



Ethical Hacking and Countermeasures

Version 6



Module XVI

Hacking Web Servers

SpeedCake4u, a cake manufacturing firm wants to set up a website for showcasing its products. Matt, a high school graduate was assigned the task of building the website. Even though Matt was not a pro in website building, the \$2000 pay was the main motivation for him to take up the task.

He builds a website with all the features that the company management asked.

The following day the cake manufacturing firm's website was defaced with the Title "Your cake stinks!"

How was it possible to deface the website?

Is Matt the culprit?



PCWorld

Hack Attack Hits 10,000 Web Sites

Infected sites feed exploits to visitors--and more sites are affected than first suspected.

Gregg Keizer, Computerworld

Friday, January 18, 2008 03:50 PM PST

A large-scale hack of legitimate Web sites to infect visitors' PCs is much more massive than first thought, researchers said Friday. At least 10,000 sites have been compromised, and have hijacked unpatched systems that steered to their URLs.

On Monday, Mary Landesman, a senior security researcher at ScanSafe Inc., said that she had uncovered [hundreds of sites which had been hacked](#) and were feeding exploits to visitors. Friday, Don Jackson, a senior researcher with Atlanta-based SecureWorks Inc., said the number was considerably larger.

According to ScanSafe's data, approximately 10,000 sites hosted on Linux servers running Apache, the popular open-source Web server software, have been hacked, most likely with purloined log-in credentials. Those servers have been infected with a pair of files that generate constantly-changing malicious JavaScript. When visitors reach the hacked site, the script calls up an exploit cocktail that includes attack code targeting recent QuickTime vulnerabilities, the long-running Windows MDAC bug, and even a fixer flaw in Yahoo Messenger.

If the visitor's PC is unpatched against any of the nine exploits Jackson listed, it's infected with new variant of Rbot, the notorious backdoor Trojan he called "a very nasty piece of software." The end result: The PC is added to a botnet.

Jackson can't prove how the sites were originally hacked, but all the evidence points to the theft of log-on credentials; one reason why he came to that conclusion is that hosts that have been cleaned of the infection -- or in some cases even had Linux reinstalled -- are quickly reinfected.

"There was no sign of brute forcing [of passwords] just prior to the infection," said Jackson, "but attackers hosting companies are hit all the time with password attacks. It's part of doing business."

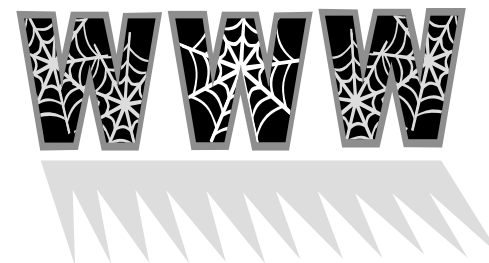
Earlier in the week, Landesman of ScanSafe drew a link between the security breach at U.K.-based Fasthosts Ltd., that country's largest Web hosting vendor, and the site hacks, saying then that the domains ScanSafe had found infected had, or had recently had, a relationship with Fasthosts.

Source: <http://www.pcworld.com/>

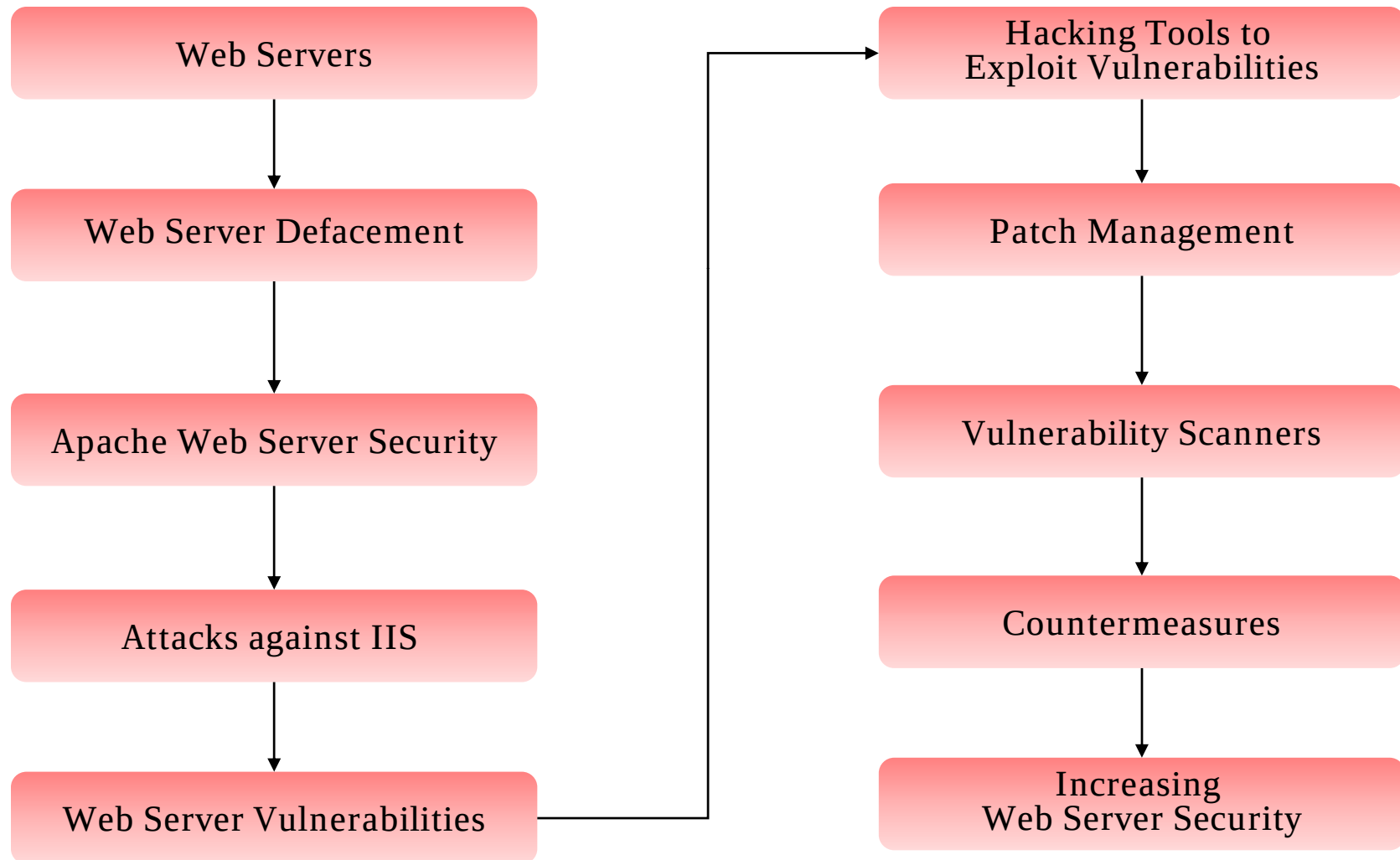
Module Objective

This module will familiarize you with :

- Web Servers
- Popular Web Servers and Common Vulnerabilities
- Apache Web Server Security
- IIS Server Security
- Attacks against Web Servers
- Tools used in Attack
- Patch Management
- Understanding Vulnerability Scanners
- Countermeasures
- Increasing Web Server Security



Module Flow



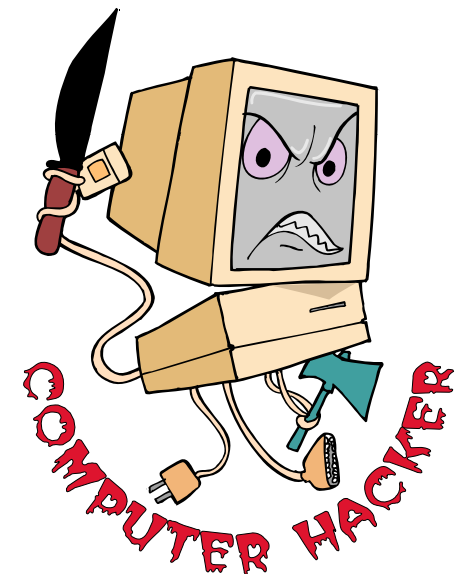
How are Web Servers Compromised

Misconfigurations, in operating systems, or networks

Bugs, OS bugs may allow commands to run on the web

Installing the server with defaults, service packs may not be applied in the process, leaving holes behind

Lack of proper security policy, procedures, and maintenance may create many loopholes for attackers to exploit



Web Server Defacement

Mirror saved on 05/12/2006

Defacer: DeltahackingSecurityTEAM	Domain: malang.	IP address:
System: Linux	Web server: Apache	Attacker stats

DeltahackingSecurityTEAM



we are : D_7J , DR.Trojan , M@asoud HIV++ , Vampire , Ignore

Mail: D_7J@deltahacking.net

website: <http://www.deltahacking.com> <http://www.deltahacking.net>

special thanks to the Delta programmers and defacers

Iranian Hackers Are The Best In The World

Special Thanks To The Zone-h

Iranian Top Attacker: Ashiyane Digital Security Team , Emperor , Nobody Coder ,
DeltahackingSecurityTEAM , Iran Hackers Sabotage

Mirror saved on 05/18/2006

Defacer: iskorpitx	Domain: http	IP address:
System: Win 2003	Web server: IIS/6.0	Attacker stats



HACKED BY iSKORPiTX (TURKISH HACKER)

ARMANIAN

) FRANCE-

GREECE

) PKK TERROR

iskorpitx, marque du monde, présente ses salutations à tout le monde.

How are Web Servers Defaced

Web Servers are defaced by using the following attacks:

- Credentials through Man-in-the-middle attack
- Password brute force Administrator account
- DNS attack through cache poisoning
- DNS attack through social engineering
- FTP server intrusion
- Mail server intrusion
- Web application bugs
- Web shares misconfigurations
- Wrongly assigned permissions
- Rerouting after firewall attack
- Rerouting after router attack
- SQL Injection
- SSH intrusion
- Telnet intrusion
- URL poisoning
- Web Server extension intrusion
- Remote service intrusion



Attacks Against IIS

IIS is one of the most widely used web server platforms on the Internet

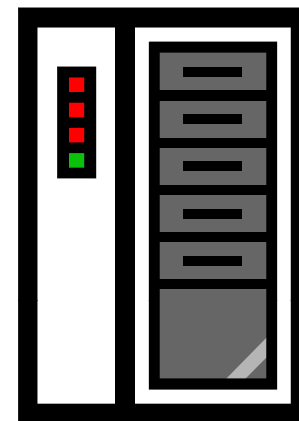
Microsoft's web server has been a frequent target over the years

Various vulnerabilities have attacked it
Examples include:

- ::\$DATA vulnerability
- showcode.asp vulnerability
- Piggy backing vulnerability
- Privilege command execution
- Buffer Overflow exploits (IIShack.exe)
- WebDav / RPC Exploits

Warning

These outdated vulnerability has been presented here as a proof of concept to demonstrate how a buffer overflow attack works



IIS 7 Components

IIS 7 contains several components that perform important functions for the application and Web server roles in Windows Server® 2008

Each component has responsibilities, such as listening for requests made to the server, managing processes, and reading configuration files

These components include protocol listeners, such as HTTP.sys, and services, such as World Wide Web Publishing Service (WWW service) and Windows Process Activation Service (WAS)

IIS Directory Traversal (Unicode) Attack

The vulnerability in unpatched Windows 2000 machine results because of a canonicalization error affecting CGI scripts and ISAPI extensions (.ASP is probably the best known ISAPI-mapped file type)

Canonicalization is the process by which various equivalent forms of a name can be resolved to a single, standard name

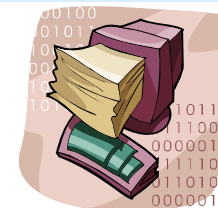
For example, "%c0%af" and "%c1%9c" are overlong representations for **/?** and **?\?**

Thus, by feeding the HTTP request (as shown below) to IIS, arbitrary commands can be executed on the server:

```
GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir=c:\ HTTP/1.0
```

Warning

This outdated vulnerability has been presented here as a proof of concept to demonstrate how a buffer overflow attack works



ASCII characters for the dots are replaced with the Unicode equivalent (%2E)

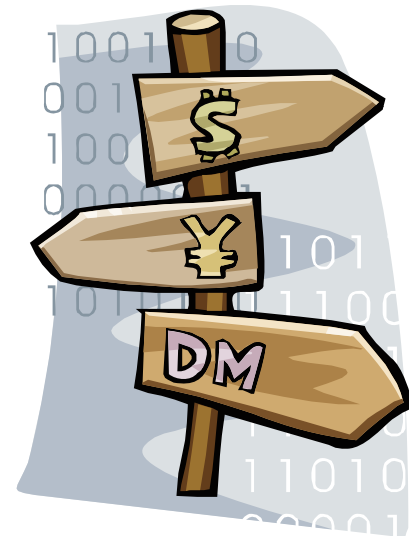
ASCII characters for the slashes are replaced with Unicode equivalent (%c0%af)

Unicode allows multiple encoding possibilities for each characters

Unicode for "/": 2f, c0af, e080af, f08080af, f8808080af, ...

Overlong Unicode is NOT malformed, but it is not allowed by a correct Unicode encoder and decoder

It is maliciously used to bypass filters that check only short Unicode





It occurs due to a canonicalization error in Microsoft IIS 4.0 and 5.0

A malformed URL could be used to access files and folders that lie anywhere on the logical drive that contains the web folders

This allows the attacker to escalate his privileges on the machine

This would enable the malicious user to add, change or delete data, run code already on the server, or upload new code to the server and run it

This vulnerability can be exploited by using the NETCAT as the backdoor (Trojan horse)

Warning

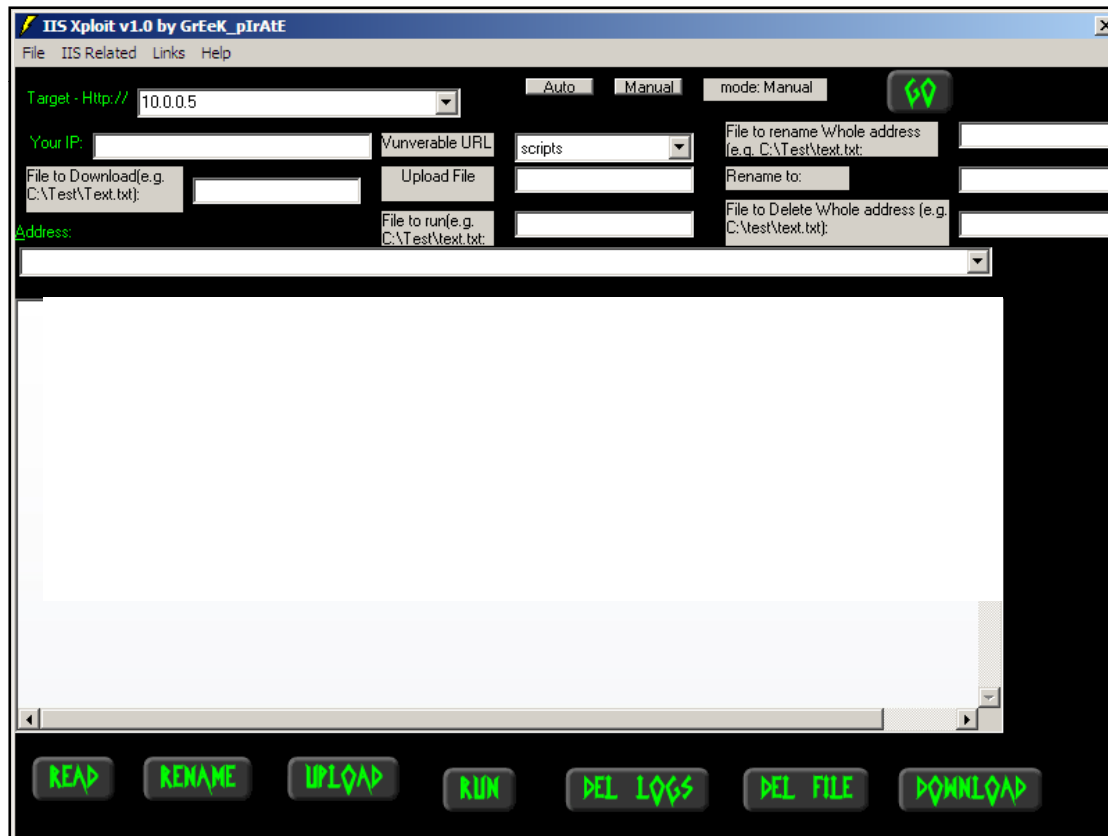
This outdated vulnerability has been presented here as a proof of concept to demonstrate how privilege escalation attack works

Hacking Tool: IISxploit.exe

This tool automates the directory traversal exploit in IIS



It created the Unicode string for exploitation



Msw3prt IPP Vulnerability

The ISAPI extension responsible for IPP is
msw3prt.dll



An oversized print request containing a valid
program code can be used to perform a new
function or load a different separate
program and cause buffer overflow



Warning

**This outdated vulnerability has been presented here as a proof of
concept to demonstrate how a buffer overflow attack works**

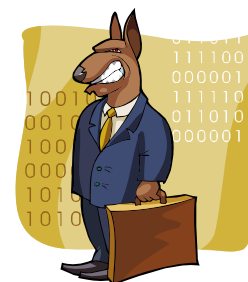
RPC DCOM Vulnerability

It exists in Windows Component Object Model (COM) subsystem, which is a critical service used by many Windows applications

DCOM service allows COM objects to communicate with one another across a network and is activated by default on Windows NT, 2000, XP, and 2003

Attackers can reach for the vulnerability in COM via any of the following ports:

- TCP and UDP ports 135 (Remote Procedure Call)
- TCP ports 139 and 445 (NetBIOS)
- TCP port 593 (RPC-over-HTTP)
- Any IIS HTTP/HTTPS port if COM Internet Services are enabled

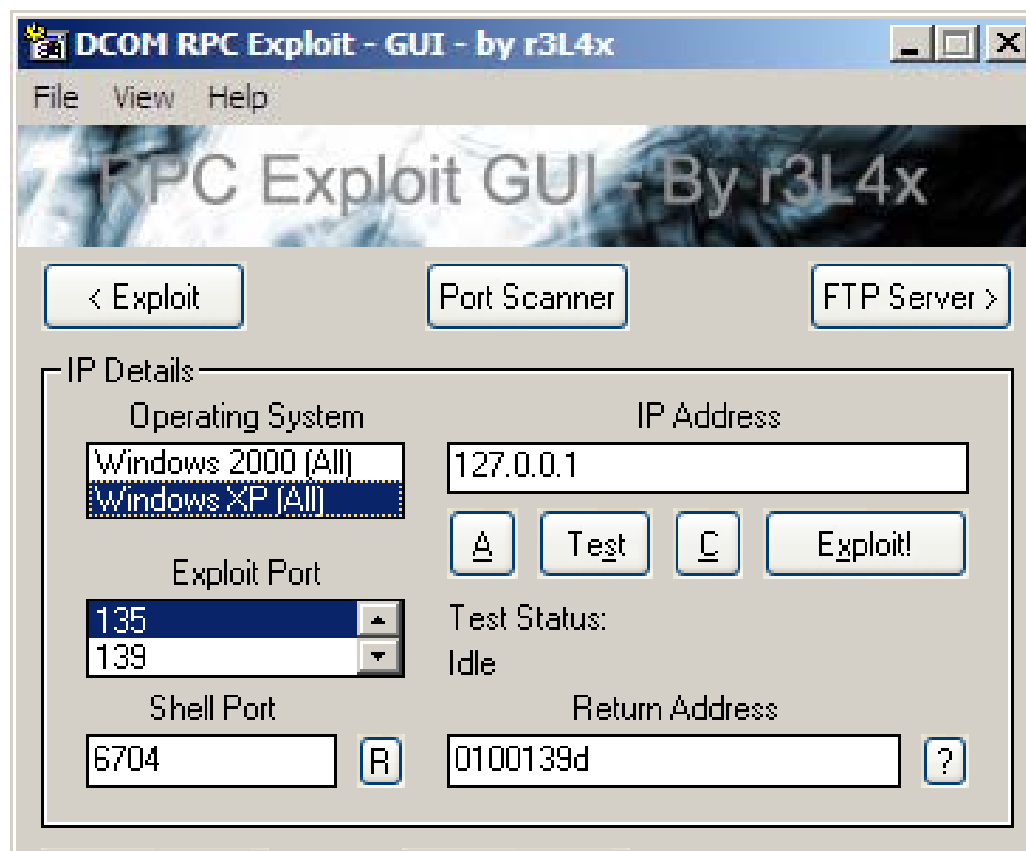


Warning

This outdated vulnerability has been presented here as a proof of concept to demonstrate how a buffer overflow works

RPC DCOM Vulnerability (cont'd)

