

Ethical Hacking and Countermeasures

Version 6



Module XVI

Hacking Web Servers



Scenario

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 <u>hundreds of sites which had been hacked</u> 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 fixed 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's 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/

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



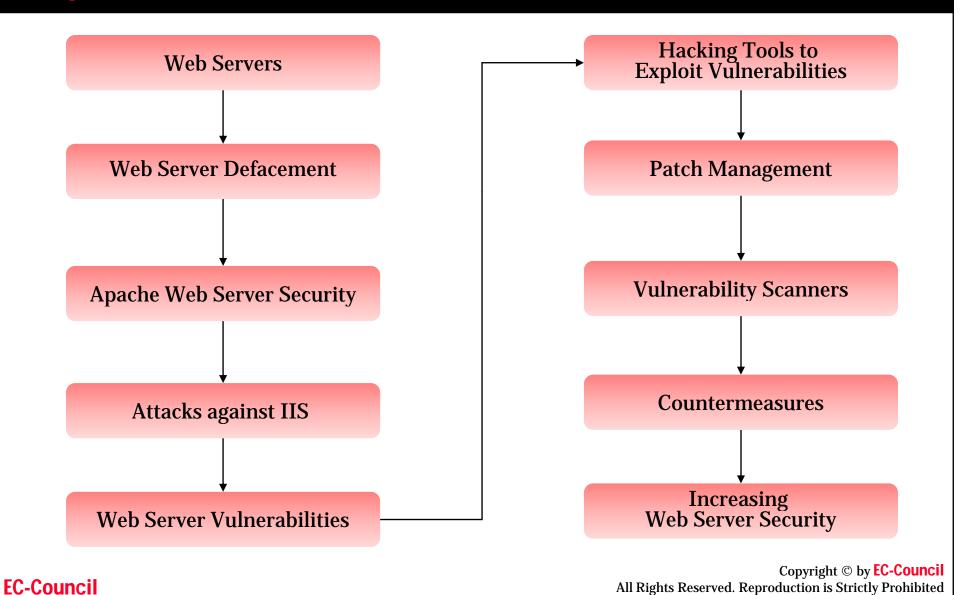
Module Objective

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









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







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





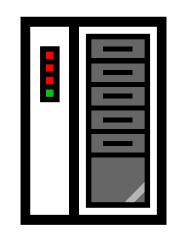
Attacks Against IIS

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

Copyright © by EC-Council

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





EH Unicode Directory Traversal Vulnerability



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

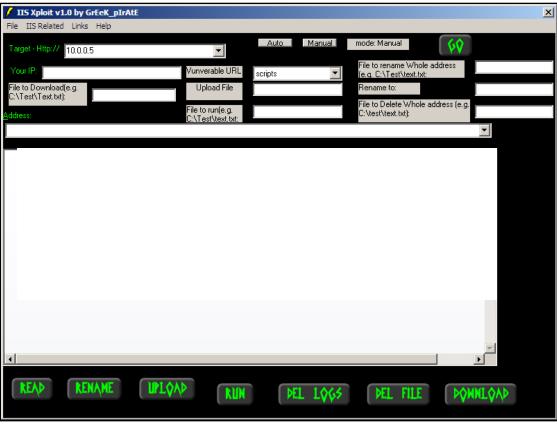


Hacking Tool: IISxploit.exe

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

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



RPC DCOM Vulnerability (cont'd)

RPC Exploit-GUI Hacking Tool





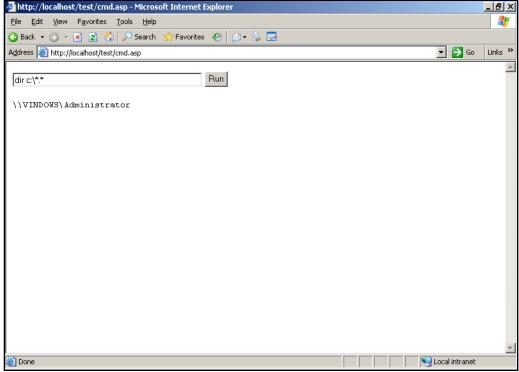
ASP Trojan (cmd.asp)

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

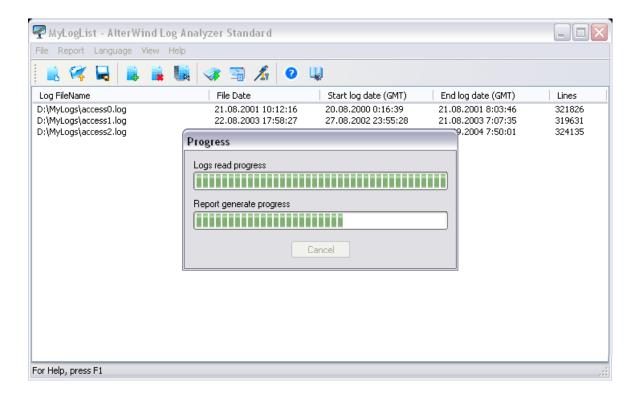
md.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1





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 pp=GET arg=http://Target IP/msadc/..%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%1c../..%c1%1c../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

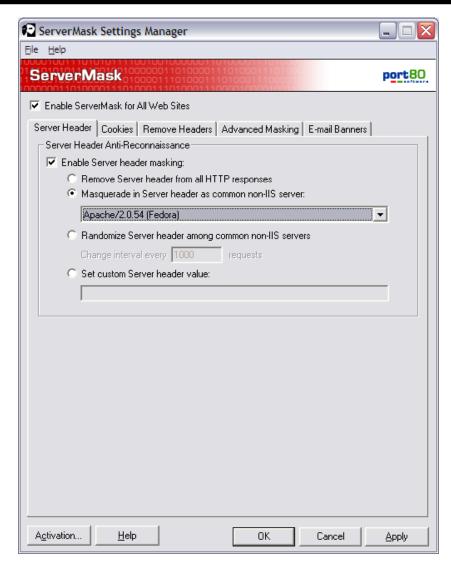


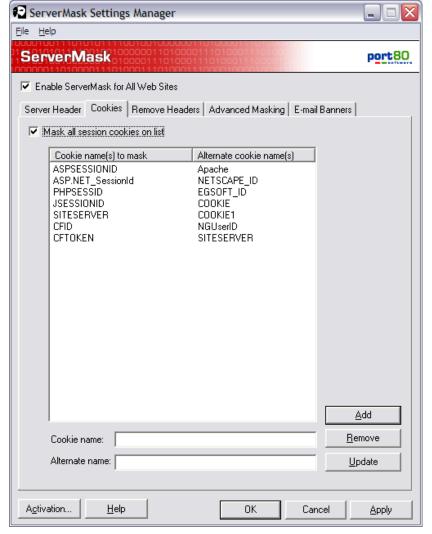
You can change the header to any string you want





Server Mask: Screenshot





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

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

HTTP request for images, PDFs, video files



- S I o w e r page loads for repeat visitors
- Decreased server throughput
- Higher bandwidth costs



Microsoft IIS Web server

Uncached response wastes repeat users' time and precious IIS resources...

