

Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

USE MRTG AS AN INTRUSION DETECTION TOOL FOR MICROSOFT GIAC Certified Windows Security Administrator (GCWN) Practical Assignment Version 5.0 Option 1 Submitted October 11, 2004 Chuntida Harinnitisuk

USE MRTG AS AN INTRUSION DETECTION TOOL FOR MICROSOFT IIS
COMPONENTS
A Install IIS
B. Configure MRTG Virtual Web Site
C. Install SNMP
D. Configure SNMP Security
E. Configure Network Security for the SNMP Service
G. Download and Install MRTG21
H. Configure MRTG22
I. How to Access SNMP Counter
J. Make MRTG To run as a Service
CONCLUSION
REFERENCES

USE MRTG AS AN INTRUSION DETECTION TOOL FOR MICROSOFT IIS COMPONENTS

ABSTRACT

Microsoft Internet Information Services (IIS) is a very popular Web Server platform. The latest data from www.Netcraft.com survey results shows that 21 percent or approximately 10.5 million web sites running on IIS. IIS includes not only Web Server application but many other subcomponents such as FTP service, SMTP service, and NNP service. Every one of these components also has several vulnerabilities. The most recent Top 20 Internet Security Vulnerabilities from www.sans.org/top20 ranks Microsoft Web Servers and Services and the number one on the list. Vulnerabilities found in IIS could affect millions of servers. Microsoft has issued patches and security hot fixes and even if we can find the Network Administrator who can keep all IIS servers up to date we still cannot stop hackers from trying to exploit existing and new vulnerabilities. This research paper is evaluating two free monitoring softwares, MRTG (MultiRouter Traffic Grapher) and Microsoft Performance Monitor. The paper focuses on monitoring HTTP, FTP and SMTP traffic. All detailed steps to implement the selected tool are provided and how to identify a possible attack is included.

SECURITY ISSUES WITH WINDOWS PLATFORM

Microsoft Web Server or Internet Information Services (IIS) includes several subcomponents such as File Transfer Protocol (FTP) Service and Simple Mail Transfer Protocol (SMTP) Service. Netcraft conducts a survey by sending a query to 33 million Web Sites and found out that 11 percent of all queried running IIS have the "root.exe" hacking program installed on them. Two major Internet worms, Code Red and Nimda, have exploited the flaws in IIS to infect thousands of IIS systems worldwide. Code Red I and II attack servers in one day.

IIS version 5.0 is installed by default with products in the Windows 2000 Server family. SMTP service is also included in the default installation. The FTP service is not installed by default with any version of IIS but can be easily added with Windows Component Add/Remove Programs dialog box in Control Panel. IIS version 6 is an optional install in the Windows 2003 and several vulnerable components from IIS version 5 have been removed. However after successfully adding IIS components Web Server with static Web pages, FTP Service and SMTP Service will be ready to go online without additional configuration. IIS version 5.1 is also available to install for Windows 2000 workstation and XP. If there is no available policy to control users' workstation from installing new application there could be a large number of IIS servers in the network without the network administrators know it.

Along with support for Web, FTP and SMTP IIS also supports NNTP Service, FrontPage Server Extensions, Internet Printing, ASP or ASP.NET and all these extra services can be easily added by just click on each check box to install on any servers and workstations. The combination of these components can pose even higher security risks.

Although Microsoft FTP service is not the most popular FTP server on the Internet, FTP is still a common method of providing an alternative way of hacking to a Web Server. The default FTP root home directory on Windows 2000 servers give everyone full access. Hackers who can find the way to compromise the system will connect to FTP server as the "anonymous" guest account and create directories and transfer files. The hard drive will eventually be filled up with stolen software, obscene images and pirated movies. And they do it in such a way that it is difficult to find and delete the files.

As described in Request for Comments (RFC) 282, sections 2.1 and 3.7, SMTP was designed with the ability to relay e-mail messages. According to Radicati Group (<u>www.radicati.com</u>) messaging and collaboration software study research the average user sends and receives a 14.7 MB of email data per day, a 53% growth over the last year. Spam is a key reason for this rise despite anti-spam solutions. The default installation of Microsoft default SMTP Virtual Server

service allows any IP address to access and relay through the server. If relay is not controlled, a malicious user might use it to relay and send bulk unsolicited commercial e-mail messages or spam mails. This process can tie up resource on the relay host. The security risk is a denial of service against the SMTP server.

Microsoft has taken more steps to secure IIS by providing IIS Security Checklist for all IIS versions for network administrators to ensure security aspects of running the IIS server. The "Secure Internet Information Services 5 Checklist" documentation is available at

http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/ tips/iis5chk.mspx and contains 9 pages of just some recommendations and best practices. IIS 6 architecture that promises significant improvements in stability and security Microsoft still recommends to download a 64 pages of documentation "Chapter 3 Securing Web Sites and Applications" from Internet Information Services (IIS) 6.0 Resource Kit at

http://www.microsoft.com/downloads/details.aspx?FamilyID=80a1b6e6-829e-49b7-8c02-333d9c148e69&displaylang=en#filelist to ensure the highest security. For network administrator to have the operational IIS servers up and running at no time for money driven business purpose by spending more time to go through lengthy security checklists basically is not always a preferable option.

Even with the most secured configuration IIS servers there are always hackers who always search for new vulnerabilities and more likely that they will find one. Nothing can stop hackers to keep scanning or attacking the servers. One of the most effective and popular methods is deploying an Intrusion Detection System. The tool will be used to monitor the IIS services to collect data and obtain a base line. When an unusual data is occurred it will help the administrators detect any possible intrusion and allow them to take action to prevent it before the system is compromised.