RPC Exploit-GUI **Hacking Tool**

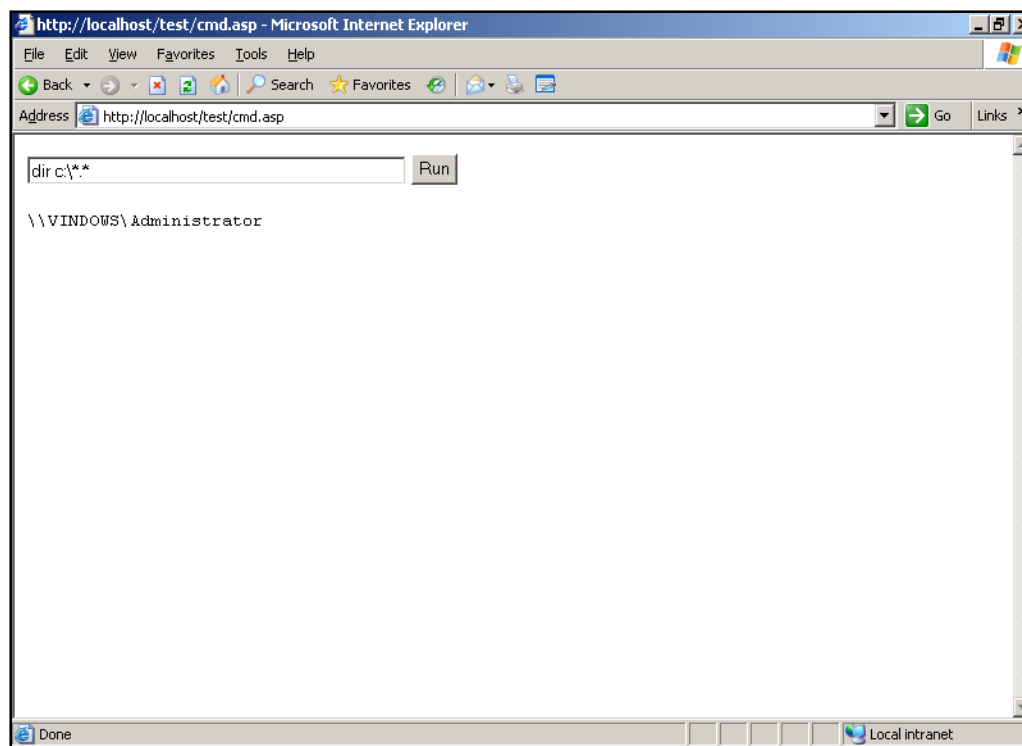


ASP Trojan (cmd.asp)

ASP Trojan is a small script which when uploaded to a Web Server, gives you complete control of the remote PC



ASP Trojan can be easily attached to shrink wrap applications thereby creating a backdoor

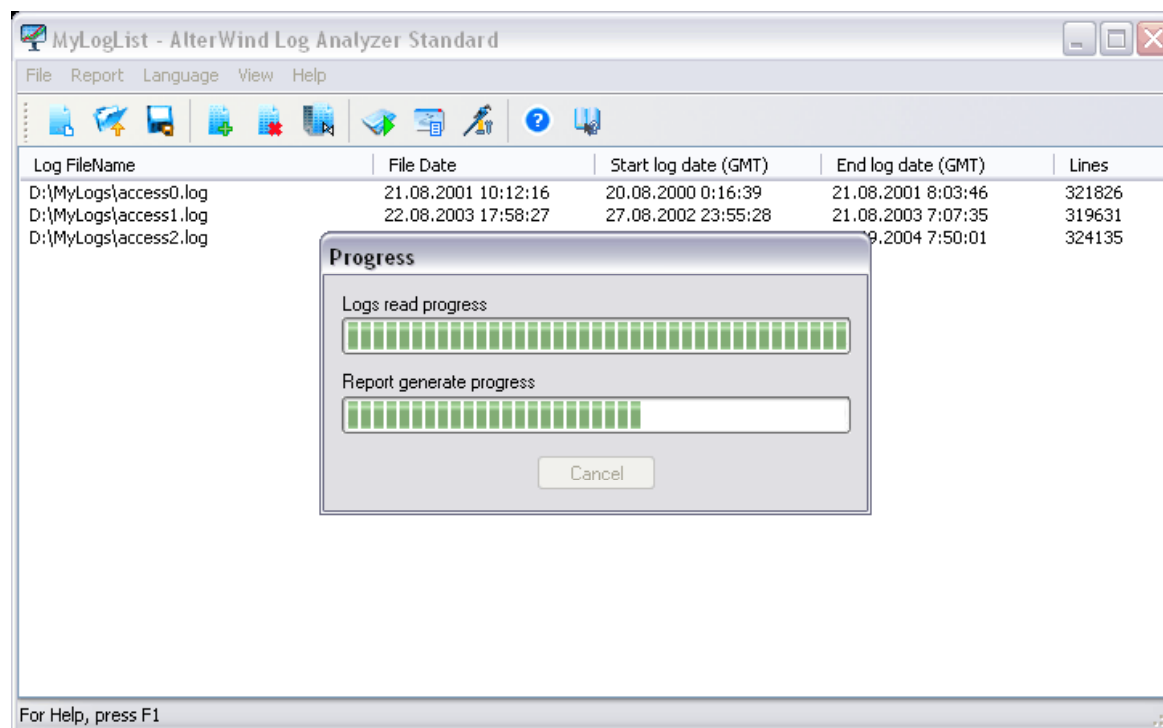


- ⦿ IIS logs all the visits in log files. The log file is located at:
`<%systemroot%>\logfiles`
- ⦿ If proxies are not used, then IP can be logged
- ⦿ This command lists the log files: `http://victim.com/scripts/..
%c0%af../..
%c0%af../..
%c0%af../..
%c0%af../..
%c0%af../..
%c0%af../winnt/system32/c
md.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1`



Network Tool: Log Analyzer

Log Analyzer tool helps to grab web server logs and build graphically rich self-explanatory reports on website usage statistics, referring sites, traffic flow, search phrases, etc.



Hacking Tool: CleanIISLog

CleanIISLog tool clears the log entries in the IIS log files filtered by an IP address



An attacker can easily cover his/her trace by removing entries based on his/her IP address in W3SVC Log Files

```
File Edit Format View Help
Jun 10 12:53:37.845 4.5.6.7 op=GET arg=http://Target
IP/msadc/...%255c.../...%255c.../...255c../winnt/system32/cmd.exe?/c+dir+c:\\*.cif/s/b
result="500 Server Error"
Jun 10 12:53:39.675 4.5.6.7 op=GET arg=http://Target
IP/a.asp/...%c1%lc../...%c1%lc../winnt/repair/sam result="404 Object Not Found"
Jun 10 12:53:43.578 4.5.6.7 op=GET arg=http://Target
IP/a.asp/...%c1%9c../...%c1%9c../winnt/repair/sam result="404 Object Not Found"
```

IIS Security Tool: Server Mask

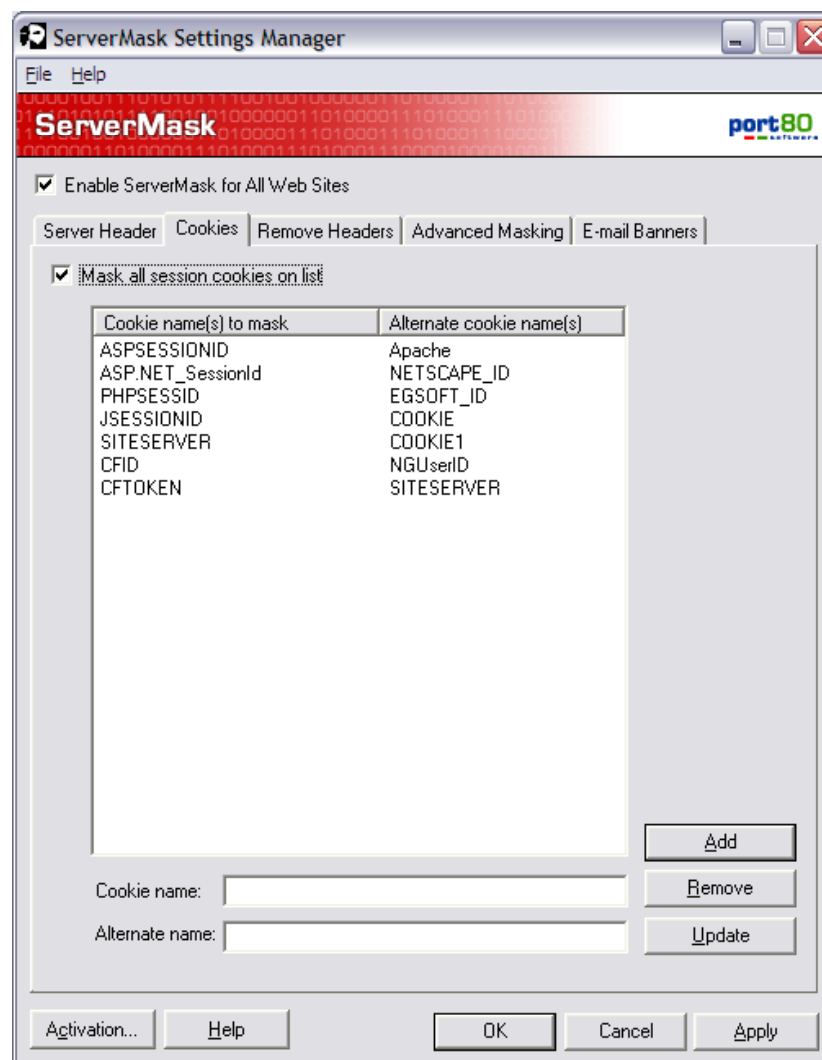
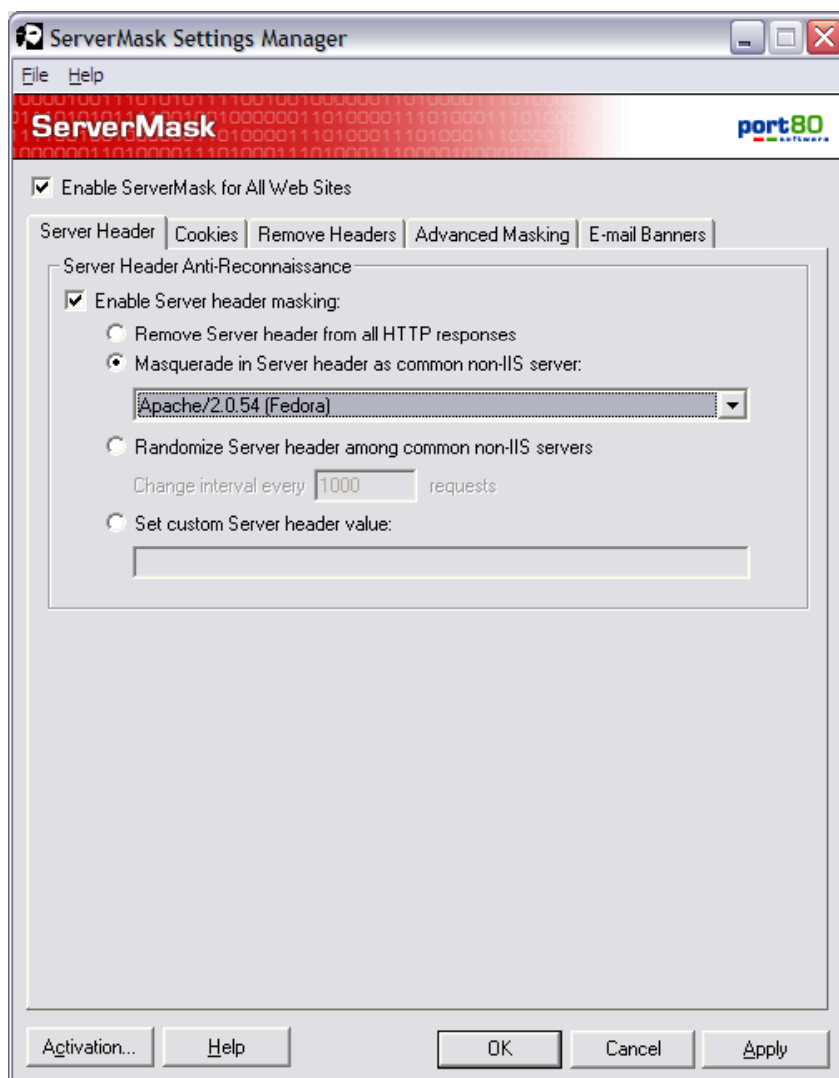
ServerMask changes or obscures the identity of your IIS Web server by safely and easily removing or modifying the unnecessary Server header in HTTP responses



You can change the header to any string you want



Server Mask: Screenshot



ServerMask ip100

ServerMask ip100 appliance stops TCP/IP fingerprinting

It stops end spoofing by adding authentication to the unprotected TCP/IP packets

It uses anomaly detection and dynamic blacklisting at the network level to stop DoS, IP spoof, session hijack, and DNS cache poisoning attacks

It has patent-pending technology that tags TCP/IP packets coming into and going out of the network layer transparently within a valid SYN/ACK response



Tool: CacheRight

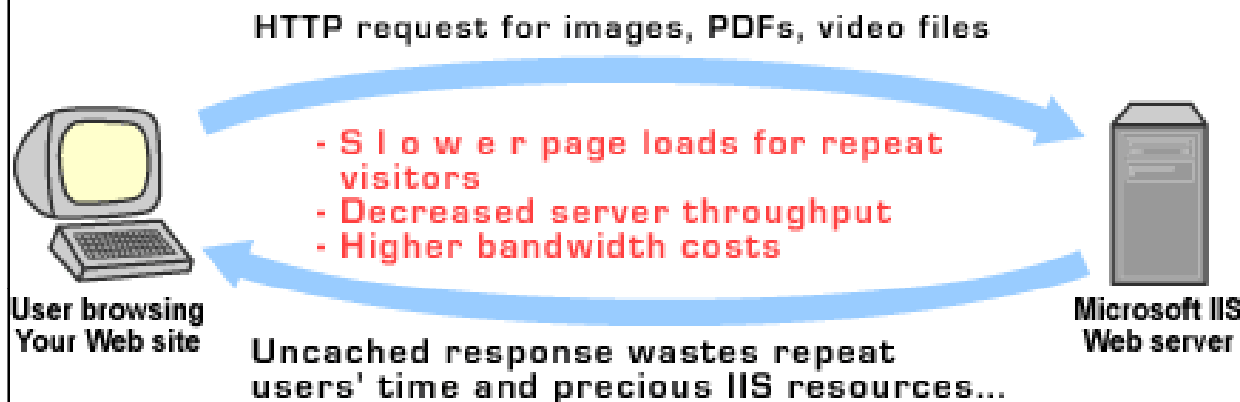
CacheRight allows developers to easily craft and administer effective cache control policies for every website resource through a single rules file, dramatically speeding up sites, reducing bandwidth consumption, and eliminating unnecessary requests and server strain

Features and Benefits:

- Manages all cache control rules for a site together in a single text file, promoting caching of binary objects like images, PDFs, and multimedia files
- Requires no MMC access to apply cache control to IIS websites and applications
- Intuitive, easy-to-master rule statements (a sample rules file is provided with detailed examples for developers)
- Reduces page load time, making for a better user experience and increased visitor retention
- Eliminates unnecessary chatter and bandwidth on server and network due to excessive conditional GET requests and 304 responses
- Saves time to deploy cache control by centralizing rules in one file and exposing cache control to developers, freeing up admins for other tasks

Tool: CacheRight (cont'd)

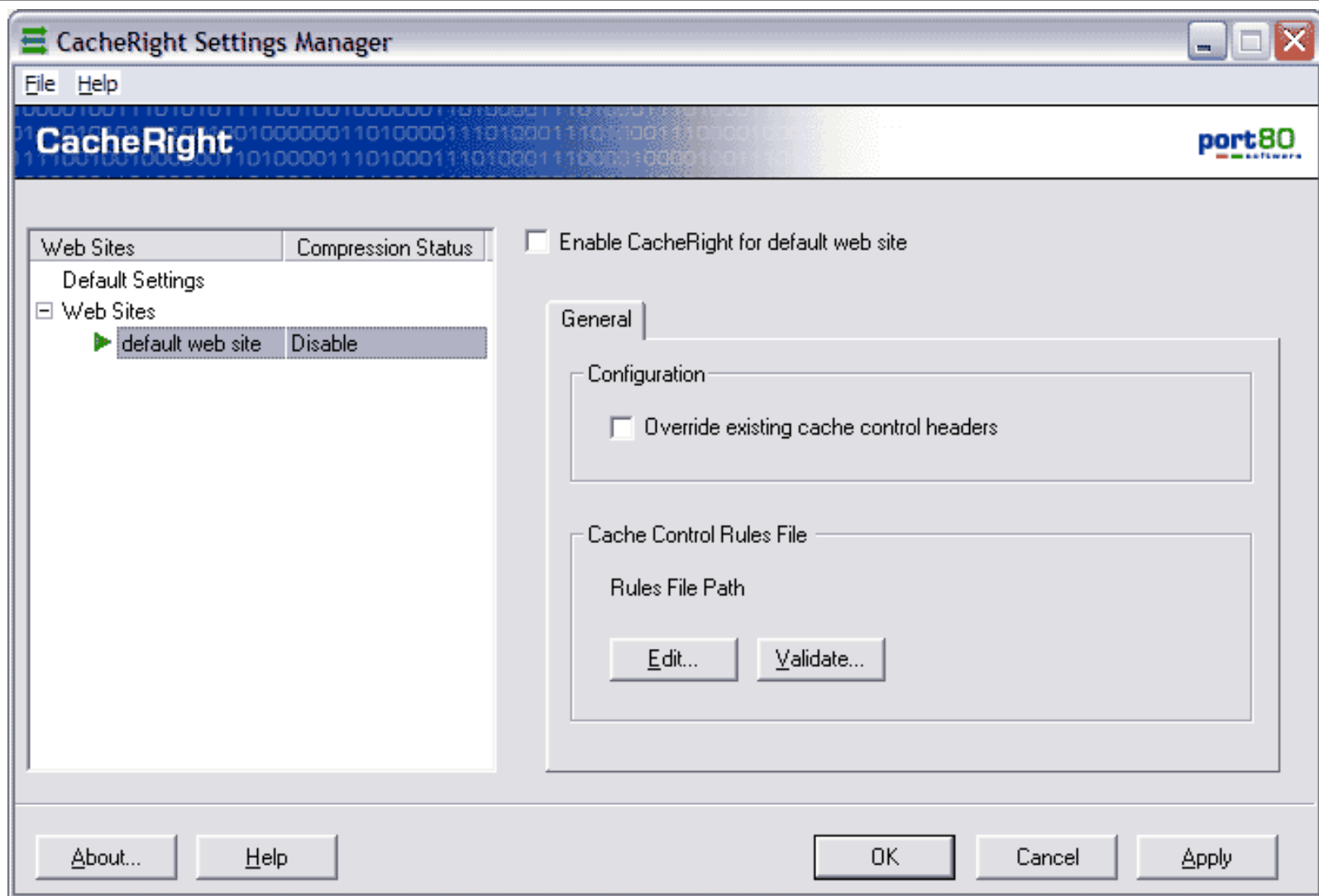
Without CacheRight



With CacheRight



CacheRight: Screenshot



Tool: CustomError

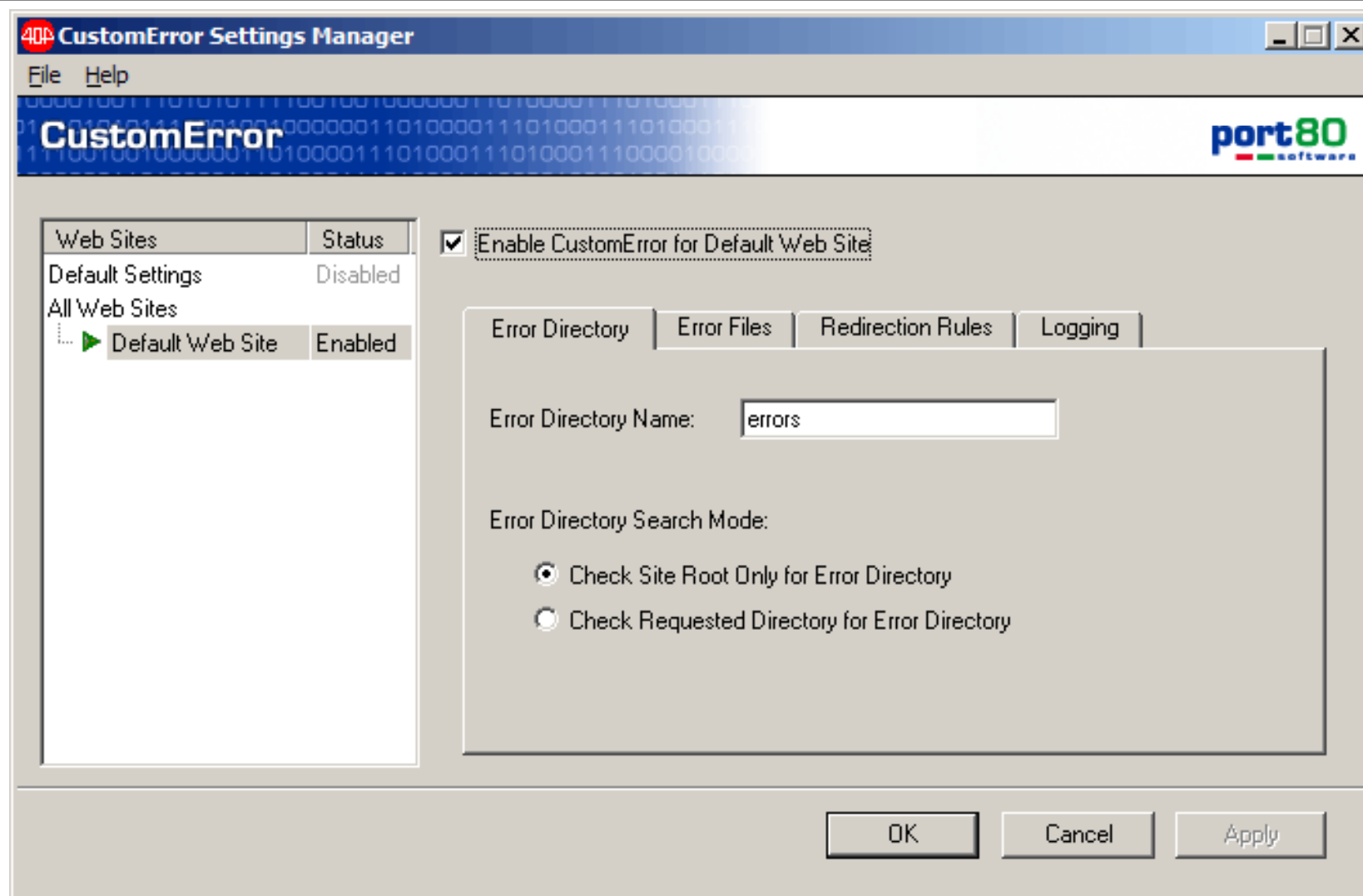
CustomError for IIS allows developers and admins to easily create customized 404 and other default error pages