With CacheRight

HTTP request for images, PDFs, video files



User browsing Your Web site

- Cached files fly out of users' browser cache on repeat visits
- Speed and more availability
- Bandwidth reduction

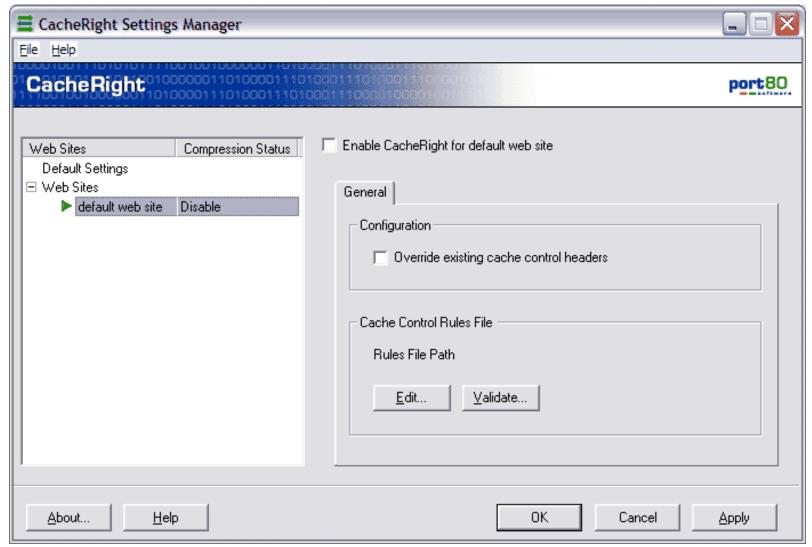


Microsoft IIS Web server

Cached response leverages the benefits of HTTP spec for speed and savings!



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

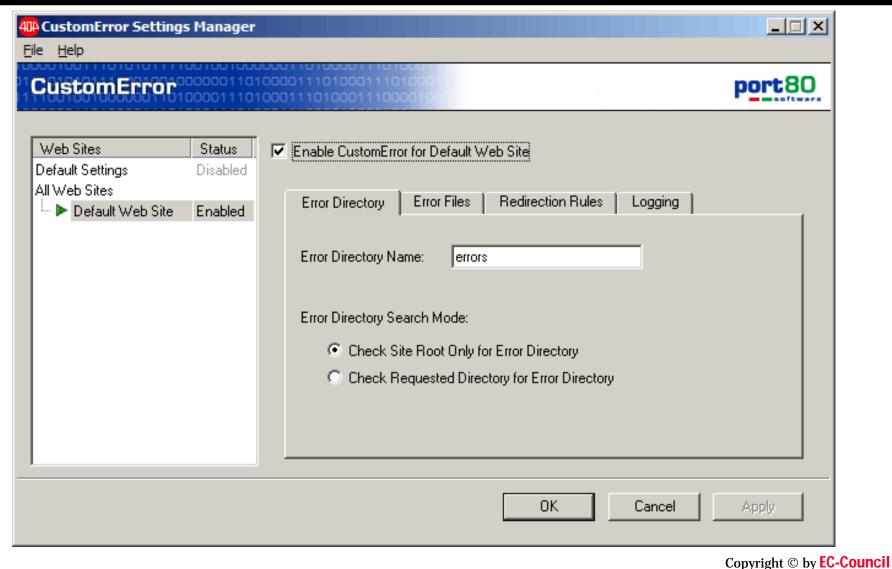
Benefits:

- 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



EC-Council

CustomError: Screenshot



All Rights Reserved. Reproduction is Strictly Prohibited

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

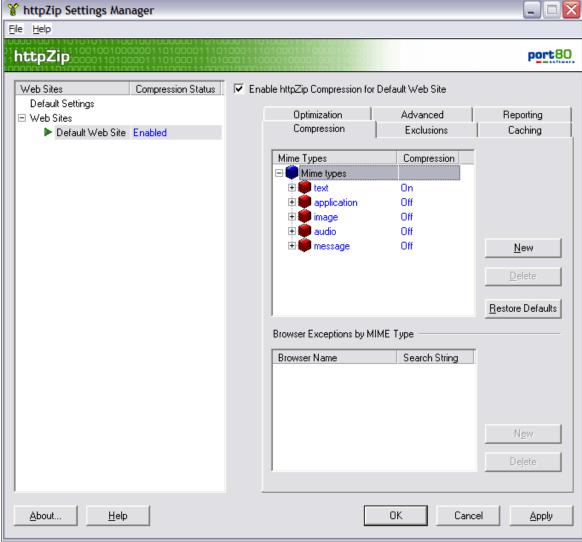
It takes compression even farther with optional HTML and CSS code optimization to improve performance and combat hackers' source sifting

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





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

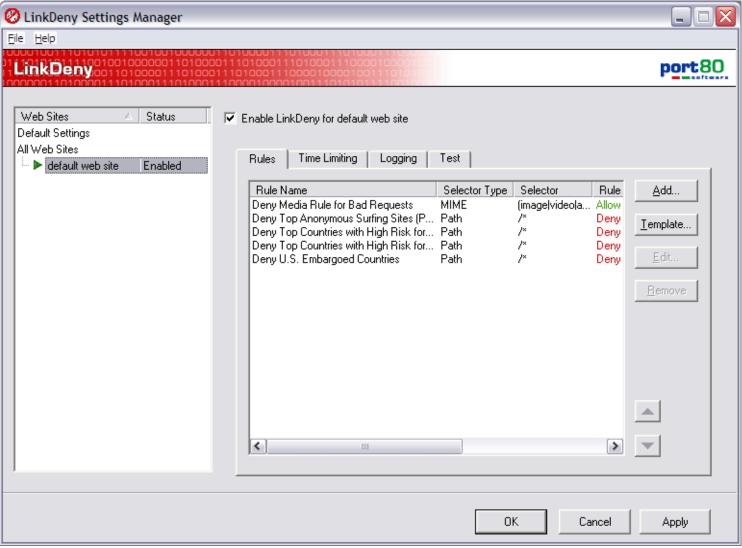
It controls access to sensitive, private, proprietary, paid, or copyrighted files and downloads

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

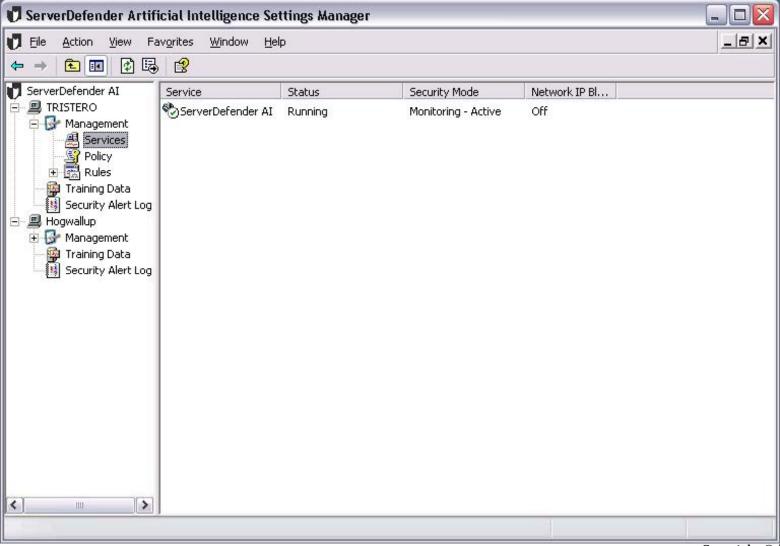
ServerDefender Artificial Intelligence (AI) is a web application firewall

