Global Information Assurance Certification Paper

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

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 (www.radicati.com) 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 www.mrtg.org. 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.
FTP Service	totalFilesSent	The total number of files sent by 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.

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

Table 2: Products Comparison

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

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.

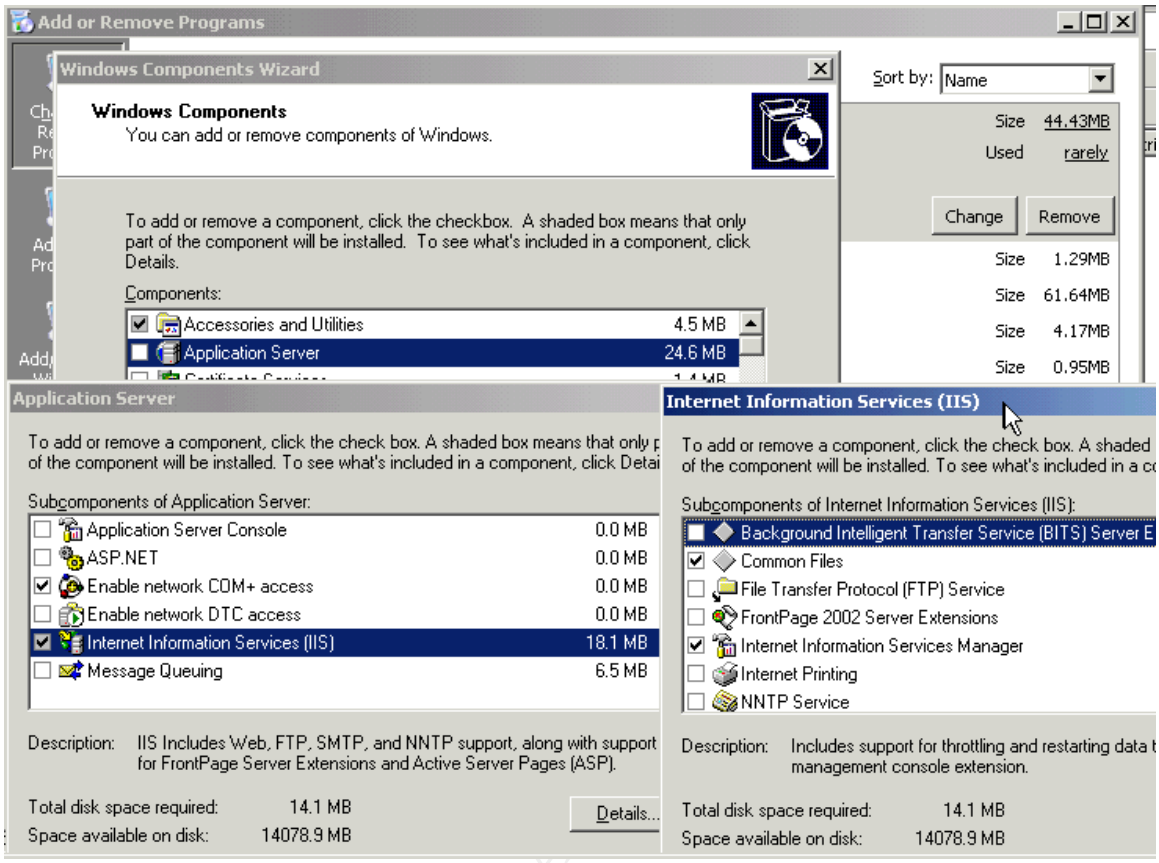
PRODUCT IMPLEMENTATION

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



4) Click **Next**

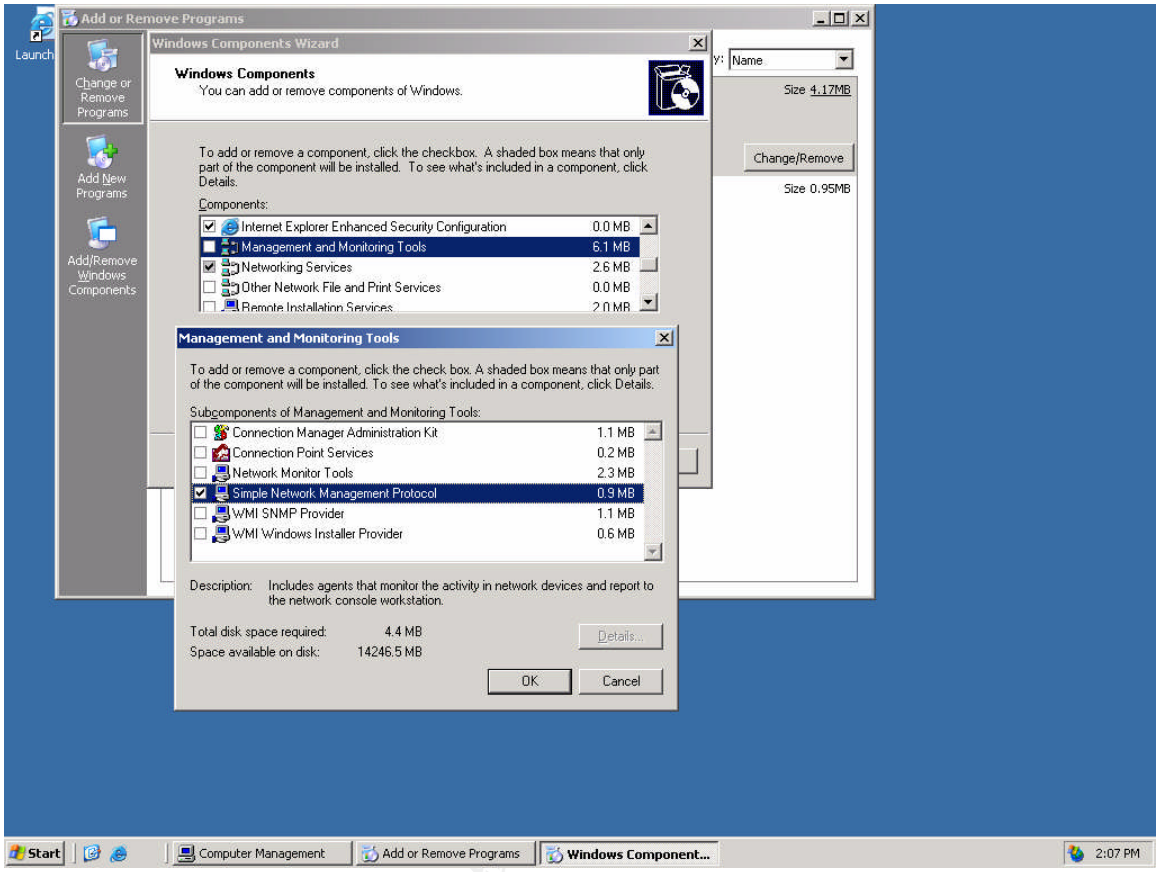
B. Configure MRTG Virtual Web Site

1) Create a new directory **MRTG** in **c:\Inetpub\wwwroot**
2) Click **Start, Administrative Tools** and **Internet Information Services (IIS) Manager**
3) 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**

