Global Information Assurance Certification Paper

An Overview of SecureIIS – Are we really secured now?

Table of Contents

1 Introduction

The objective of this practical paper is to understand how our IIS can be protected using an application firewall. There are many application firewalls available on the market – commercial and free/shareware such as eSafe, BlackIce, ZoneAlarm, and Norton Firewall to name a few. This paper, hopefully, will assist system administrators and organizations in making decision to protect their web servers.

2 Securities Issues

Since its debut, Microsoft Internet Information Server (IIS) has dominated huge percentage of web servers worldwide. IIS is used not only as static web server in small organization, but also as a backbone for dynamic and complex web server. The popularity of IIS has created both minor and major security issues. With an overwhelm security issues and patches released, the task in securing web server primarily IIS has become a nightmare job.

Majority of system administrators do not realize that securing or hardening their servers is also part of their job. Many assume that they can sit back and see their servers in action after installation completes. By default, IIS installation provides a minimum security protection for web server. This issue then leads to more hazardous dilemma such as hack attempt, defacement, and technology espionage.

To have a considerable secure web server, it requires some tedious tasks that includes patching as well as upgrading it. The patching process involves downloading series of patches and installing them on every single server. Owning one or two servers are such an easy task. Can you imaging when you are responsible for tens or maybe hundreds of servers? This calls for help.

Recently, Internet world has been swamped by Code Red Worm (CRW). It was first discovered in July 17 and its second version hit the Internet on Aug 4. As of July 18, a day after its outbreak, over 12,000 servers have been infected, and this number increased dramatically. The worm infects systems by manipulating on a known issue centered around .ida and .idq mapping relates to IIS Web servers. The original CRW only caused the Denial of Service (DoS) attack on White House server compared to the second CRW that creates a Trojan program on the web server for remote access. Apart from CRW attacks, web servers face many attack attempts from both known and unknown such as buffer overflow, folder traversal, and web mapping; it goes to as far as DoS and DDoS attacks.

3 Conventional Protection

As mentioned earlier, securing an IIS server is a tedious task. In Windows world, majority of the IIS problems lies around its operating system. These tribulations always been corrected with the issue of patches or service packs. Patches are released after the problem has been identified and corrected. However, they rarely go

through rigorous tests. Service Packs are a collection of all patches issued after the final release of product or the last service pack. They contain patches that have gone trough rigorous test. System Administrators, normally have two choices in making sure the server is in the top performance – install small patches as soon as they are published or wait for the service pack. In many cases, waiting for service pack is essential. However, applying patches is equally vital when servers are exposed to major threats such as recent Code Red Worm attack. With the frequent release of patches, applying them is a tiresome task. Thus, web servers that are not patched are vulnerable.

Have you heard of eEye or eEye Digital Security? This company has been accredited with several important vulnerability discoveries on Microsoft's IIS recently. They have recently released an application that could ease system administrators' tasks called SecureIIS. What is SecureIIS? SecureIIS is an application firewall that will protect IIS from both known and unknown attacks.

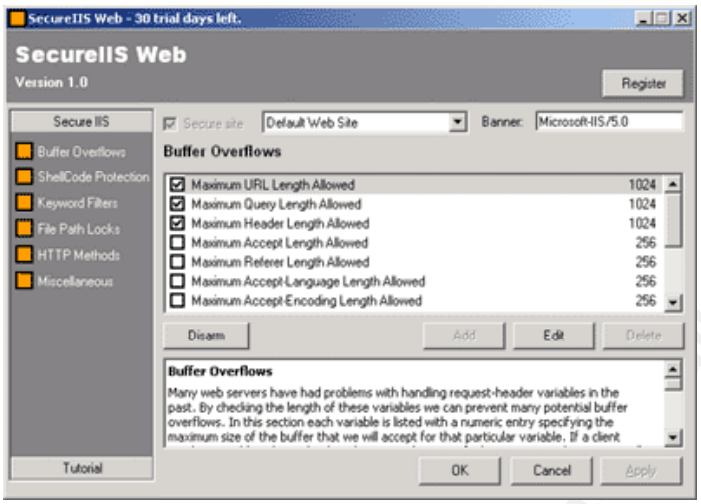
> SecureIIS wraps around IIS and works within it, verifying and analyzing incoming and outgoing Web server data for any possible security breaches. It combines the best features of Intrusion Detection Systems and Conventional Network Firewalls all into one. (Secureiis.com)

ZDNet's PC Magazine stated that application firewalls "work at the application layer and, acting as a server, accept packets from a client." Firewall can be implemented using both hardware and software or both. There are four types of firewalls techniques such as packet filter, application gateway, circuit-level gateway, and proxy server. Two or more of these techniques are commonly used. Application firewall will not replace Intrusion Detection Systems (IDS) as it is a complementary to IDS and traditional firewall because it is designed to protect specific service attack in which can stop both specific and general vulnerabilities.

