Evading IDS, Firewalls, and Honeypots

Module 17

Intrusion Detection System

An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.

ICON KEY

🗁 Valuable information

✎ Test your knowledge

💻 Web exercise

🕮 Workbook review

Lab Scenario

Due to a growing number of intrusions and since the Internet and local networks have become so ubiquitous, organizations increasingly implementing various systems that monitor IT security breaches. Intrusion detection systems (IDSes) are those that have recently gained a considerable amount of interest. An IDS is a defense system that detects hostile activities in a network. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including reconnaissance/data collection phases that involve, for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/or block a suspected connection. According to Amoroso, intrusion detection is a "process of identifying and responding to malicious activity targeted at computing and networking resources." In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers) (Source: http://www.windowsecurity.com)

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network intrusion prevention system (IPSes), IDSes, malicious network activity, and log information.

Lab Objectives

The objective of this lab is to help students learn and detect intrusions in a network, log, and view all log files. In this lab, you will learn how to:

- Install and configure Snort IDS
- Run Snort as a service
- Log snort log files to Kiwi Syslog server
- Store snort log files to two output sources simultaneously

🗁 **Tools Demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots**

Lab Environment

To carry out this lab, you need:

- A computer running Windows Server 2012 as a host machine
- A computer running Windows server 2008, Windows 8, or Windows 7 as a virtual machine
- WinPcap drivers installed on the host machine

- Notepad++ installed on the host machine
- Kiwi Syslog Server installed on the host machine
- Active Perl installed on the host machine to run Perl scripts
- Administrative privileges to configure settings and run tools
- A web browser with Internet access

Lab Duration

Time: 40 Minutes

Overview of Intrusion Detection Systems

An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. In addition, organizations use intrusion detection and prevention systems (IDPSes) for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment.

IDPSes are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

TASK 1

Overview

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in using IDSes:

- Detecting Intrusions Using Snort
- Logging Snort Alerts to Kiwi Syslog Server
- Detecting Intruders and Worms using KFSensor Honeypot IDS
- HTTP Tunneling Using HTTPort

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab

1

Detecting Intrusions using Snort

Snort is an open source network intrusion prevention and detection system (IDS/IPS).

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The trade of the intrusion detection analyst is to find possible attacks against their network. The past few years have witnessed significant increases in DDoS attacks on the Internet, prompting network security to become a great concern. Analysts do this by IDS logs and packet captures while corroborating with firewall logs, known vulnerabilities, and general trending data from the Internet. The IDS attacks are becoming more cultured, automatically reasoning the attack scenarios in real time and categorizing those scenarios becomes a critical challenge. These result in huge amounts of data and from this data they must look for some kind of pattern. However, the overwhelming flows of events generated by IDS sensors make it hard for security administrators to uncover hidden attack plans.

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network IPSes, IDSes, malicious network activity, and log information.

Tools Demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots

Lab Objectives

The objective of this lab is to familiarize students with IPSes and IDSes.

In this lab, you need to:

- Install Snort and verify Snort alerts
- Configure and validate snort.conf file
- Test the working of Snort by carrying out an attack test
- Perform intrusion detection
- Configure Oinkmaster

Lab Environment

To carry out this lab, you need:

- A computer running Windows Server 2012 as a host machine
- Windows 7 running on virtual machine as an attacker machine
- WinPcap drivers installed on the host machine
- Notepad++ installed on the host machine
- Kiwi Syslog Server installed on the host machine
- Active Perl installed on the host machine to run Perl scripts
- Administrative privileges to configure settings and run tools

Lab Duration

Time: 30 Minutes

Overview of Intrusion Prevention Systems and Intrusion Detection Systems

You can also download Snort from http://www.snort.org.

An IPS is a **network security** appliance that **monitors** a network and system activities for **malicious** activity. The main functions of IPSes are to **identify** malicious activity, **log information** about said activity, attempt to **block/stop** activity, and report activity.

An IDS is a device or software application that **monitors** network and/or system activities for **malicious** activities or **policy violations** and produces **reports** to a Management Station. It performs intrusion detection and attempt to **stop** detected possible **incidents**.