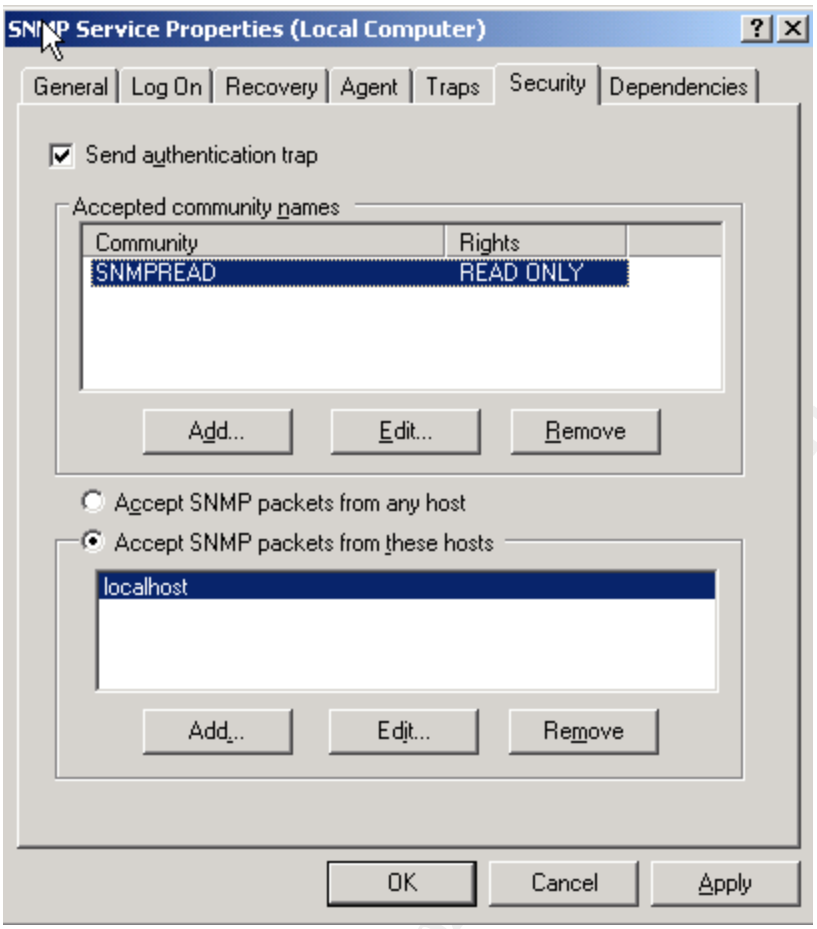
4) Click to select a check box **Simple Network Management Protocol**



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**



E. Configure Network Security for the SNMP Service

E.1 Create a Filter List

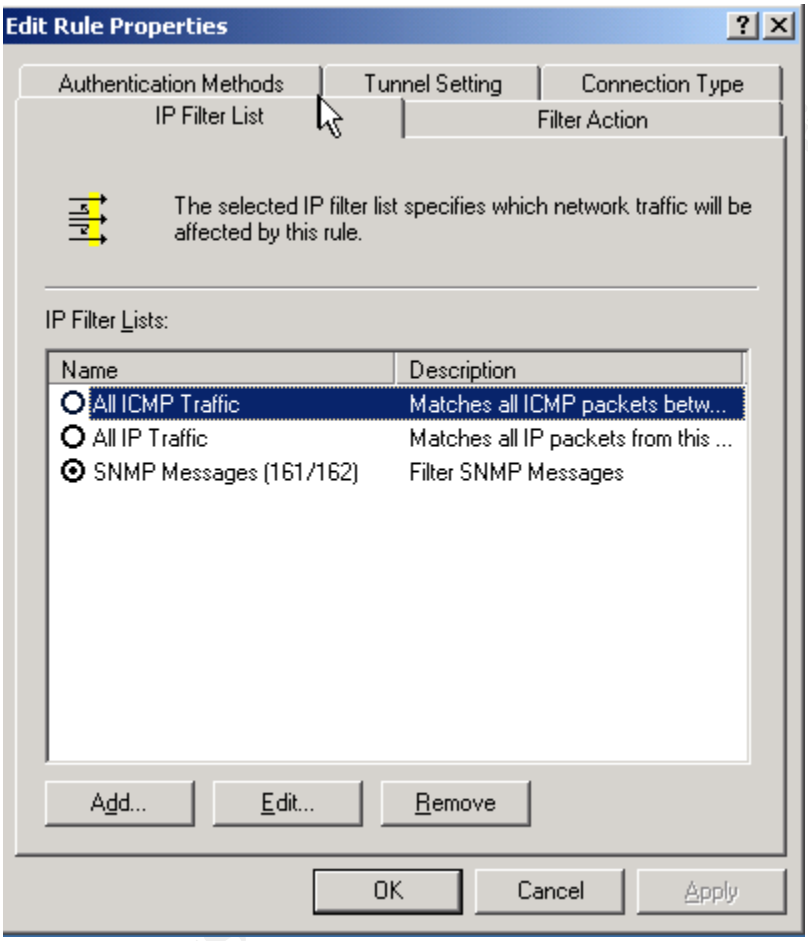
1) Click **Start**. Point to **Administrative Tools** and click **Domain Controller Security Policy for a domain controller or Local Security Policy** for member server
2) Right-click **IP Security Policies on Active Directory** and then click **Manage IP filter lists** and filter actions
3) On the **Manage 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
9) 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**