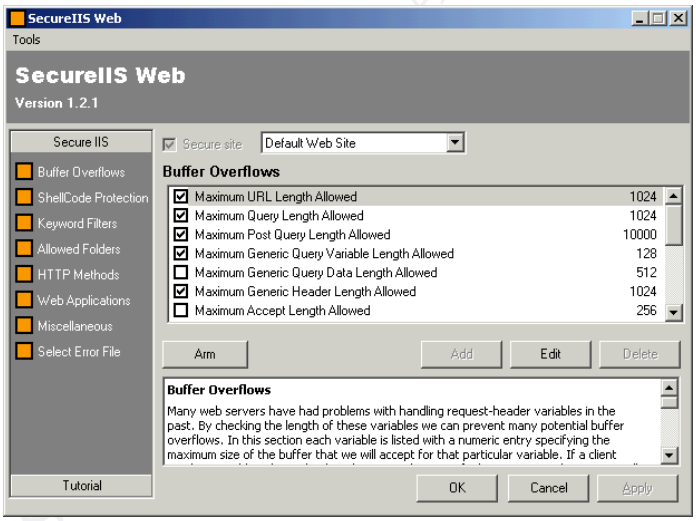
Question remains, are we really secure when we have SecureIIS deployed? Since it protects both known and unknown attacks, shall we cross our arm and do nothing in patching our servers? Let's look at SecureIIS.

4 Installation

SecureIIS installation process is simple. The evaluation copy that I received was a full version with 30-days license. I was directed to download SecureIIS from eEye's secured site. After the installation complete, the first screen appeared as shown below.



To register, click on “Register” button and I was asked to enter the license key. To obtain the license key, you need to copy the reference code given by SecureIIS to eEye’s website to get a license key. Copy that license key and you are a registered owner of SecureIIS.



5 Configuration

To secure your web server is simple. Click “Arm” button to arm the protection, and click “Disarm” button to disable it.

SecureIIS has categorized attack attempts into groups. They are:

- Buffer Overflows,
- ShellCode Protection,
- Keyword Filters,
- File Path Locks or Allowed Folders,
- HTTP Methods,
- Web Applications

- Miscellaneous

Buffer Overflows occurs when web servers have problems in handling request-header variables. SecureIIS checks the length of these variables that can prevent many potential buffer overflows. If a client sends a variable value with a length greater than specified in SecureIIS, the request will be denied and the attempt will be logged.

Allowed Folders feature allows SecureIIS to allow the client to access files that are in a set of allowable directories. This will stop attack such as "Directory Traversal Attacks".

HTTP Methods prevent many potential security risks involving the handling of unexpected HTTP request methods.

Keyword Filters protect server from a potential security risk that uses certain command shells. If a client makes a request that contains one of the selected keywords, the request will be denied and logged such as cmd.exe (located in winnt\system32), and root.exe (Code Red Worm II issue).

Web application section secures server that has Frontpage server extension installed. At the same time, it also protects against potential security in Exchange's Outlook Web Access.

Each group of SecureIIS has pre-determined rules protecting a web server, and some of these rules can be changed to meet security level. SecureIIS is able to protect web server installed with customized application or component, and it protects both encrypted and unencrypted session.

6 Evaluation Requirements

The evaluation was performed on Microsoft Windows NT4 Server and Windows 2000 Server. Both of them were installed and configured with default configuration (true for most of IIS worldwide), and updated with the latest service packs.

The test was divided into two major segments:

1. Web servers without SecureIIS installed or disarmed mode.
2. Web servers with SecureIIS installed or armed mode.

The objective of the test was to see whether SecureIIS performs as claimed in terms of its functionality and it protection against common attack such as probing.

For functionality test, tools used are listed below:

1. Netscape Navigator 4.x
2. Internet Explorer 5.x

For scanner tests, both commercial and freeware tools were used as listed below:

A. Commercial tools

a. Retina 4.02
b. Cybercop 3.5

B. Freeware/shareware tools
a. NmapNT 2.35
b. CodeRed Scanner 2.1

For attack tests, IISHack and netcat were used to simulate the attack. Both tools are freeware available for downloading.

7 Functionality Tests

The objective was to certify that SecureIIS on does not effect normal browsing. For this test, I used two most popular browsers – Microsoft Internet Explorer and Netscape Navigator.

SecureIIS has a unique feature that allows the application to be enabled, called “arm” and “disarm” without restarting the server. This will ease administrative tasks

The test started in “disarm” mode, and I started by accessing both web servers. IIS log and SecureIIS logs were recorded as a reference. This information would be used for comparison as the test progressed. The test procedure would then be followed by arming the SecureIIS on both severs. New logs were recorded and analyzed against previous logs. The test was done on both secure and normal channel.

8 Probing Tests

The objective was to see how SecureIIS handles probe attack. The probing tests were done using tools listed earlier.

Vulnerability scanners would scan the web servers searching for loopholes using pre-defined policies or criteria, and displayed servers’ vulnerabilities. All logs were recorded.

9 Attack Tests

The objective here was to find out how SecureIIS protect web server from malicious attacks using web browser. The tests were conducted using web browser by launching several URL strings, as well tools such as IISHack and netcat.

Web browsers are common “tools” to launch a Unicode attacks. This can be done by replacing valid command with special characters to launch commands such as copy, create, or delete. IISHack and netcat are also common hacker tools to attack web server. IISHack and netcat are used to logon to web server using port 80, and launch a Trojan program to attack.

We simulated attack scenario using the command “cmd.exe.” The results are

extracted from both IIS and SecureIIS log.