PRODUCTS EVALUATION

The Microsoft Windows 2000, XP and 2003 operating systems provide a performance monitoring tool called Windows Performance Monitor. The performance monitor console includes System Monitor, Performance Logs and Alerts, and Task Manager. A primary source for information about Performance monitor is available in Help documentation. Using performance monitoring utility to monitor and track real-time occurrences.

MRTG is a Web performance measurement that is widely used by network administrators. A primary source for information about MRTG is found at <u>www.mrtg.org</u>. There is also a countless list of related MRTG resources on the Internet.

Both Performance Monitor and MRTG use counters to create data and display graph. An understanding of what type of counter is being used to detect intrusion is important to the proper use and evaluate of both products. Microsoft provides numerous types of Performance monitor counters and SNMP counters for MRTG. Table 1 shows the selected counters that will be used in evaluating process. The unusual high numbers of these counters can imply that hackers might be scanning the server, using the server resource, or relaying spam messages.

Table 1: Selected Counters

Service	Counters	Descriptions
HTTP Service	currentAnonymousUser	The number of anonymous users currently connected to the HTTP Server.
	connectionAttempts	The number of connection attempts that have been made to the HTTP Server.
	totalNotFoundErrors	The total number of requests the HTTP server could not satisfy because the requested resource could not be found.
	measureBandwidth	The I/O bandwidth used by this HTTP Server, averaged over a minute.
		The total number of files east but
FIP Service	totalFilesSent	the FTP Server.
	totalFilesReceived	The total number of files received by the FTP Server.
	currentConnecions	The current number of connections to the FTP Server.
	connectionAttempts	The number of connections attempts that have been made to the FTP Server.
SMTP Service	totalDeliveredRetries	The total number of messages local deliveries retried by the SMTP Server.
	totalNonDeliveryReports	The total number non-delivery reports that have been generated by the SMTP Server.
	totalMessageSent	The total number of messages sent by the SMTP Server.
Č, Š		
Õ		

After evaluating the products the Table 2 shows the comparisons of both products.

	Microsoft Performance Monitor	MRTG
Software Source	Included in Windows Operating systems	http://www.mrtg.org
Requirements		
- Operating	Windows 2000 or 2003	Windows 2000 or 2003
Systems	Server or Windows 2000 or XP workstations	Server or Windows 2000 or XP workstations
- Additional	None	 Active Perl
Software		Note: IIS Web Server
- SNMP	Not required on	Required on all
	monitored servers	monitored servers
How it works	Uses counters on Web	Queries SNMP counters
	Service, SMTP Service	and creates HTML pages
	and FTP Service objects	with live network graphs
	to collect and display	
	data in graph, histogram	
	or report	
How to access the	Navigate to the	Via web sites
monitoring data	performance icon in the	
	administrative tools folder	
	in the control panel, from	
	the start menu or by	
	typing perfmon.msc in	
	the run box	_
Cost	Free	Free
Graph Display	All counters are	Each counter is displayed
_	displayed in one graph	in separate graph
Remote server monitoring	Yes	Yes
Operator/Administrator	Requires administrative	Does not require
Rights	right in order to monitor	administrative right
	the remote server	
Alert	Yes	No
Historical Data	Graph shows current	Graphs are automatically
	activity. Historical data	generated and are
	can be logged and	available to see counter
	viewed at later time.	graph trends for the last
		week, month or year.

Table 2: Products Comparison

Windows Performance Monitor has various capabilities as well as limitations as described in above table. The major drawbacks of Performance monitor are as follows:

- 1) Only one chart or graph view shows current activity. There is no limitation of how many counters can be added however it is not practical to even view it after the forth counter is added.
- 2) In order to see average, minimum and maximum counter numbers a line on a line chart has to be highlighted by pressing ctrl-h or click to highlight the selected counter.
- 3) Historical data graph view has to be regenerated from the logged data.
- 4) Current graphical data can be accessed only from local monitoring system while MRTG graphical data is available on the Web.

SA-SINGLORAN ANTING

PRODUCT IMPLEMENTATION

MRTG is selected to implement on the Widows 2003 server. In this implementation the MRTG is installed on the same sever that will be monitored. If the MRTG will be installed on the separate server exclude SNMP installation steps. The major steps for implementation are as follows:

- A. Install IIS
- B. Configure MRTG Virtual Web Site
- C. Install SNMP on monitored server
- D. Configure SNMP Security
- E. Configure Network Security for the SNMP Service
- F. Download and install Active Perl
- G. Download and Install MRTG
- H. Configure MRTG
- I. How to access SNMP counters
- J. Make MRTG To run as a Service

A. Install IIS

- 1) Open Control Panel and go to Add or Remove Programs
- 2) Click Add/Remove Windows Component
- 3) In Windows Components dialog box select Application Server, click **Details** and make sure Internet Information Services (IIS) is selected

🔂 Add or Remove Programs	
Windows Components Wizard	Sort by: Name
Ch. Windows Components Re You can add or remove components of Windows.	Size <u>44.43MB</u> Used <u>rarely</u>
To add or remove a component, click the checkbox. A shaded box means that only ad part of the component will be installed. To see what's included in a component, click Details	Change Remove
Components:	Size 61.64MB
🖌 🕞 Accessories and Utilities 4.5 MB 🛌	Size 4.17MB
Add, Add, Application Server 24.6 MB	Size 0.95MB
Application Server Internet Inf	ormation Services (IIS)
To add or remove a component, click the check box. A shaded box means that only p of the component will be installed. To see what's included in a component, click Detai of the comp	いしん move a component, click the check box. A shaded onent will be installed. To see what's included in a co
Sub <u>c</u> omponents of Application Server: Sub <u>c</u> ompon	ents of Internet Information Services (IIS):
🗌 🗆 🚡 Application Server Console 0.0 MB 🛛 🔳 🔶 Bac	kground Intelligent Transfer Service (BITS) Server E
🗆 🂁 ASP.NET 0.0 MB 🗹 🔷 Com	mon Files
COMB Generative COM+ access COMB Generative COM+ access COMB Generative COM+ access	Transfer Protocol (FTP) Service
COMB OUD Compared and a construction of the construct	tPage 2002 Server Extensions
Services (IIS) Services (IIS) Services (IIS) Services (IIS)	net Information Services Manager
C.5 MB	net Printing "P Service
Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP).	Includes support for throttling and restarting data t management console extension.
Total disk space required: 14.1 MB Details Total disk sp	ace required: 14.1 MB
Space available on disk: 14078.9 MB Space avail	able on disk: 14078.9 MB