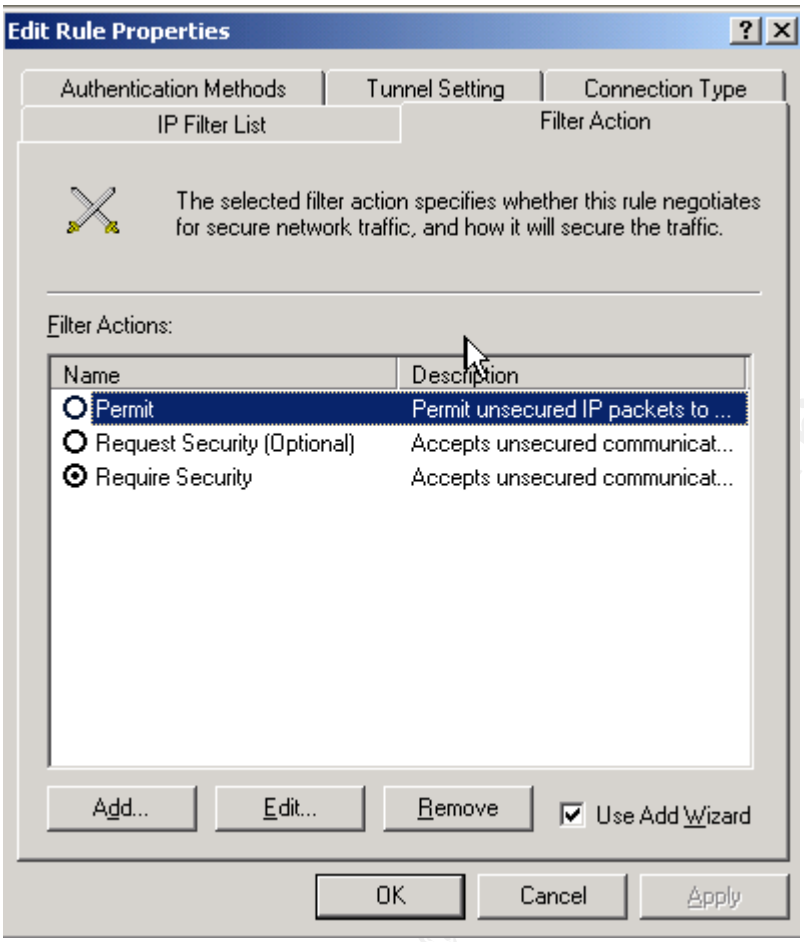
E.2 Create an IPSec Policy

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**

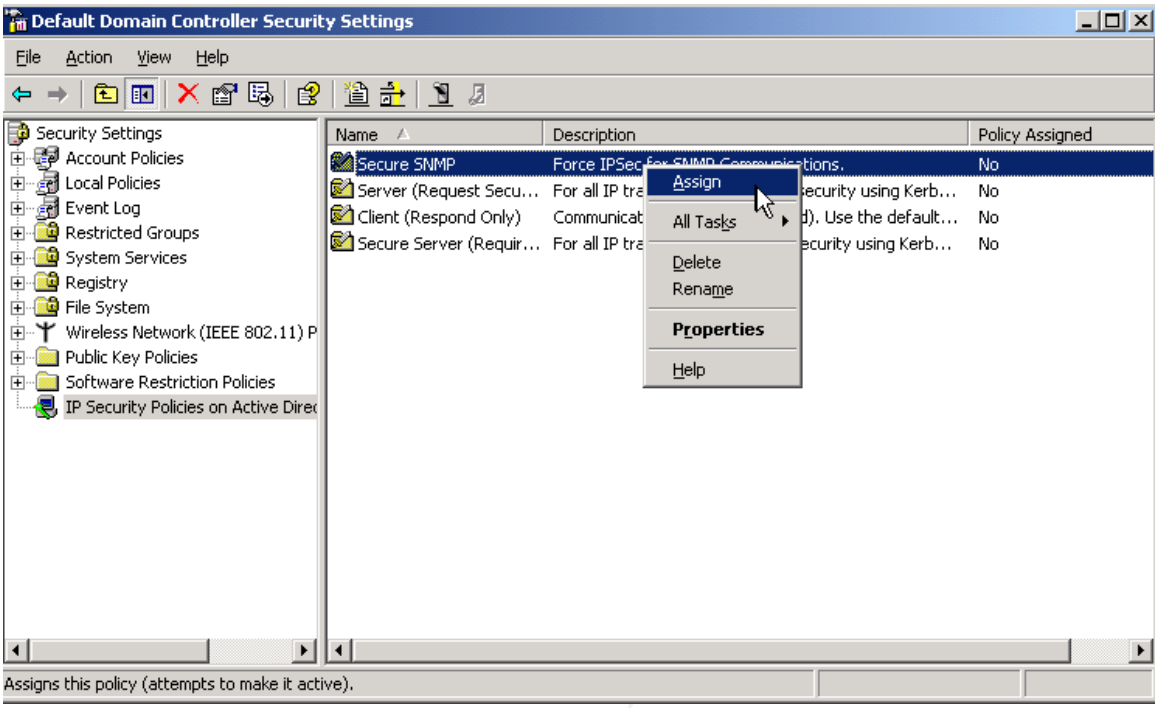
5) On **Default Response Rule Authentication Method** select **Active Directory default (Kerberos V5 protocol)** then click **Next**
6) On **Completing the IP Security Policy Wizard** make sure **Edit properties** is selected then click **Finish**
7) On **New IP Security Policy Properties** dialog box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



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



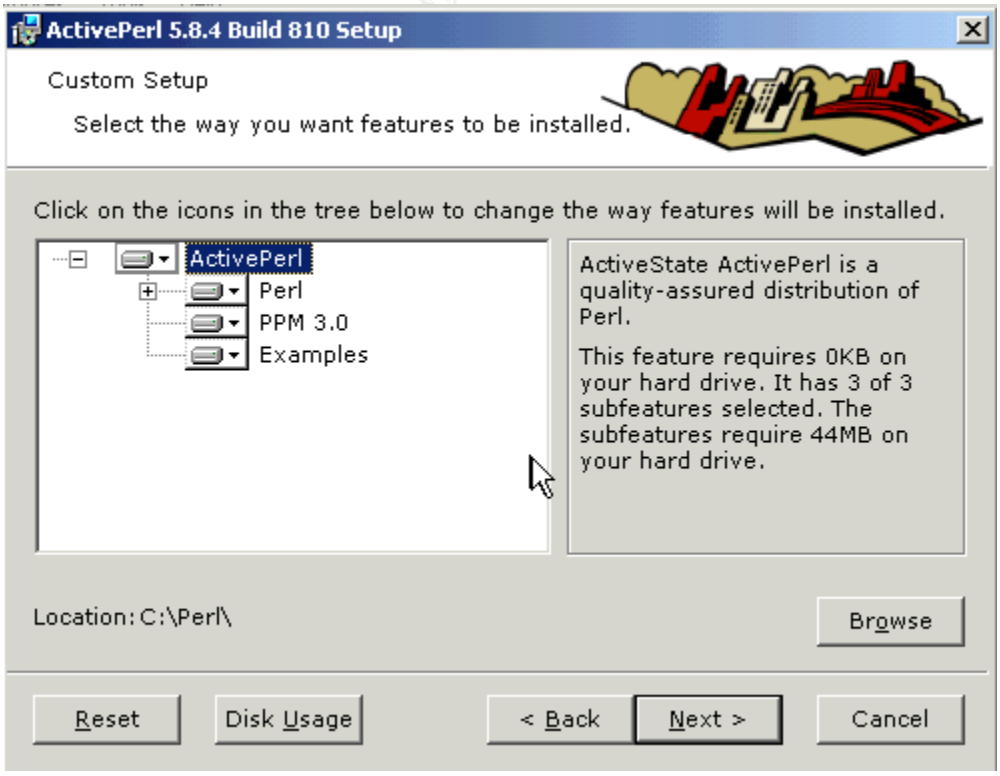
10) Click **OK**
11) Right-click **Secure SNMP** in the right pane and click **Assign**