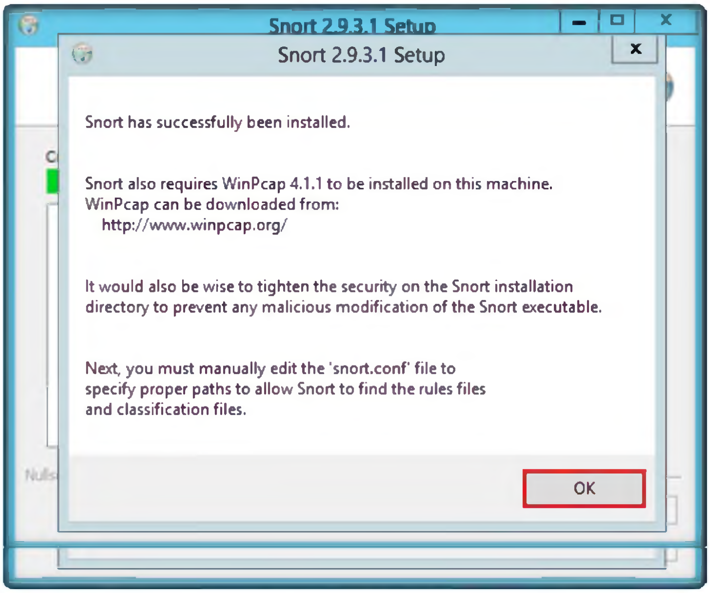
Lab Tasks

TASK 1

Install Snort

1. Start **Windows Server 2012** on the host machine. Install Snort.
2. To install Snort, navigate to **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**.
3. Double-click the **Snort_2_9_3_1_Installer.exe** file. The Snort installation wizard appears.
4. Accept the **License Agreement** and install Snort with the **default options** that appear **step-by-step** in the wizard.
5. A window appears after successful installation of Snort. Click the **Close** button.
6. Click **OK** to exit the **Snort Installation** window.

Snort is an open source network intrusion prevention and detection system (IDS/IPS).



Snort has successfully been installed.

Snort also requires WinPcap 4.1.1 to be installed on this machine.
WinPcap can be downloaded from:
http://www.winpcap.org/

It would also be wise to tighten the security on the Snort installation directory to prevent any malicious modification of the Snort executable.

Next, you must manually edit the 'snort.conf' file to specify proper paths to allow Snort to find the rules files and classification files.

Figure 1.1: Snort Successful Installation Window

7. Snort requires **WinPcap** to be installed on your machine.
8. Install WinPcap by navigating to **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**, and double-clicking **WinPcap_4_1_2.exe**.
9. By default, Snort installs itself in **C:\Snort** (C:\ or D:\ depending upon the disk drive in which OS installed).
10. Register on the Snort website **https://www.snort.org/signup** in order to download Snort Rules. After registration comples it will automatically redirect to a download page.
11. Click the **Get Rules** button to download the latest rules. In this lab we have downloaded **snortrules-snapshot-2931.tar.gz**.
12. Extract the downloaded rules and copy the extracted folder in this path: **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**.
13. Rename the extracted folder to **snortrules**.
14. Now go to the **etc** folder in the specified location **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules\etc** of the extracted Snort rules, copy the **snort.conf** file, and paste this file in **C:\Snort\etc**.
15. The **Snort.conf** file is already present in **C:\Snort\etc**; replace this file with the Snort rules **Snort.conf** file.
16. Copy the **so_rules** folder from **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules** and paste it in **C:\Snort**.

WinPcap is a tool for link-layer network access that allows applications to capture and transmit network packets bypass the protocol stack.

17. Replace the **preproc_rules** folder from **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules** and paste it in **C:\Snort**.