4) Click Next

B. Configure MRTG Virtual Web Site

- 1) Create a new directory **MRTG** in **c:\Inetpub\wwwroot**
- 2) Click Start, Administrative Tools and Internet Information Services (IIS) Manager
- Expand the Web Sites folder, right-click the Default Web Sites folder, point to New, and then click Virtual Directory. The Virtual Directory Creation Wizard appears.
- 4) Click Next
- 5) Type MRTG in the Virtual Directory Alias name box and click Next.
- 6) In the Web Site Content Directory Path box type c:\Inetpub\wwwroot\mrtg
- 7) Under Allow the following permissions, select the check boxes for Read and Run scripts (such as ASP)
- 8) Click Next
- 9) Click Finish

C. Install SNMP

- 1) Open Control Panel and go to Add or Remove Programs
- 2) Select Management and Monitoring Tools
- 3) Click Details

	Windows Components Winard	
Change or Remove Programs	Windows components Windows You can add or remove components of Windows. Image: Component of Windows.	V: Name.
Add <u>N</u> ew Programs	To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.	Change/Remove Size 0.95MB
dd/Remove Windows omponents		
	To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Subcomponents of Management and Monitoring Tools: © Connection Manager Administration Kit Connection Point Services 0.2 MB Network Monitor Tools Simple Network Management Protocol 0.9 MB WMI SNMP Provider 1.1 MB WMI Windows Installer Provider 0.6 MB	
	Description: Includes agents that monitor the activity in network devices and report to the network console workstation. Total disk space required: 4.4 MB Space available on disk: 14246.5 MB OK Cancel	

4) Click to select a check box Simple Network Management Protocol

- 5) Click OK
- 6) Click Next

D. Configure SNMP Security

- 1) Click Start
- 2) Point to Administrative Tools and click Services
- 3) In the right pane, double-click SNMP Services
- 4) Click the **Security** tab
- 5) Click to select the check box Send Authentication trap
- 6) Under Accepted community names, click Add
- 7) Select **READ ONLY** in a Community Rights drop down list
- 8) In the Community Name box add a case-sensitive Community Name
- 9) Click Add
- 10)Click OK

SNINP Service Properties (Local Computer)	? ×
General Log On Recovery Agent Traps Security Dependencies	
Send authentication trap	
Accepted community names	
Community Rights	
SNMPREAD READ ONLY	
Add <u>E</u> dit <u>R</u> emove	
C Accept SNMP packets from any host	
Accept SNMP packets from these hosts	
localhost	
Add Edit Remove	
OK Cancel <u>Apply</u>	y
Sec. 1	

E. Configure Network Security for the SNMP Service

E.1 Create a Filter List

- Click Start. Point to Administrative Tools and click Domain Controller Security Policy for a domain controller or Local Security Policy for member server
- 2) Right-click IP Security Policies on Active Directory and then click Manage IP filter lists and filter actions
- On the Manage IP Filter Lists tab, click Add, Enter SNMP Messages(161/162) in a name box and enter Filter SNMP Messages on the description box
- 4) Clear **Use Add Wizard** check box
- 5) Click Add to open IP Filter Properties
- 6) On the Addresses tab in the Source address drop down box select Any IP address and select My IP Address in the Destination address
- 7) Click to select Make sure Mirrored. Match packets with the exact opposite source and destination addresses check box

- 8) Click the **Protocol** tab and select **UDP** in **Select a protocol type** drop down list
- In the Set the IP protocol port select From this port and enter 161 in the box. Select To this port and enter 161 in the box
- 10)Click OK
- 11)In the IP Filter List dialog box click Add to open IP Filter Properties
- 12)On the Addresses tab in the Source address drop down box select Any IP address and select My IP Address in the Destination address
- 13)Click to select Make sure Mirrored. Match packets with the exact opposite source and destination addresses check box
- 14)Click the **Protocol tab** and select **TCP** in **Select a protocol type** drop down list
- 15)In the Set the IP protocol port select From this port and enter 161 in the box. Select To this port and enter 161 in the box
- 16)Click OK
- 17) In the IP Filter List dialog box click Add to open IP Filter Properties
- 18)On the Addresses tab in the Source address drop down box select Any IP address and select My IP Address in the Destination address.
- 19)Click to select Make sure Mirrored. Match packets with the exact opposite source and destination addresses check box.
- 20)Click the **Protocol tab** and select **UDP** in **Select a protocol type** drop down list
- 21)In the Set the IP protocol port select From this port and enter 162 in the box. Select To this port and enter 162 in the box
- 22)Click OK
- 23) In the IP Filter List dialog box click Add to open IP Filter Properties
- 24)On the Addresses tab in the Source address drop down box select Any IP address and select My IP Address in the Destination address
- 25)Click to select Make sure Mirrored. Match packets with the exact opposite source and destination addresses check box.
- 26)Click the **Protocol tab** and select **TCP** in **Select a protocol type** drop down list
- 27) In the Set the IP protocol port select From this port and enter 162 in the box. Select To this port and enter 162 in the box
 28) Click OK
- 28)Click OK