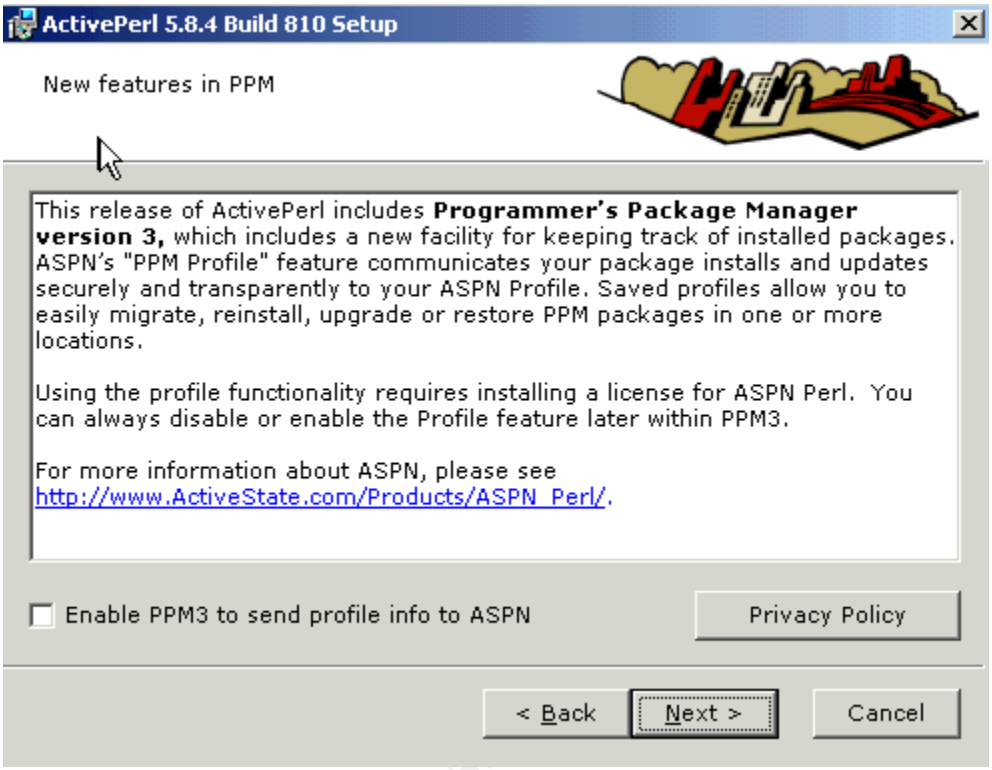
F. Download and Install ActivePerl

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

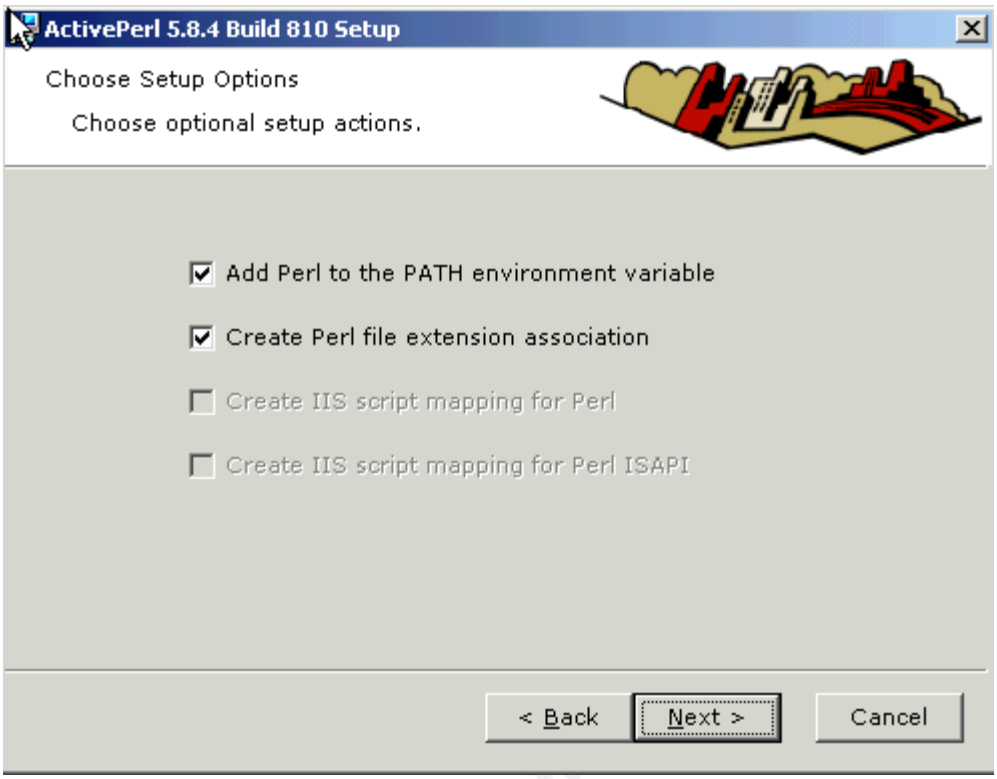
3) Choose **I Accept the terms in the License Agreement** and click **Next**
4) Accept the installation location **C:\Perl** or click **Browse** to select other location



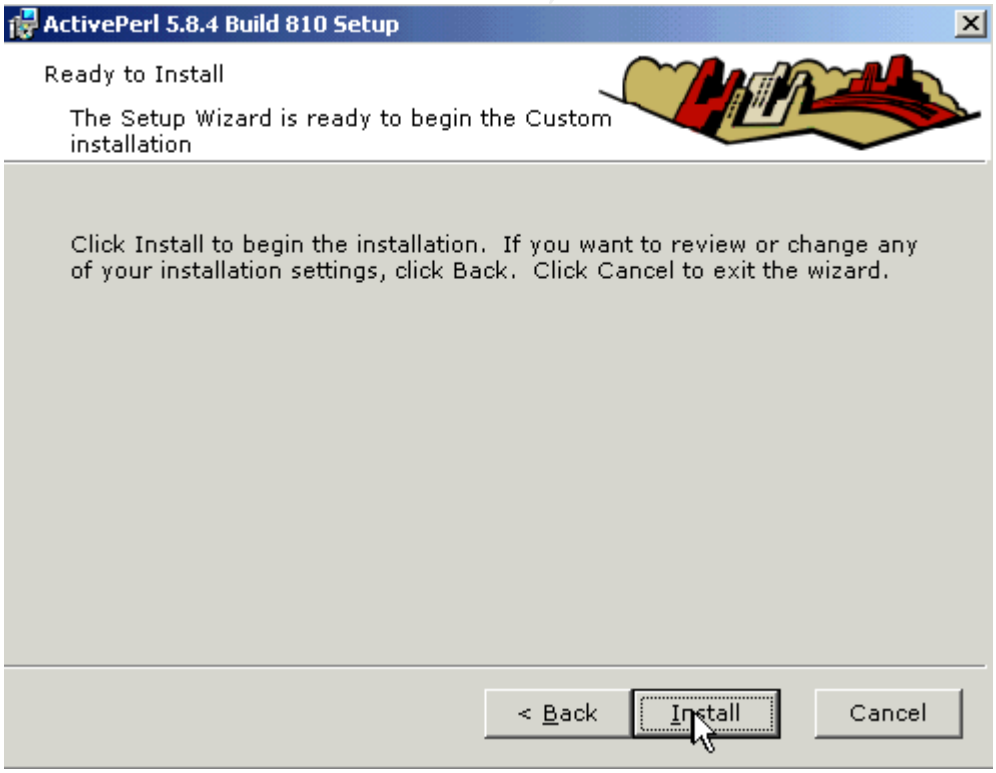
5) Leave the check box **Enable PPM3 to send profile info to ASPN** blank and click **Next**



