (Cont'd)

To manually restore the SCE user interface to its default appearance

- Click **Start**, **Run**, type **regedit.exe** and press ENTER to open the Registry Editor tool
- Navigate to **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SecEdit\Reg Values**
- Each subkey in this location represents one item in the Security Options section of the SCE. Carefully delete all of the subkeys. **Do not delete the parent key** (Reg Values), but only the subkeys that are contained within it
- Open a command prompt and execute the command **regsvr32 scecli.dll** to re-register the SCE DLL
- Subsequent launches of the SCE will only display the original registry values that were included with your version of Windows

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

TCP/IP-Related Registry Entries

The computer has to be up to date with latest security fixes, to prevent DoS (Denial of Service) attack

The default TCP/IP stack configuration is tuned to handle standard intranet traffic

The DoS attacks directed at TCP/IP stack are of two classes:

Attack that spend many system resources

Attacks that send specially crafted packets causing the network stack or the entire operating system to fail

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

TCP/IP-Related Registry Entries (Cont'd)

The following registry settings help to protect against the attacks that are directed at the TCP/IP stack

The registry settings in the following table were added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ subkey

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

TCP/IP-Related Registry Entries (Cont'd)

Registry entry	Format	XP SP2 default	2003 SP1 default	Most secure value (decimal)
DisableIPSourceRouting	DWORD	1	1	2
EnableDeadGWDetect	DWORD	1	1	0
EnableICMPRedirect	DWORD	1	1	0
KeepAliveTime	DWORD	7200000	7200000	300,000
PerformRouterDiscovery	DWORD	2	2	0
SynAttackProtect	DWORD	0	1	1
TcpMaxConnectResponseRetransmissions	DWORD	2	2	2
TcpMaxDataRetransmissions	DWORD	5	5	3

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disableipsourcerouting: IP Source Routing Protection Level (Protects Against Packet Spoofing)

This entry appears as MSS: (DisableIPSourceRouting) IP source routing protection level **in the SCE**

It is a process which allows the sender to find the IP route followed by a datagram through a network

Vulnerability

- The source routing packets can be used by an attacker to identify the location

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disableipsourcerouting: IP Source Routing Protection Level (Protects Against Packet Spoofing) (Cont'd)

Countermeasure

- **Configure the** MSS: (DisableIPSourceRouting) IP source routing protection level entry to a value of Highest protection, source routing is completely disabled
- **The possible values for the registry entry are:**
  - 0, 1, or 2. The default configuration is 1 (source routed packets are not forwarded)
- **In the SCE UI,** this list of options appears:
  - No additional protection, source routed packets are allowed
  - Medium, source routed packets ignored when IP forwarding is enabled
  - Highest protection, source routing is completely disabled
  - Not Defined

Potential Impact

- If this value is configured to 2, incoming source routed packets will be dropped

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enabledeadgwdetect: Allow Automatic Detection Of Dead Network Gateways (Could Lead To Dos)

It allows automatic detection of dead network gateways in SCE.

If enabled, and the number of connections experience difficulty the IP will change to a backup gateway.

Vulnerability

- An attack makes the server to switch gateways, probable to an unintended one.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enabledeadgwdetect: Allow Automatic Detection Of Dead Network Gateways (Could Lead To Dos)

Countermeasure

- This setting allows automatic detection of dead network gateways entry to a value of disabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled) on Windows Server 2003
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- If configured to 0, Windows cannot detect dead gateways and switches to alternates

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enableicmpredirect: Allow ICMP Redirects To Override OSPF Generated Routes

This entry allows ICMP redirects to override OSPF generated routes in the SCE

The host routes are pumped by redirecting ICMP (Internet Control Message Protocol)

These routes re-write Open Shortest Path First (OSPF)-generated routes

Vulnerability

- This is an expected behavior that a 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation through which traffic is no longer routed properly for host

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enableicmpredirect: Allow ICMP Redirects To Override OSPF Generated Routes

Countermeasure

- Configure this entry to Disabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled)
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- The connected interface subnet routes are not imported accurately as RRAS (Routing and Remote Access) is configured as an ASBR (autonomous system boundary router)

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Keepalivetime: How Often Keep-alive Packets Are Sent In Milliseconds (300,000 Is Recommended)