10 Test Results

10.1 Functionality Tests

Despite using SecureIIS in arm mode, IIS performs as usual without any hiccup (see IIS logs in Result Test Logs). SecureIIS produces access log located in its home folder namely "SecureIISLog.txt"

10.2 Probing Tests

Cybercop Scanner (running from lab2-2k)

Item	IIS 4	IIS 5
Without Secure IIS	Vulnerability detected: 1009 : Anonymous FTP check 1036 : WWW Web Server Version 1041 : Trace route to host 10037 : IIS newdsn.exe bug 10056 : IIS Association reveal webroot 10067 : IIS codebvws.asp Vulnerability	Vulnerability detected: 1008 : FTP Banner Check 1009 : Anonymous FTP check 1032 : ICMP time stamp obtained 1036 : WWW Web Server Version 1041 : Trace route to host
With Secure IIS	Vulnerability detected: 1008 : FTP Banner Check 1009 : Anonymous FTP check 1036 : WWW Web Server Version 1041 : Trace route to host	Vulnerability detected: 1008 : FTP Banner Check 1009 : Anonymous FTP check 1032 : ICMP time stamp obtained 1036 : WWW Web Server Version 1041 : Trace route to host

Comment:
We noticed that when SecureIIS was armed, there was no vulnerability detected on IIS4. IIS5 however, there was no different in result whether IIS was armed or not.

NmapNT

Items	IIS 4	IIS 5
Without Secure IIS	6 ports were scanned open. (Refer appendix B)	Too many of open ports scanned. (Result appendix B)
With Secure IIS	Same result as above	Same result as above

Comments:
NmapNT is best used to scan any open port on remote server. All reports show no vulnerability except ports opened.

Retina

Items	IIS 4	IIS 5
Without Secure IIS	CGI Scripts: MSADCS RDS Vulnerability Web Servers: IIS4-5 escape characters decode vulnerability CGI Scripts: CGI - Bdir.htr CGI Scripts: CGI - ExAir advsearch DoS CGI Scripts: CGI - ExAir query DoS CGI Scripts: CGI - ExAir search DoS Web Servers: IDQ Real Path Attack Web Servers: IIS - ISM Source Fragment Disclosure CGI Scripts: IIS Web administration hole	Web Servers: IIS4-5 escape characters decode vulnerability Web Servers: IIS45 IDA remote system overflow
With Secure IIS	No audit report	No audit report

Comments:
Retina is one of commercial vulnerability scanners available. It scans and detects any vulnerability on remote servers, and shows how to fix or at least where to find the fix. When IIS was armed with SecureIIS, retina could not find any vulnerability on both servers.

10.3 Attack Tests

CodeRed Scanner

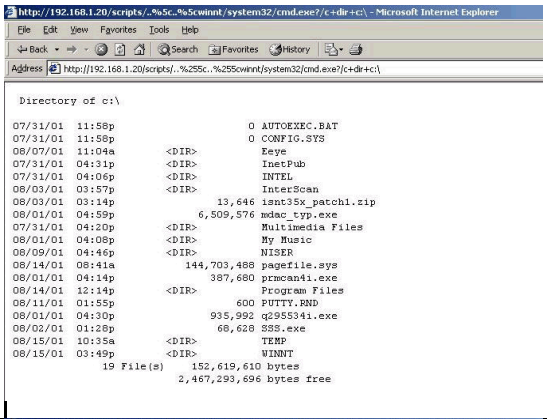
Item	IIS 4		IIS 5	
Without Secure IIS	Microsoft-IIS/4.0	Not vulnerable!	Microsoft-IIS/5.0	VULNERABLE!
With Secure IIS	Microsoft-IIS/4.0	Not vulnerable!	Microsoft-IIS/5.0	Not vulnerable!

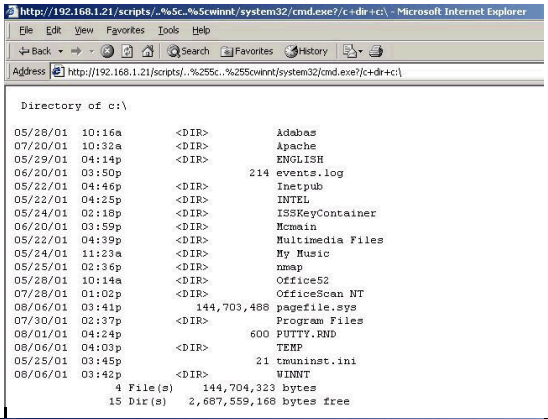
Comment:
CodeRed Scanner is a freeware tools from eEye that scans server for Code Red Worm vulnerability only. It does not detect any other vulnerability. Using SecureIIS armed, IIS5 was protected from CodeRed Worm. There was no effect on IIS4.