It requires no administrator intervention

Benefits:

- Empowers web developers to deploy custom error pages on their sites, enhancing security and user experience
- Transforms dead, broken links into good traffic with 404 redirection management that is easy to manage
- Offloads error page mapping and broken link redirection chores to developers or website managers
- Works with virtual servers, so hosting vendors can offer custom errors to their clients without administrative or security hassles
- Works with error handling mechanisms in ASP, ASP.NET, and ColdFusion

CustomError: Screenshot



Tool: HttpZip

httpZip is an IIS server module for ISAPI-based compression on IIS 4, 5, and 6.0 Web servers

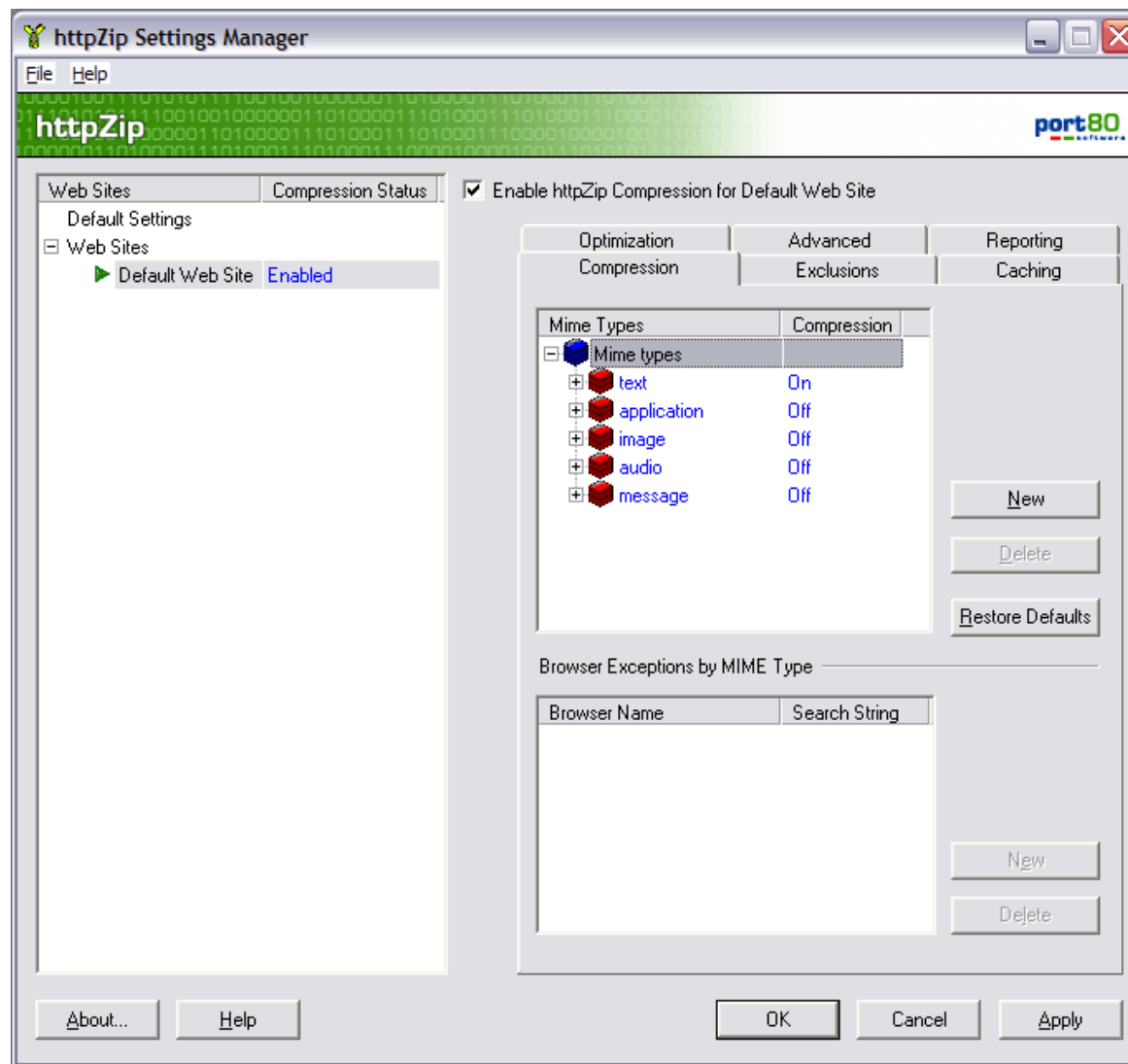
It compresses static and dynamic web content using encoding algorithms supported by all modern browsers, with flawless decompression secured by real-time browser compatibility checking

It takes compression even farther with optional HTML and CSS code optimization to improve performance and combat hackers' source sifting

Static and dynamic files can be accessed in pre-compressed format to minimize recompression processing with its built-in caching feature

Detailed httpZip reporting shows your files reduced to as little as 2% of their original size

HttpZip: Screenshot



Tool: LinkDeny

LinkDeny's powerful access control features allow you to transparently stop bandwidth pirates and potential hackers

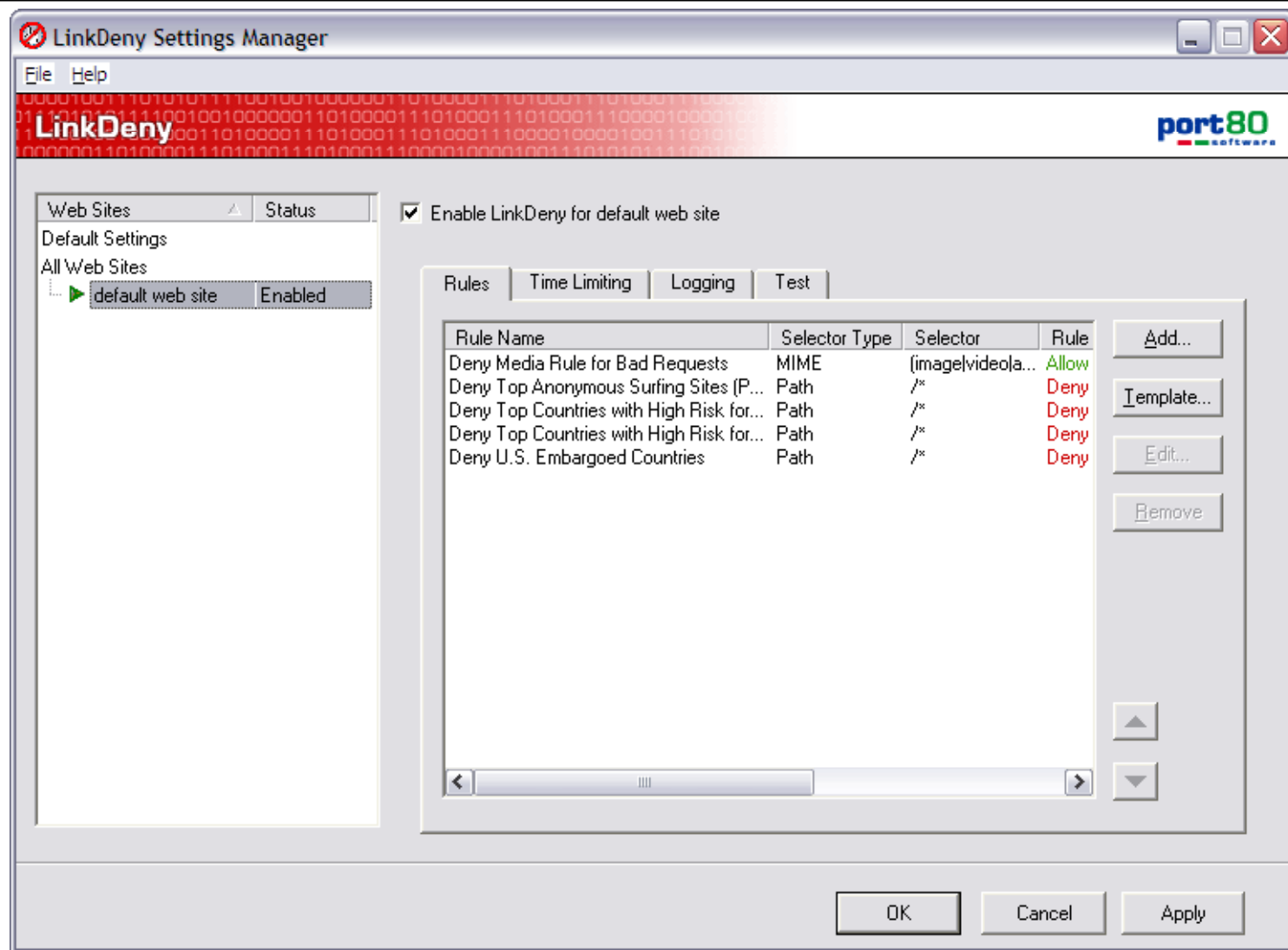
It addresses all sorts of common site problems from simple security to traffic management

It controls access to sensitive, private, proprietary, paid, or copyrighted files and downloads

It limits the access of hackers via a Web request's:

- IP address
- Referring URL
- Country or geographic location
- Demographics
- Length of user session
- Type of Web browser
- Existence of cookie
- HTTP request header type and content

LinkDeny: Screenshot



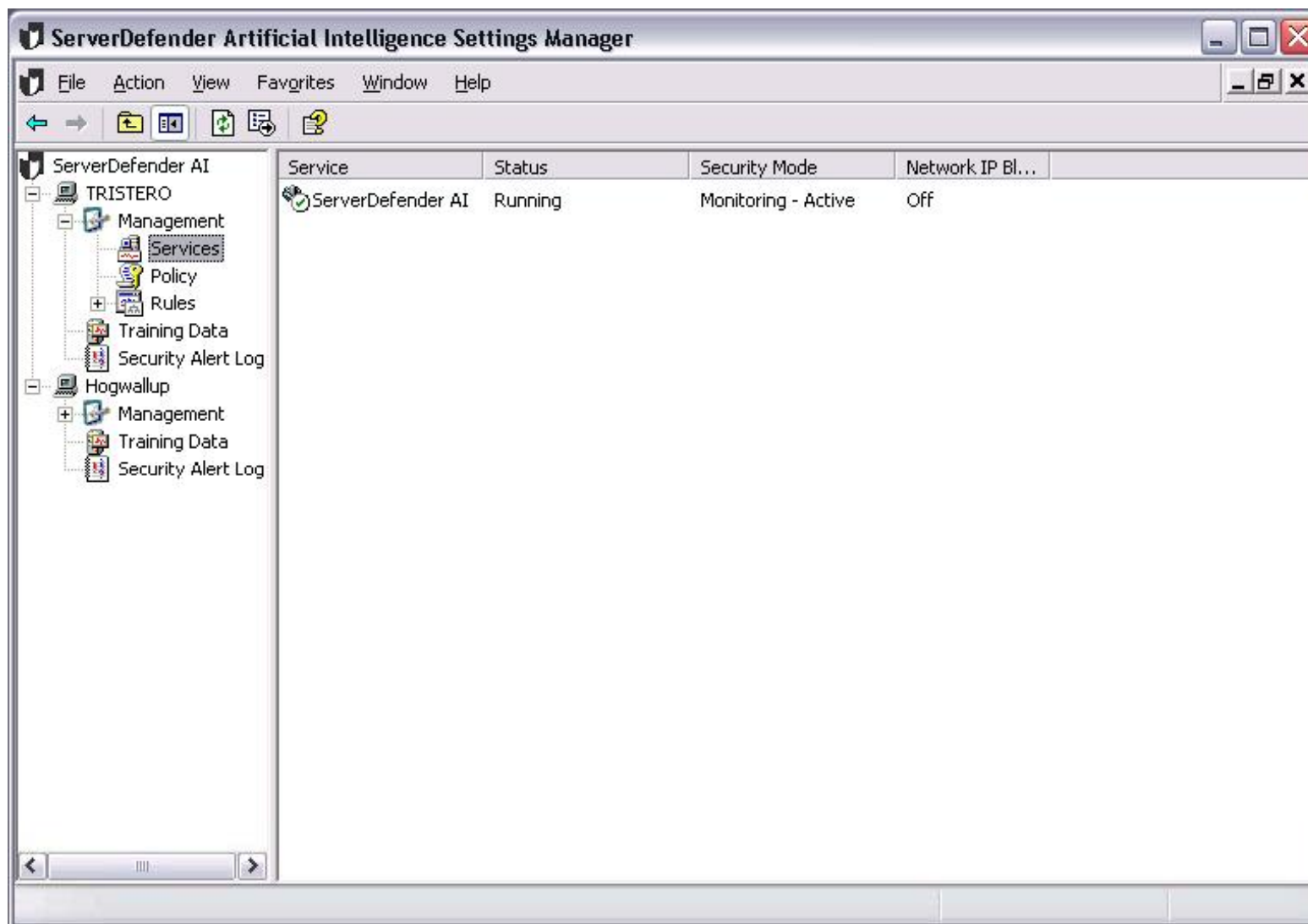
Tool: ServerDefender AI

ServerDefender Artificial Intelligence (AI) is a web application firewall

Benefits:

- Protects against known and unknown HTTP and HTTPS attacks and exploits with real-time alerts and countermeasures
- Goes beyond the limited pattern matching and policy-based systems to profile your web traffic for trusted and untrusted web request events
- Protects from patches, older/third party code, poorly coded web applications, and zero day attacks
- Bolsters regulatory compliance with internal and external standards like PCI
- Manages web application security for multiple IIS web servers on a local area network from one console

ServerDefender AI: Screenshot



Tool: ZipEnable

ZipEnable allows you to easily extract the absolute of IIS 6 built-in compression

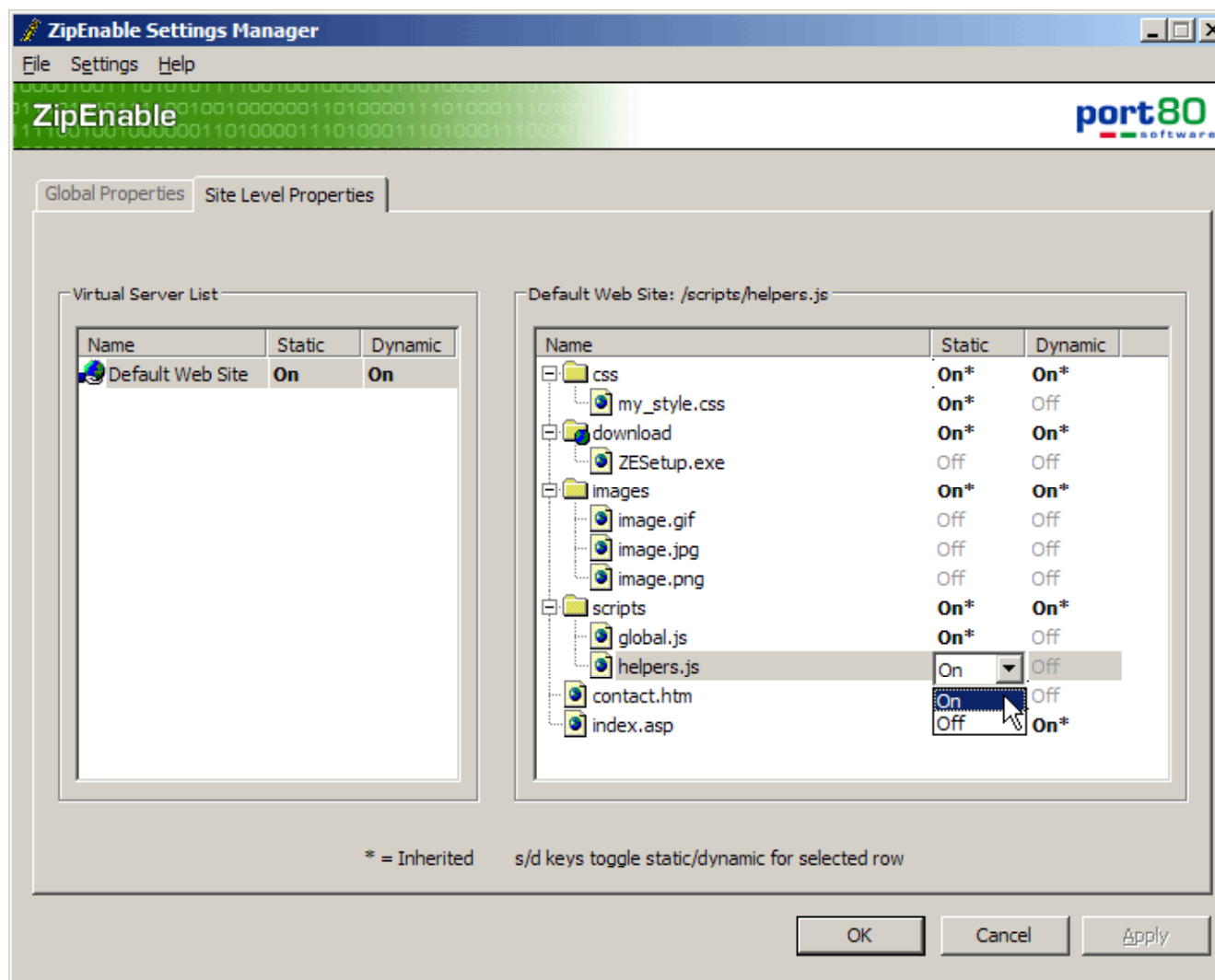
It is the best ISAPI compression solution for windows web servers

It is used to configure compression on all static and dynamic files

Features:

- Global compression configuration
- Configures compression at directory and file levels for individual virtual servers (sites)
- Browser Compatibility Detection
- CPU Roll-off option
- Manages cache directory, size, and location
- Sets priority of default Gzip and Deflate compression schemes

ZipEnable: Screenshot



Tool: W3compiler

w3compiler optimizes all or selected (X)HTML, CSS, JavaScript, ASP, CFM, and PHP files in your site

It removes redundant structures from your code before you load files on the server

Features:

- Reduces page load time
- Speeds up your site
- Secures your code
- Works with common web development best practices using staging and production sites
- Makes easy deployment tasks by copying entire or selected sites
- Delivers verifiable optimization through dashboard metrics and side-by-side preview interface

W3compiler: Screenshot

w3compiler - T:\inetpub\wwwroot\w3compiler\w3compiler.wcp

File Edit View Action Options Help

Target Files

Target Files	File Type	Last Modified	Original Size	Optimized Size	% Saved	Status
httpzipreport	File Folder	Mon Nov 03 13:39:34 2003				
images	File Folder	Mon Nov 03 13:39:28 2003				
includes	File Folder	Mon Nov 03 13:39:32 2003				
javascript	File Folder	Mon Nov 03 13:39:30 2003				
CVS	File Folder	Mon Nov 03 13:39:30 2003				
BuyForm.js	JScript Script ...	Tue Nov 04 17:52:56 2003	1416	1162	17.94	Previously Optimized
display_next_pop.js	JScript Script ...	Tue Nov 04 17:52:56 2003	560	428	23.57	Previously Optimized
formcheck.js	JScript Script ...	Mon Nov 10 18:33:36 2003	20502	6987	65.92	Optimized
global_functions_level1.js	JScript Script ...	Tue Nov 04 17:52:58 2003	1644	1288	21.65	Previously Optimized
global_functions_leveln.js	JScript Script ...	Tue Nov 04 17:52:58 2003	1874	1518	19.00	Previously Optimized
global_functions_root.js	JScript Script ...	Tue Nov 04 17:52:58 2003	1614	1258	22.06	Previously Optimized
global_functions_secure.js	JScript Script ...	Tue Nov 04 17:52:58 2003	2034	1678	17.50	Previously Optimized
pop_try.js	JScript Script ...	Tue Nov 04 17:52:58 2003	91	50	45.05	Previously Optimized
print_css_level1.js	JScript Script ...	Tue Nov 04 17:52:58 2003	463	389	15.98	Previously Optimized
print_css_root.js	JScript Script ...	Tue Nov 04 17:52:58 2003	457	383	16.19	Previously Optimized
print_css_secure.js	JScript Script ...	Tue Nov 04 17:52:58 2003	541	467	13.68	Previously Optimized
notrack	File Folder	Mon Nov 03 13:39:28 2003				

Project Source Project Target

GENERAL STATISTICS

Files Evaluated: 1
Bytes Saved: 13515
Percentage Saved: 65.92%
Files Optimized: 1
Files Unmodified: 0

General Statistics File Remapping Variable Remapping Errors/Warnings Project Log

1 Optimized Files: 65.92% Saved, 13515 Bytes Saved

Tool: Yersinia

Yersinia is a network tool designed to take advantage of some weakness in different network protocols

It pretends to be a solid framework for analyzing and testing the deployed networks and systems

Attacks for the following network protocols are implemented:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

Yersinia...

The Black Death for nowadays networks

by Slay & tomac

<http://yersinia.wasahero.org>
yersinia@wasahero.org

Prune your MSTP, RSTP, STP tree!!!!