This decides how often keep-alive packets are sent in milliseconds in the SCE

A keep-alive packet is sent by TCP to check that an idle connection is still intact

Vulnerability

- An attacker can start many connections to start a DoS condition

Countermeasure

- Configure this value to 300000 or 5 minutes
- **The possible values for this registry entry are:**
- 1 through 0xFFFFFFFF. The default configuration is 7,200,000 (two hours)

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Keepalivetime: How Often Keep-alive Packets Are Sent In Milliseconds (300,000 Is Recommended)

In the SCE UI, the following list of options appears:

- 150000 or 2.5 minutes
- 300000 or 5 minutes **(recommended)**
- 600000 or 10 minutes
- 1200000 or 20 minutes
- 2400000 or 40 minutes
- 3600000 or 1 hour
- 7200000 or 2 hours **(default value)**
- Not Defined

Potential Impact

Some applications may need keep-active packets by default and that configures TCP stack flag

For this process the value can be changed from 5 minutes to two hours

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Synattackprotect: Syn Attack Protection Level (Protects Against Dos)

This entry protects system again DoS. It adjusts TCP for retransmission of SYN-ACKs

The overhead of incomplete transmission in a connect request attack is minimized by setting this request

By this setting Windows send messages as broadcast rather than multicast

Vulnerability

- In SYN flood attack the attacker sends SYN packets to a server which leaves an half open connection until load increases and will not be able to respond a genuine request

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Synattackprotect: Syn Attack Protection Level (Protects Against Dos) (Cont'd)

Countermeasure

- **Configure this entry** to Connections time out
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled) for Windows Server 2003 SP1 and 0 (disabled) for Windows XP SP2
- **In the SCE UI, these options appear as:**
  - Connections time out more quickly if a SYN attack is detected
  - No additional protection, use default settings
  - Not Defined

Potential Impact

- This value increases connection delay and TCP connection request quickly time out when an SYN attack is in progress

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Tcpmaxconnectresponseretransmissions: SYN-ACK Retransmissions When A Connection Request Is Not Acknowledged

This entry retransmits when a connection request is not acknowledged in the SCE

The number of times the TCP retransmits a SYN before stopping the attempt

Vulnerability

- In SYN flood attack the attacker sends SYN packets to a server which leaves an half open connection until load increases and will not be able to respond a genuine request

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Tcpmaxconnectresponseretransmissions: SYN-ACK Retransmissions When A Connection Request Is Not Acknowledged (Cont'd)

Countermeasure

- Configure this to a value of 3 seconds, half-open connections dropped after nine seconds
- The possible values for this registry entry are:
  - 0-0xFFFFFFFF. The default configuration is 2
- In the SCE UI, the following options appear and correspond to a value of 0, 1, 2, and 3, respectively:
  - No retransmission, half-open connections dropped after 3 seconds
  - 3 seconds, half-open connections dropped after 9 seconds
  - 3 & 6 seconds, half-open connections dropped after 21 seconds
  - 3, 6, & 9 seconds, half-open connections dropped after 45 seconds
- Not Defined

Potential Impact

- If the value is more than 2, a SYN attack will be employed internally
- If the value is less than 2, the registry values cannot be read
- If the value is 0, Syn-ATKs will not be retransmitted, and will be out by 3 seconds

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Tcpmaxdataretransmissions: How Many Times Unacknowledged Data Is Retransmitted (3 Recommended, 5 Is Default)

This entry decides how many times the unacknowledged data is retransmitted in the SCE. It controls the count of the retransmitting data connection before aborting.

The retransmission time is doubled every time a retransmission is issued.

Vulnerability

- A user can weaken the sender by not replying with an acknowledgement message for the transmitted data.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Tcpmaxdataretransmissions: How Many Times Unacknowledged Data Is Retransmitted (3 Recommended, 5 Is Default)

Countermeasure

- **Configure this entry to a value of 3. The possible values for this registry entry are:**
  - 0 to 0xFFFFFFFF. The default configuration is 5
- **In the SCE UI, this setting can be adjusted using a text entry box:**
  - A user-defined number
- Not Defined

Potential Impact

- TCP start a timer when a transmission starts and if no acknowledgement is sent back, retransmission is issued for 3 times

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Miscellaneous Registry Entries