Traversal Attacks (using Internet Explorer)

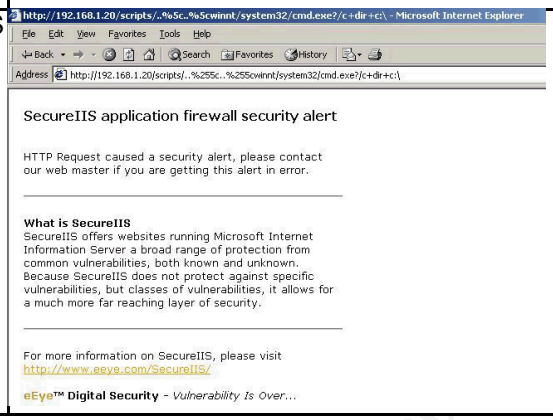
Items	IIS 4	IIS 5

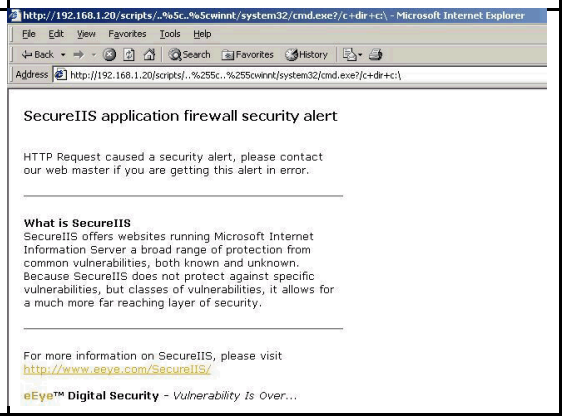
Without Secure IIS





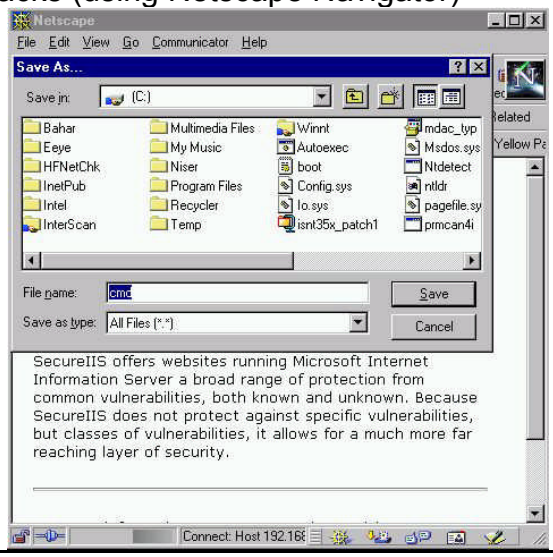
With Secure IIS

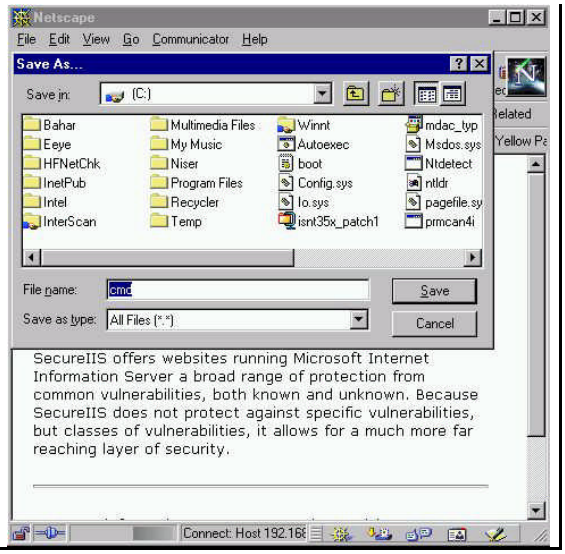


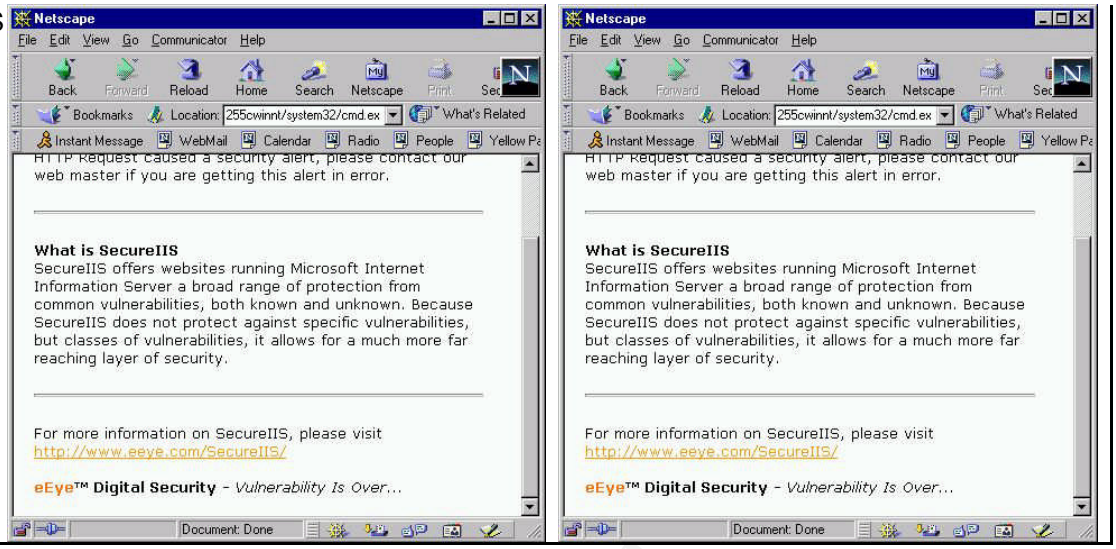


Traversal Attacks (using Netscape Navigator)

Without Secure IIS





With Secure IIS 

Comments:
I tried both IE and Navigator browsers in simulating the Unicode and traversal attacks. The traversal attacks together with Unicode string is a common attack on web server. The results show that SecureIIS does not allow any keyword listed in “keyword filtering” being processed. Traversal attacks are also prevented from occurring.