Try 'yersinia protocol -h' to see protocol_options help

Please, see the man page for a full list of options and many examples.
Send your bugs & suggestions to the Yersinia developers <yersinia@wasahero.org>

```
MOTD: Who dares wins
prodigy:/home/tomac/work/projects/yersinia-sf/yersinia/yersinia/src#
```

```
prodigy:/home/tomac/work/projects/yersinia-sf/yersinia/yersinia/src# telnet localhost 12000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.
```

```
Welcome to yersinia version 0.5.5.1.
Copyright 2004 Slay & Tomac.
```

```
login: root
password:
```

```
MOTD: Do you have a Lexicon LX-7? Share it!! ;)
```

```
yersinia> en
Password:
yersinia# sh
attacks Show running attacks
cdp Cisco Discovery Protocol (CDP) information
dhcp Dynamic Host Configuration Protocol (DHCP) information
dot1q 802.1Q information
dtp Dynamic Trunking Protocol (DTP) information
history Display the session command history
hsrp Hot Standby Router Protocol (HSRP) information
interfaces Interface status
stats Show statistics
stp Spanning Tree Protocol (STP) information
users Display information about terminal lines
version System hardware and software status
vtp Virtual Trunking Protocol (VTP) information
```

```
yersinia# sh ver
Chaos Internetwork Operating System Software
yersinia (tm) Software (i686), Version 0.5.5.1, RELEASE SOFTWARE
Copyright (c) 2004-2004 by tomac & Slay, Inc.
Compiled Sun 07-Aug-2005 21:10 by someone
```

```
yersinia uptime is 51 seconds
```

```
Running Multithreading Image on Linux 2.6.12.3 supporting:
01 console terminal(s)
02 tty terminal(s)
05 vty terminal(s)
```

```
yersinia# sh users
User      Terminal      From      Since
----      -
* root    vty0          127.0.0.1:60715 Sun Aug 7 23:51:01 2005
```

```
yersinia#
```

yersinia 0.5.5 by Slay & tomac - CDP mode

[20:37:55]

TTL	DevID	Platform	Iface	Last seen
0A	zape	cisco WS-C2950T-24	eth0	07 Aug 20:37:53

```

#####
2#00022#22
#2220##02#22
22020##220022#
0200#2222#22022#
2020#22222#002022
220022222222#02##22
#2220#22222222#020##22
22202##2222222222#0022022
2##0020#2222222222#022#22
#220#22222222222222#0202#
22#20#22222222222222#0202#
#22022##2222222222##22
#22002##2222222222##22
2#20220#2222222222#0222
2#22#020####222222
22#0022200200#22
  
```

Chaos Internetwork Operating System Software
yersinia (tm) Software (i686), Version 0.5.5, RELEASE SOFTWARE
Copyright (c) 2004-2004 by tomac & Slay, Inc.
Compiled Tue 02-Aug-2005 22:37 by someone
yersinia uptime is 30 minutes, 04 seconds

Running Multithreading Image on
Linux 2.6.8.1 supporting:

01 console terminal(s)
02 tty terminal(s)
05 vty terminal(s)

Total Packets: 1323 — CDP Packets: 361 — MAC Spoofing [X]

CDP Fields

Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00
Version	00	TTL	00
Checksum	0000	TLV	

Tool: Metasploit Framework

Metasploit framework is an advanced open-source platform for developing, testing, and using exploit code

A tool for penetration testing, exploit development, and vulnerability research

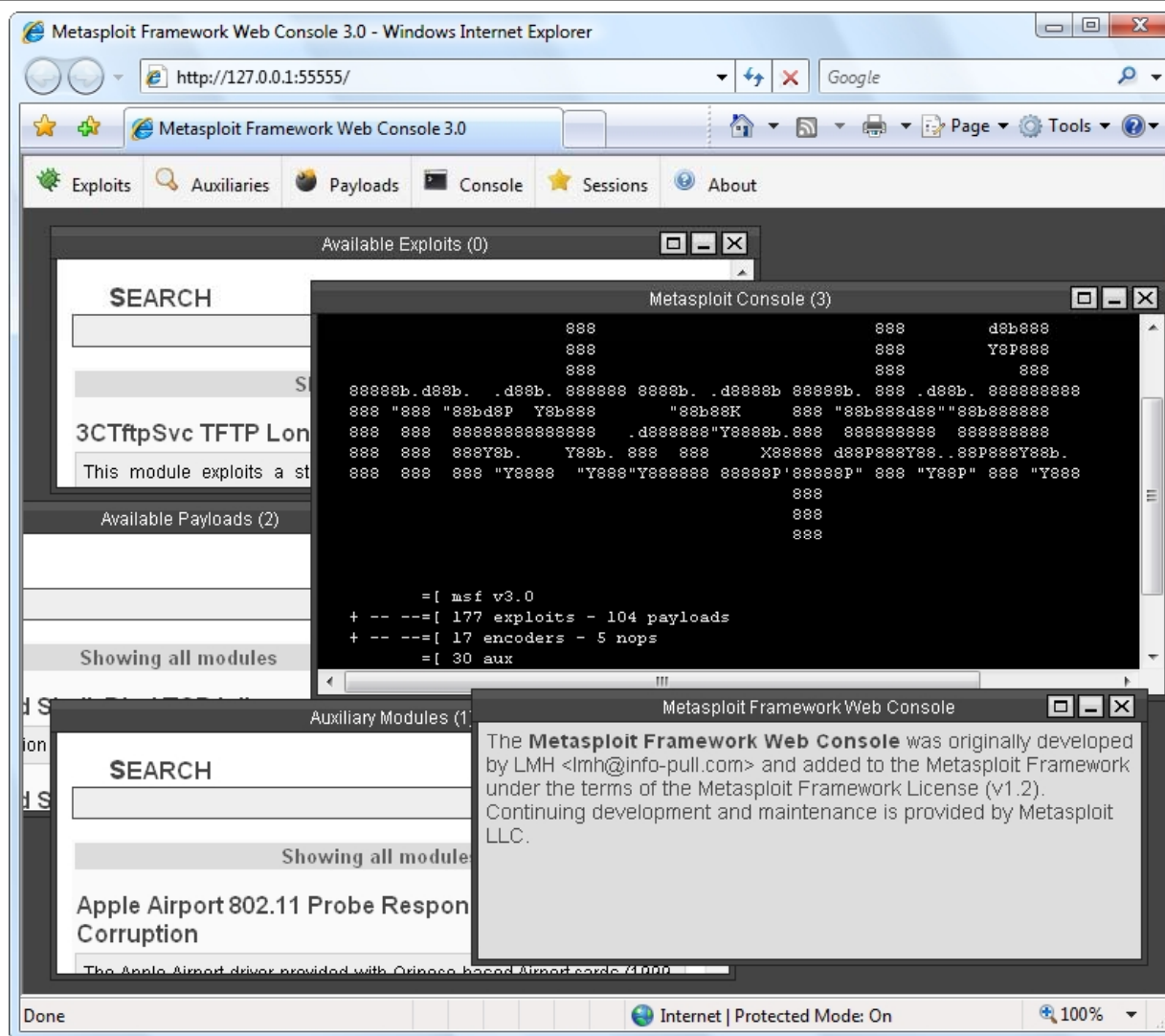
The framework was composed in Perl scripting language and consists of several components written in C, assembler, and Python

It runs on any UNIX-like system under its default configuration

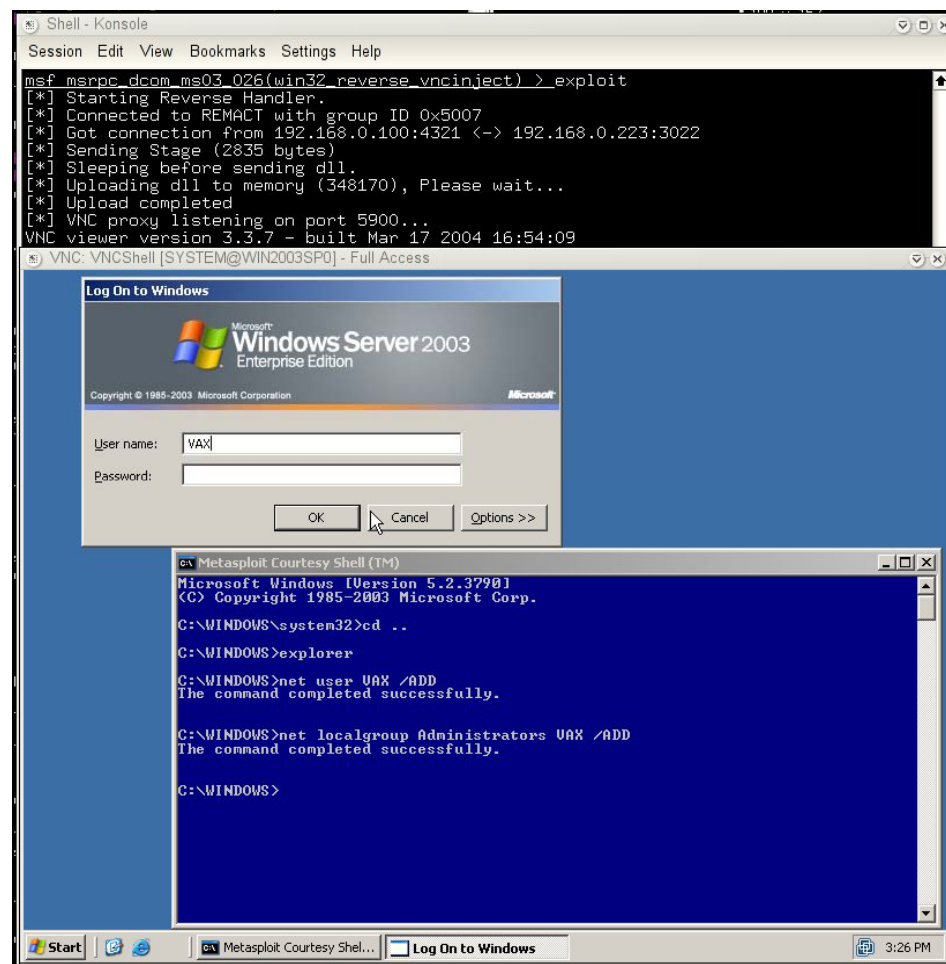
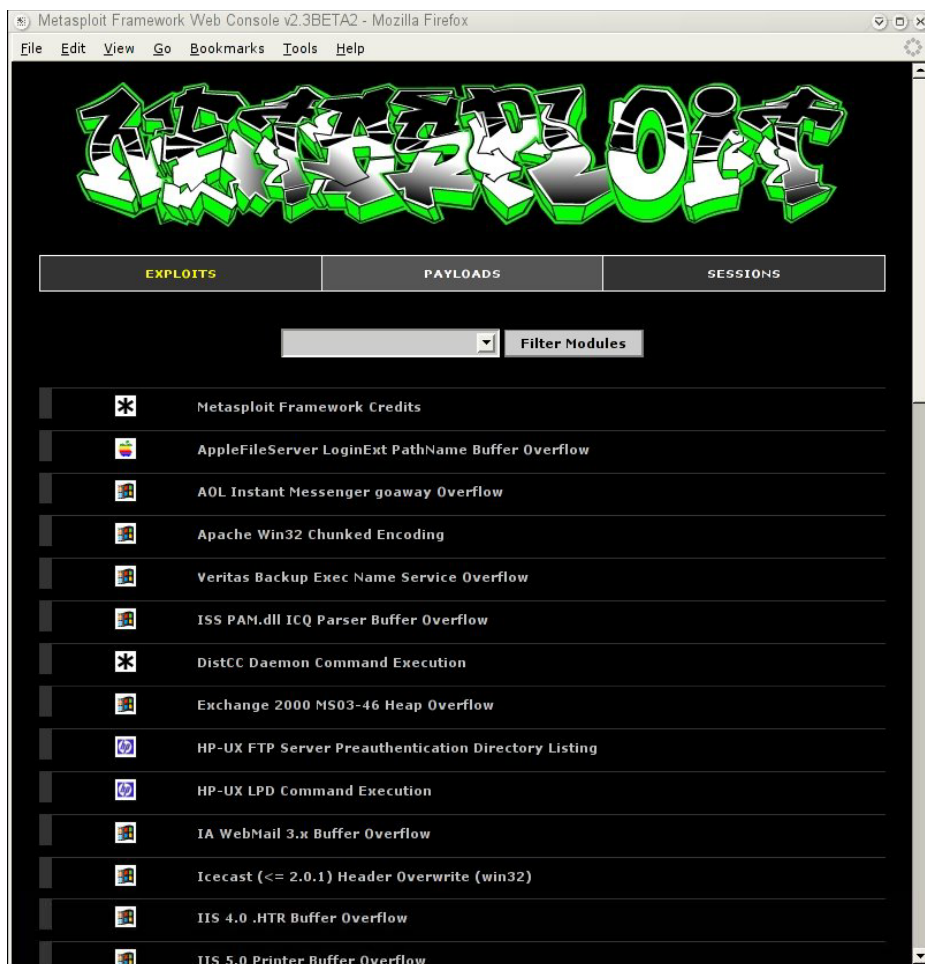
A customized Cygwin environment for windows OS users

<http://www.metasploit.com>

Metasploit Framework: Screenshot



Metasploit Framework: Screenshot



Tool: Immunity CANVAS Professional

Immunity's CANVAS makes hundreds of exploits, an automated exploitation system, and a comprehensive, reliable exploit development framework available to penetration testers and security professionals worldwide

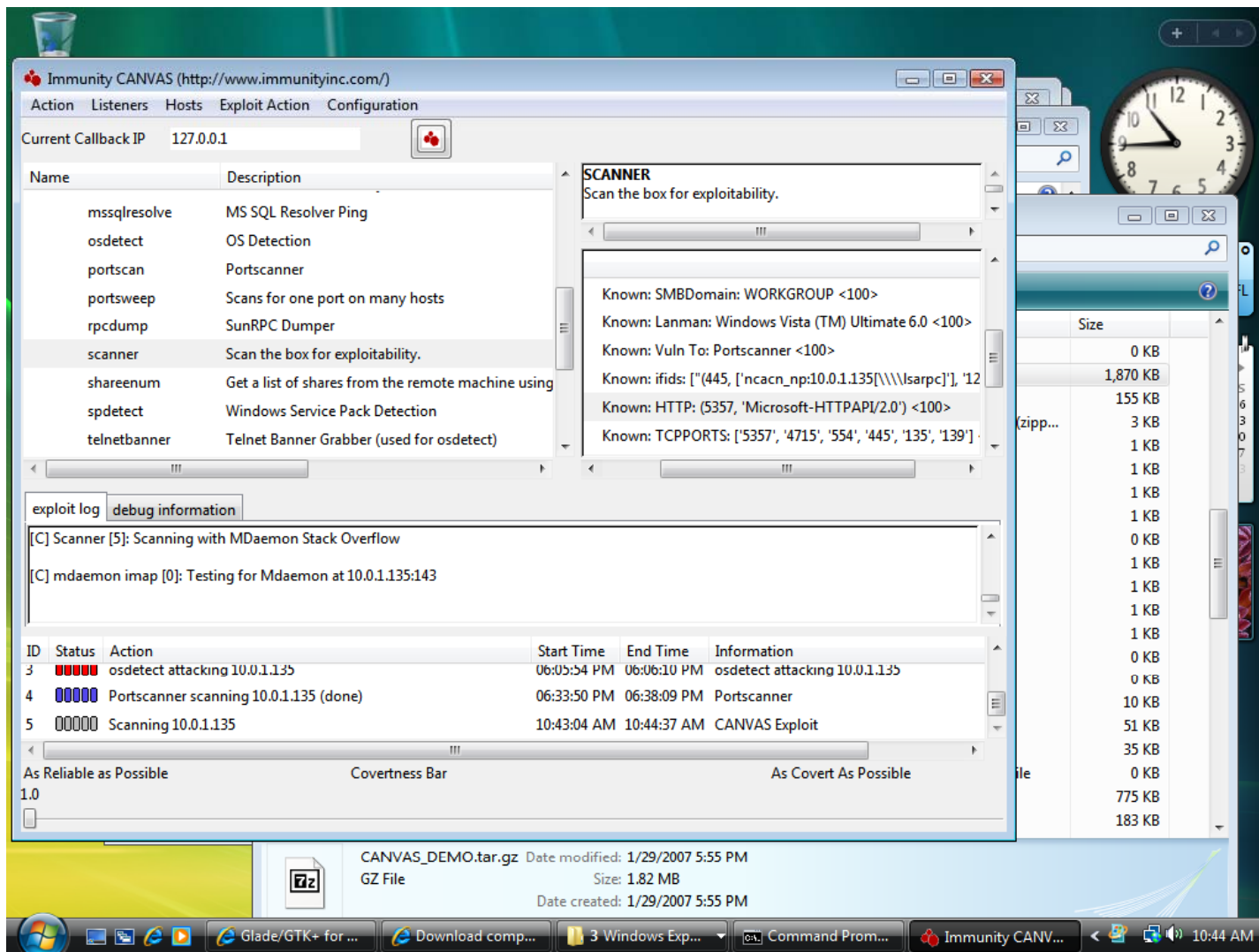
CANVAS Professional's completely open design allows a team to adapt it to their environment and needs

CANVAS Professional supports Windows, Linux MacOSX, and other Python environments

One license costs \$ 1244 and one license allows up to 10 users/installations

Source: <http://www.immunitysec.com/products-canvas.shtml>

Immunity CANVAS Professional: Screenshot 1



Immunity CANVAS Professional: Screenshot 2

The screenshot displays the Immunity CANVAS Professional interface. The main window shows a list of exploit modules under the 'Current' category, with 'dtspcd' (dtspcd heap overflow) selected. The 'Listeners' tab is active, showing a list of listeners with their status and information. A 'Listener Shell' window is open, showing the results of a command execution on a listener.

Current Local IP Address: 192.168.1.101

Name	Description
Current	Attacks against the current host
cachefsd_lpd	cachefsd .cfs_mnt File Stack Overflow (requires in.lpd for file upload)
cmsd_xdrarray	rpc.cmsd xdr_array heap overflow
dtspcd	dtspcd heap overflow
in_lpd	in.lpd command execution (Solaris 8)
kcms_server	kcms_server file retrieval
portscan	Portscanner
rpcdump	SunRPC Dumper
sadmind	Sadmind Remote Exploit for Solaris
samba_nttrans	Samba Nttrans Overflow
samba_trans2	Samba Trans2 Stack Overflow
snmpXdmid	snmpXdmid Buffer Overflow
sunlogin	Solaris Login Overflow
sunlogin_pamh	Solaris Login pamh Overflow
ttldb_xdrarray	rpc.ttldbserverd xdr_array Heap Overflow
Exploits	CANVAS Exploit Modules

References: <http://xforce.iss.net/alerts/adviser101.php> <http://www.kb.cert.org>
CVE Name: CVE-2001-0803
Date public: Nov 06, 2001
CERT Advisory: <http://www.cert.org/advisories/CA-2001-31.html>

ID	Status	Information
0	00000	Scanning 192.168.1.101 (done)
1	00000	Scanning 192.168.1.25 (done)
2	00000	dtspcd attacking 192.168.1.25:6112 (succeeded)
3	00000	Shell at [192.168.1.25, 6112]

Listener Shell

Download: [] To: [] Browse Go
 Upload: [] Browse Go
 cd: [] Go
 Spawn Process: [] Go
 Dir: [] Go
 pwd: (Gets Current Working Directory) Go
 Piped Command: [] Go
 unlink: [] Go

Command 'id -a' returned: *uid=0(root) gid=0(root)*
 Command 'echo "owned!"' returned: *owned!*