The registry entries in the table are recommended:

Registry entry	Format	Most secure value (decimal)
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	DWORD	Not defined, except for highly secure environments, which should use 0.
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)	DWORD	Not defined, except for highly secure environments, which should use 0.
MSS: (AutoShareWks) Enable Administrative Shares (not recommended except for highly secure environments)	DWORD	Not defined, except for highly secure environments, which should use 1.
MSS: (DisableSavePassword) Prevent the dial-up passsword from being saved (recommended)	DWORD	1

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Miscellaneous Registry Entries (Cont'd)

MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)	DWORD	Not defined, except for highly secure environments, which should use 1.
MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)	DWORD	1 for computers that run Windows XP, 3 for computers that run Windows Server 2003.
MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)	DWORD	0xFF
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers (Only recommended for servers)	DWORD	1
MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)	DWORD	1
MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	DWORD	1
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	String	0
MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	DWORD	0

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure Automatic Reboot from System Crashes

This entry allows windows to automatically restart after a system crash in the SCE

This finds whether the system restarts automatically or not

You can add this registry value to the template file in the

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\ **subkey**

Vulnerability

- In some situations computer could struck in an end less loop of failures and reboots. The measure to this is just to stop running the computer

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure Automatic Reboot from System Crashes (Cont'd)

Countermeasure

- Configure this to Disabled.
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled).
- **In the SCE UI, the following options are available:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- The computer will no longer reboot automatically after a failure.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enable Administrative Shares

This entry enables administrative Shares in the SCE.

By default, Windows XP Professional creates admin shares automatically.

You can add this registry value to the template file in the

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\ **subkey.**

Vulnerability

- These shares are available in all computers; a user can access them to find out password by a brute force attack.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enable Administrative Shares (Cont'd)

Countermeasure

- Do not configure this entry to Enabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled).
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- If these shares are deleted, problem can be created for administrators and the files using the shares

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Saving of Dial-Up Passwords

This entry prevents from the dial-up password to be saved in the SCE

You can add this registry value to the template in the

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters\ **subkey**

Vulnerability

- If this entry is enabled, an attacker can connect to the network by steeling a mobile user computer

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Saving of Dial-Up Passwords (Cont'd)

Countermeasure

- Configure this entry to Disabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 0 (disabled)
- **In the SCE UI, the following options are available:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- The logon credentials (dial-up and VPN) of the users can not be stored automatically

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Hide the Computer from Network Neighborhood Browse Lists: Hide Computer From the Browse List

This entry hides computers from the browser list in the SCE

Configure a computer not to send announcements to browser as if it is done the computer will be hidden from the browser list

You can add this registry value to the template file in the

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\ **subkey**

Vulnerability

- If enabled, this will help in reducing traffic and removes the a method that an attacker can use

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Hide the Computer from Network Neighborhood Browse Lists: Hide Computer From the Browse List (Cont'd)

Countermeasure

- Do not configure this entry to Enabled.
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 0 (disabled).
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- The computer will not appear on any other computer or network.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure Netbios Name Release Security: Allow the Computer to Ignore Netbios Name Release Requests Except from WINS Servers

This entry allows the computer to ignore NetBIOS name release request exception from WINS server in SEC

You can add this registry value to the template file in the

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\ **subkey**

Vulnerability

- The NetBT protocol do not use authentication and is vulnerable to spoofing.
- An attacker can send a name conflict datagram, to give up and not to respond the query

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure Netbios Name Release Security: Allow the Computer to Ignore Netbios Name Release Requests Except from WINS Servers (Cont'd)

Countermeasure

- Configure this entry to Enabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled).
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- An attacker sends a request on network to release its NetBIOS name

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enable Safe DLL Search Order: Enable Safe DLL Search Mode (Recommended)

This entry enables safe DLL search mode in the SCE

The order for DLL search order can be configured as:

If SafeDllSearchMode is configured to 1, the search order is as follows:

- The directory from which the application loaded
- The system directory
- The 16-bit system directory. There is no function that obtains the path of this directory, but it is searched

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enable Safe DLL Search Order: Enable Safe DLL Search Mode (Recommended) (Cont'd)

If SafeDllSearchMode is configured to 1:

- The Windows directory
- The current directory
- The directories that are listed in the PATH environment variable