IISHack and netcat

Items	IIS 4	IIS 5
Without Secure IIS	Able to connect and manipulated the server	Able to connect and manipulated the server
With Secure IIS	Unable to connect	Unable to connect

Comments:
IISHack and netcat are two separate Trojan programs used to break into remote servers using abnormal port. SecureIIS does protect this intrusion from occurring as shown in table result.

11 Summary

Most of the techniques presented here were commonly used by both security professionals as well hackers. By using combination of those techniques, ones can bypass many firewalls and make contact with web servers. Once the web servers are their hands, the entire network is on their mercy.

Protecting servers requires a lot of task. It starts from they day of installation, and keeping all servers attack-free is a tedious work, from monitoring to installing patches and service packs.

The recent case of Code Red Worm and a mutation of the worm such as Code Red Worm II, pose a continued and serious threat to Internet users. Immediate actions must be taken to combat this threat. Keeping up with the latest security patches is one

option system administrators have. SecureIIS gives them an option in protecting web servers without installing patches. However, by having a depth measure of securing network, we can be assured that the task of system administrator is not such a big headache.

12 List of Reference

1. "SecureIIS™ Application Firewall." eEye Digital Security Website.URL: http://www.secureiis.com/html/Products/SecureIIS/index.html (Aug 5, 2001)

2. Lemos, Robert. ""Code Red" worm claims 12,000 servers" C|Net news.com. July 18, 2001 URL: http://news.cnet.com/news/0-1003-200-6604515.html?tag=tp_pr (Aug 15, 2001)

3. "Code Red Threat FAQ." Incident.org website. Aug 5, 2001URL: http://www.incidents.org/react/code_red.php (Aug 15, 2001)

4. Junnarkar, Sandeep and Fried, Ian. "Code Red offshoot packs a bigger punch." C|Net news.com Aug 6, 2001 URL: http://news.cnet.com/news/0-1003-200-6792918.html (Aug 15, 2001)

5. Dwyer, Paul. "How Firewalls Work." PC Magazine: Net Tools website. URL: http://www.zdnet.com/pcmag/pclabs/nettools/1620/cover/sb1.htm. (Sep 11, 2001)

6. Permeh, Ryan. "The Use of Application Specific Security Measures in a Modern Computing Environment." Janteknology White Paper. URL: http://www.janteknology.com.au/products/eeye/secureiis/wp.application.specific.security.measures.asp (Sep 11, 2001)

7. "firewall." Webopedia website. Jun 25, 2001. URL: http://www.webopedia.com/TERM/f/firewall.html (Sep 12, 2001)

8. "Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise." Jun 18, 2001. Microsoft Security Bulletin website URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-033.asp. (Aug 5, 2001)

9. "CERT® Advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL." Jun 19 – Aug 16, 2001. URL: http://www.cert.org/advisories/CA-2001-13.html. (Aug 5, 2001)

13 Test Results and Logs

13.1 Functionality Test Log

IIS4 Log (SecureIIS – disarmed mode)

192.168.1.30, -, 8/15/01, 16:20:22, W3SVC1, LAB3, 192.168.1.20, 100, 249, 4603, 200, 0, GET, /Default.htm, -,
192.168.1.30, -, 8/15/01, 16:20:22, W3SVC1, LAB3, 192.168.1.20, 81, 254, 10510, 200, 0, GET,
/samples/images/backgrnd.gif, -,
192.168.1.30, -, 8/15/01, 16:20:22, W3SVC1, LAB3, 192.168.1.20, 60, 252, 5308, 200, 0, GET,
/samples/images/h_logo.gif, -,
192.168.1.30, -, 8/15/01, 16:20:22, W3SVC1, LAB3, 192.168.1.20, 150, 251, 1070, 200, 0, GET,
/samples/images/SPACE.gif, -,
192.168.1.30, -, 8/15/01, 16:20:22, W3SVC1, LAB3, 192.168.1.20, 20, 251, 2740, 200, 0, GET,
/samples/images/tools.gif, -,
192.168.1.30, -, 8/15/01, 16:20:22, W3SVC1, LAB3, 192.168.1.20, 60, 250, 3120, 200, 0, GET,
/samples/images/docs.gif, -,
192.168.1.30, -, 8/15/01, 16:20:22, W3SVC1, LAB3, 192.168.1.20, 70, 252, 1050, 200, 0, GET,
/samples/images/SPACE2.gif, -,
192.168.1.30, -, 8/15/01, 16:20:22, W3SVC1, LAB3, 192.168.1.20, 20, 254, 3264, 200, 0, GET,
/samples/images/h_browse.gif, -,
192.168.1.30, -, 8/15/01, 16:20:22, W3SVC1, LAB3, 192.168.1.20, 40, 253, 2985, 200, 0, GET,
/samples/images/powered.gif, -,
192.168.1.30, -, 8/15/01, 16:20:22, W3SVC1, LAB3, 192.168.1.20, 140, 252, 6287, 200, 0, GET,
/samples/images/h_samp.gif, -,