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

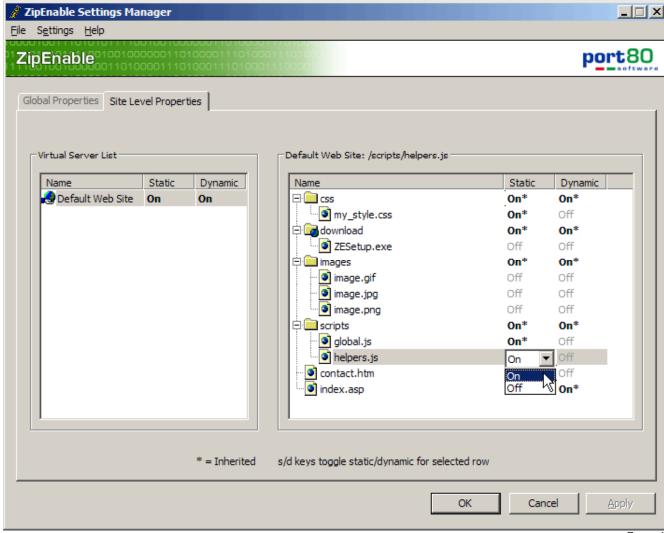
It is used to configure compression on all static and dynamic files

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



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



Tool: W3compiler

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

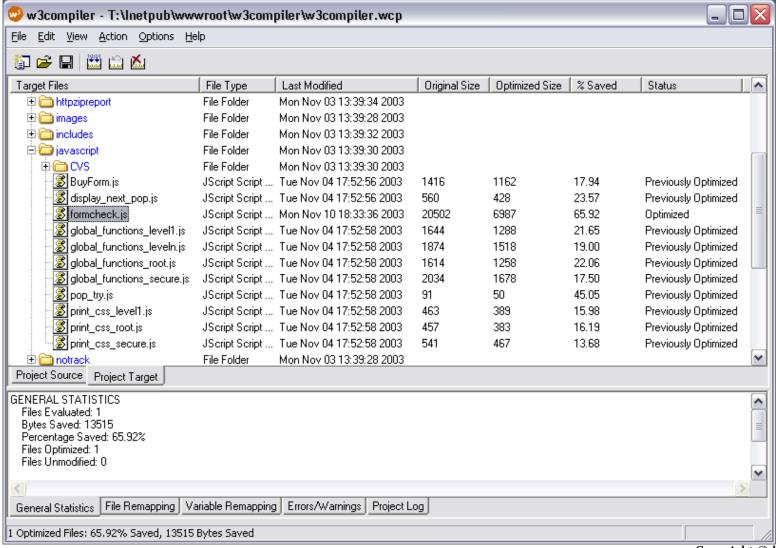
It removes redundant structures from your code before you load files on the server

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



EC-Council

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

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

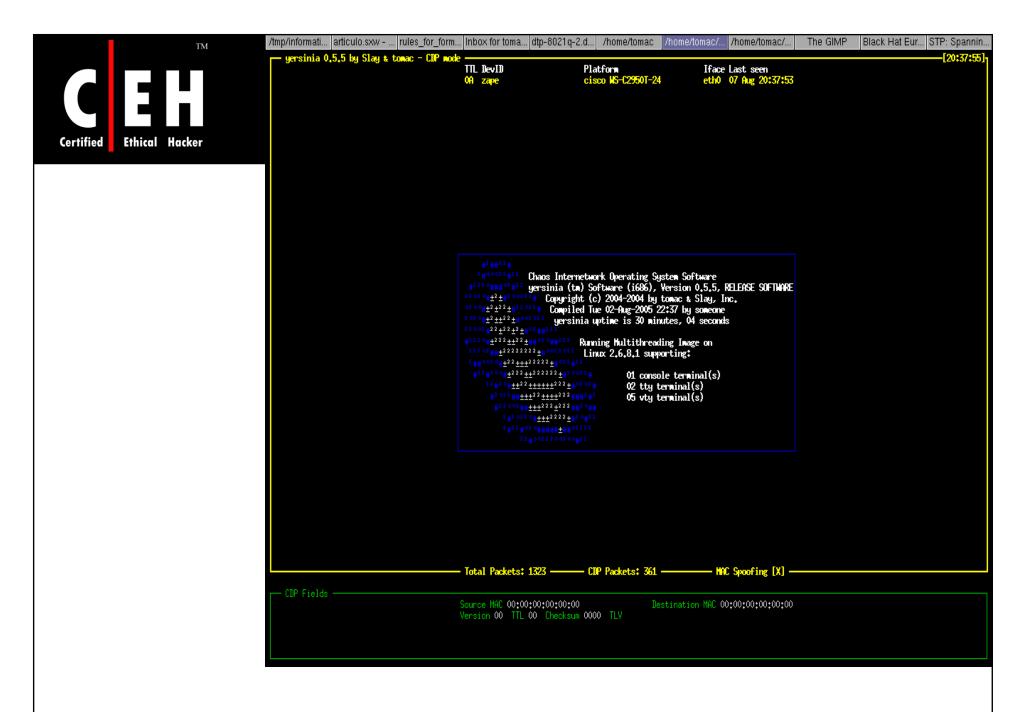
Attacks for the following network protocols are implemented:

- 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)

```
articulo-fredy.sxw - ..
                                                        Inbox for tomac@wa...
                                                                                        Correo S21sec
                                                                                                                   /home/tomac<1>
                                                                                                                                                    The GIMP
                                                                                                                                                                        /home/tomac/work/p... /home/tomac/work/p.
 prodigy:/home/tomac/work/projects/yersinia-sf/yersinia/yersinia/src# ./yersinia -h
    2 <u>(j°°°°2 2 (j</u>°2 2
  2202001121020022211
22.00[Http://doc.org
                                             The Black Death for nowadays networks
 22202(jjtt22222223)p022022
2(jj0020pj224+2222223pj00202)
22(jj00pj224+222222pj0002)
[j2022(jj0+224+422222pj000)]
[j2022(jj0+224+42222pj000)]
2(jj0020)[j0+4222+2220pj00j00
2(jj0020)[j0+42222222pj00pj00
2(jj0020)[j000j00j00j000]
2(jj0020)[j000j00j00j000]
2(jj0020)[j000j000j000]
                                              Prune your MSTP, RSTP, STP trees!!!!
                 22 100222 002 00122
 Usage: yersinia [-hVIDd] [-l logfile] [-c conffile] protocol [protocol_options]
                Program version.
                This help screen.
                Interactive mode (ncurses).
          -D
               Daemon mode.
          -d Debug.
          -1 logfile Select logfile.
         -c conffile Select config file.
   protocol Can be one of the following: cdp, dhcp, 802.1q, dtp, hsrp, stp, vtp, isl.
 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#
```



```
Correo S21sec
                        Inbox for tomac@wasa..
                                                                                                                                       The GIMP
                                                                                /home/tomac<1>
                                                                                                      /home/tomac/work/proj..
                                                                                                                                                         /home/tomac/work/proje.
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
             Cisco Discovery Protocol (CDP) information
             Dynamic Host Configuration Protocol (DHCP) information
  dhcp
             802.1Q information
  dot1q
  dtp
             Dynamic Trunking Protocol (DTP) information
             Display the session command history
  history
             Hot Standby Router Protocol (HSRP) information
  interfaces Interface status
  stats
             Show statistics
              Spanning Tree Protocol (STP) information
  stp
  users
             Display information about terminal lines
             System hardware and software status
  version
             Virtual Trunking Protocol (VTP) information
 √ersinia# sh ver
Chaos Internetwork Operating System Software
yersinia (tm) Software (1686), 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)
 √ersinia# sh users
   User
                 Terminal
                                 From
                                                   Since
   root
                                 127.0.0.1:60715 Sun Aug 7 23:51:01 2005
                     vty0
yersinia#
```