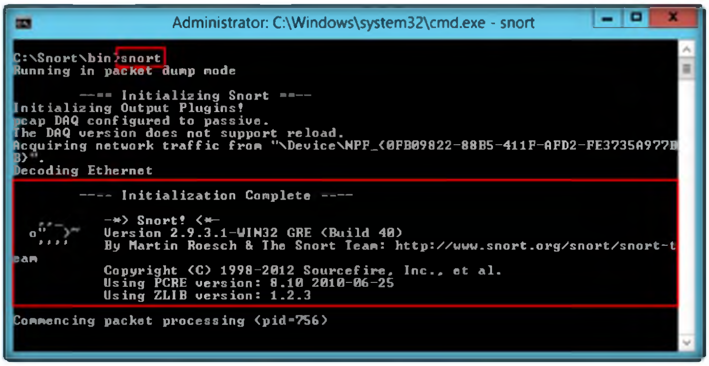
18. Copy all the files from this location: **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules\rules** to **C:\Snort\rules**.

TASK 2

Verify Snort Alert

19. Now navigate to **C:\Snort** and right-click folder **bin**, and click **CmdHere** from the context menu to open it in a command prompt.

20. Type **snort** and press **Enter**.



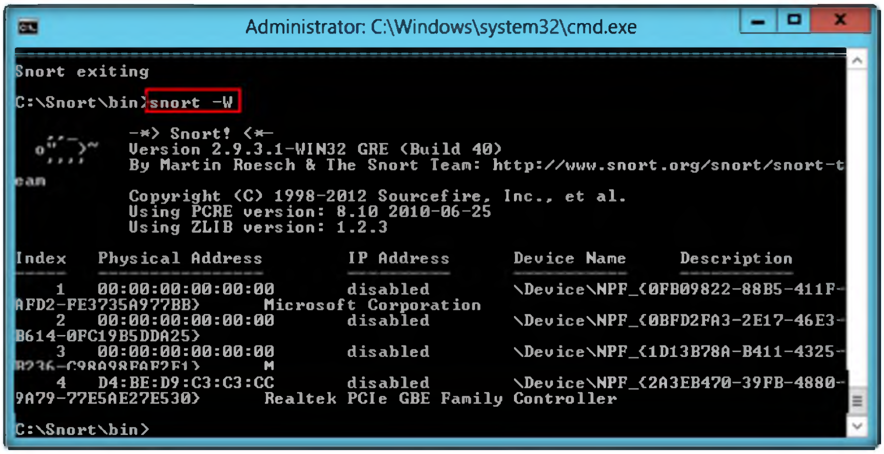
```
C:\Snort\bin>snort
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{0FB09822-88B5-411F-AFD2-FE3735A977B
B}".
Decoding Ethernet

        --== Initialization Complete ==--

           -*> Snort! <*-
  o"  )~   Version 2.9.3.1-WIN32 GRE (Build 40)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 1998-2012 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Commencing packet processing (pid=756)
```

Figure 1.2: Snort Basic Command

To print out the TCP/IP packet headers to the screen (i.e. sniffer mode), type: snort –v.

21. The **Initialization Complete** message displays. Press **Ctrl+C**. Snort exits and comes back to **C:\Snort\bin**.

22. Now type **snort –W**. This command lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default.



```
Snort exiting

C:\Snort\bin>snort -W

           -*> Snort! <*-
  o"  )~   Version 2.9.3.1-WIN32 GRE (Build 40)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 1998-2012 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{0FB09822-88B5-411F-
AFD2-FE3735A977BB}      Microsoft Corporation
    2   00:00:00:00:00:00       disabled        \Device\NPF_{0BFD2FA3-2E17-46E3-
B614-0FC19B5DDA25}
    3   00:00:00:00:00:00       disabled        \Device\NPF_{1D13B78A-B411-4325-
B236-C9BA9BFAF2F1}      M
    4   D4:BE:D9:C3:C3:CC       disabled        \Device\NPF_{2A3EB470-39FB-4880-
9A79-77E5AE27E530}      Realtek PCIe GBE Family Controller

C:\Snort\bin>
```