If SafeDllSearchMode is configured to 0, the search order is as follows:

- The directory from which the application loaded
- The current directory
- The system directory
- The 16-bit system directory. There is no function that obtains the path of this directory, but it is searched

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enable Safe DLL Search Order: Enable Safe DLL Search Mode (Recommended) (Cont'd)

If SafeDllSearchMode is configured to 0:

- The Windows directory
- The directories that are listed in the PATH environment variable

You can add this registry value the template file in the

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ **subkey**

Vulnerability

- If an user accidentally executes some bad code, it could increase the type and degree of damage that can be rendered

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Enable Safe DLL Search Order: Enable Safe DLL Search Mode (Recommended) (Cont'd)

Countermeasure

- Configure this entry to Enabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration for Windows XP it is 0 and 1 for Windows Server 2003
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- Applications are forced to search for DLLs in the system path

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Log Near Capacity Warning: Percentage Threshold for the Security Event Log at which the System will Generate a Warning

This entry will generate a percentage for the security event log for the generated warnings in the SCE

You can add this registry value to the template file in the

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\ **subkey**

Vulnerability

- If the log capacity reaches to 90 percent and it is configured not to overwrite events the recent events will not be written and if the log capturing capacity is exceeded the system can even shut down if it is configured to do so

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Log Near Capacity Warning: Percentage Threshold for the Security Event Log at which the System will Generate a Warning (Cont'd)

Countermeasure

- Configure this entry to a value of 90.
- **The possible values for this registry entry are:**
  - 0 to 100. The default configuration is 0 (no warning event is generated).
- **In the SCE UI, the following options are available:**
  - 50%
  - 60%
  - 70%
  - 80%
  - 90%
- Not Defined

Potential Impact

- System generates an audit event when log reaches 90 percent

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Registry Entries Available In Windows XP With SP2 And Windows Server 2003 With SP1

The following registry events are for both Windows XP with SP2 and Windows Server 2003 with SP1.n RestrictRemoteClients

The RestrictRemoteClients registry key makes RPC to perform additional security checks

The **RestrictRemoteClients** registry key can have one of three DWORD values:

- **0**. This is a default value and it makes the computer to bypass the RPC interface restriction
- **1**. This is the default value in Windows XP with SP2. It makes all remote un-known calls to be rejected by the RPC runtime
- **2**. All remote un-known calls are rejected by the RPC

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Registry Entries Available In Windows XP With SP2 And Windows Server 2003 With SP1 (Cont'd)

The applications passing flags can be modified to the RPC sub system which shows that the default client and server accept un-known RPC requests.

Vulnerability	• Corrupted code can be spread by exploiting buffer remotely
Countermeasure	• The RestrictRemoteClient have a default configuration which can allow backward compatibility • Configure RestrictRemoteClient to 1 or 2
Potential Impact	• If enabled, un-known user cannot access the RPC Endpoint Mapper Interface

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

RunInvalidSignatures

This prevents the installation of code which has invalid signatures

Internet Explorer 6.0 blocks the installation of signed code with invalid signatures

The service pack shows this action to all applications

Vulnerability

- A control which has been corrupted may be downloaded and run

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

RunInvalidSignatures (Cont'd)

Countermeasure

- The default value of RunInvalidSignatures blocks this vulnerability

Potential Impact

- Applications which are legitimately signed will not function if there signature is invalid

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Registry Entries Available in Windows XP with SP2

These registry entries are available only in Windows XP with SP2

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Center Registry Entries for XP

Registry values for security centre determining whether the user receives alerts for the feature

If the key has a value of 0, **the notification icon and alert system for that feature are enabled**

- **These values are in** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center**:**
  - **AntiVirusDisableNotify**
  - **FirewallDisableNotify**
  - **UpdatesDisableNotify**

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Security Center Registry Entries for XP (Cont'd)

Vulnerability

- If the alert feature is disabled for some users they will not receive any warnings

Countermeasure

- **Apply a Group Policy registry entry to implement the warning configuration**

Potential Impact

- If Security Centre functionality is enabled, the values are visible in Security Centre user interface

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

StorageDevicePolicies\WriteProtect

By default the USB device can be mounted and users can use it without any limit

If necessary this ability can be restricted, To do so add WriteProtect DWORD value to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies and configure it to 1