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

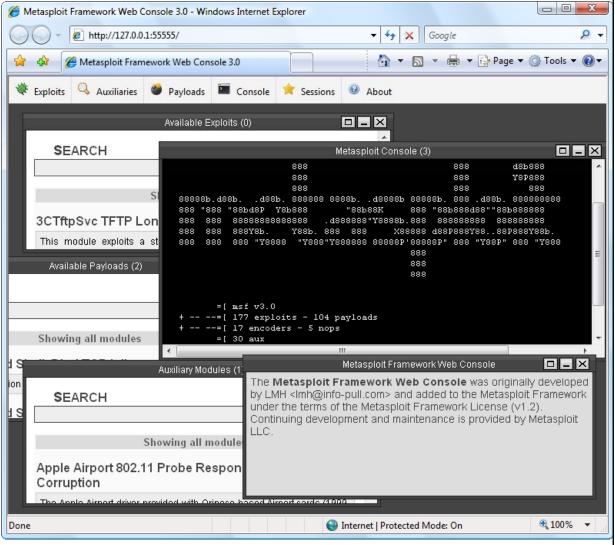
It runs on any UNIX-like system under its default configuration

A customized Cygwin environment for windows OS users

http://www.metasploit.com

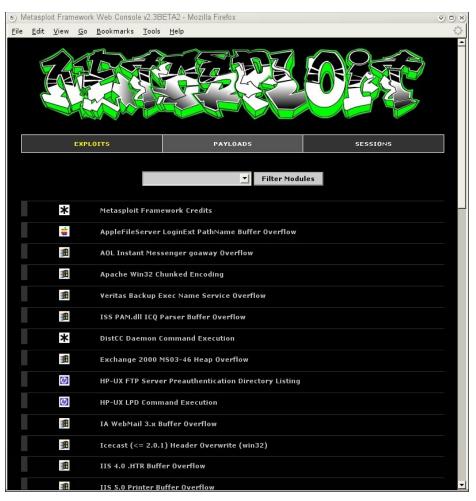


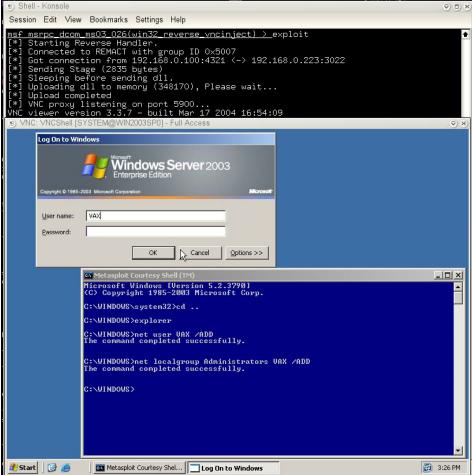
Metasploit Framework: Screenshot





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

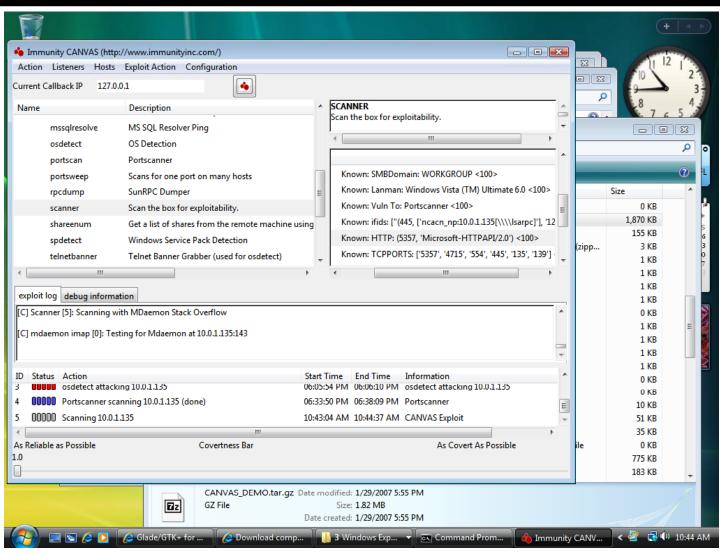
CANVAS Professional supports Windows, Linux MacOSX, and other Python environments