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**

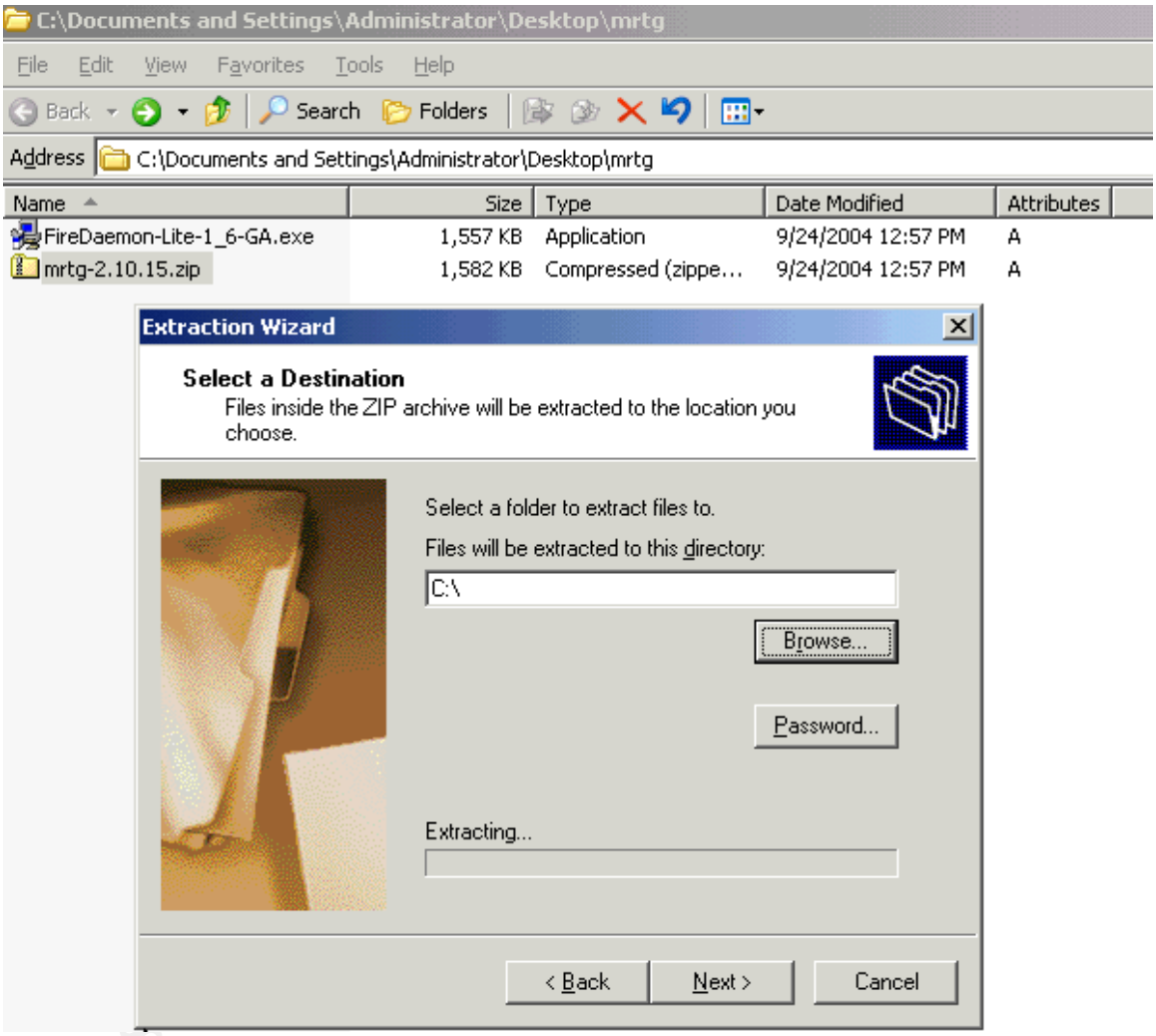


7) Click **Install** to begin the installation

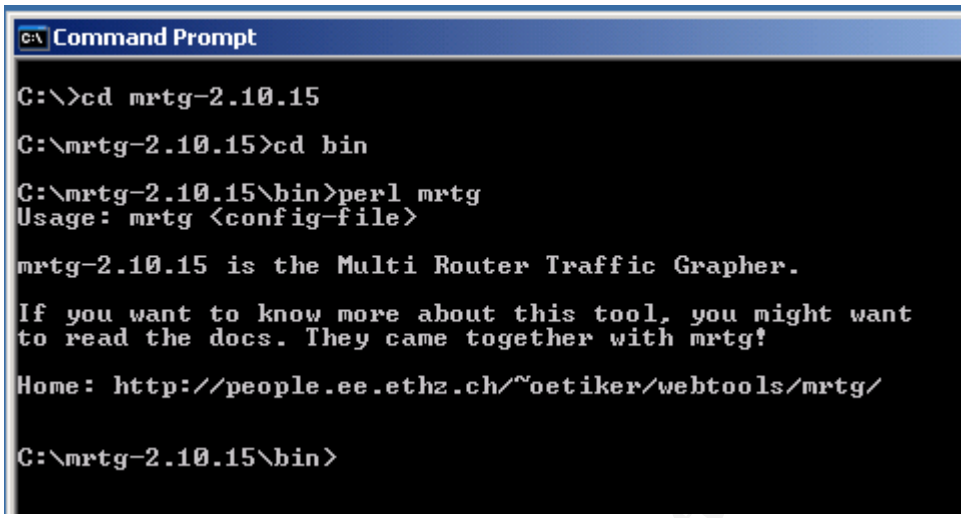


G. Download and Install MRTG

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



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.



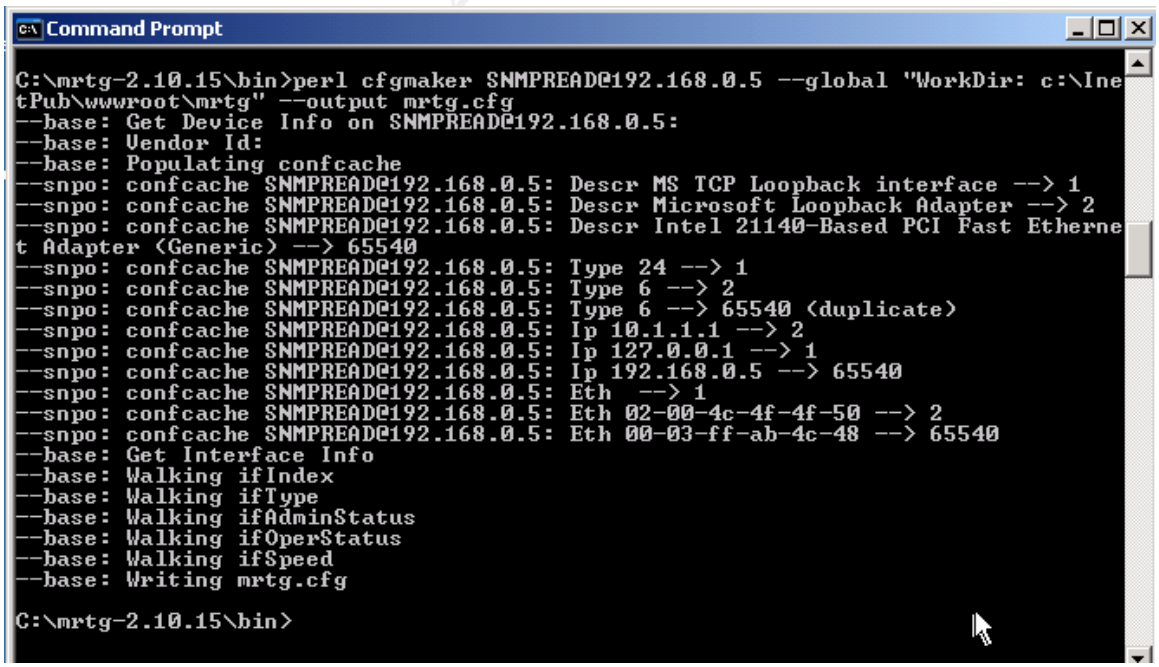
6) MRTG has been successfully installed.

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**
7) 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>
#    <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>
#    <TR><TD>Ip:</TD>         <TD>127.0.0.1 (esc7870-2003.esc7870.vp)</TD></TR>
#  </TABLE>