IIS 5 Log (SecureIIS – disarmed mode)

#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2001-08-20 07:38:13
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status
2001-08-15 08:21:34 192.168.1.30 - 192.168.1.21 80 GET /iisstart.asp - 200
2001-08-15 08:21:34 192.168.1.30 - 192.168.1.21 80 GET /pagerror.gif - 304

SecureIIS Log (SecureIIS – armed mode)

2001/08/20-15:37:59-SECUREIIS LOG START

SecureIIS Log (SecureIIS – armed mode)

2001/08/20-15:38:10-SECUREIIS LOG START

13.2 Probing Test Log

SecureIIS Log (SecureIIS – disarmed mode)

2001/08/16-11:37:59-SECUREIIS LOG START

SecureIIS Log (SecureIIS – armed mode)

2001/08/16-12:12:31-SECUREIIS LOG START
DEBUG : 2001/08/16-12:12:31 : Web 2: No Lock Directory checks found
2001/08/16-12:12:58[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:12:58[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:12:58[1-192.168.1.21]:Failed in VerifyMethod: HEAD

2001/08/16-12:12:58[1-192.168.1.21]:Failed in VerifyFileExists: /CFDOCS/EXPEVAL/OPENFILE.CFM -
E:\INETPUB\WWWROOT\CFDOCS\EXPEVAL\OPENFILE.CFM
2001/08/16-12:12:58[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/FAXSURVEY -
E:\INETPUB\WWWROOT\CGI-BIN\FAXSURVEY
2001/08/16-12:12:58[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:12:58[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/FAXSURVEY -
E:\INETPUB\WWWROOT\CGI-BIN\FAXSURVEY
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/CAMPAS -
E:\INETPUB\WWWROOT\CGI-BIN\CAMPAS
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyKeywords UQUERY - keyword:..\
badstring:ICATCOMMAND=..\..\WINNT\WIN.INI&CATALOGNAME=CATALOG
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/WEBDIST.CGI -
E:\INETPUB\WWWROOT\CGI-BIN\WEBDIST.CGI
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/MACHINEINFO -
E:\INETPUB\WWWROOT\CGI-BIN\MACHINEINFO
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyFileExists: /IAMASCARYCYBERCOP.SNI -
E:\INETPUB\WWWROOT\IAMASCARYCYBERCOP.SNI
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyKeywords UQUERY - keyword:../
badstring:(../../../../../../../../SBIN/PING-C%D%S|)
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-WIN/UPLOADER.EXE/CGI-WIN/ -
E:\INETPUB\WWWROOT\CGI-WIN\UPLOADER.EXE
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyFileExists: /SCRIPTS/IISADMIN/ISM.DLL -
E:\INETPUB\SCRIPTS\IISADMIN\ISM.DLL
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyFileExists:
/CFDOCS/EXPEVAL/DISPLAYOPENEDFILE.CFM -
E:\INETPUB\WWWROOT\CFDOCS\EXPEVAL\DISPLAYOPENEDFILE.CFM
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyKeywords UQUERY - keyword:../
badstring:SOURCE=/../../../../BOOT.INI
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyFileExists: /ASPSAMP/ -
E:\INETPUB\WWWROOT\ASPSAMP\
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyKeywords UQUERY - keyword:../
badstring:SOURCE=/MSADC/SAMPLES/../../../../../BOOT.INI
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyFileExists: /SCRIPTS/CCMOD10056.IDA -
E:\INETPUB\SCRIPTS\CCMOD10056.IDA
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-
BIN/HANDLER/NETWORKASSOCIATESINC; CAT /ETC/PASSWD| - E:\INETPUB\WWWROOT\CGI-
BIN\HANDLER\NETWORKASSOCIATESINC; CAT \ETC\PASSWD|
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyFileExists: /IAMASCARYCYBERCOP.SNI -
E:\INETPUB\WWWROOT\IAMASCARYCYBERCOP.SNI
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyFileExists: /IAMASCARYCYBERCOP.SNI -
E:\INETPUB\WWWROOT\IAMASCARYCYBERCOP.SNI
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/GUESTBOOK.PL -
E:\INETPUB\WWWROOT\CGI-BIN\GUESTBOOK.PL
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyKeywords UQUERY - keyword:../
badstring:/../../../../../../../../../../..
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyFileExists: /CFDOCS/EXPEVAL/EXPRCALC.CFM -
E:\INETPUB\WWWROOT\CFDOCS\EXPEVAL\EXPRCALC.CFM
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyKeywords PQUERY - keyword:../
badstring:DRIVER=MICROSOFT%2BACCESS%2BDRIVER%2B%28*.MDB%29&DSN=NAI+TEST&DBQ=..%2F
WWWROOT%2FNAI-32497.HTM&NEWDB=CREATE_DB&ATTR=
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:12:59[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/TEST-CGI -
E:\INETPUB\WWWROOT\CGI-BIN\TEST-CGI

```
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/FORMMAIL.PL -
E:\INETPUB\WWWROOT\CGI-BIN\FORMMAIL.PL
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-12:13:01[1-192.168.1.21]:Failed in VerifyFileExists: /SCRIPTS/CCMOD10056.IDC -
E:\INETPUB\SCRIPTS\CCMOD10056.IDC
2001/08/16-12:13:01[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/FINGER -
E:\INETPUB\WWWROOT\CGI-BIN\FINGER
2001/08/16-12:13:01[1-192.168.1.21]:Failed in VerifyHighBit(PQUERY): +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+-+-+-+-+-+-+-+-+-+-
+H^X%FF%E6%FF%D4%83%C62J%01V%8A%06<_U%03%80.?FAI%84%C0U%F0%BATO|_%B9T`}`%03%C
A%FF%D1%BAX_|_%B9XP|`%03%CA%FF%D1C:\COMMAND.COM_/C_COPY_\WEBSITE\README.1ST_\WE
BSITE\HTDOCS\CYBERCOP.HTM
2001/08/16-12:13:00[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/ANYFORM2 -
E:\INETPUB\WWWROOT\CGI-BIN\ANYFORM2
2001/08/16-12:13:01[1-192.168.1.21]:Failed in VerifyFileExists: /SCRIPTS/SNORK.BAT -
E:\INETPUB\SCRIPTS\SNORK.BAT
2001/08/16-12:13:01[1-192.168.1.21]:Failed in VerifyHighBit(PQUERY): +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+-+-+-+-+-+-+-+-+-+-
+H^X%FF%E6%FF%D4%83%C6LJ%01V%8A%06<_U%03%80.?FAI%84%C0U%F0H0%10%F0WYHM\Y[X%05
0PZPA9%01U%F0%83%E9%10%FF%D1H0%10%F0WYH%D0PVLX%0500VPA9%01U%F0%83%E9%1C%FF
%D1CMD.EXE_/C_COPY_\WEBSITE\README.1ST_\WEBSITE\HTDOCS\X1.HTM
2001/08/16-12:13:01[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/PERL.EXE -
E:\INETPUB\WWWROOT\CGI-BIN\PERL.EXE
2001/08/16-12:13:01[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/GUESTBOOK -
E:\INETPUB\WWWROOT\CGI-BIN\GUESTBOOK
2001/08/16-12:13:01[1-192.168.1.21]:Failed in VerifyFileExists: /ASPSAMP/ -
E:\INETPUB\WWWROOT\ASPSAMP\
2001/08/16-12:13:01[1-192.168.1.21]:Failed in VerifyFileExists: /CGI-BIN/FORMMAIL -
E:\INETPUB\WWWROOT\CGI-BIN\FORMMAIL
2001/08/16-12:13:02[1-192.168.1.21]:Failed in VerifyFileExists: /SCRIPTS/CCMOD10056.STM -
E:\INETPUB\SCRIPTS\CCMOD10056.STM
2001/08/16-12:13:02[1-192.168.1.21]:Failed in VerifyFileExists: /CYBERCOP.HTM -
E:\INETPUB\WWWROOT\CYBERCOP.HTM
```