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

StorageDevicePolicies\WriteProtect (Cont'd)

Vulnerability	• An attacker could copy data to a removable USB device and steal it
Countermeasure	• When the WriteProtect value is set to 1, Windows XP with SP2 will block writes to USB block storage devices
Potential Impact	• There are other ways that a skilled attacker to steal data with a USB device

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Registry Entries Available in Windows Server 2003 with SP1

These registry entries are available only in Windows Server 2003 with SP1

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

UseBasicAuth

Distributed Authoring and Versioning (DAV) is an HTTP–based protocol which allows remote access to file systems and file servers

The UNC path can be used to access files on DAV server

Windows Server 2003 SP1 introduces the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\UseBasicAuth subkey

If it is configured to 1, the WebDAV can communicate with web servers which support basic authentication

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

UseBasicAuth (Cont'd)

Vulnerability

- Attackers can setup Web servers with basic authentication and trick or spoof user attempt to connect it to capture their credentials.

Countermeasure

- By default the WebDAV will not use basic authentication.

Potential Impact

- Applications supporting WebDAV to access web resources will fail if web server only support authentication.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DisableBasicOverClearChannel

The WebDAV redirector is part of remote file system stack

When user opens an URL the credentials may be exposed if the server support only basic authentication

The UseBasicAuth registry entry controls whether basic authentication can be used for WebDAV requests. If you configure the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\DisableBasicOverClearChannel** value to 1, the use of basic authentication with other Web resources is blocked

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

DisableBasicOverClearChannel (Cont'd)

Vulnerability	• A Web Server can be setup by the attacker which uses basic authentication • They make the users to connect it to capture their credentials
Countermeasure	• Configure the DisableBasicOverClearChannel value to 1 on client computers
Potential Impact	• Embedded devices offering HTTP access only supports basic authentication

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Additional Countermeasures

This describes the implementation of security accounts for additional countermeasures

Member Server Hardening Procedures

- Most of the counter measures can be applied by Group Policy; some additional measures are difficult or impossible to apply through this

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Securing the Accounts

The most known built in account in Windows Server 2003 are Guest and Administrator, these accounts can be renamed but not deleted

Vulnerability

- By default, the guest account is disabled on the computers. The configuration should not be changed
- In the built in administrator account attackers may attempt to comprise a server. To overcome the admin account name should be changed
- This kind of attacks is minimized as the account is not much recognized by its name but by its SID
- This value uniquely identifies each user, group, and computer account and logon session on a network

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Securing the Accounts (Cont'd)

Countermeasure

- Change the Administrator account and change the password to a long & complex value on every server.
- To rename the account, configure the Rename administrator account setting in Group Policy at the following location:
- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security\Options
- If the organization uses same account names and passwords on all of the servers, attacker who gains access to one member server will be able to gain access to all others.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Securing the Accounts (Cont'd)

Potential Impact

- The users must keep track on what account name is assigned to each computer as to manage the computer

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

NTFS

The NTFS partitions support access control list (ACL's) and encryption

The support is not available with the file allocation table (FAT), FAT32, or FAT32x file systems

Vulnerability

- Files which are not protected by ACLs can be accessed, modified and deleted by unauthorized users
- In this the encryption gives more protection and is more viable to files that are accessed by a single user

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

NTFS (Cont'd)

Countermeasure

- Format all drives on each server to NTFS from FAT, but this gives full control on the ACLs on the converted drives
- Apply following security templates to configure the default file system ACLs:
  - **For workstations**. %windir%\inf\defltwk.inf
  - **For servers**. %windir%\inf\defltsv.inf
  - **For domain controllers**. %windir%\inf\defltdc.inf

Potential Impact

- No negative impact is detected

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

NTFS (Cont'd)

Microsoft recommends the following additional technologies that can help lessen the impact of these types of attacks:

- Use Syskey with an offline password to prevent startup of the Windows operating system by unauthorized persons.
- Use EFS to encrypt user data. Instruct users to use their domain accounts and either configure no recovery agent or configure it for domain administrator accounts rather than the local administrator account.
- Use BIOS passwords to deny unauthorized users the ability to start computers within your organization.
- Configure the system BIOS to disable the ability of computers to start from CD-ROM drives and floppy disk drives. This configuration will deny the ability of unauthorized users to start computers with their own operating system.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Data and Application Segmentation