WorkDir: c:\InetPub\wwwroot\mrtg

###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.
5
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
```

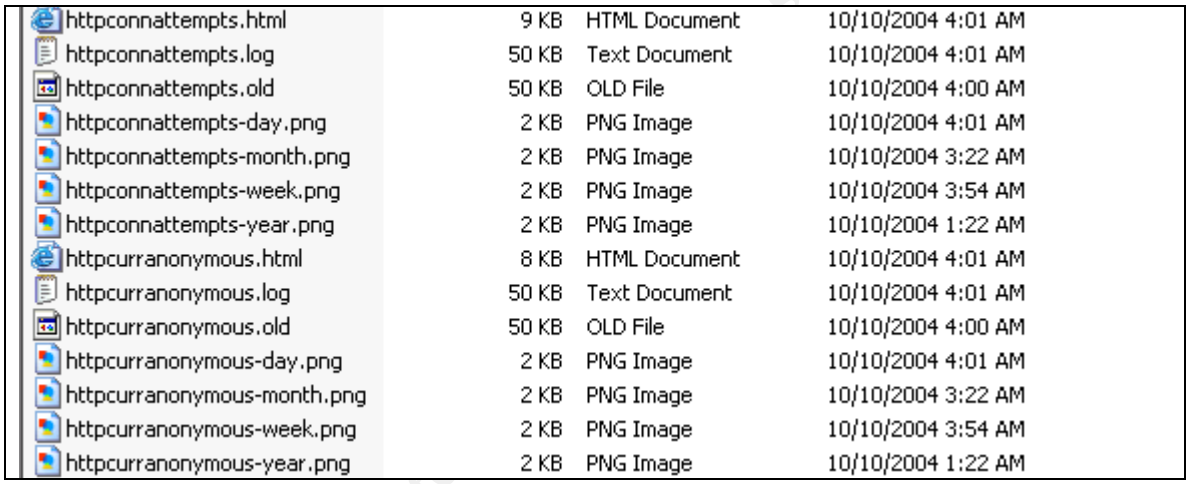
```
Legend2[ftpFilesent]: -
Legend3[ftpFilesent]: -
Legend4[ftpFilesent]: -
LegendI[ftpFilesent]: files:
LegendO[ftpFilesent]: files:
Title[ftpFilesent]: Number of files sent by this FTP Server
PageTop[ftpFilesent]: <H1>Number of files sent by this FTP Server</H1>
Colours[ftpFilesent]: GREEN#00eb0c,BLUE#0000ff,GRAY#AAAAAA,VIOLET#ff00ff
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#AAAAAA,VIOLET#ff00ff
WithPeak[FTP_NumberConnections]: ymw
```

8) 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

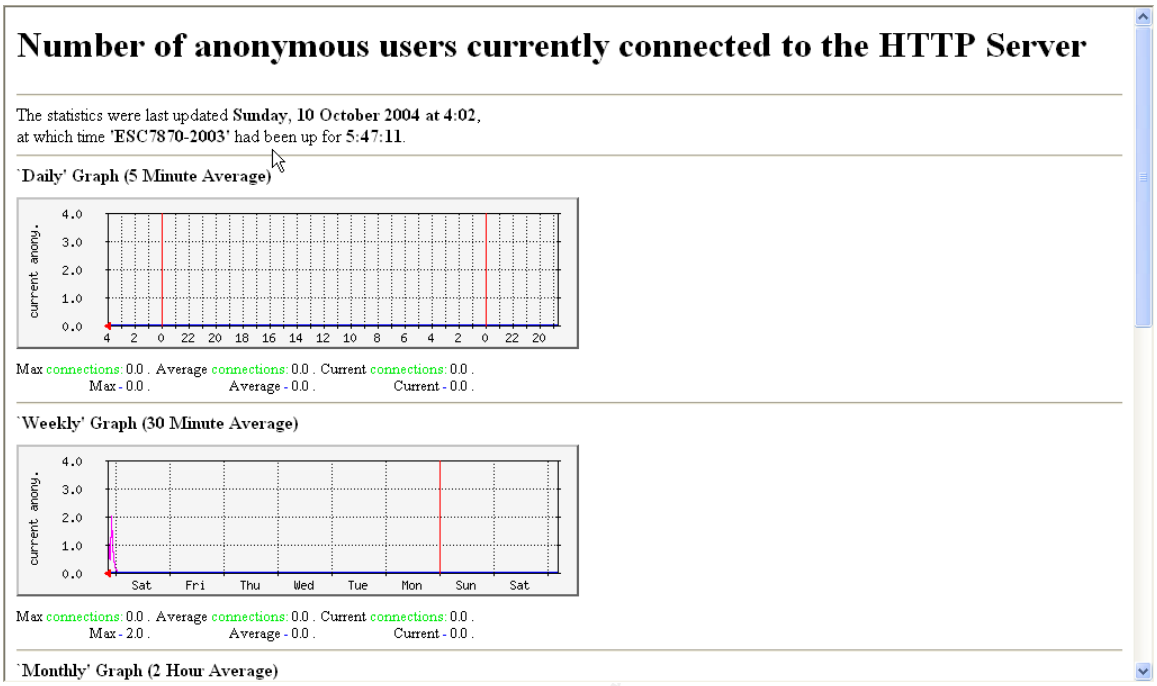
```
perl mrtg mrtg.cfg
```

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

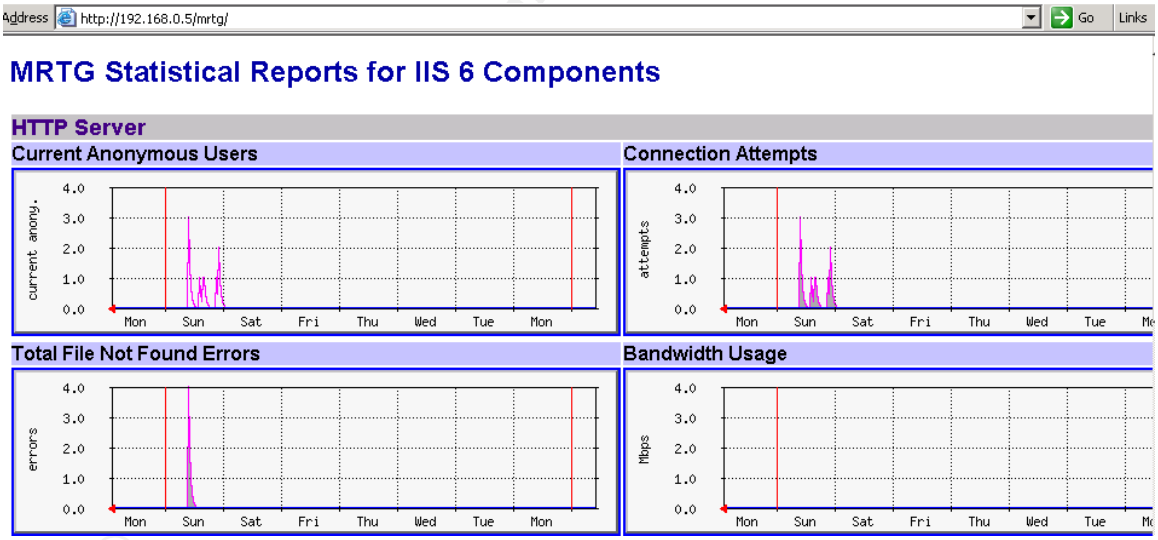


httpconnattempts.html	9 KB	HTML Document	10/10/2004 4:01 AM
httpconnattempts.log	50 KB	Text Document	10/10/2004 4:01 AM
httpconnattempts.old	50 KB	OLD File	10/10/2004 4:00 AM