E.2 Create an IPSec Policy

- 1) Right-click the IP Security Policies on Active Directory and then click Create IP Security Policy
- 2) Click Next on Welcome to the IP Security Policy Wizard dialog box.
- 3) On IP Security Policy Name type Secure SNMP in Name input box and type Force IPSec for SNMP Communications in Description input box then click Next
- 4) On Requests for Secure Communication click check box **Activate the** default response rule then click **Next**

- 5) On Default Response Rule Authentication Method select Active Directory default (Kerberos V5 protocol) then click Next
- 6) On **Completing the IP Security Policy Wizard** make sure **Edit** properties is selected then click **Finish**
- 7) On New IP Security Policy Properties dialog box click Add.
- 8) Click IP Filter List tab in IP Filter Lists select SNMP Messages (161/162)

dit Rule Properties	<u>?</u> ×
Authentication Methods Tu IP Filter List	nnel Setting Connection Type Filter Action
The selected IP filter lis	t specifies which network traffic will be
IP Filter Lists:	
Name	Description
O All ICMP Traffic	Matches all ICMP packets betw
	Matches all IP packets from this
	Filler ShimF Messages
A <u>d</u> d <u>E</u> dit	<u>R</u> emove
0	K Cancel Apply

9) Click Filter Action tab in Filter Actions box select Require Security



- 10) Click **OK**
- 11) Right-click Secure SNMP in the right pane and click Assign

🚡 Default Domain Controller Securi	ty Settings		
<u>Eile Action View H</u> elp			
← → 🗈 📧 🗙 😭 🗟 🔮	1 🗎 🚠 🔟 🖉		
Security Settings Cocal Policies Co	Name A Server (Request Secu Client (Respond Only) Secure Server (Requir	Description For all IP tra Communicat For all IP tra Delete Rename Properties Help	Policy Assigned No No No No No
Assigns this policy (attempts to make it act	ive).		

F. Download and Install ActivePerl

- Download a copy of ActivePerl MSI package for Windows from <u>http://www.activestate.com/Products/ActivePerl/</u>
 Double-click the MSI install file and click Next
- 2) Double-click the MSI install file and click **Next**



- 3) Choose I Accept the terms in the License Agreement and click Next
- 4) Accept the installation location C:\Perl\ or click Browse to select other location

🙀 ActivePerl 5.8.4 Build 810 Setup	×
Custom Setup Select the way you want features to be inst	alled.
Click on the icons in the tree below to change t	he way features will be installed. ActiveState ActivePerl is a quality-assured distribution of Perl. This feature requires 0KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 44MB on your hard drive.
Location: C:\Perl\	Br <u>o</u> wse
<u>R</u> eset Disk <u>U</u> sage < <u>B</u> a	ick <u>N</u> ext > Cancel

5) Leave the check box Enable PPM3 to send profile info to ASPN blank and click Next

🛃 ActivePerl 5.8.4 Build 810 Setup		2	
New features in PPM	\sim		
		\sim	
~			
This release of ActivePerl includes Pr version 3, which includes a new faci ASPN's "PPM Profile" feature commun securely and transparently to your AS easily migrate, reinstall, upgrade or r locations.	ogrammer's Pack lity for keeping track licates your package SPN Profile. Saved p restore PPM package	age Manager k of installed packages, e installs and updates vrofiles allow you to es in one or more	
Using the profile functionality requires installing a license for ASPN Perl. You can always disable or enable the Profile feature later within PPM3.			
For more information about ASPN, ple http://www.ActiveState.com/Products	ease see :/ASPN_Perl/.		
Enable PPM3 to send profile info to	ASPN	Privacy Policy	
	< <u>B</u> ack	ext > Cancel	

6) In Choose Setup Options box click to select a check box Add Perl to the PATH environment variable and a check box Create Perl file extension association then click Next

ActivePerl 5.8.4 Build 810 Setup	×
Choose Setup Options	
Choose optional setup actions.	
🔽 Add Perl to the PATH e	nvironment variable
🔽 Create Perl file extensi	on association
🗖 Create IIS script mapp	ing for Perl
Create IIS script mapp	ing for Peri ISAPI
	< Back

7) Click Install to begin the installation

🚰 ActivePerl 5.8.4 Build 810 Setup
Ready to Install
The Setup Wizard is ready to begin the Custom
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
< <u>B</u> ack Install Cancel
· · · · · · · · · · · · · · · · · · ·

G. Download and Install MRTG

- 1) Download the latest version of MRTG from http://www.mrtg.org
- 2) Select the latest version of MRTG zip file for Windows platform. At the time of this research paper the latest version is mrtg-2.10.15.zip
- 3) Unzip the downloaded MRTG file mrtg-2.10.15.zip to the c:\ directory or any directory you desire

🗁 C:\Documents and Settings\Administrator\Desktop\mrtg						
<u>File Edit View Favorites Tools H</u> elp						
🕙 Back 👻 🌖 👻 🦻 Search 🌔 Folders 🛛 🎼 🎯 🗙 🎽 🛄 🗸						
Address 🛅 C:\Documents and Sett	ings\Administrator\[Desktop\mrtg				
Name 🔺	Size	Туре	Date Modified	Attributes		
FireDaemon-Lite-1_6-GA.exe	1,557 KB	Application	9/24/2004 12:57 PM	А		
inrtg-2.10.15.zip	1,582 KB	Compressed (zippe	9/24/2004 12:57 PM	А		
Extraction Wizard			×			
Select a Destin Files inside the choose.	ation e ZIP archive will be	extracted to the location	you 🖏			
	Select a fold Files will be C:\ Extracting	der to extract files to. extracted to this <u>directory</u> :	Browse			
		< <u>B</u> ack <u>N</u> ext >	Cancel			

- 4) After successful extraction test the installation by opening a Command Prompt, go to c:\mrtg-2.10.15\bin directory and type perl mrtg
- 5) The message should show the command MRTG missing a config file.