Locate the data, application and log files on separate storage device to improve performance

By this you can prevent an attack of Directory Traversal account

Vulnerability

- If application, data and log files are located on the same storage device: Two vulnerabilities are detected
  - The users may accidentally or deliberately fill an application log file or upload files to the server and fill the storage volume with data
  - A directory traversal exploit, in which an attacker takes advantage of a bug in a network service to navigate the directory tree to the root of the system volume to execute a utility remotely

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Data and Application Segmentation (Cont'd)

Countermeasure

- If possible relocate web contents, applications log files to a separate partition from the system volume

Potential Impact

- The impact would be less for organizations maintaining the server consistently

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure SNMP Community Name

SNMP (**Simple Network Management Protocol**) is a network management standard widely used is TCP/IP networks. It provides a way to manage networks

Computers running network management software SNMP management systems or SNMP managers

Vulnerability

- SNMP is week in the view of security, that is all vendors set a default community string name
- When connecting SNMP management device to client the data is in-secured as SNMP traffic is sent in plaintext, without encryption

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure SNMP Community Name (Cont'd)

Countermeasure

- Configure the SNMP community string for read access on all computers to a random alphanumeric value.
  - At the Services console, double-click **SNMP Service**.
  - Click the **Security** tab on the **SNMP Service Properties** dialog box.
  - Select **public** from the **Accepted community names** list.
  - Click the **Edit** button, and then type the new community name in the **SNMP Service Community Name** dialog box when it appears.
  - Click the **OK** button to close each of the dialog boxes.
- Leave write access through SNMP disabled.

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure SNMP Community Name (Cont'd)

Countermeasure	• The community name is stored in the registry as a registry value with a DWORD value of 4 The value is stored in: HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities
Potential Impact	• Also configure community string for all management tools using SNMP protocol

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable NetBIOS and SMB on Public Facing Interfaces

It discusses about servers which are not fully controlled as publicly accessible web servers and email gateways

Vulnerability

- If server message block and NetBIOS on TCP/IP are disabled, a servers attack chances are reduced
- The measures will protect servers from compromise through the SMB and NetBIOS

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable NetBIOS and SMB on Public Facing Interfaces (Cont'd)

Countermeasure

- The SMB will be in use even if NetBIOS will be disabled as it uses port 445
- So the necessary steps should be taken to disable SMB
- **NetBIOS uses the following ports:**
  - UDP/137 (NetBIOS name service)
  - UDP/138 (NetBIOS datagram service)
  - TCP/139 (NetBIOS session service)
- **SMB uses the following ports:**
  - TCP/139
  - TCP/445
- For accessing servers form internet, remove file and printer sharing for Microsoft Network and Client

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable NetBIOS and SMB on Public Facing Interfaces (Cont'd)

To disable SMB

- In Control Panel, double-click **Network Connections**
- Right-click any Internet facing connection, and then click **Properties**
- In the **Properties** dialog box, click select **Client for Microsoft Networks**, and then click **Uninstall**
- Follow the uninstall steps
- Select **File and Printer Sharing for Microsoft Networks**, and then click **Uninstall**
- Follow the uninstall steps

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable NetBIOS and SMB on Public Facing Interfaces (Cont'd)

To disable NetBIOS over TCP/IP

- In Control Panel, double-click **System**, click the **Hardware** tab, and then click the **Device Manager** button
- On the **View** menu, click **Show hidden devices**
- Expand **Non-Plug and Play Drivers**
- Right-click **NetBios over Tcpip**, and then click **Disable**
- This will disable the SMB on TCP/IP and UDP 445

Potential Impact

- Computers cannot connect to the server through SMB and connect to files and folder on the network

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Dr. Watson: Disable Automatic Execution of Dr. Watson System Debugger

The debuggers make it easy to trouble shoot the computers and applications

The Dr. Watson tool included with Windows Server 2003 and Windows XP is automated system debugger; to records information about system state and applications which are active

Vulnerability

- An attacker who has already gained administrative privileges has complete control of the computer, so attackers could still pursue other paths if you disable Dr. Watson