httpconnattempts-day.png	2 KB	PNG Image	10/10/2004 4:01 AM
httpconnattempts-month.png	2 KB	PNG Image	10/10/2004 3:22 AM
httpconnattempts-week.png	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.

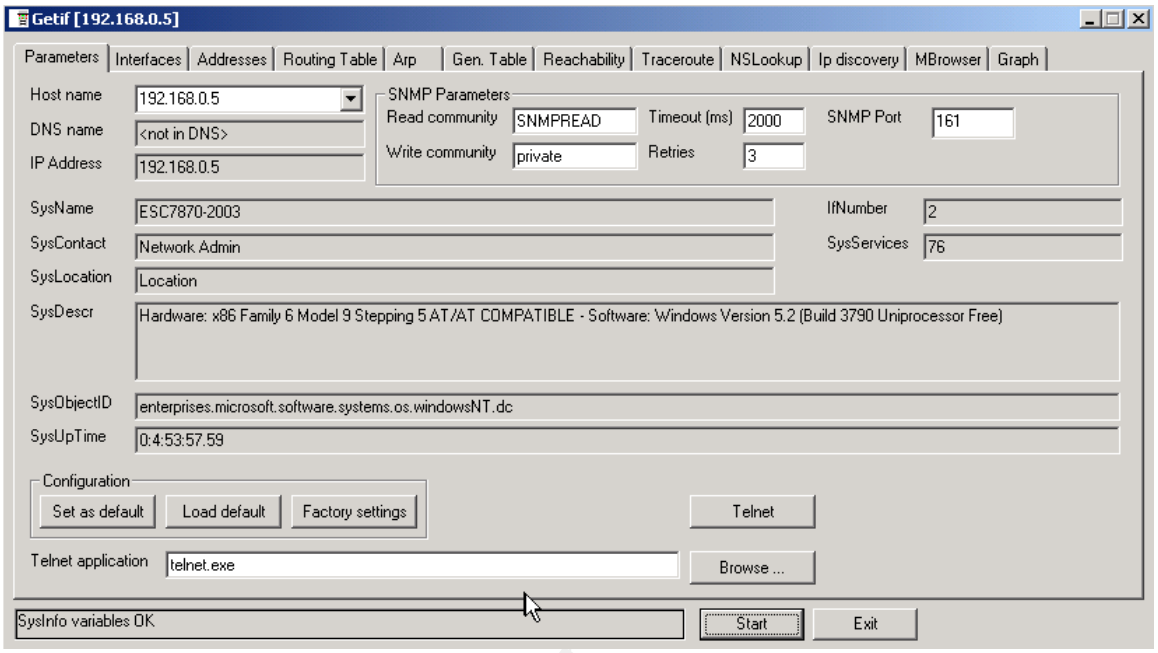


11) Create an html file as a summary file to include a daily graph from all counters

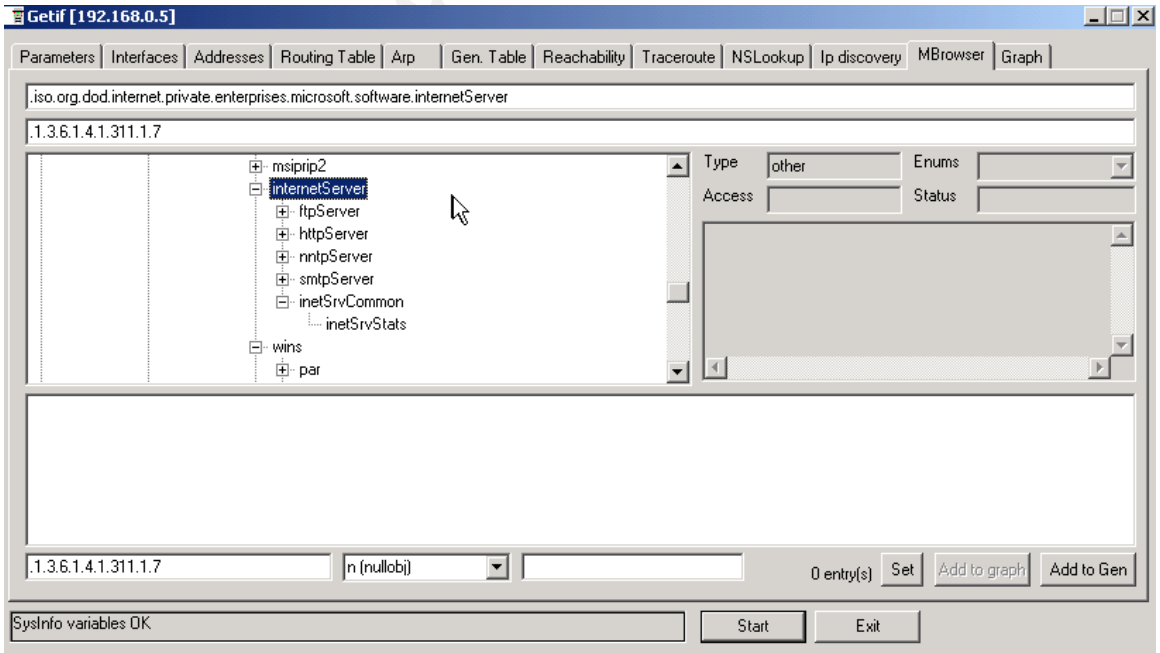


I. How to Access SNMP Counter

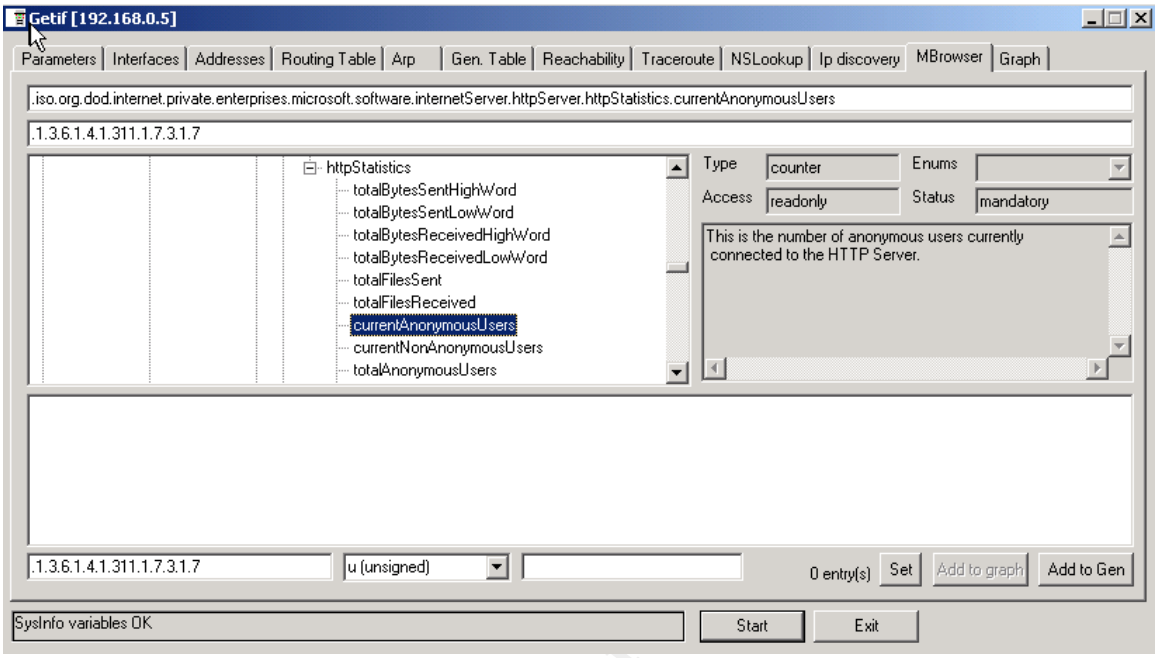
1) Download a program Getif 2.3.1 from http://www.snmp4tpc.com/Files/Tools/SNMP/getif/getif-2.3.1.zip
2) Extract the file and install Getif 2.3.1 to c:\Program Files\Getif 2.3.1
3) Download a collection of MIBs from http://www.wtcs.org/snmp4tpc/FILES/Tools/SNMP/getif/getif-Mibs.zip
4) Extract the getif-Mibs.zip 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:



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

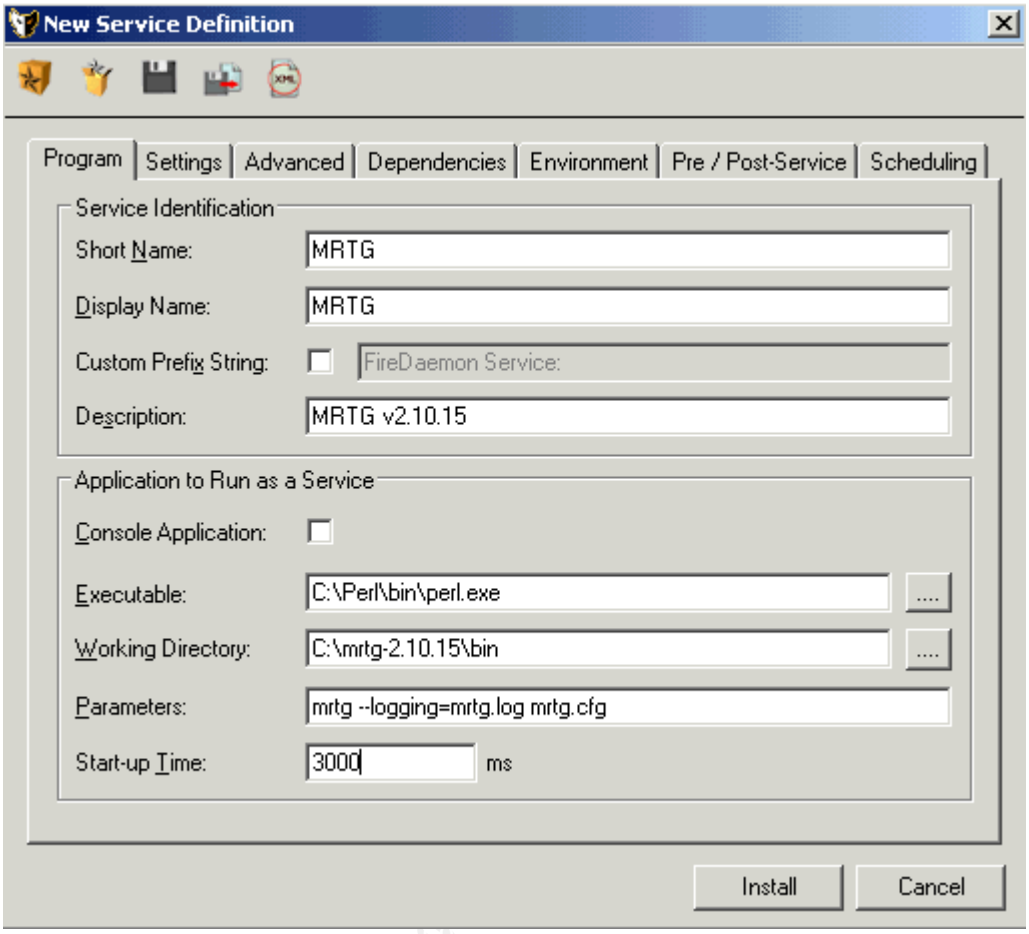


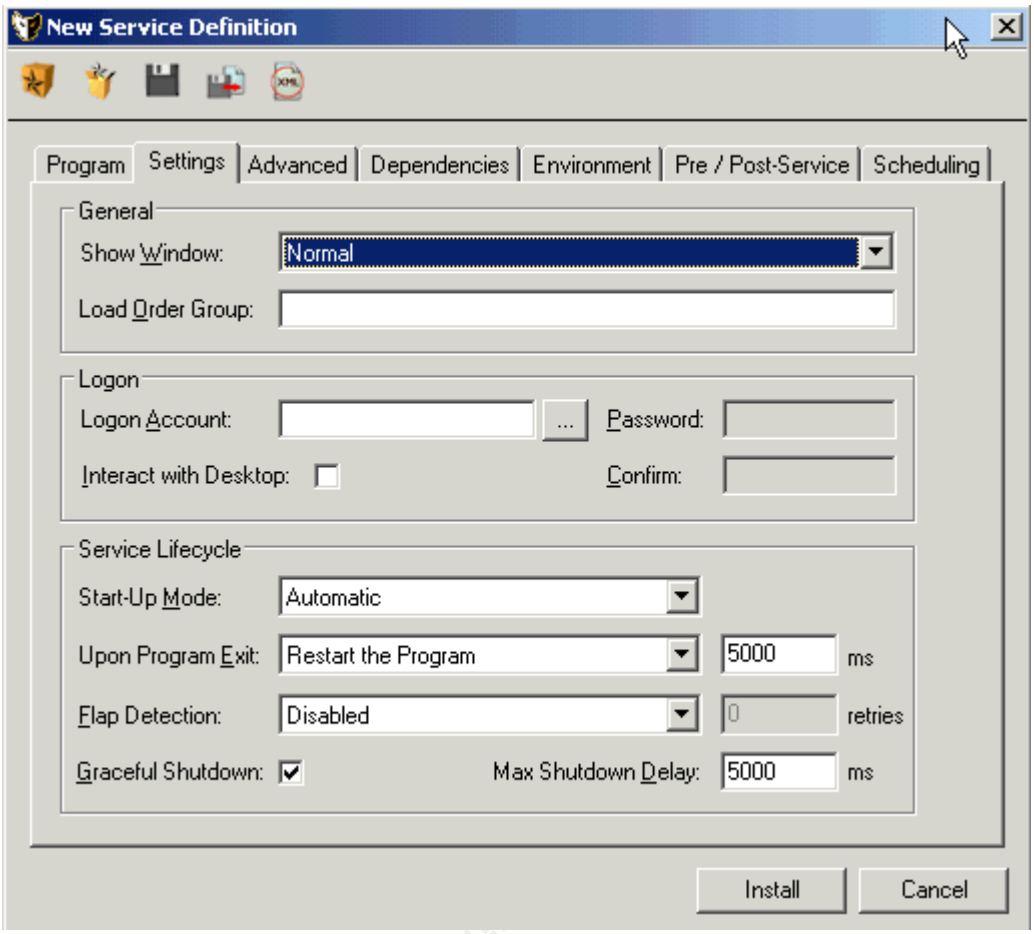
11) Expand httpServer, httpStatistics and select currentAnonymousUsers