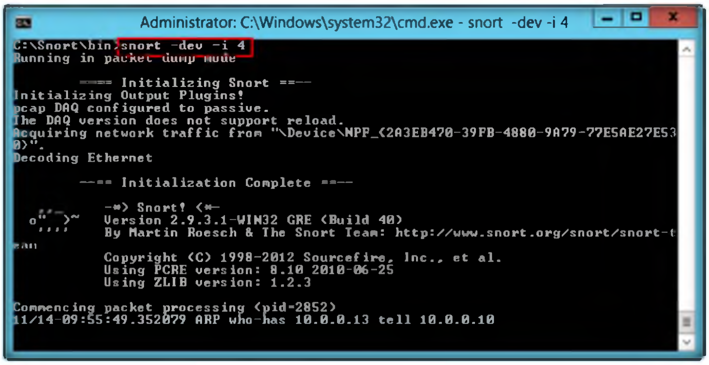
Figure 1.3: Snort -W Command

23. Observe your Ethernet Driver **index number** and write it down; in this lab, the Ethernet Driver index number is **1**.

24. To enable the Ethernet Driver, in the command prompt, type **snort –dev –i 2** and press **Enter**.

25. You see a rapid scroll text in the command prompt. It means that the Ethernet Driver is enabled and working properly.

To specify a log into logging directory, type snort –dev –l /logdirectorylocationand, Snort automatically knows to go into packet logger mode.

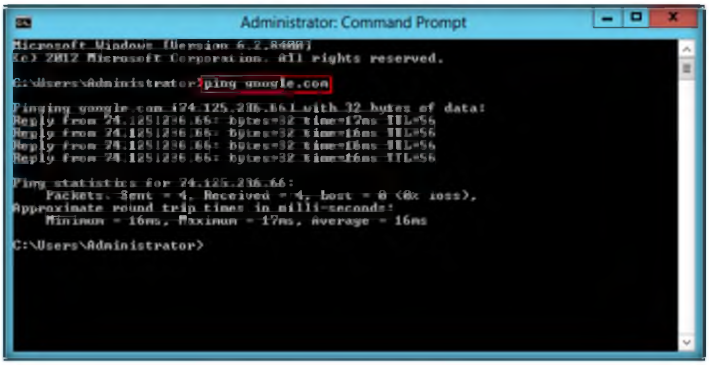

Administrator: C:\Windows\system32\cmd.exe - snort -dev -i 4

```
C:\Snort\bin>snort -dev -i 4
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{2A3EB470-39FB-4880-9A79-77E5AE27E53
0}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.3.1-WIN32 GRE (Build 40)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 1998-2012 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Commencing packet processing (pid=2852)
11/14-09:55:49.352079 ARP who-has 10.0.0.13 tell 10.0.0.10
```

Figure 1.4: Snort –dev –i 4 Command

26. Leave the Snort command prompt window open, and launch another command prompt window.

27. In a new command prompt, type **ping google.com** and press **Enter**.

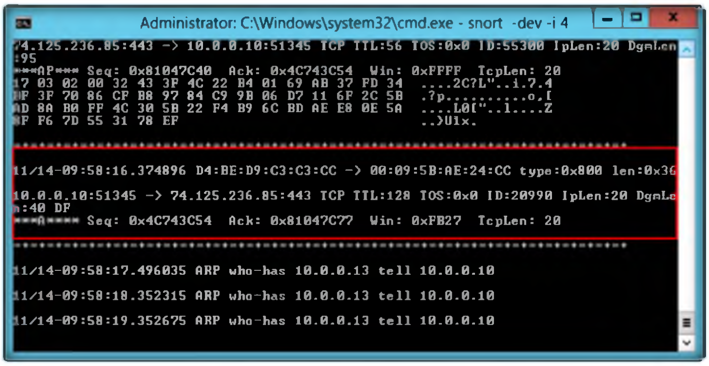


```
Microsoft Windows [Version 6.2.8400]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.com

Pinging google.com [74.125.236.66] with 32 bytes of data:
Reply from 74.125.236.66: bytes=32 time=17ms TTL=56
Reply from 74.125.236.66: bytes=32 time=16ms TTL=56
Reply from 74.125.236.66: bytes=32 time=16ms TTL=56
Reply from 74.125.236.66: bytes=32 time=16ms TTL=56

Ping statistics for 74.125.236.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 17ms, Average = 16ms

C:\Users\Administrator>
```