IIS4 Server (SecureIIS – disarmed mode)

nmapNT result

```
Starting nmapNT V. 2.53 by ryan@eEye.com
eEye Digital Security (http://www.eEye.com)
Based on nmap by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host LAB3 (192.168.1.20) appears to be up ... good.
Initiating SYN half-open stealth scan against LAB3 (192.168.1.20)
Adding TCP port 139 (state open).
Adding TCP port 21 (state open).
Adding TCP port 135 (state open).
Adding TCP port 80 (state open).
Adding TCP port 443 (state open).
Adding TCP port 1030 (state open).
The SYN scan took 0 seconds to scan 1523 ports.
For OSScan assuming that port 21 is open and port 1 is closed and neither are firewalled
Interesting ports on LAB3 (192.168.1.20):
(The 1517 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
80/tcp     open        http
135/tcp    open        unknown
```

```
139/tcp    open       unknown
443/tcp    open       unknown
1030/tcp   open       iad1

TCP Sequence Prediction: Class=trivial time dependency
                    Difficulty=3 (Trivial joke)

Sequence numbers: 1C3D78B3 1C3D78BD 1C3D78C7 1C3D78C9 1C3D78DB 1C3D78ED
Remote operating system guess: Windows NT4 / Win95 / Win98

    Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
```

IIS4 Server (SecureIIS – armed mode)

nmapNT Result

```
Starting nmapNT V. 2.53 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
Based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )
Host LAB3 (192.168.1.20) appears to be up ... good.
Initiating SYN half-open stealth scan against LAB3 (192.168.1.20)
Adding TCP port 21 (state open).
Adding TCP port 135 (state open).
Adding TCP port 443 (state open).
Adding TCP port 80 (state open).
Adding TCP port 1030 (state open).
Adding TCP port 139 (state open).
The SYN scan took 1 second to scan 1523 ports.
For OSScan assuming that port 21 is open and port 1 is closed and neither are firewalled
Interesting ports on LAB3 (192.168.1.20):
(The 1517 ports scanned but not shown below are in state: closed)
Port       State      Service
21/tcp     open       ftp
80/tcp     open       http
135/tcp    open       unknown
139/tcp    open       unknown
443/tcp    open       unknown
1030/tcp   open       iad1

TCP Sequence Prediction: Class=trivial time dependency
                    Difficulty=7 (Trivial joke)

Sequence numbers: 1C3D7814 1C3D7817 1C3D781A 1C3D782D 1C3D7840 1C3D784B
Remote operating system guess: Windows NT4 / Win95 / Win98

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

IIS5 Server (SecureIIS – disarmed mode)

nmapNT result