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

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

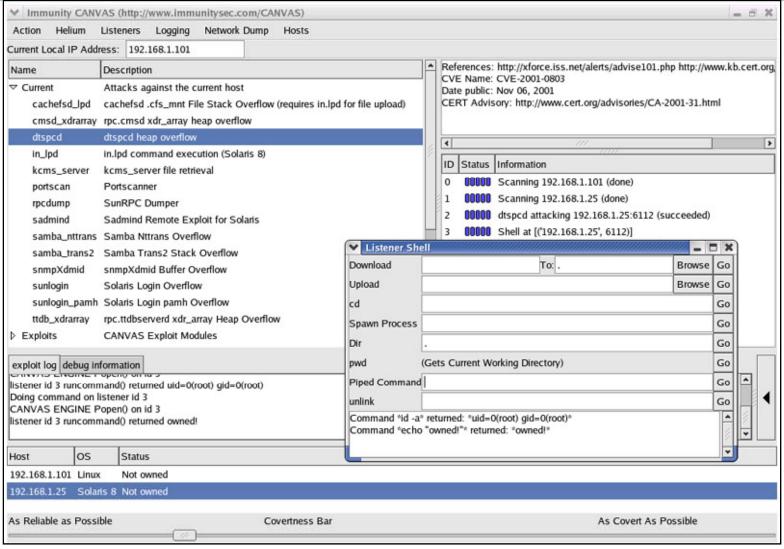


Immunity CANVAS Professional: Screenshot 1





Immunity CANVAS Professional: Screenshot 2





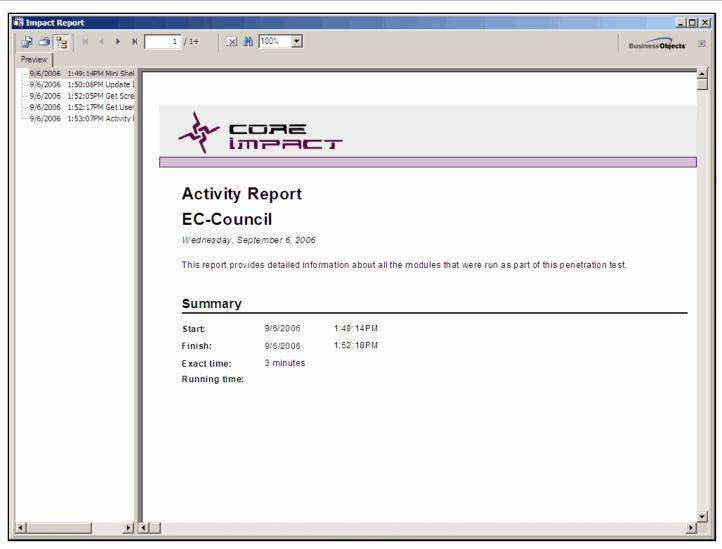
Tool: Core Impact

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

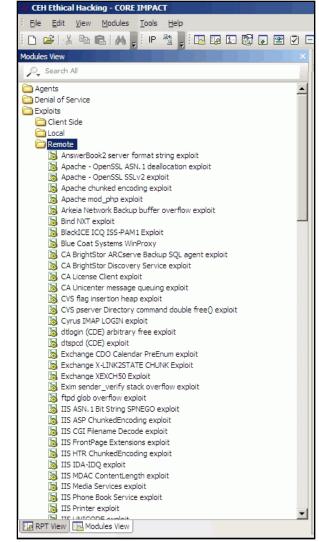
By safely exploiting vulnerabilities in your network infrastructure, the product identifies real, tangible risks to information assets while testing the effectiveness of your existing security investments

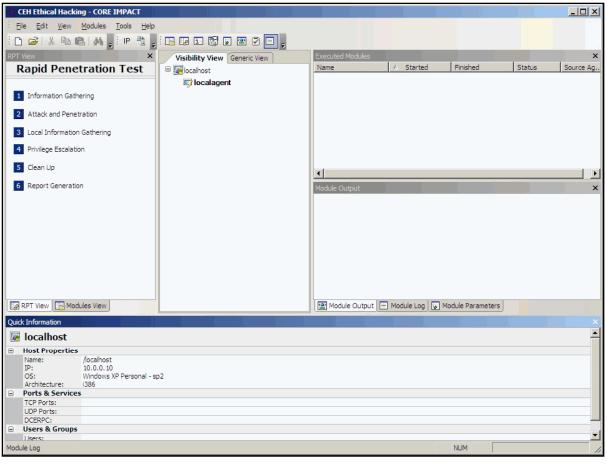




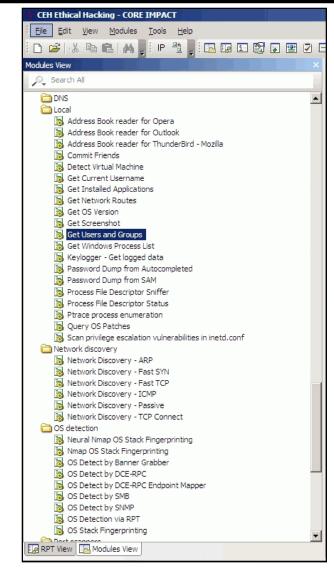


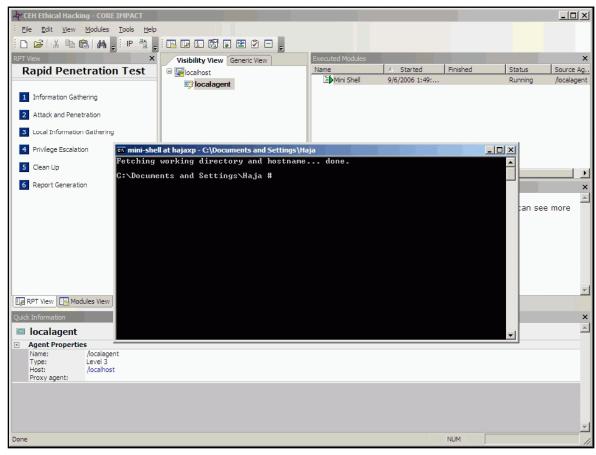
Certified Ethical Hacker



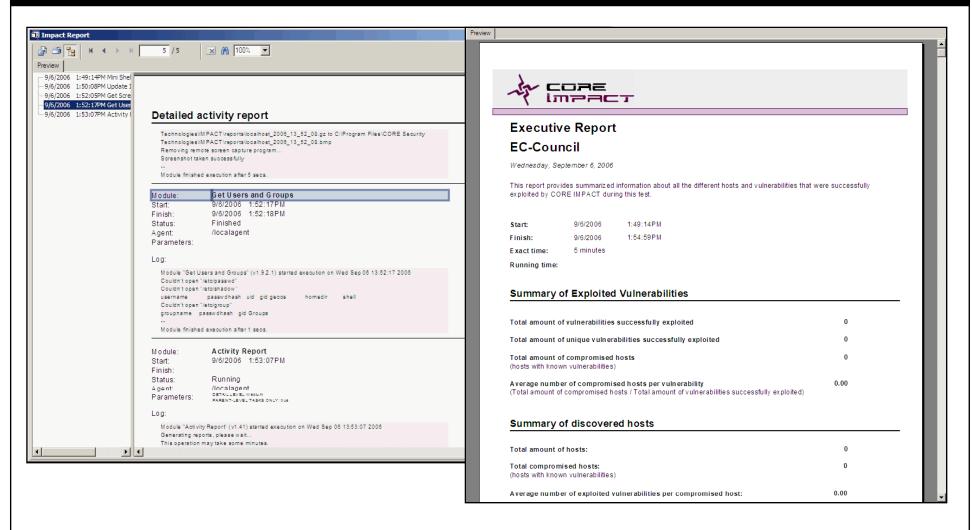


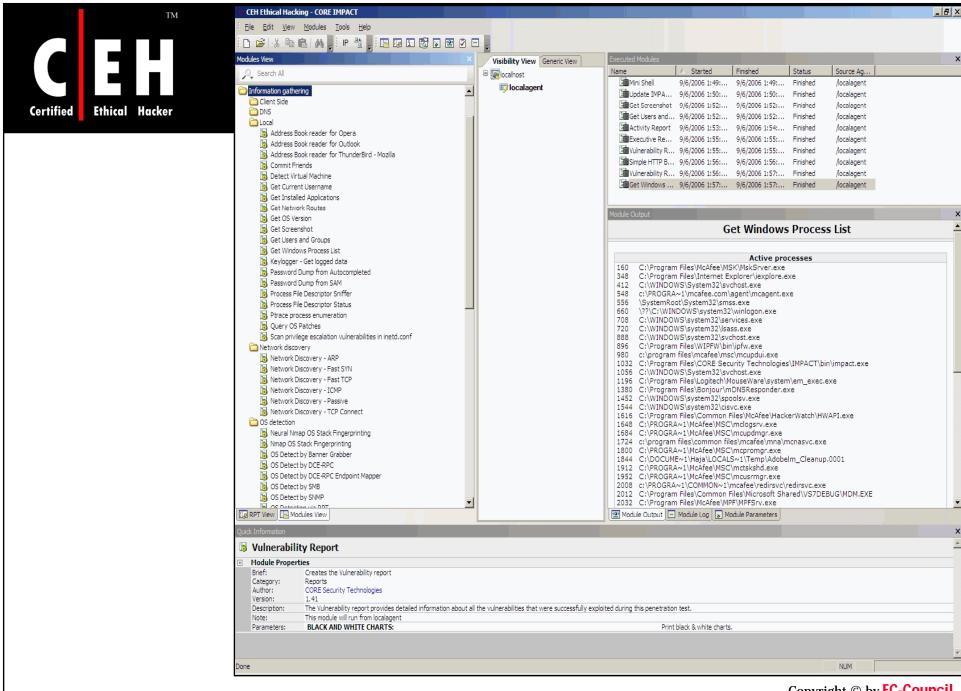
Certified Ethical Hacker











EC-Council

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

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 include exploits for:

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



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



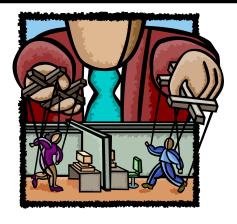


Neosploit: Screenshot



MEOSPLOIT 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:

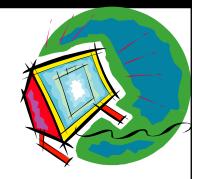
- Choosing, verifying, testing, and applying patches
- Updating previously applied patches with current patches
- Listing patches applied previously to the current software
- Recording repositories, or depots, of patches for easy selection
- Assigning and deploying the applied patches





Solution: UpdateExpert

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

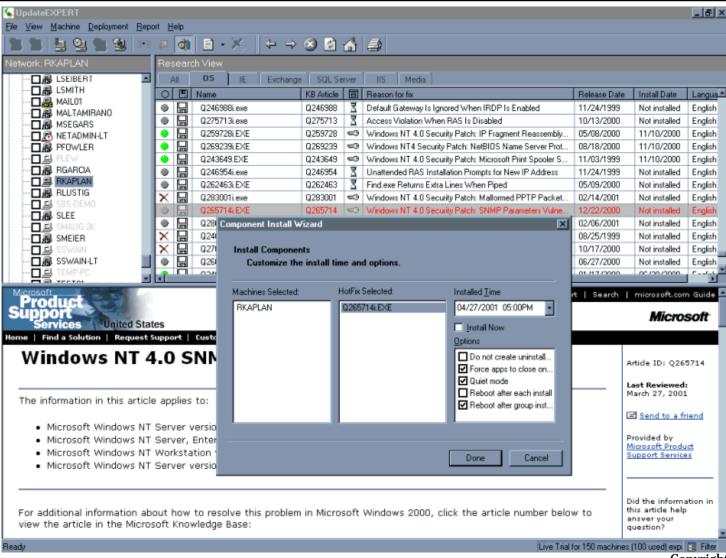


Microsoft constantly releases updates for the OS and mission critical applications, which fix security vulnerabilities and system stability problems

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



UpdateExpert: Screenshot



Copyright © by **EC-Council**

All Rights Reserved. Reproduction is Strictly Prohibited



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\Micr osoft\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.
           Current on system.
           Current on system.
KB823559:
           Current on system.
KB824105: Current on system.
 B825119: Current on system.
 B826232: Current on system.
(B828035: Current on system.
KB828741: Current on system.
           Current on system.
KB842526: Current on system.
KB842773: Current on system.
KB871250: Current on system.
           Current on system.
           Current on system.
           Current on system.
KB885835:
           Current on system.
           Current on system.
(B893803:
          Current on system.
          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

```
MICRON

Patch NOT Found MS00-077 Q299796
Patch NOT Found MS00-079 Q276471
Patch NOT Found MS01-007 Q285851
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
```