Figure 1.5: Ping google.com Command

Ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list

28. This ping command triggers a Snort alert in the Snort command prompt with rapid scrolling text.


Administrator: C:\Windows\system32\cmd.exe - snort -dev -i 4

```
74.125.236.85:443 -> 10.0.0.10:51345 TCP TTL:56 TOS:0x0 ID:55300 IpLen:20 DgmLen
:95
***AP*** Seq: 0x81047C40  Ack: 0x4C743C54  Win: 0xFFFF  TcpLen: 20
17 03 02 00 32 43 3F 4C 22 B4 01 69 AB 37 FD 34  .....2C?L"..i.7.4
DF 3F 70 86 CF B8 97 84 C9 9B 06 D7 11 6F 2C 5B  .?p..........o,[
AD 8A B0 FF 4C 30 5B 22 F4 B9 6C BD AE E8 0E 5A  ....L0["..l....Z
8F F6 7D 55 31 78 EF                             ..}U1x.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/14-09:58:16.374896 D4:BE:D9:C3:C3:CC -> 00:09:5B:AE:24:CC type:0x800 len:0x36

10.0.0.10:51345 -> 74.125.236.85:443 TCP TTL:128 TOS:0x0 ID:20990 IpLen:20 DgmLe
n:40 DF
***A**** Seq: 0x4C743C54  Ack: 0x81047C77  Win: 0xFB27  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/14-09:58:17.496035 ARP who-has 10.0.0.13 tell 10.0.0.10

11/14-09:58:18.352315 ARP who-has 10.0.0.13 tell 10.0.0.10

11/14-09:58:19.352675 ARP who-has 10.0.0.13 tell 10.0.0.10
```

Figure 1.6: Snort Showing Captured Google Request

To enable Network Intrusion Detect ion System (NIDS) mode so that you don't record every single packet sent down the wire, type: snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf.

29. Close both command prompt windows. The verification of Snort installation and triggering alert is complete, and Snort is working correctly in verbose mode.

TASK 3

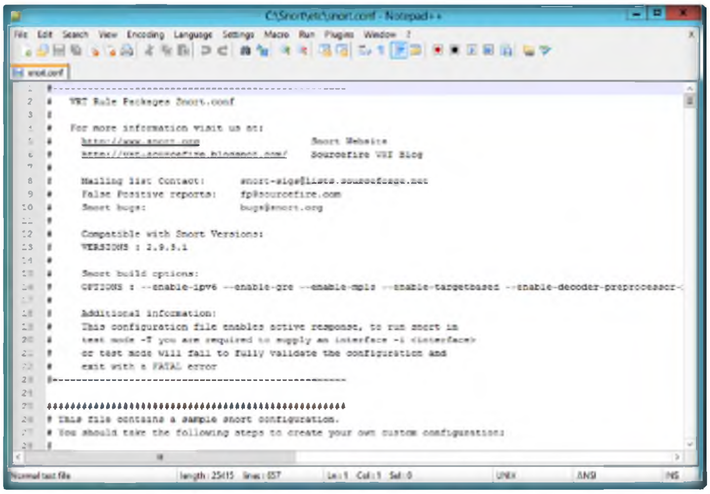
Configure snort.conf File

30. Configure the **snort.conf** file located at **C:\Snort\etc**.

31. Open the **snort.conf** file with Notepad++.

32. The **snort.conf** file opens in Notepad++ as shown in the following screenshot.

Make sure to grab the rules for the version you are installing Snort for.