Host	OS	Status
192.168.1.101	Linux	Not owned
192.168.1.25	Solaris 8	Not owned

As Reliable as Possible Covertness Bar As Covert As Possible

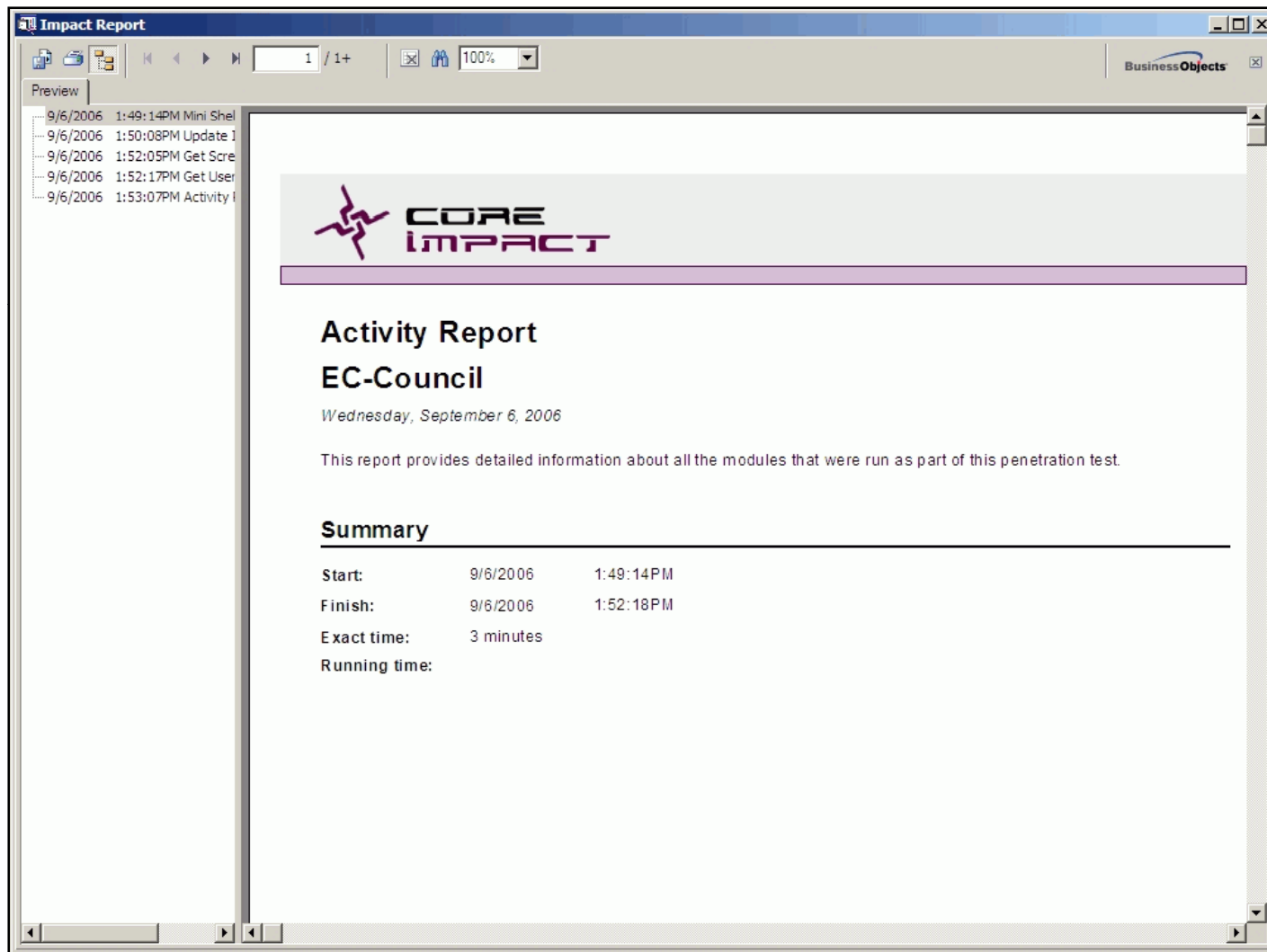
Tool: Core Impact

CORE IMPACT is the first automated, comprehensive penetration testing product for assessing specific information security threats to an organization

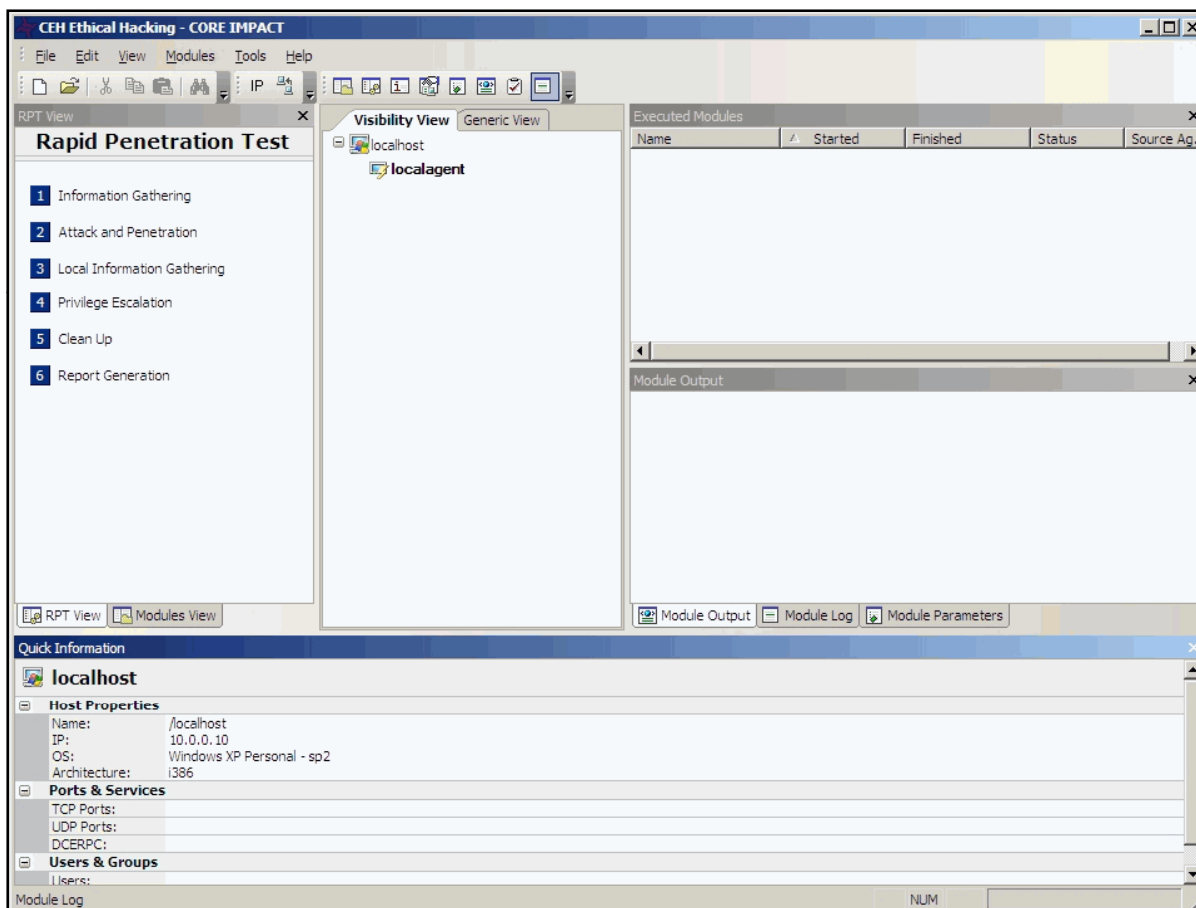
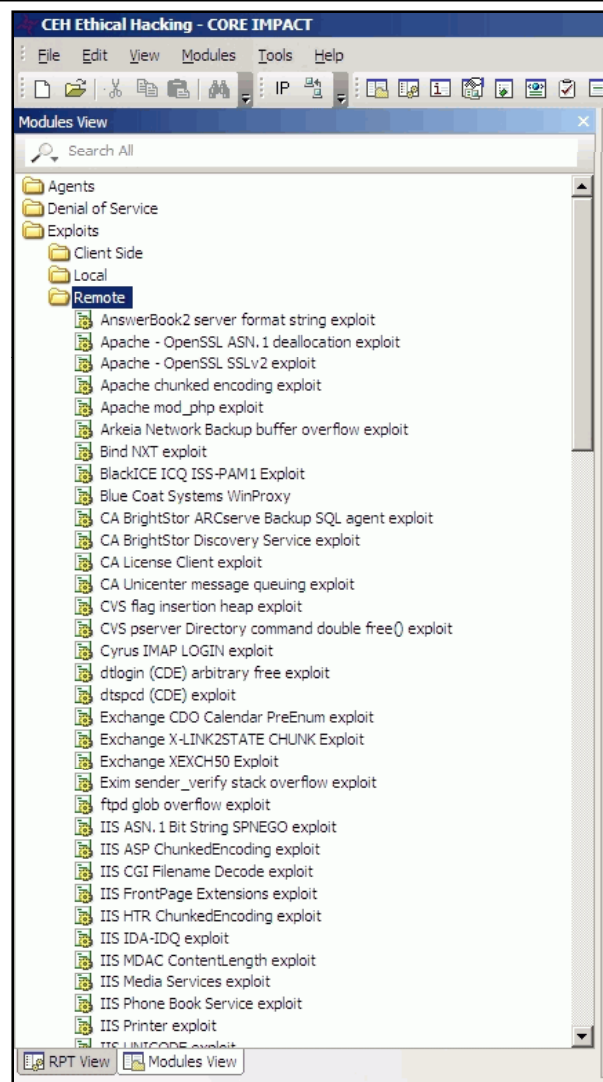
By safely exploiting vulnerabilities in your network infrastructure, the product identifies real, tangible risks to information assets while testing the effectiveness of your existing security investments



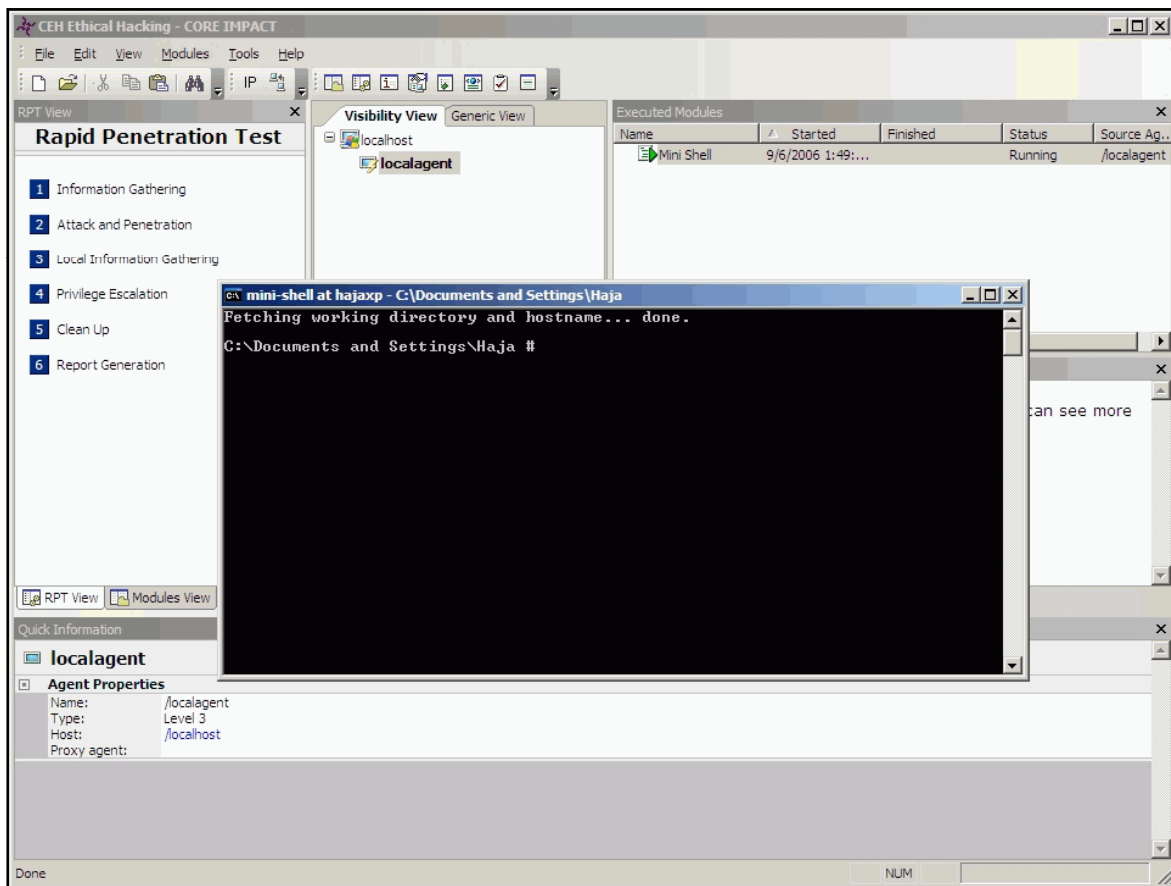
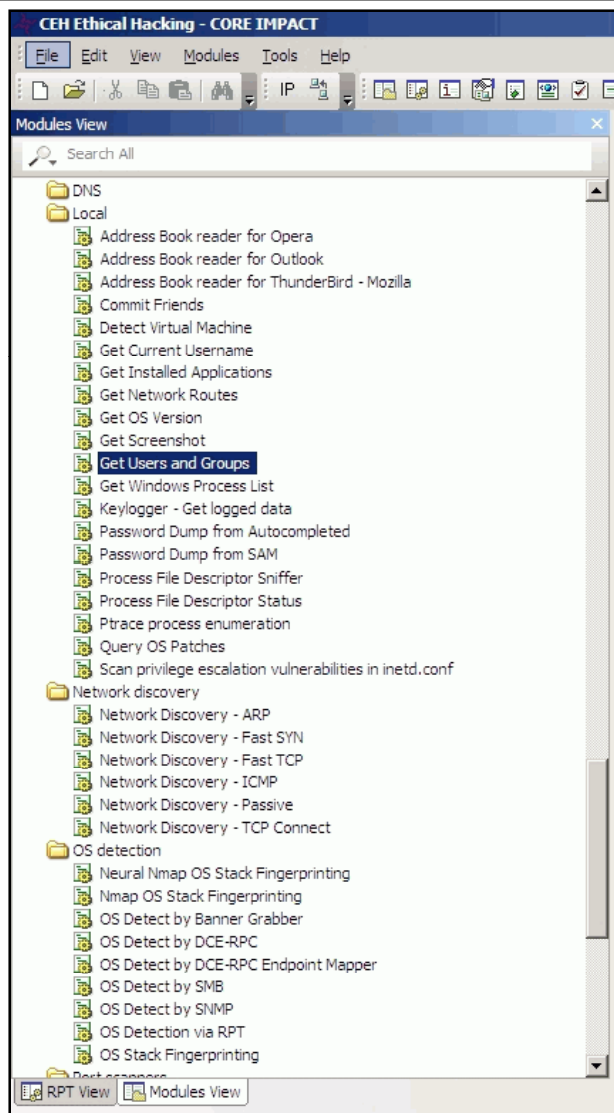
Core Impact: Screenshot 1



Core Impact: Screenshot 2



Core Impact: Screenshot 3



Core Impact: Screenshot 4

Impact Report
 5 / 5
 100%

9/6/2006 1:49:14PM Mini Shell

9/6/2006 1:50:08PM Update 1

9/6/2006 1:52:05PM Get Screenshot

9/6/2006 1:52:17PM Get Users and Groups

9/6/2006 1:53:07PM Activity Report

Detailed activity report

Technologies\IMPACT\reports\localhost_2006_13_52_08.gz to C:\Program Files\CORE Security Technologies\IMPACT\reports\localhost_2006_13_52_08.bmp

Removing remote screen capture program...

Screenshot taken successfully

--

Module finished execution after 5 secs.

Module: Get Users and Groups

Start: 9/6/2006 1:52:17PM

Finish: 9/6/2006 1:52:18PM

Status: Finished

Agent: /localagent

Parameters:

Log:

Module "Get Users and Groups" (v1.9.2.1) started execution on Wed Sep 06 13:52:17 2006

Couldn't open "/etc/passwd"

Couldn't open "/etc/shadow"

username	passwdhash	uid	gid	gecos	homedir	shell
root	\$1\$root\$	0	0	root	/	/bin/bash
bin	\$1\$bin\$	1	1	bin	/	/bin/bash
daemon	\$1\$daemon\$	2	2	daemon	/	/bin/bash
adm	\$1\$adm\$	3	3	adm	/	/bin/bash
lp	\$1\$lp\$	4	4	lp	/	/bin/bash
sync	\$1\$sync\$	5	5	sync	/	/bin/bash
shutdown	\$1\$shutdown\$	6	6	shutdown	/	/bin/bash
halt	\$1\$halt\$	7	7	halt	/	/bin/bash
mail	\$1\$mail\$	8	8	mail	/	/bin/bash
news	\$1\$news\$	9	9	news	/	/bin/bash
uucp	\$1\$uucp\$	10	10	uucp	/	/bin/bash
operator	\$1\$operator\$	11	11	operator	/	/bin/bash
games	\$1\$games\$	12	12	games	/	/bin/bash
man	\$1\$man\$	13	13	man	/	/bin/bash
irc	\$1\$irc\$	14	14	irc	/	/bin/bash
at	\$1\$at\$	15	15	at	/	/bin/bash
atd	\$1\$atd\$	16	16	atd	/	/bin/bash
rpc	\$1\$rpc\$	17	17	rpc	/	/bin/bash
rpcu	\$1\$rpcu\$	18	18	rpcu	/	/bin/bash
sshd	\$1\$sshd\$	19	19	sshd	/	/bin/bash
sshd	\$1\$sshd\$	20	20	sshd	/	/bin/bash
sshd	\$1\$sshd\$	21	21	sshd	/	/bin/bash
sshd	\$1\$sshd\$	22	22	sshd	/	/bin/bash
sshd	\$1\$sshd\$	23	23	sshd	/	/bin/bash
sshd	\$1\$sshd\$	24	24	sshd	/	/bin/bash
sshd	\$1\$sshd\$	25	25	sshd	/	/bin/bash
sshd	\$1\$sshd\$	26	26	sshd	/	/bin/bash
sshd	\$1\$sshd\$	27	27	sshd	/	/bin/bash
sshd	\$1\$sshd\$	28	28	sshd	/	/bin/bash
sshd	\$1\$sshd\$	29	29	sshd	/	/bin/bash
sshd	\$1\$sshd\$	30	30	sshd	/	/bin/bash
sshd	\$1\$sshd\$	31	31	sshd	/	/bin/bash
sshd	\$1\$sshd\$	32	32	sshd	/	/bin/bash
sshd	\$1\$sshd\$	33	33	sshd	/	/bin/bash
sshd	\$1\$sshd\$	34	34	sshd	/	/bin/bash
sshd	\$1\$sshd\$	35	35	sshd	/	/bin/bash
sshd	\$1\$sshd\$	36	36	sshd	/	/bin/bash
sshd	\$1\$sshd\$	37	37	sshd	/	/bin/bash
sshd	\$1\$sshd\$	38	38	sshd	/	/bin/bash
sshd	\$1\$sshd\$	39	39	sshd	/	/bin/bash
sshd	\$1\$sshd\$	40	40	sshd	/	/bin/bash
sshd	\$1\$sshd\$	41	41	sshd	/	/bin/bash
sshd	\$1\$sshd\$	42	42	sshd	/	/bin/bash
sshd	\$1\$sshd\$	43	43	sshd	/	/bin/bash
sshd	\$1\$sshd\$	44	44	sshd	/	/bin/bash
sshd	\$1\$sshd\$	45	45	sshd	/	/bin/bash
sshd	\$1\$sshd\$	46	46	sshd	/	/bin/bash
sshd	\$1\$sshd\$	47	47	sshd	/	/bin/bash
sshd	\$1\$sshd\$	48	48	sshd	/	/bin/bash
sshd	\$1\$sshd\$	49	49	sshd	/	/bin/bash
sshd	\$1\$sshd\$	50	50	sshd	/	/bin/bash
sshd	\$1\$sshd\$	51	51	sshd	/	/bin/bash
sshd	\$1\$sshd\$	52	52	sshd	/	/bin/bash
sshd	\$1\$sshd\$	53	53	sshd	/	/bin/bash
sshd	\$1\$sshd\$	54	54	sshd	/	/bin/bash
sshd	\$1\$sshd\$	55	55	sshd	/	/bin/bash
sshd	\$1\$sshd\$	56	56	sshd	/	/bin/bash
sshd	\$1\$sshd\$	57	57	sshd	/	/bin/bash
sshd	\$1\$sshd\$	58	58	sshd	/	/bin/bash
sshd	\$1\$sshd\$	59	59	sshd	/	/bin/bash
sshd	\$1\$sshd\$	60	60	sshd	/	/bin/bash
sshd	\$1\$sshd\$	61	61	sshd	/	/bin/bash
sshd	\$1\$sshd\$	62	62	sshd	/	/bin/bash
sshd	\$1\$sshd\$	63	63	sshd	/	/bin/bash
sshd	\$1\$sshd\$	64	64	sshd	/	/bin/bash
sshd	\$1\$sshd\$	65	65	sshd	/	/bin/bash
sshd	\$1\$sshd\$	66	66	sshd	/	/bin/bash
sshd	\$1\$sshd\$	67	67	sshd	/	/bin/bash
sshd	\$1\$sshd\$	68	68	sshd	/	/bin/bash
sshd	\$1\$sshd\$	69	69	sshd	/	/bin/bash
sshd	\$1\$sshd\$	70	70	sshd	/	/bin/bash
sshd	\$1\$sshd\$	71	71	sshd	/	/bin/bash
sshd	\$1\$sshd\$	72	72	sshd	/	/bin/bash
sshd	\$1\$sshd\$	73	73	sshd	/	/bin/bash
sshd	\$1\$sshd\$	74	74	sshd	/	/bin/bash
sshd	\$1\$sshd\$	75	75	sshd	/	/bin/bash
sshd	\$1\$sshd\$	76	76	sshd	/	/bin/bash
sshd	\$1\$sshd\$	77	77	sshd	/	/bin/bash
sshd	\$1\$sshd\$	78	78	sshd	/	/bin/bash
sshd	\$1\$sshd\$	79	79	sshd	/	/bin/bash
sshd	\$1\$sshd\$	80	80	sshd	/	/bin/bash
sshd	\$1\$sshd\$	81	81	sshd	/	/bin/bash
sshd	\$1\$sshd\$	82	82	sshd	/	/bin/bash
sshd	\$1\$sshd\$	83	83	sshd	/	/bin/bash
sshd	\$1\$sshd\$	84	84	sshd	/	/bin/bash
sshd	\$1\$sshd\$	85	85	sshd	/	/bin/bash
sshd	\$1\$sshd\$	86	86	sshd	/	/bin/bash
sshd	\$1\$sshd\$	87	87	sshd	/	/bin/bash
sshd	\$1\$sshd\$	88	88	sshd	/	/bin/bash
sshd	\$1\$sshd\$	89	89	sshd	/	/bin/bash
sshd	\$1\$sshd\$	90	90	sshd	/	/bin/bash
sshd	\$1\$sshd\$	91	91	sshd	/	/bin/bash
sshd	\$1\$sshd\$	92	92	sshd	/	/bin/bash
sshd	\$1\$sshd\$	93	93	sshd	/	/bin/bash
sshd	\$1\$sshd\$	94	94	sshd	/	/bin/bash
sshd	\$1\$sshd\$	95	95	sshd	/	/bin/bash
sshd	\$1\$sshd\$	96	96	sshd	/	/bin/bash
sshd	\$1\$sshd\$	97	97	sshd	/	/bin/bash
sshd	\$1\$sshd\$	98	98	sshd	/	/bin/bash
sshd	\$1\$sshd\$	99	99	sshd	/	/bin/bash
sshd	\$1\$sshd\$	100	100	sshd	/	/bin/bash

Couldn't open "/etc/group"

groupname passwdhash gid Groups

--

Module finished execution after 1 secs.