🛋 Command Prompt

```
C:\>cd mrtg-2.10.15
C:\mrtg-2.10.15>cd bin
C:\mrtg-2.10.15\bin>perl mrtg
Usage: mrtg <config-file>
mrtg-2.10.15 is the Multi Router Traffic Grapher.
If you want to know more about this tool, you might want
to read the docs. They came together with mrtg!
Home: http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
C:\mrtg-2.10.15\bin>
```

6) MRTG has been successfully installed.

H. Configure MRTG

- 1) Make a default config file by open a Command Prompt and go to c:\mrtg-2.10.15\bin directory.
- 2) Type the following command

```
perl cfgmaker SNMPREAD@192.168.0.5 --global "WorkDir:
c:\www\InetPub\wwwroot\mrtg" --output mrtg.cfg
```

3) The sample of output on the Command Prompt should show as follows:

- 4) Use Notepad to open mrtg.cfg that was created in directory c:\mrtg-2.10.15\bin
- 5) Add the following lines for each counter to the end of the mrtg.cfg file

```
###The number of anonymous users currently connected to the HTTP Server.###
Target[httpCurrAnonymous]:
.1.3.6.1.4.1.311.1.7.3.1.7.0&.1.3.6.1.4.1.311.1.7.3.1.15.0:SNMPREAD@192.168.0.5
YLegend[httpCurrAnonymous]: current anony.
ShortLegend[httpCurrAnonymous]: .
MaxBytes[httpCurrAnonymous]: 1250000
Options[httpCurrAnonymous]: nopercent, unknaszero
Legend1[httpCurrAnonymous]: Number of anonymous users currently connected to
the HTTP Server
Legend2[httpCurrAnonymous]: -
Legend3[httpCurrAnonymous]: -
Legend4[httpCurrAnonymous]: -
LegendI[httpCurrAnonymous]: connections:
LegendO[httpCurrAnonymous]: -
Title[httpCurrAnonymous]: Number of anonymous users currently connected to the
HTTP Server
PageTop[httpCurrAnonymous]: <H1>Number of anonymous users currently connected
to the HTTP Server</H1>
Colours[httpCurrAnonymous]: GREEN#00eb0c,BLUE#0000ff,GRAY#AAAAAA,VIOLET#ff00ff
WithPeak[httpCurrAnonymous]: ymw
```