C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
snort.conf
Normal text file
length : 25415 lines : 657
Ln : 1 Col : 1 Sel : 0
UNIX
ANSI
INS

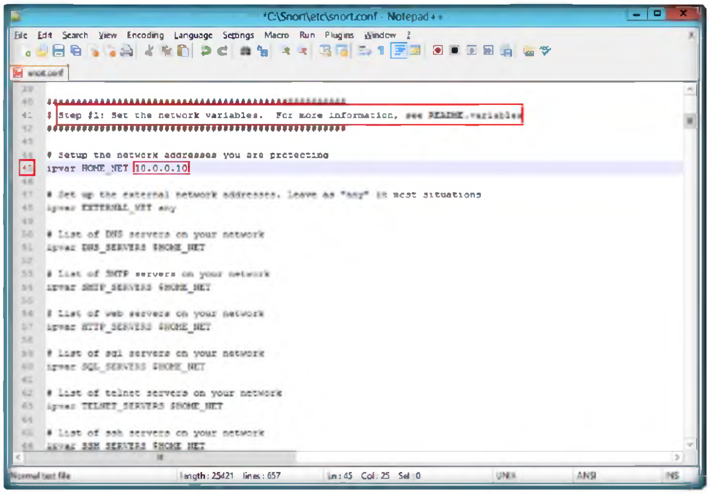
```
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#     http://www.snort.org                   Snort Website
#     http://vrt.sourcefire.blogspot.com/    Sourcefire VRT Blog
#
#     Mailing list Contact:      snort-sigs@lists.sourceforge.net
#     False Positive reports:    fp@sourcefire.com
#     Snort bugs:                bugs@snort.org
#
#     Compatible with Snort Versions:
#     VERSIONS : 2.9.5.1
#
#     Snort build options:
#     OPTIONS : --enable-ipv6 --enable-gre --enable-mpls --enable-targetbased --enable-decoder-preprocessor-
#
#     Additional information:
#     This configuration file enables active response, to run snort in
#     test mode -T you are required to supply an interface -i <interface>
#     or test mode will fail to fully validate the configuration and
#     exit with a FATAL error
#--------------------------------------------------

###################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
```

Figure 1.7: Configuring Snort.conf File in Notepad++

Log packets in tcpdump format and to produce minimal alerts, type: snort -b -A fast -c snort.conf.

33. Scroll down to the **Step #1: Set the network variables** section (Line 41) of snort.conf file. In the **HOME_NET** line, replace any with the IP addresses (Line 45) of the machine where Snort is running.

Notepad++ is a free source code editor and Notepad replacement that supports several languages. It runs in the MS Windows environment.


*C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
snort.conf
Normal text file
length : 25421 lines : 657
Ln : 45 Col : 25 Sel : 0
UNIX
ANSI
INS

```
39
40 ###################################################
41 # Step #1: Set the network variables.  For more information, see README.variables
42 ###################################################
43
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET 10.0.0.10
46
47 # Set up the external network addresses. Leave as "any" in most situations
48 ipvar EXTERNAL_NET any
49
50 # List of DNS servers on your network
51 ipvar DNS_SERVERS $HOME_NET
52
53 # List of SMTP servers on your network
54 ipvar SMTP_SERVERS $HOME_NET
55
56 # List of web servers on your network
57 ipvar HTTP_SERVERS $HOME_NET
58
59 # List of sql servers on your network
60 ipvar SQL_SERVERS $HOME_NET
61
62 # List of telnet servers on your network
63 ipvar TELNET_SERVERS $HOME_NET
64
65 # List of ssh servers on your network
66 ipvar SSH_SERVERS $HOME_NET
```

Figure 1.8: Configuring Snort.conf File in Notepad++

34. Leave the **EXTERNAL_NET any** line as it is.

The element 'any' can be used to match all IPs, although 'any' is not allowed. Also, negated IP ranges that are more general than non-negated IP ranges are not allowed.

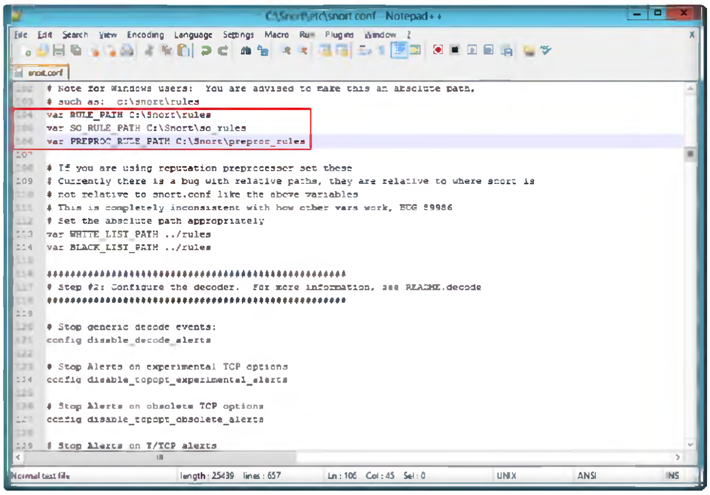
35. If you have a **DNS Server**, then make changes in the **DNS_SERVERS** line by replacing **$HOME_NET** with your DNS Server IP address; otherwise, leave this line as it is.