Module: Activity Report

Start: 9/6/2006 1:53:07PM

Finish:

Status: Running

Agent: /localagent

Parameters: DETAILS=LEVEL:Medium PARENT-LEVEL-TASKS:ONLY:True

Log:

Module "Activity Report" (v1.41) started execution on Wed Sep 06 13:53:07 2006

Generating reports, please wait.

This operation may take some minutes.

Executive Report

EC-Council

Wednesday, September 6, 2006

This report provides summarized information about all the different hosts and vulnerabilities that were successfully exploited by CORE IMPACT during this test.

Start: 9/6/2006 1:49:14PM

Finish: 9/6/2006 1:54:59PM

Exact time: 5 minutes

Running time:

Summary of Exploited Vulnerabilities

Total amount of vulnerabilities successfully exploited	0
Total amount of unique vulnerabilities successfully exploited	0
Total amount of compromised hosts (hosts with known vulnerabilities)	0
Average number of compromised hosts per vulnerability (Total amount of compromised hosts / Total amount of vulnerabilities successfully exploited)	0.00

Summary of discovered hosts

Total amount of hosts:	0
Total compromised hosts: (hosts with known vulnerabilities)	0
Average number of exploited vulnerabilities per compromised host:	0.00



CEH Ethical Hacking - CORE IMPACT

File Edit View Modules Tools Help

Modules View

Search All

Information gathering

- Client Side
- DNS
- Local
 - Address Book reader for Opera
 - Address Book reader for Outlook
 - Address Book reader for ThunderBird - Mozilla
 - Commit Friends
 - Detect Virtual Machine
 - Get Current Username
 - Get Installed Applications
 - Get Network Routes
 - Get OS Version
 - Get Screenshot
 - Get Users and Groups
 - Get Windows Process List
 - Keylogger - Get logged data
 - Password Dump from AutoCompleted
 - Password Dump from SAM
 - Process File Descriptor Sniffer
 - Process File Descriptor Status
 - Ptrace process enumeration
 - Query OS Patches
 - Scan privilege escalation vulnerabilities in inetd.conf
- Network discovery
 - Network Discovery - ARP
 - Network Discovery - Fast SYN
 - Network Discovery - Fast TCP
 - Network Discovery - ICMP
 - Network Discovery - Passive
 - Network Discovery - TCP Connect
- OS detection
 - Neural Nmap OS Stack Fingerprinting
 - Nmap OS Stack Fingerprinting
 - OS Detect by Banner Grabber
 - OS Detect by DCE-RPC
 - OS Detect by DCE-RPC Endpoint Mapper
 - OS Detect by SMB
 - OS Detect by SNMP
 - OS Detection via RDP

Visibility View

Generic View

localhost

localagent

Executed Modules

Name	Started	Finished	Status	Source Ag...
Mini Shell	9/6/2006 1:49:...	9/6/2006 1:49:...	Finished	/localagent
Update IMPA...	9/6/2006 1:50:...	9/6/2006 1:50:...	Finished	/localagent
Get Screenshot	9/6/2006 1:52:...	9/6/2006 1:52:...	Finished	/localagent
Get Users and...	9/6/2006 1:52:...	9/6/2006 1:52:...	Finished	/localagent
Activity Report	9/6/2006 1:53:...	9/6/2006 1:54:...	Finished	/localagent
Executive Re...	9/6/2006 1:55:...	9/6/2006 1:55:...	Finished	/localagent
Vulnerability R...	9/6/2006 1:55:...	9/6/2006 1:55:...	Finished	/localagent
Simple HTTP B...	9/6/2006 1:56:...	9/6/2006 1:56:...	Finished	/localagent
Vulnerability R...	9/6/2006 1:56:...	9/6/2006 1:57:...	Finished	/localagent
Get Windows ...	9/6/2006 1:57:...	9/6/2006 1:57:...	Finished	/localagent

Module Output

Get Windows Process List

Active processes

160	C:\Program Files\McAfee\MSK\MskServer.exe
348	C:\Program Files\Internet Explorer\iexplore.exe
412	C:\WINDOWS\System32\svchost.exe
548	c:\PROGRA~1\mcafee.com\agent\mcagent.exe
556	\SystemRoot\System32\smss.exe
660	\\?\C:\WINDOWS\system32\winlogon.exe
708	C:\WINDOWS\system32\services.exe
720	C:\WINDOWS\system32\svchost.exe
888	C:\WINDOWS\system32\svchost.exe
896	C:\Program Files\WIPFW\bin\ipfw.exe
980	c:\program files\mcafee\msc\mcupdui.exe
1032	C:\Program Files\CORE Security Technologies\IMPACT\bin\impact.exe
1056	C:\WINDOWS\System32\svchost.exe
1196	C:\Program Files\Logitech\MouseWare\system\em_exec.exe
1380	C:\Program Files\Bonjour\mDNSResponder.exe
1452	C:\WINDOWS\system32\spoolsv.exe
1544	C:\WINDOWS\system32\cisvc.exe
1616	C:\Program Files\Common Files\McAfee\HackerWatch\HWAPI.exe
1648	C:\PROGRA~1\McAfee\MSC\mclogsrv.exe
1684	C:\PROGRA~1\McAfee\MSC\mcupdmgr.exe
1724	c:\program files\common files\mcafee\mna\mcnasvc.exe
1800	C:\PROGRA~1\McAfee\MSC\mcpromgr.exe
1844	C:\DOCUME~1\Haja\LOCALS~1\Temp\Adobelm_Cleanup.0001
1912	C:\PROGRA~1\McAfee\MSC\mctskshd.exe
1952	C:\PROGRA~1\McAfee\MSC\mcusrmgr.exe
2008	c:\PROGRA~1\COMMON~1\mcafee\redirsvc\redirsvc.exe
2012	C:\Program Files\Common Files\Microsoft Shared\VS7DEBUG\MDM.EXE
2032	C:\Program Files\McAfee\MPF\MPFSrv.exe

Quick Information

Vulnerability Report

Module Properties

Brief: Creates the Vulnerability report

Category: Reports

Author: CORE Security Technologies

Version: 1.41

Description: The Vulnerability report provides detailed information about all the vulnerabilities that were successfully exploited during this penetration test.

Note: This module will run from localagent

Parameters: BLACK AND WHITE CHARTS: Print black & white charts.

Done

NUM

Tool: MPack

MPack is a powerful web exploitation tool that claims about 50 percent success in attacks silently launched against web browsers

Mpack or Web Attacker II is a collection of PHP software components designed to be hosted and run from a PHP server running a database on the backend

The kit uses techniques similar to previous attacks, which leverage legitimate web sites that have been compromised to redirect visitors to the malicious download sites

The software uses HTTP header information to send exploits that target the victim's specific browser



MPack (cont'd)

Mpack include exploits for:

- Animated cursor
- ANI overflow
- MS06-014, MS06-006, MS06-044
- XML Overflow
- WebViewFolderIcon Overflow
- WinZip ActiveX Overflow
- QuickTime Overflow

Server time/date snapshot: 5-May-2007 10:18:46
(United States)

MPack v0.90 stats

Attacked hosts (total - uniq)		Traffic (total - uniq)	
IE XP ALL	114721 - 96104	Total traff	159073 - 129089
QuickTime	2175 - 2048	Exploited	44804 - 35574
Win2000	7033 - 6260	Loads count	17408 - 15968
Firefox	12885 - 12514	Loader's response	38.85% - 44.89%
Opera7	1271 - 1264	Efficiency	10.94% - 12.37%

Browser stats (total)		Modules state	
MSIE	4 0%	Statistic type	MySQL-based
Opera	1 0%	User blocking	ON
		Country blocking	OFF

Country	Traff	Loads	Efficiency
RU - Russian federation	112793 70.9%	12653 72.7%	11.22%
UA - Ukraine	16666 10.5%	1670 9.6%	10.02%
IT - Italy	7045 4.4%	593 3.4%	8.42%
GE - Georgia	5775 3.6%	673 3.9%	11.65%
BY - Belarus	5419 3.4%	657 3.8%	12.12%
KZ - Kazakstan	3098 1.9%	376 2.2%	12.14%
US - United states	1117 0.7%	50 0.3%	4.48%
AZ - Azerbaijan	1060 0.7%	128 0.7%	12.08%
MD - Moldova, republic of	683	101	14.79%

Tool: Neosploit

NeoSploit is a toolkit which is packed with security exploits to launch the attack

It can do the following activities:

- Install programs
- Deletes programs
- Invoke dll components
- Create Run Keys.Runs other programs
- Hijack running processes
- Create known malware
- Create copies of itself



Neosploit: Screenshot

Neosploit Change Log

Latest version: 1.0.5 RC

16 April 2007

- new exploit module added
- removed ANI exploit
- fixed crypt algorithm

11 April 2007

- new exploit module added

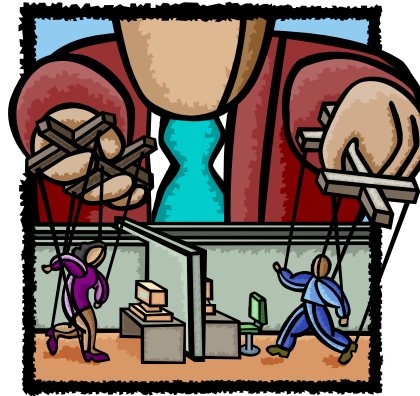
Neosploit v1.0.3 RC

Username:

Password:

Login

NEOSPLOIT FORCE EXPLOITS



Patch Management

Hotfixes and Patches

A hotfix is a code that fixes a bug in a product. The users may be notified through emails or through the vendor's website

Hotfixes are sometimes packaged as a set of fixes called a combined hotfix or service pack

A patch can be considered as a repair job in a piece of programming problem. A patch is the immediate solution that is provided to users



What is Patch Management

“Patch management is a process used to ensure that the appropriate patches are installed on a system”

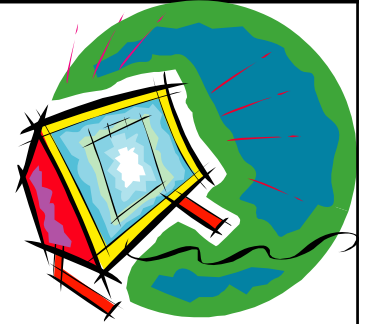
It involves the following:

- Choosing, verifying, testing, and applying patches
- Updating previously applied patches with current patches
- Listing patches applied previously to the current software
- Recording repositories, or depots, of patches for easy selection
- Assigning and deploying the applied patches



Solution: UpdateExpert

UpdateExpert is a windows administration program that helps you to secure your systems by remotely managing service packs and hotfixes



Microsoft constantly releases updates for the OS and mission critical applications, which fix security vulnerabilities and system stability problems

UpdateExpert enhances security, keeps systems up-to-date, eliminates sneaker-net, improves system 'sreliability, and QoS

UpdateExpert: Screenshot

The screenshot displays the UpdateExpert application window. The main interface is divided into several sections:

- Network:** A list of machines on the network, including LSEIBERT, LSMITH, MAIL01, MALTAMIRANO, MSEGARS, NETADMIN-LT, PFOWLER, PLEW, RGARCIA, RKAPLAN (selected), RLUSTIG, SBS-DEMO, SLEE, SMAUG-2K, SMEIER, SSWAIN, SSWAIN-LT, TEMP-PC, and TFC701.
- Research View:** A table of updates with columns for Name, KB Article, Reason for fix, Release Date, Install Date, and Language. The table lists various Windows NT 4.0 security patches and updates.
- Component Install Wizard:** A dialog box for customizing the installation of the selected update (Q265714.EXE) on the selected machine (RKAPLAN). It includes options for installation time, installation mode, and reboot settings.

The 'Component Install Wizard' dialog box shows the following details:

- Machines Selected:** RKAPLAN
- HotFix Selected:** Q265714.EXE
- Installed Time:** 04/27/2001 05:00PM
- Options:**
 - ☐ Install Now
 - ☐ Do not create uninstall..
 - ☒ Force apps to close on...
 - ☒ Quiet mode
 - ☐ Reboot after each install
 - ☒ Reboot after group inst...

The background shows a Microsoft Product Support Services page for Windows NT 4.0 SNM, with article ID Q265714.

Patch Management Tool: qfecheck

Qfecheck allows customers to diagnose and eliminate the effects of anomalies in the packaging of hotfixes for Microsoft Windows

Qfecheck.exe determines which hotfixes are installed by reading the information stored in the following registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates



```
G:\CEH\Haja\patch>qfecheck /v
```

```
Windows 2000 Hotfix Validation Report for \\SYSTEM5  
Report Date: 5/17/2005 2:23pm
```

```
Current Service Pack Level: Service Pack 4
```

```
Hotfixes Identified:
```

```
Q327194: Current on system.  
KB820888: Current on system.  
KB822831: Current on system.  
KB823182: Current on system.  
KB823559: Current on system.  
KB824105: Current on system.  
KB825119: Current on system.  
KB826232: Current on system.  
KB828035: Current on system.  
KB828741: Current on system.  
KB828749: Current on system.  
KB835732: Current on system.  
KB837001: Current on system.  
KB839645: Current on system.  
KB840315: Current on system.  
KB840987: Current on system.  
KB841356: Current on system.  
KB841533: Current on system.  
KB841872: Current on system.  
KB841873: Current on system.  
KB842526: Current on system.  
KB842773: Current on system.  
KB871250: Current on system.  
KB873333: Current on system.  
KB873339: Current on system.  
KB885250: Current on system.  
KB885835: Current on system.  
KB885836: Current on system.  
KB888113: Current on system.  
KB890047: Current on system.  
KB890175: Current on system.  
KB890859: Current on system.  
KB891711: Current on system.  
KB891781: Current on system.  
KB893066: Current on system.  
KB893086: Current on system.  
KB893803: Current on system.  
Q818043: Current on system.
```

Patch Management Tool: HFNetChk

HFNetChk is a command-line tool that enables the administrator to check the patch status of all the machines in a network remotely

It does this function by referring to an XML database that Microsoft constantly updates

```
C:\WINNT\System32\cmd.exe
MICRON
-----

WINDOWS 2000 SP2

Patch NOT Found MS00-077 Q299796
Patch NOT Found MS00-079 Q276471
Patch NOT Found MS01-007 Q285851
Patch NOT Found MS01-013 Q285156
WARNING MS01-022 Q296441
Patch NOT Found MS01-025 Q296185
Patch NOT Found MS01-037 Q302755
Patch NOT Found MS01-041 Q298012

Internet Information Services 5.0

Patch NOT Found MS01-025 Q296185

Internet Explorer 5.5 SP2

INFORMATION
All necessary hotfixes have been applied
```

caccls.exe Utility

Built-in Windows 2000 utility (caccls.exe) can set access control list (ACLs) permissions globally

To change permissions on all executable files to System:Full, Administrators:Full

- `C:\>caccls.exe c:\myfolder\*.exe /T /G System:F Administrators:F`



```
Command Prompt

C:\Snort>caccls.exe *.exe /T /G System:F Administrators:F
Are you sure (Y/N)?y
processed file: C:\Snort\snort.exe

C:\Snort>
```



Vulnerability Scanners

Vulnerability Scanners

The different types of vulnerability scanners according to their availability are:

- Online Scanners : e.g. www.securityseers.com
- Open Source scanners: e.g. Snort, Nessus Security Scanner, and Nmap
- Linux Proprietary Scanners: The resource for scanners on Linux is SANE (Scanner Access Now Easy). Besides SANE there is XVScan, Parallel Port Scanners under Linux, and USB Scanners on Linux
- Commercial Scanners: You can purchase these from the vendors





Online Vulnerability Search Engine



Sponsored by
DHS National Cyber Security Division/US-CERT



NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	Product Dictionary	Impact Metrics	Data Feeds	Statistics	
Home	ISAP/SCAP	SCAP Validated Tools	SCAP Events	About	Contact	Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 29705 [CVE Vulnerabilities](#)
- 150 [Checklists](#)
- 132 [US-CERT Alerts](#)
- 2152 [US-CERT Vuln Notes](#)
- 3171 [OVAL Queries](#)
- 13723 [Vulnerable Products](#)

Last updated: 02/25/08

There are **126** matching records. Displaying matches **1** through **20**.

[Next 20 Matches](#)

[CVE-2007-1748](#) [TA07-128A](#) [TA07-103A](#) [VU#555920](#)
[oval:org.mitre.oval:def:1228](#)

Summary: Stack-based buffer overflow in the RPC interface in the Domain Name System (DNS) Server Service in Microsoft Windows 2000 Server SP 4, Server 2003 SP 1, and Server 2003 SP 2 allows remote attackers to execute arbitrary code via a long zone name containing character constants represented by escape sequences.
Published: 4/13/2007
CVSS Severity: 10.0 (High)

[CVE-2006-7052](#)

Summary: Multiple PHP remote file inclusion vulnerabilities in DotWidget For Articles (dotwidgeta) 0.2 allow remote attackers to execute arbitrary code via a URL in the (1) file_path parameter to (a) index.php, (b) showcatpicks.php, and (c) showarticle.php; and the (2) admin_header_file and (3) admin_footer_file parameters to (d) admin/authors.php, (e) admin/index.php, (f) admin/categories.php, (g) admin/editconfig.php, and (h) admin/articles.php.
Published: 2/23/2007
CVSS Severity: 10.0 (High)

[CVE-2006-6199](#)

Network Tool: Whisker

Whisker is an automated vulnerability scanning software that scans for the presence of exploitable files on remote web servers

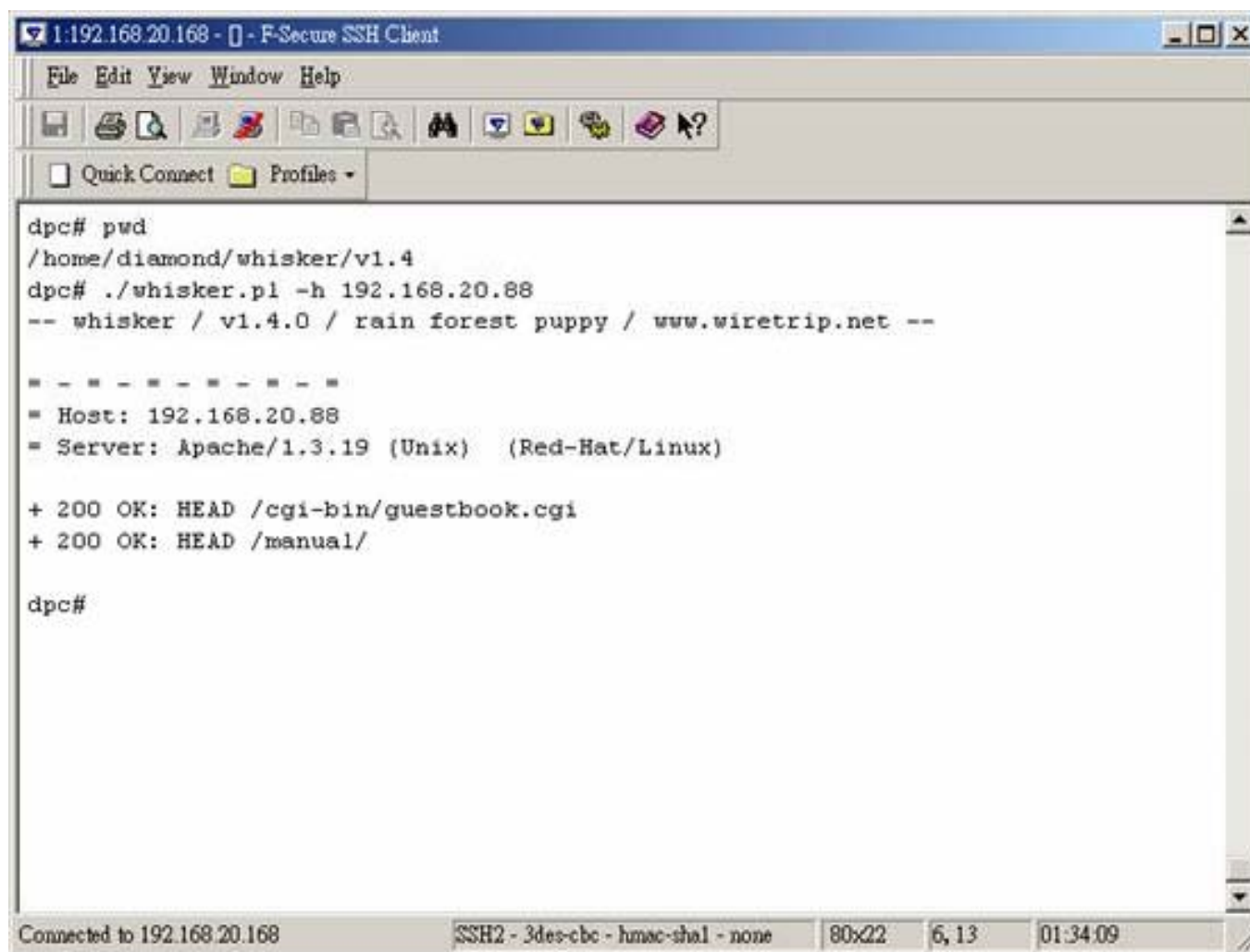
It refers to the output of this simple scan below and you will see that Whisker has identified several potentially dangerous files on this IIS5Server

```
c:\>whisker.pl -h victim.com -s scan.db

=====
= Host: victim.com
= Server: Microsoft-IIS/5.0
+ 200 OK: GET /whisker.ida
+ 200 OK: GET /whisker.idg
+ 200 OK: HEAD /_vti_inf.html
+ 200 OK: HEAD /_vti_bin/shtml.dll
+ 200 OK: HEAD /_vti_bin/shtml.exe
```