cacls.exe Utility

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

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

• C:\>cacls.exe c:\myfolder*.exe /T /G System:F
Administrators:F



```
C:\Snort>cacls.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. <u>www.securityseers.com</u>
- 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



vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.q. FISMA).

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)

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 undated: 02/25/08

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

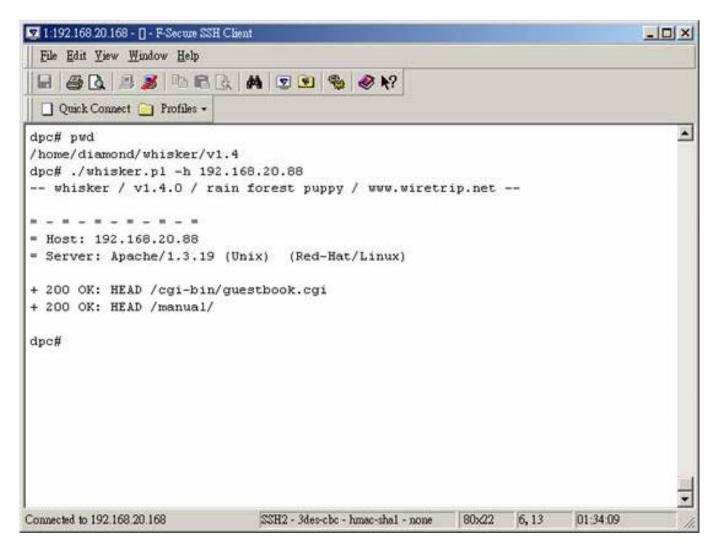
Whisker is an automated vulnerability scanning software that scans for the presence of exploitable files on remote web servers

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



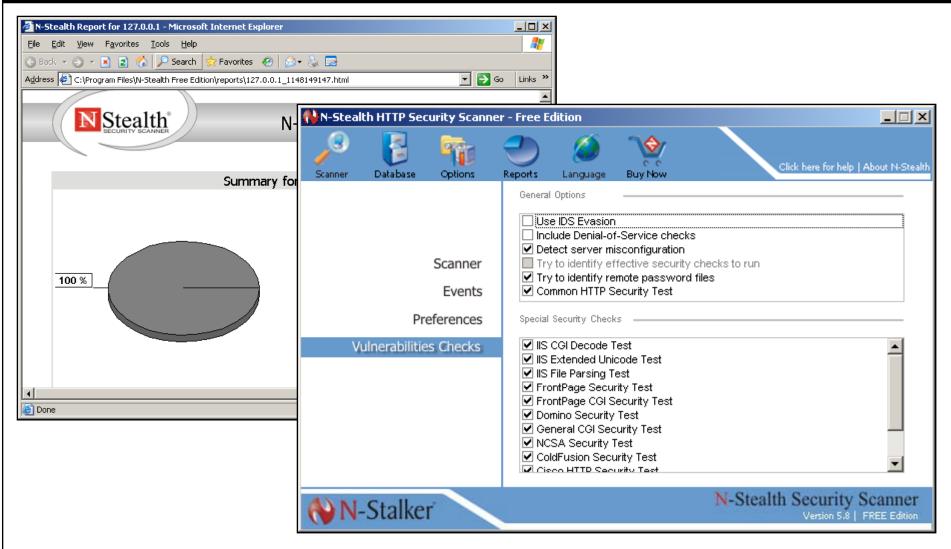


Whisker: Screenshot





Network Tool: N-Stealth HTTP Vulnerability Scanner

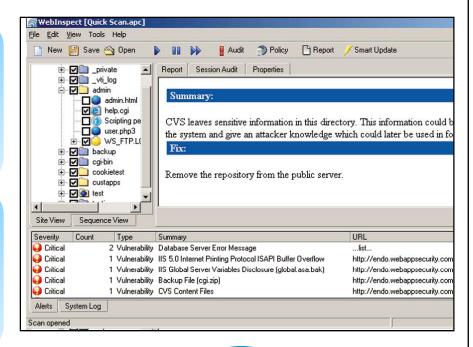


Hacking Tool: WebInspect

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



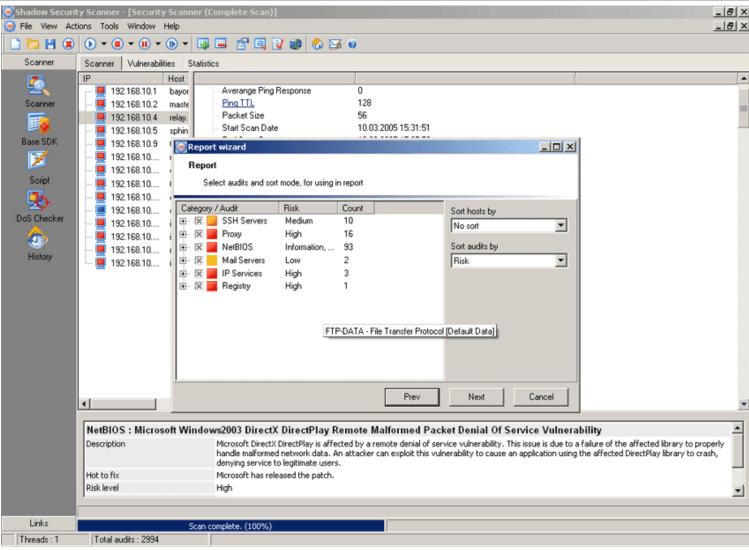
Shadow Security Scanner includes vulnerability auditing modules for many systems and services



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, PostgressSQL, Interbase, MiniSQL, and more

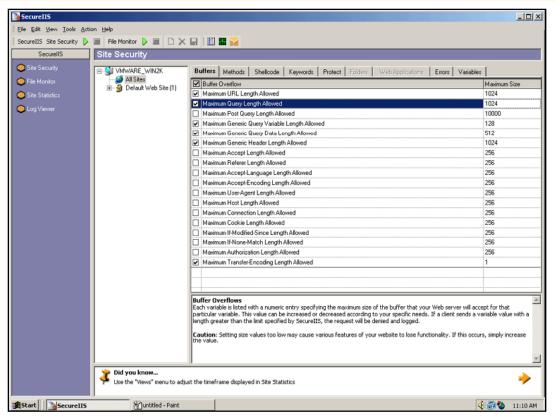


Shadow Security Scanner: Screenshot





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





Copyright © by EC-Council

All Rights Reserved. Reproduction is Strictly Prohibited