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Disable Dr. Watson: Disable Automatic Execution of Dr. Watson System Debugger (Cont'd)

Potential Impact

- No debugger will run and no report is created
- The admin will not have much data to solve the system problems

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure IPsec Policies

IPsec is a tool used by the network security administrators to permit , block, or negotiate security for TCP/IP traffic

IPsec is independent and transparent to applications

An adequate host level protection is gives by Windows firewall component

IPsec should be used to secure host-to-host and host-to-client

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure IPsec Policies (Cont'd)

Vulnerability

- The security personnel's mostly concentrate on preventing attacks from outside in a company But the attacks can even occur from inside the company
- Attackers may use NetBT null session to get information
- Firewalls between internal network and internet can not give any security for internal threats
- Authenticated access controls are needed to protect client and server

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure IPsec Policies (Cont'd)

Countermeasure

- To create a traffic map
- Determine the base network services that are required for the server role
- Identify the protocols and ports that are required by each service. Use tools such as the Netstat.exe command to view open ports and active connections
- Document the IPsec filtering rules that are necessary to allow only the identified traffic

Service	Protocol	Source port	Destination port	Source address	Destination address	Action	Mirror
HTTP Server	TCP	ANY	80	ANY	ME	PERMIT	YES
HTTPS Server	TCP	ANY	443	ANY	ME	PERMIT	YES
DNS Client	TCP	ANY	53	ME	DNS	PERMIT	YES
Block everything	ANY	ANY	ANY	ANY	ANY	BLOCK	YES

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure IPsec Policies (Cont'd)

Network Traffic Map (Sample)

- IPsec policies that use Windows Server 2003 features such as this one should not be assigned to Windows 2000 or Windows XP computers
- A mirrored block filter will block unicast IP traffic from an IP address from a computer
- Any of the following solutions could be used to block the inbound attack:
  - Use additional IPsec filtering rules to block an attacker from using port 80 to gain inbound access to open ports
  - Use a front-end stateful filtering firewall or router to block inbound traffic from source port 80 unless it corresponds to an outbound connection

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure IPsec Policies (Cont'd)

Network Traffic Map (Sample)

- In addition to this IPsec policy, configure Windows Firewall on the server's external network adapter to provide stateful filtering for all outbound traffic that is permitted by IPsec filters. Because Windows Firewall is layered above IPsec, Windows Firewall must also be configured to permit TCP ports 80 and 443 inbound.
- You can apply IPsec policies in several ways:
  - Apply them on an individual computer.
  - Attach them to an OU or domain using Group Policy.
  - Write a script for the netsh ipsec command, and then apply the script on select computers.

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure IPsec Policies (Cont'd)

Potential Impact

- Using IPsec the server can be hardened against network attacks
- IPsec filtering is designed for a simple packet filtering scenario
- Limitations of IPsec filtering include the following:
  - Cannot be applied for a particular application, defined for protocols and ports
  - They are static and do not provide "stateful" outbound traffic filtering. It cannot guard against an attacker using the static inbound permit filter which allows access to any open port
  - Do not differentiate between different types of ICMP messages

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configure IPsec Policies (Cont'd)

Potential Impact

- Do not perform inspection of the contents of IP packets for the purpose of intrusion detection.
  - They can overlap, but cannot be manually ordered. This service internally calculates a weight that provides an automatic filter order.
  - These filters are not interface-specific.
  - These filters cannot be explicitly configured as inbound or outbound.
  - Policy does not support duplicate filters.
  - Windows Server 2003 slowly improves the performance of IPsec filtering.

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configuring Windows Firewall

In Windows XP and Windows Server 2003 a built in Windows firewall can be used to protect organization network fro network attacks with the external firewalls

- Click **Start**, and then click **Control Panel**
- Click **Windows Firewall**
- Click the **On (recommended)** radio button
- If necessary, click the **Exceptions** tab and configure exceptions for protocols that you want to allow through the firewall
- Click **OK** to activate Windows Firewall

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited

Configuring Windows Firewall (Cont'd)

Windows Firewall is only contains a basic intrusion prevention feature

Windows Firewall does not do extensive outbound filtering

Windows Firewall can centrally be managed by the Group Policies

EC-Council

Copyright © by EC-Council All Rights Reserved.
Reproduction is Strictly Prohibited