- 6) Add other InternetServer statistics by changing the Target SNMP counter number to the associated counter from step I how to access counter number
- The following is a complete config file that includes all counters in the Table 1

```
# Created by
# cfgmaker SNMPREAD@192.168.0.5 --global 'WorkDir: c:\InetPub\wwwroot\mrtg' --
output mrtg.cfg
### Global Config Options
# for UNIX
# WorkDir: /home/http/mrtg
# or for NT
# WorkDir: c:\mrtgdata
### Global Defaults
# to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits
EnableIPv6: no
# System: ESC7870-2003
# Description: Hardware: x86 Family 6 Model 9 Stepping 5 AT/AT COMPATIBLE -
Software: Windows Version 5.2 (Build 3790 Uniprocessor Free)
# Contact:
# Location:
```

```
******
### Interface 1 >> Descr: 'MS-TCP-Loopback-interface' | Name: '' | Ip:
'127.0.0.1' | Eth: '' ###
### The following interface is commented out because:
### * it is a Software Loopback interface
# Target[192.168.0.5_1]: 1:SNMPREAD@192.168.0.5:
# SetEnv[192.168.0.5_1]: MRTG_INT_IP="127.0.0.1" MRTG_INT_DESCR="MS-TCP-
Loopback-interface"
# MaxBytes[192.168.0.5_1]: 1250000
# Title[192.168.0.5_1]: Traffic Analysis for 1 -- ESC7870-2003 📉
# PageTop[192.168.0.5_1]: <H1>Traffic Analysis for 1 -- ESC7870-2003</H1>
 <TABLE>
#
    <TR><TD>System:</TD>
                            <TD>ESC7870-2003 in </TD></TR>
#
#
    <TR><TD>Maintainer:</TD> <TD></TD>
   <TR><TD>Description:</TD><TD>MS-TCP-Loopback-interface </TD></TR>
#
#
    <TR><TD>ifType:</TD> <TD>softwareLoopback (24)</TD></TR>
#
    <TR><TD>ifName:</TD>
                            <TD></TD></TR>
    <TR><TD>Max Speed:</TD> <TD>1250.0 kBytes/s</TD></TR>
#
                           <TD>127.0.0.1 (esc7870-2003.esc7870.vp)</TD></TR>
#
    <TR><TD>Ip:</TD>
 </TABLE>
WorkDir: c:\InetPub\wwwroot\mrtq
###The number of anonymous users currently connected to the HTTP Server.###
Target[httpCurrAnonymous]:
.1.3.6.1.4.1.311.1.7.3.1.7.0&.1.3.6.1.4.1.311.1.7.3.1.15.0:SNMPREAD@192.168.0.5
YLegend[httpCurrAnonymous]: current anony.
ShortLegend[httpCurrAnonymous]: .
MaxBytes[httpCurrAnonymous]: 1250000
Options[httpCurrAnonymous]: nopercent, unknaszero
Legend1[httpCurrAnonymous]: Number of anonymous users currently connected to
the HTTP Server
Legend2[httpCurrAnonymous]: -
Legend3[httpCurrAnonymous]: -
Legend4[httpCurrAnonymous]: -
LegendI[httpCurrAnonymous]: connections:
LegendO[httpCurrAnonymous]: connections:
Title[httpCurrAnonymous]: Number of anonymous users currently connected to the
HTTP Server
PageTop[httpCurrAnonymous]: <H1>Number of anonymous users currently connected
to the HTTP Server</H1>
Colours[httpCurrAnonymous]: GREEN#00eb0c,BLUE#0000ff,GRAY#AAAAAA,VIOLET#ff00ff
WithPeak[httpCurrAnonymous]: ymw
###The number of connection attempts made to the HTTP Server.###
Target[httpConnAttempts]:
.1.3.6.1.4.1.311.1.7.3.1.15.0&.1.3.6.1.4.1.311.1.7.3.1.15.0:SNMPREAD@192.168.0.
YLegend[httpConnAttempts]: attempts
ShortLegend[httpConnAttempts]: .
MaxBytes[httpConnAttempts]: 1250000
Options[httpConnAttempts]: nopercent, unknaszero
```

```
Legend1[httpConnAttempts]: Number of connection attempts made to the HTTP
Server
Legend2[httpConnAttempts]: -
Legend3[httpConnAttempts]: -
Legend4[httpConnAttempts]: -
LegendI[httpConnAttempts]: attempts:
LegendO[httpConnAttempts]: attempts:
Title[httpConnAttempts]: Number of connection attempts made to the HTTP Server
PageTop[httpConnAttempts]: <H1>Number of connection attempts made to the HTTP
Server</H1>
Colours[httpConnAttempts]: GREEN#00eb0c,BLUE#0000ff,GRAY#AAAAAA,VIOLET#ff00ff
WithPeak[httpConnAttempts]: ymw
###The number of File Not Found errors from the HTTP Server.###
Target[httpFileErrors]:
.1.3.6.1.4.1.311.1.7.3.1.43.0&.1.3.6.1.4.1.311.1.7.3.1.43.0:SNMPREAD@192.168.0.
5
YLegend[httpFileErrors]: errors
ShortLegend[httpFileErrors]: .
MaxBytes[httpFileErrors]: 1250000
Options[httpFileErrors]: nopercent, unknaszero
Legend1[httpFileErrors]: Number of File Not Found Errors
Legend2[httpFileErrors]: -
Legend3[httpFileErrors]: -
Legend4[httpFileErrors]: -
LegendI[httpFileErrors]: errors:
LegendO[httpFileErrors]: errors:
Title[httpFileErrors]: Number of File Not Found Errors
PageTop[httpFileErrors]: <H1>Number of File Not Found Errors</H1>
Colours[httpFileErrors]: GREEN#00eb0c,BLUE#0000ff,GRAY#AAAAAA,VIOLET#ff00ff
WithPeak[httpFileErrors]: ymw
###HTTP Server Bandwidth Usage ###
Target[httpBandwidth]:
.1.3.6.1.4.1.311.1.7.3.1.45.0&.1.3.6.1.4.1.311.1.7.3.1.45.0:SNMPREAD@192.168.0.
5
YLegend[httpBandwidth]: Mbps
ShortLegend[httpBandwidth]:
MaxBytes[httpBandwidth]: 1250000
Options[httpBandwidth]: nopercent, unknaszero
Legend1[httpBandwidth]: Bandwidth
Legend2[httpBandwidth]: -
Legend3[httpBandwidth]: -
Legend4[httpBandwidth]: -
LegendI[httpBandwidth]: Mbps:
LegendO[httpBandwidth]: Mbps:
Title[httpBandwidth]: HTTP Server Bandwidth Usage
PageTop[httpBandwidth]: <H1>HTTP Server Bandwidth Usage </H1>
Colours[httpBandwidth]: GREEN#00eb0c,BLUE#0000ff,GRAY#AAAAAA,VIOLET#ff00ff
WithPeak[httpBandwidth]: ymw
###Total Number of files sent by this FTP Server###
Target[ftpFilesent]:
1.3.6.1.4.1.311.1.7.2.1.5.0&1.3.6.1.4.1.311.1.7.2.1.5.0:SNMPREAD@192.168.0.6
YLegend[ftpFilesent]: files
ShortLegend[ftpFilesent]: .
MaxBytes[ftpFilesent]: 1250000
Options[ftpFilesent]: nopercent, unknaszero
Legend1[ftpFilesent]: Total Number of files sent by this FTP Server
```

```
Legend2[ftpFilesent]: -
Legend3[ftpFilesent]: -
Legend4[ftpFilesent]: -
LegendI[ftpFilesent]: files:
LegendO[ftpFilesent]: files:
Title[ftpFilesent]: Number of files sent by this FTP Server
PageTop[ftpFilesent]: <H1>Number of files sent by this FTP Server</H1>
Colours[ftpFilesent]: GREEN#00eb0c,BLUE#0000ff,GRAY#AAAAAA,VIOLET#ff00ff
WithPeak[ftpFilesent]: ymw
###Total Number of files received by this FTP Server###
Target[ftpFilerecieve]:
.1.3.6.1.4.1.311.1.7.2.1.6.0&.1.3.6.1.4.1.311.1.7.2.1.6.0:SNMPREAD@192.168.0.6
YLegend[ftpFilerecieve]: files
ShortLegend[ftpFilerecieve]: .
MaxBytes[ftpFilerecieve]: 1250000
Options[ftpFilerecieve]: nopercent, unknaszero
Legend1[ftpFilerecieve]: Total Number of files sent by this FTP Server
Legend2[ftpFilerecieve]: -
Legend3[ftpFilerecieve]: -
Legend4[ftpFilerecieve]: -
LegendI[ftpFilerecieve]: files:
LegendO[ftpFilerecieve]: files:
Title[ftpFilerecieve]: Number of files received by this FTP Server
PageTop[ftpFilerecieve]: <H1>Number of files received by this FTP Server</H1>
Colours[ftpFilerecieve]: GREEN#00eb0c,BLUE#0000ff,GRAY#AAAAAA,VIOLET#ff00ff
WithPeak[ftpFilerecieve]: ymw
###Total Number of current connections to the FTP Server###
Target[ftpConn]:
.1.3.6.1.4.1.311.1.7.2.1.13.0&.1.3.6.1.4.1.311.1.7.2.1.13.0:SNMPREAD@192.168.0.
6
YLegend[ftpConn]: connections
ShortLegend[ftpConn]: .
MaxBytes[ftpConn]: 1250000
Options[ftpConn]: nopercent, unknaszero
Legend1[ftpConn]: Total Number of current connections to the FTP Server
Legend2[ftpConn]: -
Legend3[ftpConn]: -
Legend4[ftpConn]: -
LegendI[ftpConn]: connections:
LegendO[ftpConn]: connections:
Title[ftpConn]: Number of current connections to the FTP Server
PageTop[ftpConn]: <H1>Number of current connections to the FTP Server</H1>
Colours[ftpConn]: GREEN#00eb0c,BLUE#0000ff,GRAY#AAAAAA,VIOLET#ff00ff
WithPeak[ftpConn]: ymw
###The number of connections attempts that have been made to the FTP server###
Target[FTP NumberConnections]:
1.3.6.1.4.1.311.1.7.2.1.15.0&1.3.6.1.4.1.311.1.7.2.1.15.0:SNMPREAD@192.168.0.6
YLegend[FTP_NumberConnections]: attempts
ShortLegend[FTP_NumberConnections]: .
MaxBytes[FTP_NumberConnections]: 1250000
Options[FTP_NumberConnections]: nopercent, unknaszero
Legend1[FTP_NumberConnections]: Total Number of connections
Legend2[FTP_NumberConnections]: -
Legend3[FTP_NumberConnections]: -
Legend4[FTP_NumberConnections]: -
LegendI[FTP_NumberConnections]: attempts:
LegendO[FTP_NumberConnections]: attempts:
```

```
Title[FTP_NumberConnections]: Number of connection attempts made to the FTP
server
PageTop[FTP_NumberConnections]: <H1> Number of connection attempts made to the
FTP server</H1>
Colours[FTP_NumberConnections]:
GREEN#00eb0c,BLUE#0000ff,GRAY#AAAAA,VIOLET#ff00ff
WithPeak[FTP_NumberConnections]: ymw
```