Tool: ServersCheck Monitoring

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

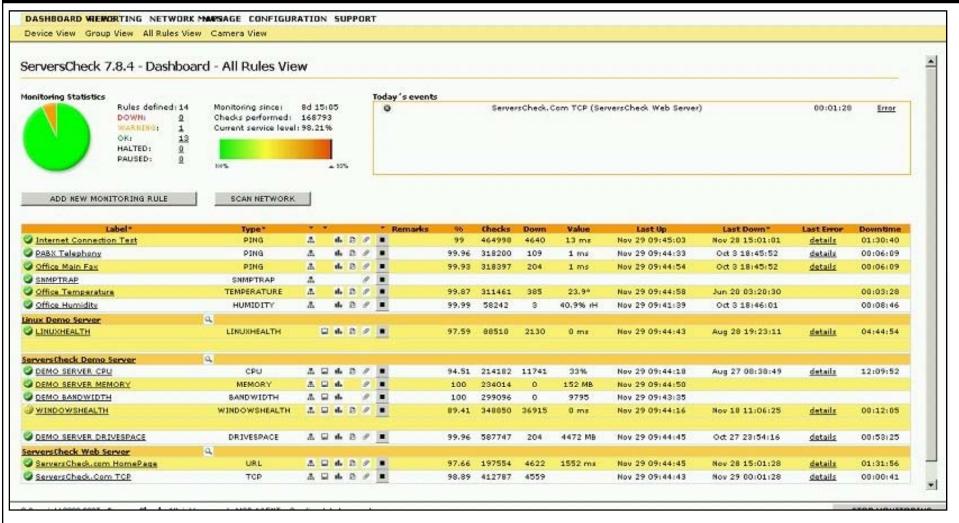
It monitors your network for bandwidth, outages, and performance issues

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

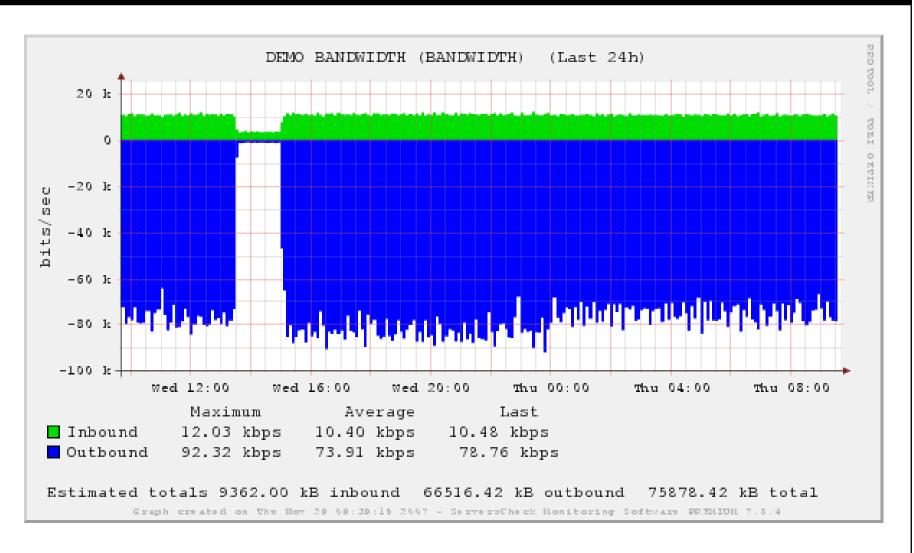


ServersCheck Monitoring: Screenshot 1





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

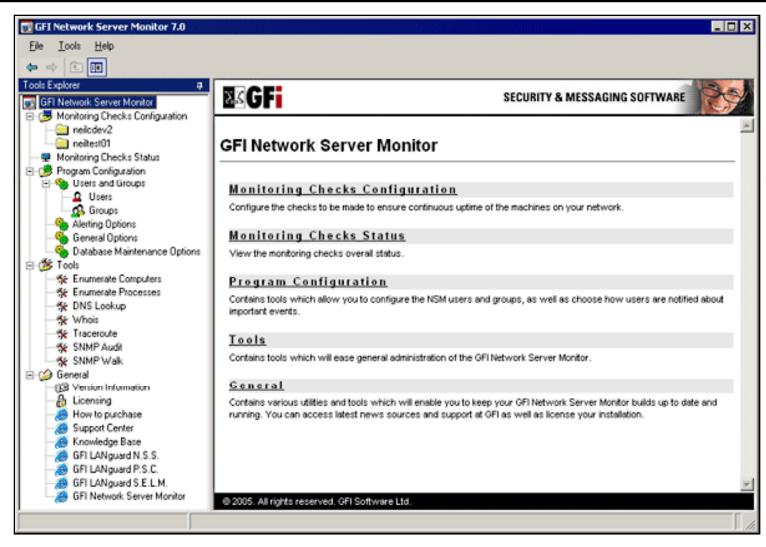
It also takes corrective action by rebooting the machine, restarting the service, or running a script

Features:

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

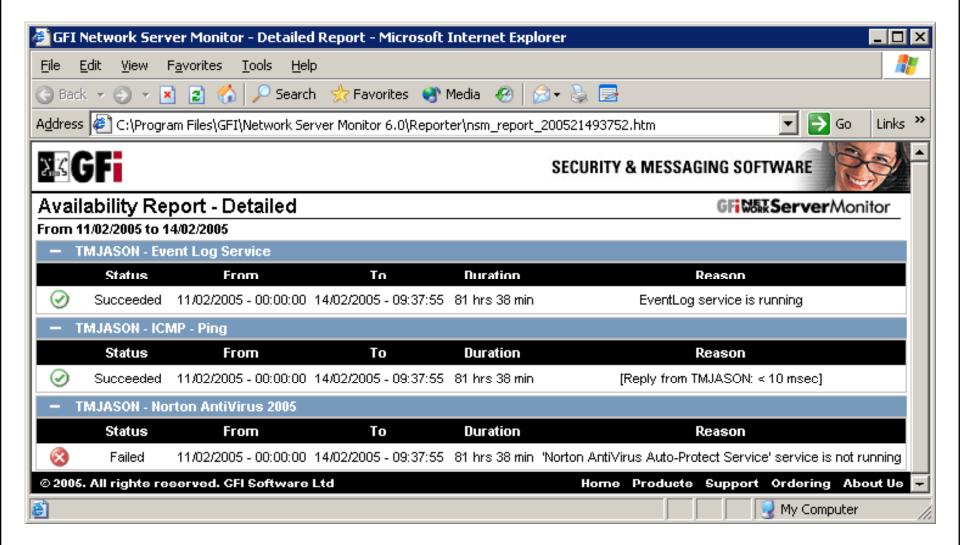


GFI Network Server Monitor: Screenshot 1





GFI Network Server Monitor: Screenshot 2





GFI Network Server Monitor: Screenshot 3



Copyright © by **EC-Council**

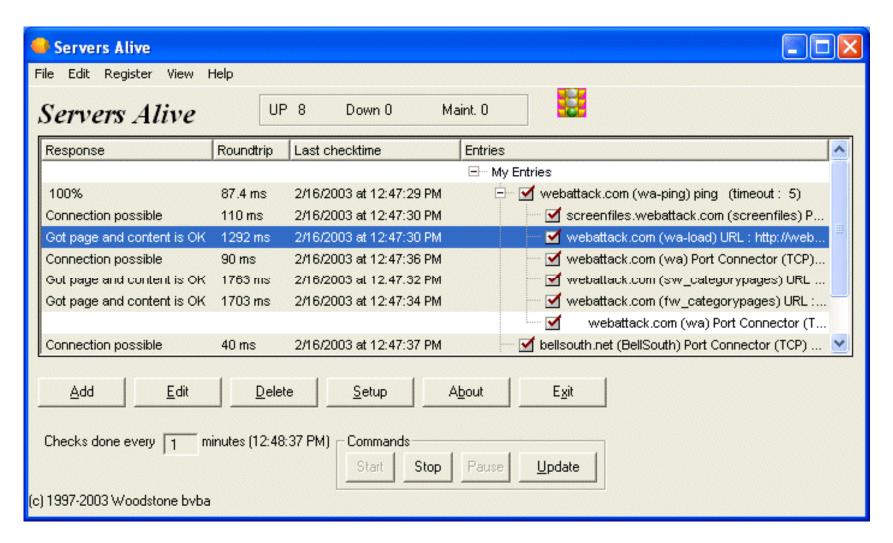
Servers Alive is the server monitoring tool

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

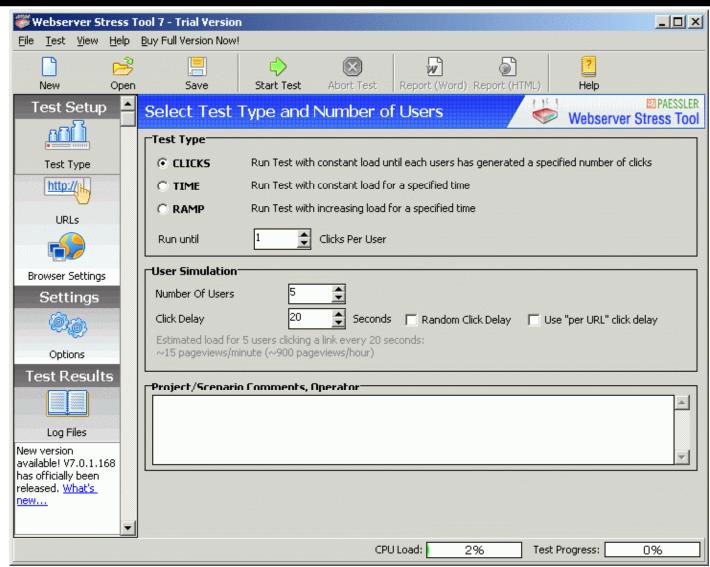
Features:

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



EC-Council

Webserver Stress Tool: Screenshot



Copyright © by **EC-Council**



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

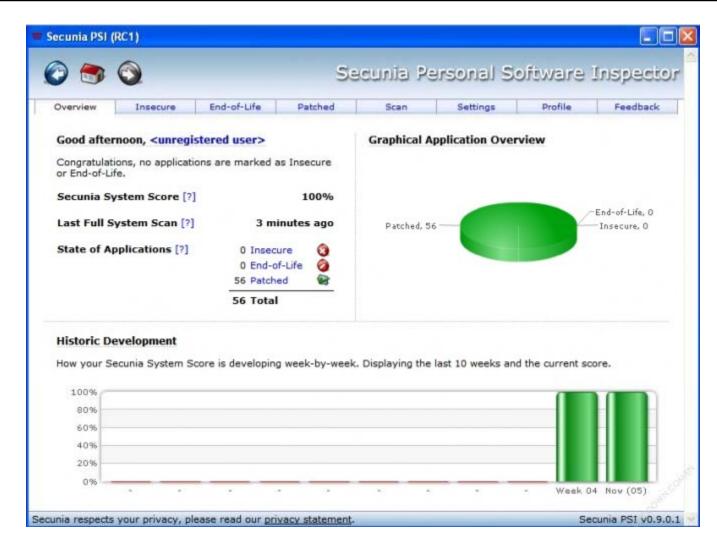
It relies on the meta-data of executables and library files

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



Countermeasures

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.

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."