Whisker: Screenshot



The screenshot shows a terminal window titled "1:192.168.20.168 - F-Secure SSH Client". The terminal displays the following commands and output:

```
dpc# pwd
/home/diamond/whisker/v1.4
dpc# ./whisker.pl -h 192.168.20.88
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net --

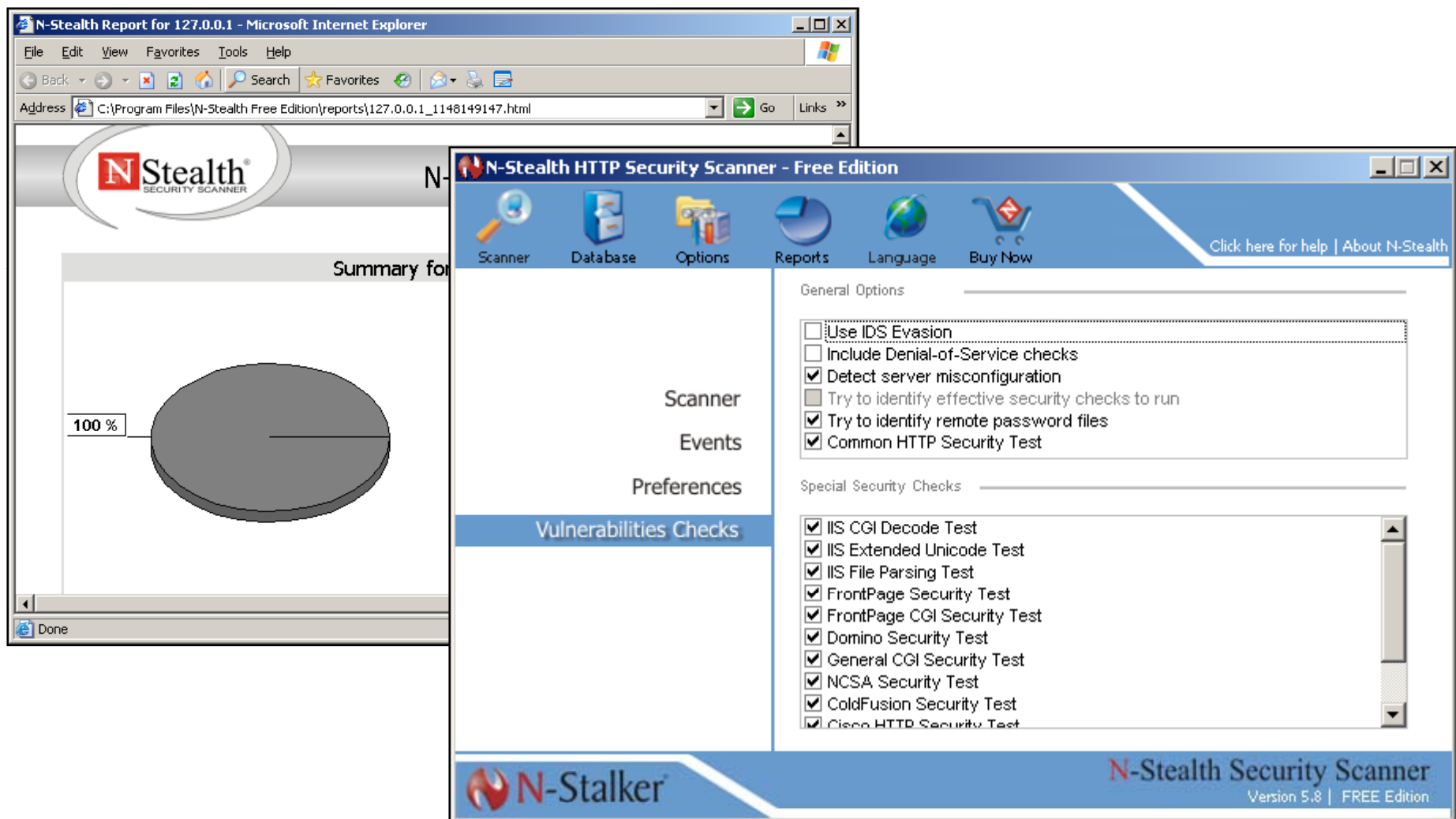
= - - - - -
= Host: 192.168.20.88
= Server: Apache/1.3.19 (Unix) (Red-Hat/Linux)

+ 200 OK: HEAD /cgi-bin/guestbook.cgi
+ 200 OK: HEAD /manual/

dpc#
```

The status bar at the bottom of the window indicates: "Connected to 192.168.20.168", "SSH2 - 3des-cbc - hmac-sha1 - none", "80x22", "6, 13", and "01:34:09".

Network Tool: N-Stealth HTTP Vulnerability Scanner

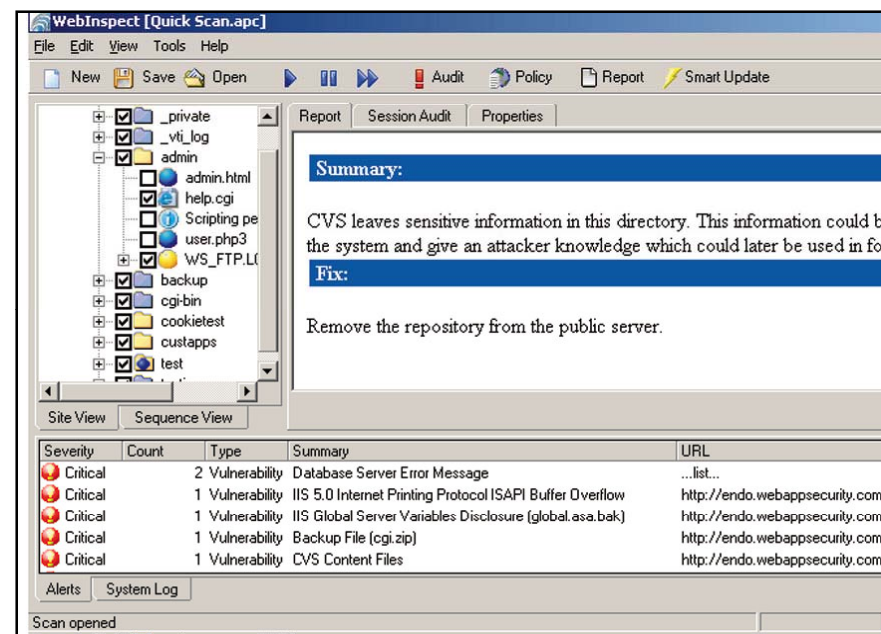


Hacking Tool: WebInspect

WebInspect is an impressive web server and application-level vulnerability scanner that scans over 1,500 known attacks

It checks site contents and analyzes for rudimentary application-issues like smart guesswork checks, password guessing, parameter passing, and hidden parameter checks

It can analyze a basic web server in 4 minutes, cataloging over 1,500 HTML pages



Network Tool: Shadow Security Scanner

Security scanner is designed to identify known and unknown vulnerabilities, suggest fixes to identified vulnerabilities, and report possible security holes within a network's Internet, intranet, and extranet environments

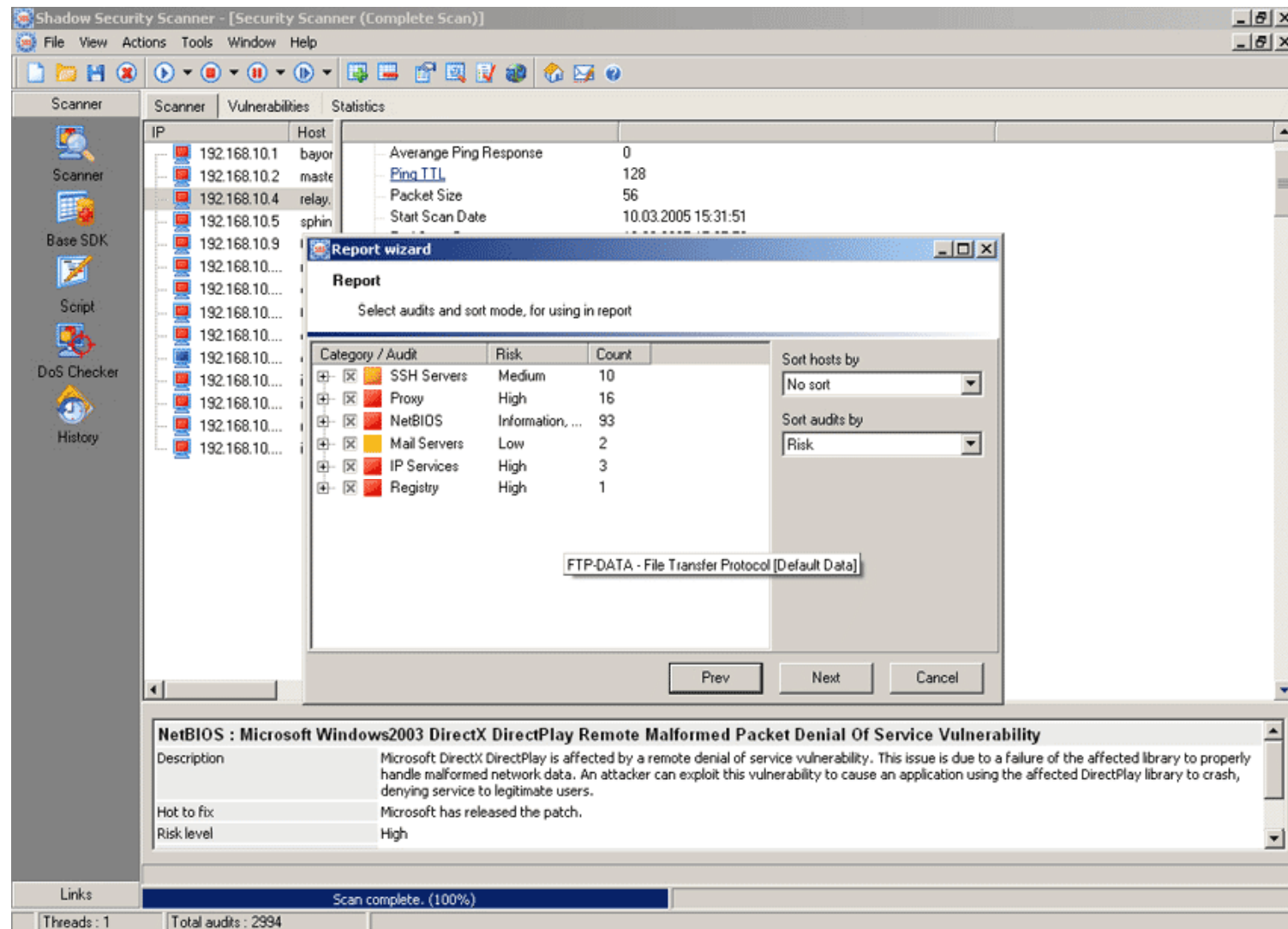


Shadow Security Scanner includes vulnerability auditing modules for many systems and services



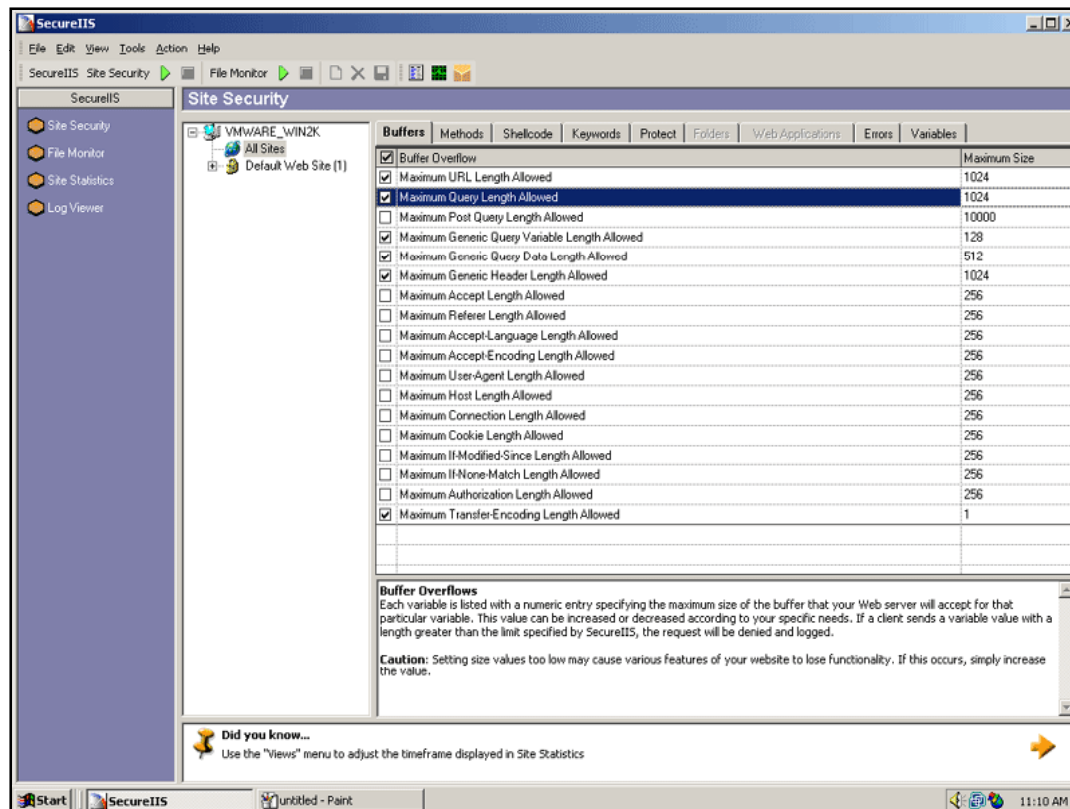
These include NetBIOS, HTTP, CGI and WinCGI, FTP, DNS, DoS vulnerabilities, POP3, SMTP, LDAP, TCP/IP, UDP, Registry, Services, users and accounts, password vulnerabilities, publishing extensions, MSSQL, IBM DB2, Oracle, MySQL, PostgreSQL, Interbase, MiniSQL, and more

Shadow Security Scanner: Screenshot



Tool: SecureIIS

Developed by eEye Digital Security specifically for Windows-based web servers, SecureIIS operates within Microsoft's IIS to protect your servers against known and unknown attacks



Tool: ServersCheck Monitoring

ServersCheck Monitoring is a web based network monitoring software and server monitoring tool



It monitors your network for bandwidth, outages, and performance issues

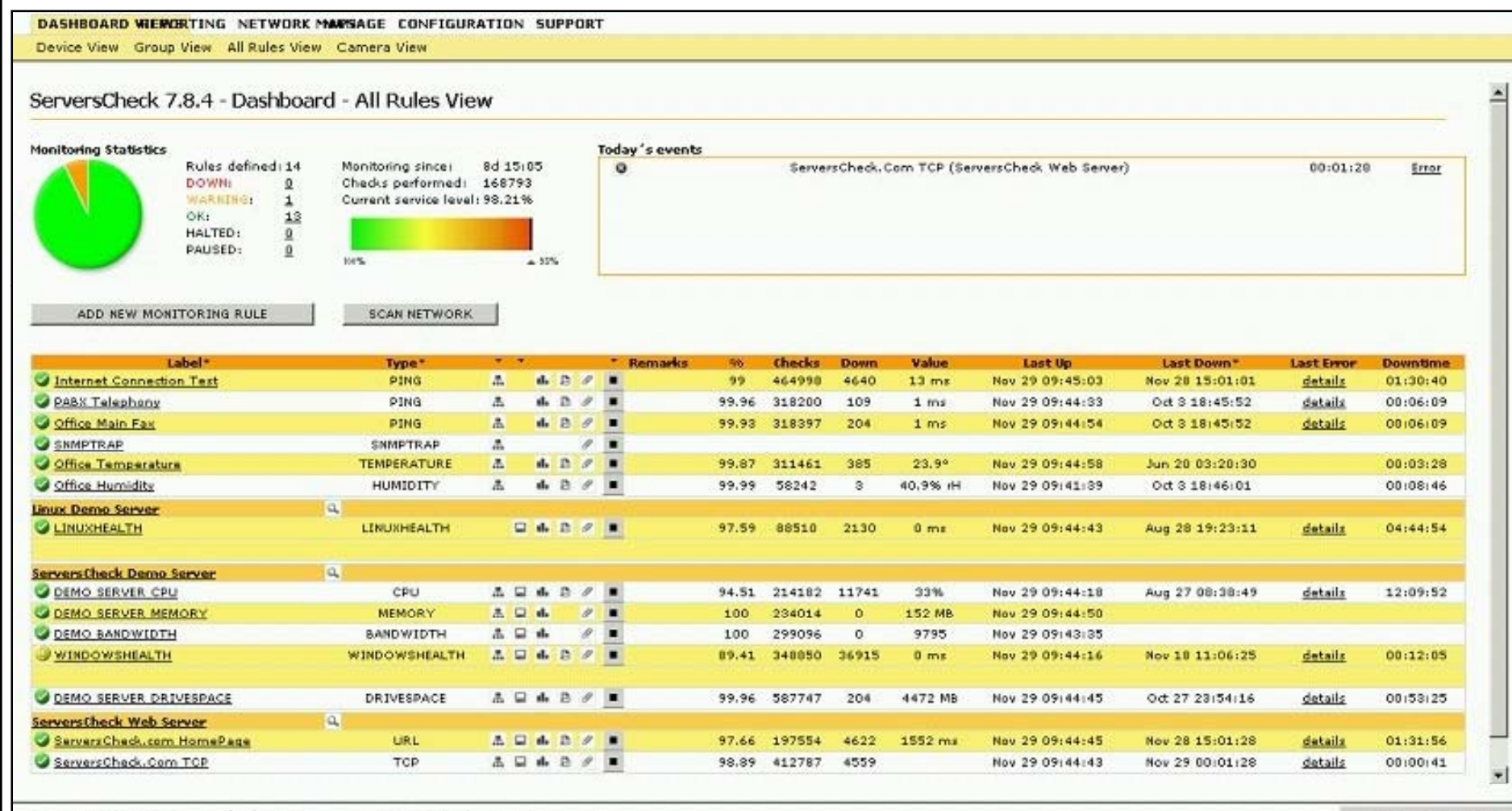


When problems are detected, then it alerts you via cell phone text messages (SMS), e-mail, or MSN

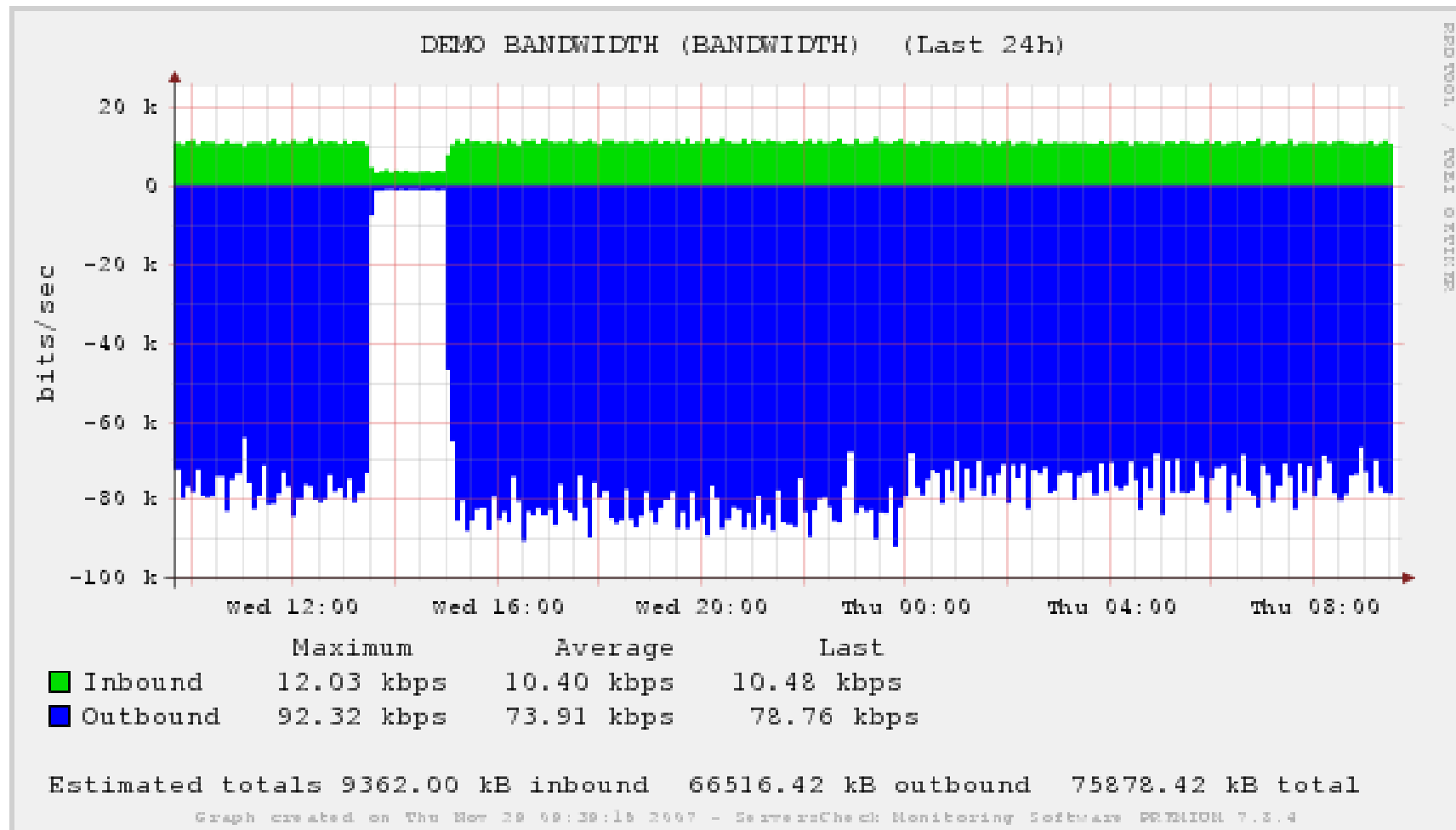


It can even take corrective actions by restarting a server or service

ServersCheck Monitoring: Screenshot 1



ServersCheck Monitoring: Screenshot 2



Tool: GFI Network Server Monitor

GFI Network Server Monitor is a network monitoring software

It monitors all aspects of your Windows and Linux servers, workstations, and devices