```
Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )
Interesting ports on LAB2-2K (192.168.1.21):
(The 73 ports scanned but not shown below are in state: closed)
Port       State      Service
1/tcp      open       tcpmux
```

```
2/tcp     open      compressnet
3/tcp     open      compressnet
4/tcp     open      unknown
5/tcp     open      rje
6/tcp     open      unknown
7/tcp     open      echo
8/tcp     open      unknown
9/tcp     open      discard
                                                    |
                                                    |
                                                    |
                                                (Continue)
32776/tcp  open      sometimes-rpc15
32777/tcp  open      sometimes-rpc17
32778/tcp  open      sometimes-rpc19
32779/tcp  open      sometimes-rpc21
32780/tcp  open      sometimes-rpc23
32786/tcp  open      sometimes-rpc25
32787/tcp  open      sometimes-rpc27
43188/tcp  open      reachout
47557/tcp  open      dbbrowse

Nmap run completed -- 1 IP address (1 host up) scanned in 68 seconds
```

IIS5 Server (SecureIIS – armed mode)

nmapNT result

```
Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )
Interesting ports on LAB2-2K (192.168.1.21):
(The 73 ports scanned but not shown below are in state: closed)
Port      State     Service
1/tcp     open      tcpmux
2/tcp     open      compressnet
3/tcp     open      compressnet
4/tcp     open      unknown
5/tcp     open      rje
6/tcp     open      unknown
7/tcp     open      echo
8/tcp     open      unknown
9/tcp     open      discard
                                                    |
                                                    |
                                                    |
                                                (Continue)
32776/tcp  open      sometimes-rpc15
32777/tcp  open      sometimes-rpc17
32778/tcp  open      sometimes-rpc19
32779/tcp  open      sometimes-rpc21
32780/tcp  open      sometimes-rpc23
32786/tcp  open      sometimes-rpc25
32787/tcp  open      sometimes-rpc27
43188/tcp  open      reachout
47557/tcp  open      dbbrowse

Nmap run completed -- 1 IP address (1 host up) scanned in 68 seconds
```

13.3 Attack Test Log

CodeRed Scanner

IIS 5 Log (SecureIIS – disarmed mode)

#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2001-08-16 07:22:24
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status
2001-08-16 07:22:24 192.168.1.30 - 192.168.1.21 80 HEAD /iisstart.asp - 302
2001-08-16 07:22:24 192.168.1.30 - 192.168.1.21 80 GET /scripts/root.exe /c 404
2001-08-16 07:22:24 192.168.1.30 - 192.168.1.21 80 GET /x.ida
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 200

IIS5 Log (SecureIIS – armed mode)

#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2001-08-16 07:23:43
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status
2001-08-16 07:23:43 192.168.1.30 - 192.168.1.21 80 HEAD / - 406
2001-08-16 07:23:43 192.168.1.30 - 192.168.1.21 80 GET /scripts/root.exe /c 406
2001-08-16 07:24:23 192.168.1.30 - 192.168.1.21 80 GET /x.ida
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 406

IIS4 Log (SecureIIS – disarmed mode)

192.168.1.30, -, 8/16/01, 15:10:23, W3SVC1, LAB3, 192.168.1.20, 0, 54, 270, 200, 0, HEAD, /Default.htm, -,
192.168.1.30, -, 8/16/01, 15:10:23, W3SVC1, LAB3, 192.168.1.20, 0, 94, 623, 404, 2, GET, /scripts/root.exe, /c,
192.168.1.30, -, 8/16/01, 15:11:06, W3SVC1, LAB3, 192.168.1.20, 0, 323, 623, 404, 2, GET, /x.ida,
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X,

IIS4 Log (SecureIIS – armed mode)

192.168.1.30, -, 8/16/01, 15:11:53, W3SVC1, LAB3, 192.168.1.20, 70, 54, 1303, 406, 0, HEAD, /, -,
192.168.1.30, -, 8/16/01, 15:11:53, W3SVC1, LAB3, 192.168.1.20, 50, 94, 1303, 406, 0, GET, /scripts/root.exe, /c,
192.168.1.30, -, 8/16/01, 15:12:32, W3SVC1, LAB3, 192.168.1.20, 60, 323, 1303, 406, 0, GET, /x.ida,
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X,

SecureIIS Log (SecureIIS – armed mode)

2001/08/16-15:37:59-SECUREIIS LOG START
DEBUG : 2001/08/16-15:37:59 : Web 2: No Lock Directory checks found
2001/08/16-15:38:13[1-192.168.1.21]:Failed in VerifyMethod: HEAD
2001/08/16-15:38:13[1-192.168.1.21]:Failed in VerifyKeywords URL - keyword:ROOT.EXE
badstring:/SCRIPTS/ROOT.EXE
2001/08/16-15:38:52[1-192.168.1.21]:Failed in VerifyBufferSize(QUERY - querysize-lastvar:220 / allowedsize: 128):
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X