 After adding all counters open Command Prompt, change the directory to c:\mrtg-2.10.15\bin and run the following commands for MRTG to create result files

perl mrtg mrtg.cfg

9) The following result files were created in WorkDir c:\InetPub\wwwroot\mrtg

Attp://www.attempts.html	9 KB	HTML Document	10/10/2004 4:01 AM
🗐 httpconnattempts.log	50 KB	Text Document	10/10/2004 4:01 AM
🖬 httpconnattempts.old	50 KB	OLD File	10/10/2004 4:00 AM
🖻 httpconnattempts-day.png	2 KB	PNG Image	10/10/2004 4:01 AM
🔊 httpconnattempts-month.png	2 KB	PNG Image	10/10/2004 3:22 AM
🔊 httpconnattempts-week.png	2 KB	PNG Image	10/10/2004 3:54 AM
🔊 httpconnattempts-year.png	2 KB	PNG Image	10/10/2004 1:22 AM
🙆 httpcurranonymous.html	8 KB	HTML Document	10/10/2004 4:01 AM
🗐 httpcurranonymous.log	50 KB	Text Document	10/10/2004 4:01 AM
🗟 httpcurranonymous.old	50 KB	OLD File	10/10/2004 4:00 AM
🖻 httpcurranonymous-day.png	2 KB	PNG Image	10/10/2004 4:01 AM
🖻 httpcurranonymous-month.png	2 KB	PNG Image	10/10/2004 3:22 AM
🖻 httpcurranonymous-week.png	2 KB	PNG Image	10/10/2004 3:54 AM
🖻 httpcurranonymous-year.png	2 KB	PNG Image	10/10/2004 1:22 AM

10)The html file shows daily graph, weekly graph, monthly graph and yearly graph.



11)Create an html file as a summary file to include a daily graph from all counters





I. How to Access SNMP Counter

- 1) Download a program Getif 2.3.1 from http://www.snmp4tpc.com/Files/Tools/SNMP/getif/getif-2.3.1.zip
- 2) Extract the file and install Getif 2.3.1 to c:\Program Files\Getif 2.3.1
- Download a collection of MIBs from <u>http://www.wtcs.org/snmp4tpc/FILES/Tools/SNMP/getif/getif-Mibs.zip</u>
- 4) Extract the getif-Mibs.zip file to C:\Program Files\Getif 2.3.1\Mibs
- 5) Click Start, All Programs and open Getif 2.3.1
- 6) On the Parameters tab, enter the host name or IP address of the host you want to monitor.
- 7) Enter the SNMP Read community string in SNMP Parameters and click Start
- 8) The system information should appears as follows:

📱 Getif [192.10	68.0.5]	_ 🗆 X				
Parameters In	iterfaces Addresses Routing Table Arp Gen. Table Reachability Traceroute NSLookup Ip discovery MBrowser Graph					
Host name DNS name	192.168.0.5 Image: Simple restance Read community SNMPREAD Timeout (ms) 2000 SNMP Port 161					
IP Address	192.168.0.5					
SysName	ESC7870-2003 IfNumber 2					
SysContact	Network Admin SysServices 76					
SysLocation	Location					
SysDescr Hardware: x86 Family 6 Model 9 Stepping 5 AT /AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Uniprocessor Free)						
SysObjectID	enterprises.microsoft.software.systems.os.windowsNT.dc					
SysUpTime	0:4:53:57.59					
Configuration Set as default Load default Factory settings Telnet						
Telnet application telnet.exe Browse						
SysInfo variables	s OK Exit					