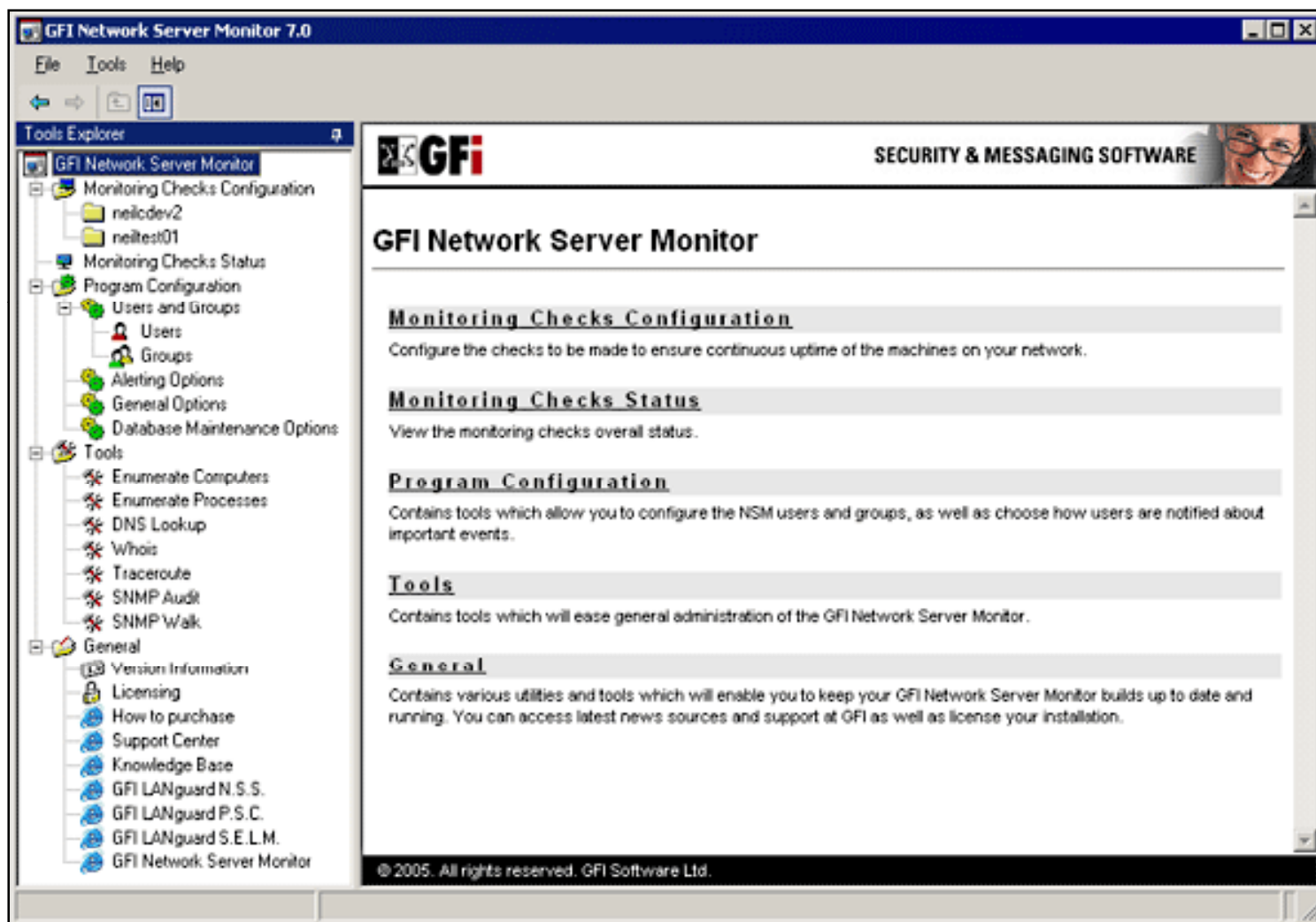
When a failure is detected, GFI's network monitor can alert you by email, pager, or SMS

It also takes corrective action by rebooting the machine, restarting the service, or running a script

Features:

- Includes checks for Exchange 2000/2003, ISA server, IIS
- Monitors terminal servers by actually logging in
- Monitors your database servers
- Monitors Linux servers

GFI Network Server Monitor: Screenshot 1



GFI Network Server Monitor: Screenshot 2

GFI Network Server Monitor - Detailed Report - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address Go Links

GFI SECURITY & MESSAGING SOFTWARE

Availability Report - Detailed

From 11/02/2005 to 14/02/2005

TMJASON - Event Log Service

Status	From	To	Duration	Reason	
	Succeeded	11/02/2005 - 00:00:00	14/02/2005 - 09:37:55	81 hrs 38 min	EventLog service is running

TMJASON - ICMP - Ping

Status	From	To	Duration	Reason	
	Succeeded	11/02/2005 - 00:00:00	14/02/2005 - 09:37:55	81 hrs 38 min	[Reply from TMJASON: < 10 msec]

TMJASON - Norton AntiVirus 2005

Status	From	To	Duration	Reason	
	Failed	11/02/2005 - 00:00:00	14/02/2005 - 09:37:55	81 hrs 38 min	'Norton AntiVirus Auto-Protect Service' service is not running

© 2005. All rights reserved. GFI Software Ltd

Home Products Support Ordering About Us

My Computer

GFI Network Server Monitor: Screenshot 3

New Check

HTTP/HTTPs
Check the availability of HTTP and HTTPs sites.



URL: http(s)://

☐ Use server verification (https) for this site

☐ Check for availability only

☒ Check that the page

☒ contains the following text

☐ does not contain the following text

☐ Use http web site authentication
NOTE: The credentials to be used are specified in the "Logon credentials" tab.

☐ Use proxy server

 Use a URL string like 'domainname.com:1010' to connect to a port other than the default port (port 8080).
Click [here](#) to load a sample.

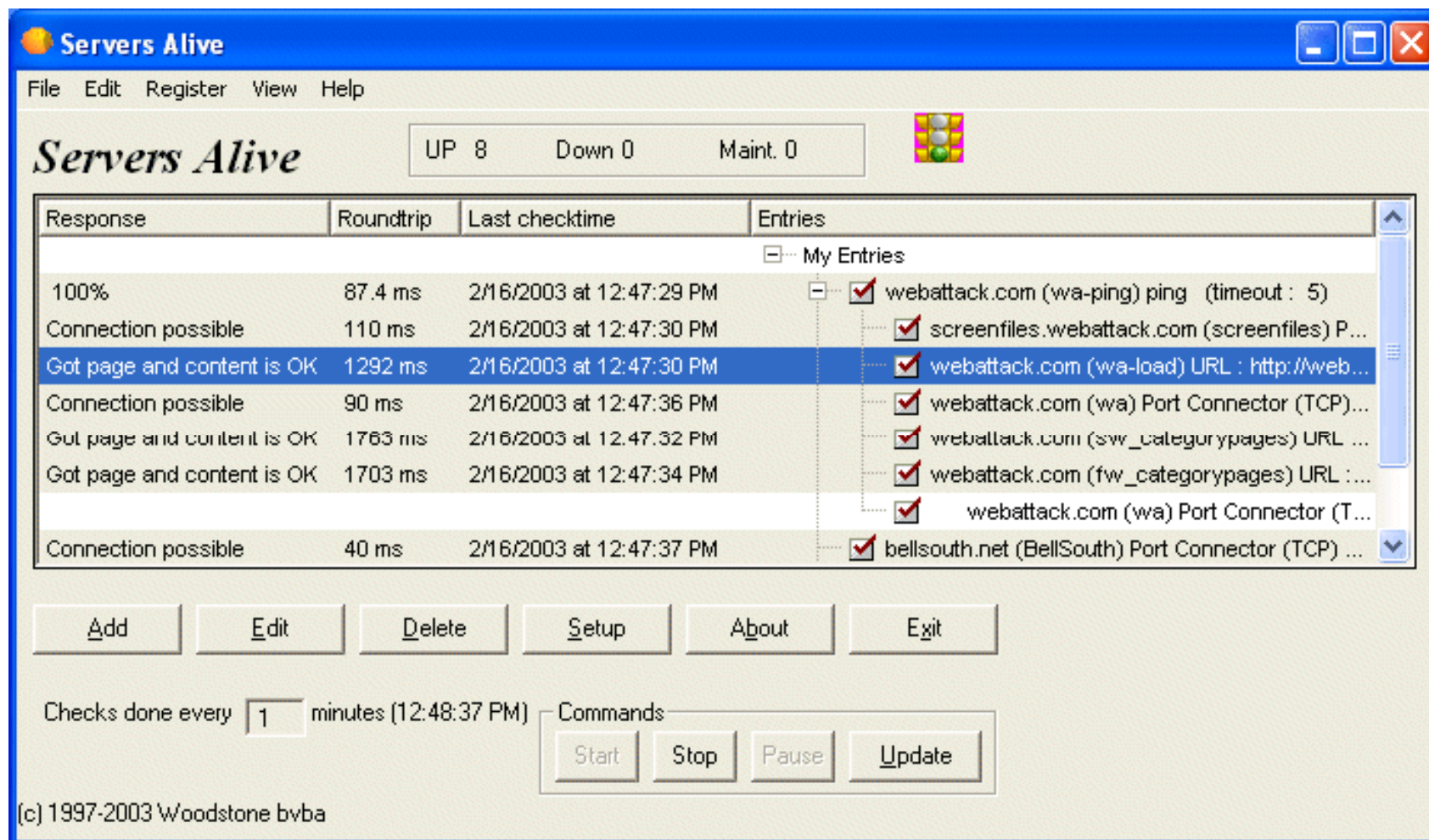
Tool: Servers Alive

Servers Alive is the server monitoring tool

It can monitor any WinSock service (TCP:FTP, HTTP, POP3, SMTP, IMAP4, DNS, and UDP: Radius and Quake II etc.)

The program offers a variety of notification options including SMS, email, pager, and even ICQ or MSN Messenger notifications

Servers Alive: Screenshot



Webserver Stress Tool

Webserver Stress Tool is a HTTP-client/server test application designed to pinpoint critical performance issues in your web site or web server

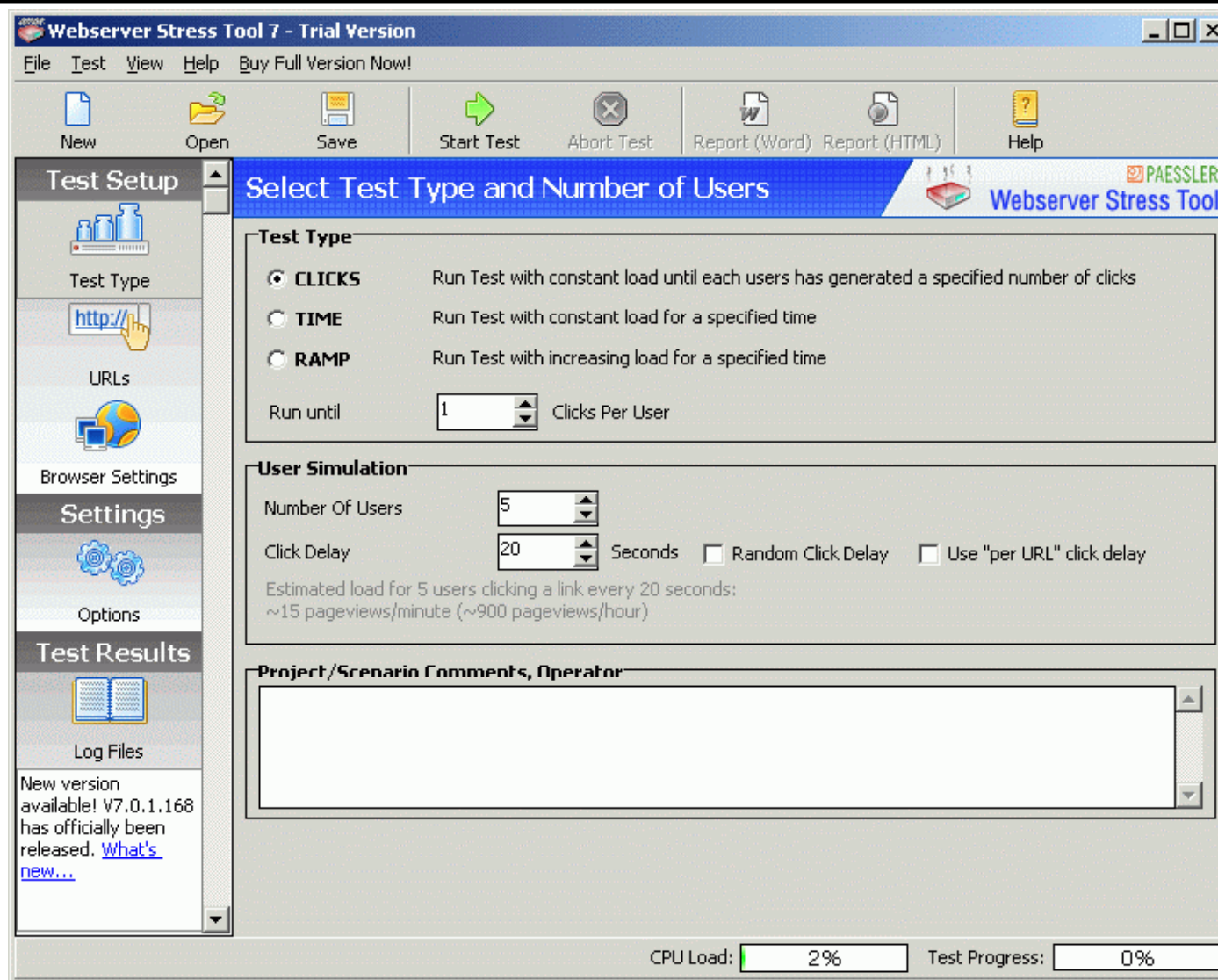
It simulates any number of users accessing your website at the same time

It can simulate upto 10.000 users who independently click their way through a set of URLs

Features:

- Resolve performance critical issues in your webserver
- Maximize performance
- Perform load tests and stress tests
- Can test any script—CGI, ASP, and PHP

Webserver Stress Tool: Screenshot



Monitoring Tool: Secunia PSI

Secunia PSI is an invaluable tool to use while assessing the security patch state of software installed on your system

It constantly monitors your system for insecure software installations and notifies you when an insecure application is installed

It provides you with detailed instructions for updating the application when available

It relies on the meta-data of executables and library files

It works by examining files on your computer (primarily .exe, .dll, and .ocx files)

This data is same for all users and originates from the installed programs on your computer and never from their configuration

Secunia PSI: Screenshot



IISLockdown:

- IISLockdown restricts anonymous access to system utilities as well as the ability to write to web content directories
- It disables Web Distributed Authoring and Versioning (WebDAV)
- It installs the URLScan ISAPI filter

URLScan:

- UrlScan is a security tool that screens all incoming requests to the server by filtering the requests based on rules that are set by the administrator

MBSA Utility:

- Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool that determines the security state in accordance with Microsoft security recommendations and offers specific remediation guidance

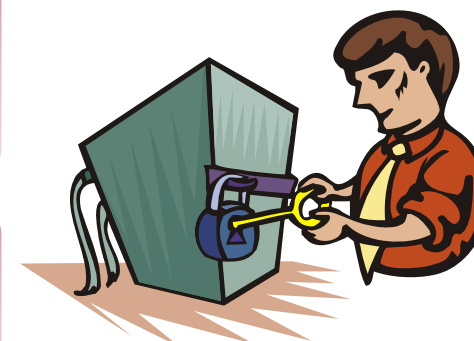
File System Traversal Countermeasures

Microsoft recommends setting the NTFS ACLS on cmd.exe and several other powerful executables to Administration and SYSTEM: Full Control only

Remove the sample files

Monitor the audit logs

Apply Microsoft patches and hotfixes regularly



Increasing Web Server Security

Use of Firewalls

Administrator Account Renaming

Disabling the Default Websites

Removal of Unused Application Mappings

Disabling Directory Browsing

Legal Notices

Service Packs, Hotfixes, and Templates

Checking for Malicious Input in Forms and Query Strings

Disabling Remote Administration



Web Server Protection Checklist

Patches and Updates

- Run MBSA utility on a regular interval to check for the latest operating system and components updates

Auditing and Logging

- Enable failed logon attempts in the log
- Relocate and secure IIS log files

IISLockdown

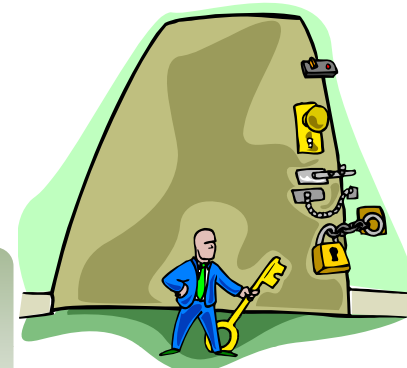
- Run IISLockdown and URLScan to lock down the servers
- Sites and Virtual Directories

Services

- Disable unnecessary Windows services
- Run essential services with the least privileges

Script Mappings

- Extensions not used by the application are mapped to 404.dll (.idq,.htw, .ida, .shtml, .shtm, .stm, idc, .htr, .printer)



Web Server Protection Checklist (cont'd)

Protocols

- Disable WebDAV
- Disable NetBIOS and SMB (Block ports 137, 138, 139, and 445)



ISAPI Filters

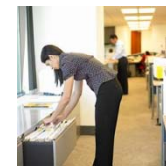
- Remove unused ISAPI Filters

Accounts

- Remove unused accounts
- Disable guest
- Rename administrator account
- Disable null user connections
- Enable administrator to log on locally

Files and Directories

- Files and directories are contained on NTFS volumes
- Web site content is located on a non-system NTFS volume
- Web site root directory has deny write for IUSR COMPUTERNAME



Web Server Protection Checklist (cont'd)

IIS Metabase

- Access to the metabase is restricted by using NTFS permissions

Server Certificates

- The certificate's public key is valid, all the way to a trusted root authority

Shares

- Administrative shares (C\$ and Admin\$) are removed

Machine.config

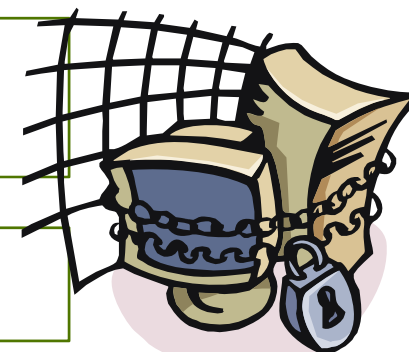
- Unused HttpModules are removed
- Tracing is disabled `<trace enable="false"/>`

Ports

- Web applications are restricted to use only port 80 and 443

Code Access Security

- Code access security is enabled on the server



What Happened Next

Jason Springfield, an Ethical Hacker was called in to investigate the matter. During his tests, Jason found that the website had all default configurations, and no precautionary steps were taken while building the website.

The test exposed lot of security loopholes in the website.

The defacement was possible as the website was built with all default configuration.

The web server was not updated and hot fixes were not installed.

There was a flaw in the Index.htm file of the website.

The attacker exploited this flaw, and defacing was a piece of cake for him!!

Jason fixed the holes and changed the default configurations. This incident made the management of SpeedCake4u realize the need for a professional web designer.

Summary

Web servers assume critical importance in the realm of Internet security

Vulnerabilities exist in different releases of popular web servers and respective vendors patch these often

The inherent security risks owing to the compromised web servers have impact on the local area networks that host these websites, even on the normal users of web browsers

Looking through the long list of vulnerabilities that had been discovered and patched over the past few years, it provides an attacker ample scope to plan attacks to unpatched servers

Different tools/exploit codes aid an attacker in perpetrating web server's hacking

Countermeasures include scanning for the existing vulnerabilities and patching them immediately, anonymous access restriction, incoming traffic request screening, and filtering

Copyright 2001 by Randy Glasbergen.
www.glasbergen.com



**“Customers aren’t impressed by our web site anymore.
We need to put the ‘gee’ back in ‘technologee’!”**

Copyright 2004 by Randy Glasbergen.
www.glasbergen.com



**“Install a patch for the update of the new version.
If that doesn’t work, install the new version of
the update for the patch. If all else fails, install
a patch for the new version of the update.”**

Copyright 2005 by Randy Glasbergen.
www.glasbergen.com



**“We back up our data on sticky notes because
sticky notes never crash.”**