12) The associated counter number appears on the top in the input box. Use this number for MRTG config file



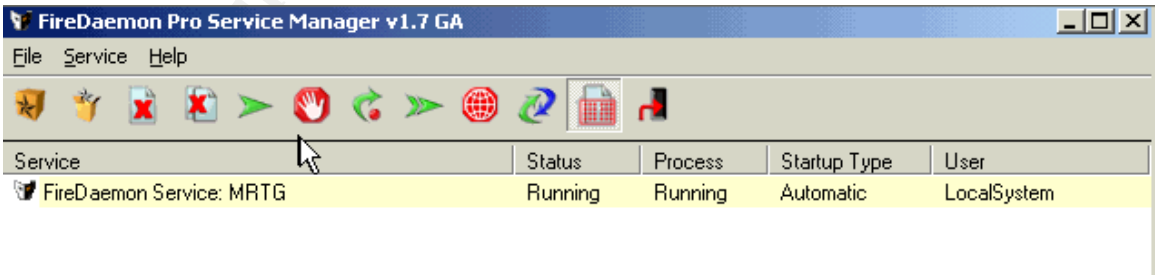
J. Make MRTG To run as a Service

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.
3) 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





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.



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: http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/tips/iis5chk.mspx (June 29, 2000)

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

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

NetCraft. “October 2004 Web Server Survey”. URL: http://news.netcraft.com/archives/2004/10/01/october_2004_web_server_survey.html (October 1, 2004)

SANS. “The SANS Top 20 Internet Security Vulnerabilities”. URL: http://www.sans.org/top20/ (October 8, 2004)

Tabona, Andrew. “Windows 2003 Performance Monitor” URL: http://www.wown.com/articles_tutorials/Windows_2003_Performance_Monitor.html (March 29, 2004)