9) Click MBrowser tab

10)Expand the directory tree to .iso.org.dod.internet.private.enterprises.microsoft.software.internetServer

🖥 Getif [192.168.0.5]		. 🗆 🗙
Parameters Interfaces Addresses Routing Table Arp	Gen. Table Reachability Traceroute NSLookup Ip discovery MBrowser Graph	
.iso.org.dod.internet.private.enterprises.microsoft.software.inte	ternetServer	
.1.3.6.1.4.1.311.1.7		
the msiprip2 the msiprip2 the msiprip2 the msiprip2 the trpServer the ntpServer the ntpServer the smtpServer the smtpServer	Access Status	Y
inetSrvStats ⊡ wins ⊡ par		
.1.3.6.1.4.1.311.1.7 n (nullobj) Systnfo variables OK	O entry(s) Set Add to graph Add to	Gen

- 11)Expand httpServer, httpStatistics and select currentAnonymousUsers
- 12) The associated counter number appears on the top in the input box. Use this number for MRTG config file

.iso.org.dod.internet.private.ente	prises.microsort.sortware.internets.erver.nttpServer.nttp - totalBytesSentHighWord - totalBytesSentLowWord - totalBytesReceivedHighWord - totalBytesReceivedLowWord - totalFilesSent - totalFilesSent - currentAnonymousUsers - currentNonAnonymousUsers - totalAnonymousUsers	Stanstics.cu	Type Access This is th connec	counter readonly he number of anor ted to the HTTP \$	Enums Status hymous users Gerver.	mandatory currently	× × ×
.1.3.6.1.4.1.311.1.7.3.1.7	u (unsigned)			0 entry(s)	Set Add	i to graph	dd to Gen

J. Make MRTG To run as a Service

- 1) Download the latest version of FireDaemon from http://www.firedaemon.com/downloads/
- 2) Install the downloaded file FireDaemon-Pro1_7.exe in the chosen destination location.
- Click Start, points to All Programs and choose FireDaemon Service Manager
- 4) Click Service and choose New in the Toolbar
- 5) Fill out the panel as per the screen shot below

💓 N	ew Service Definition	×
¥	🍟 💾 📫 🤗)
P	rogram Settings Adva Service Identification	anced Dependencies Environment Pre / Post-Service Scheduling
	Display Name:	MRTG
		MRTG v2.10.15
	Application to Hun as a <u>Console Application:</u>	
	<u>E</u> xecutable: <u>W</u> orking Directory:	C:\Perl\bin\perl.exe
	<u>P</u> arameters: Start-up <u>T</u> ime:	mrtglogging=mrtg.log mrtg.cfg 3000 ms
		Install Cancel

Shine and

New Service Definition	DN			×
🖲 🍟 💾 👘				Ŭ
Program Settings Ad	lvanced Dependenci	es Environment F	Pre / Post-Service	Scheduling
General				
Show <u>W</u> indow:	Normal			
Load <u>O</u> rder Group:				
Logon				
Logon <u>A</u> ccount:		<u> </u>	rd:	
Interact with Deskto	p:	<u>C</u> onfirm:		
Service Lifecycle				
Start-Up <u>M</u> ode:	Automatic		•	
Upon Program <u>E</u> xit:	Restart the Program		5000	ms
Elap Detection:	Disabled		•	retries
<u>G</u> raceful Shutdown:	V	Max Shutdown <u>D</u> ela	ay: 5000	ms
			Install	Cancel

6) Click Install. The service should install successfully and start automatically. Check that the service has been started successfully by having a FireDaemon Service:MRTG status as "running" in the FireDaemon Pro Service Manager v1.7 GA panel and that MRTG statistics are being updated.

👽 FireDaemon Pro Service Manager v1.7 GA			
<u>File S</u> ervice <u>H</u> elp			
😻 🍸 🖹 🖹 🥆 🚫 🖒 🍉 🌐	🩋 🚹 📕		
Service	Status Process	Startup Type	User
🐨 FireDaemon Service: MRTG	Running Running	Automatic	LocalSystem

CONCLUSION

The MRTG has installed successfully installed and detects traffic on HTTP service, FTP service and SMTP service. As mentioned earlier this collection of data can be used to create a base line of the activity to monitor any suspicious events.

REFERENCES

Divins, David., Pierce, Steve., Oeitker, Tobi. "mrtg-nt-guide – The Windows NT Guide to MRTG 2.10.15". URL:

http://people.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg-nt-guide.html (August 8, 2004)

Howard, Michael. "Secure Internet Information Services 5 Checklist". URL: <u>http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/tips/iis5chk.mspx</u> (June 29, 2000)

Microsoft. "Internet Information Services (IIS) 6.0 Resource Kit". URL: <u>http://www.microsoft.com/downloads/details.aspx?FamilyID=80a1b6e6-829e-49b7-8c02-333d9c148e69&displaylang=en#filelist</u> (April 14, 2004)

Microsoft "HOW TO: Configure Network Security for the SNMP Service in Windows Server 2003" <u>http://support.microsoft.com/?kbid=324261</u> (April 5, 2004)

NetCraft. "October 2004 Web Server Survey". URL: <u>http://news.netcraft.com/archives/2004/10/01/october_2004_web_server_survey.</u> <u>html</u> (October 1, 2004)

SANS. "The SANS Top 20 Internet Security Vulnerabilities". URL: <u>http://www.sans.org/top20/</u> (October 8, 2004)

Tabona, Andrew. "Windows 2003 Performance Monitor" URL: <u>http://www.wown.com/articles_tutorials/Windows_2003_Performance_Monitor.ht</u> <u>ml</u> (March 29, 2004)