36. The same applies to SMTP_SERVERS, HTTP_SERVERS, SQL_SERVERS, TELNET_SERVERS, and SSH_SERVERS.

37. Remember that if you don't have any servers running on your machine, leave the line as it is. **DO NOT** make any changes in that line.

38. Scroll down to **RULE_PATH** (Line 104). In Line 104 replace **../rules** with **C:\Snort\rules**, in Line 105 **../so_rules** replace with **C:\Snort\so_rules**, and in Line 106 replace **../preproc_rules** with **C:\Snort\preproc_rules**.

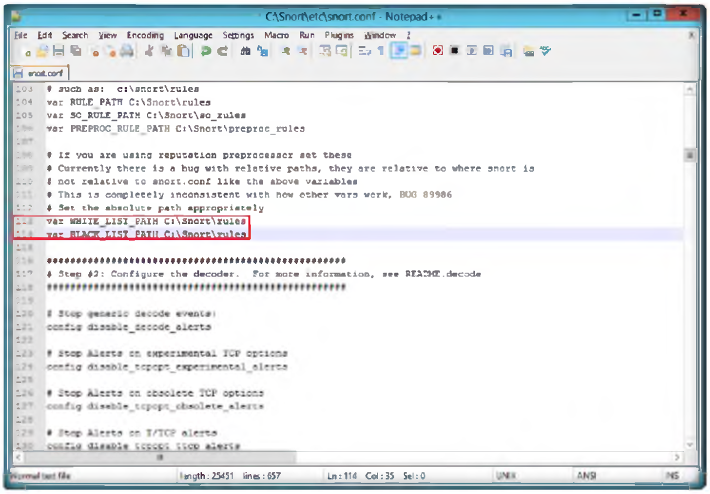
Rule variable names can be modified in several ways. You can define meta-variables using the $ operator. These can be used with the variable modifier operators ? and -


C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
snort.conf
Normal text file
length : 25439 lines : 657
Ln : 106 Col : 45 Sel : 0
UNIX
ANSI
INS

```
102 # Note for Windows users:  You are advised to make this an absolute path,
103 # such as:  c:\snort\rules
104 var RULE_PATH C:\Snort\rules
105 var SO_RULE_PATH C:\Snort\so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
107
108 # If you are using reputation preprocessor set these
109 # Currently there is a bug with relative paths, they are relative to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG 89986
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH ../rules
114 var BLACK_LIST_PATH ../rules
115
116 ###################################################
117 # Step #2: Configure the decoder.  For more information, see README.decode
118 ###################################################
119
120 # Stop generic decode events:
121 config disable_decode_alerts
122
123 # Stop Alerts on experimental TCP options
124 config disable_tcpopt_experimental_alerts
125
126 # Stop Alerts on obsolete TCP options
127 config disable_tcpopt_obsolete_alerts
128
129 # Stop Alerts on T/TCP alerts
```

Figure 1.9: Configuring Snort.conf File in Notepad++

39. In Line 113 and 114 replace **../rules** with **C:\Snort\ rules**.


C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
snort.conf
Normal text file
length : 25451 lines : 657
Ln : 114 Col : 35 Sel : 0
UNIX
ANSI
INS

```
103 # such as:  c:\snort\rules
104 var RULE_PATH C:\Snort\rules
105 var SO_RULE_PATH C:\Snort\so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
107
108 # If you are using reputation preprocessor set these
109 # Currently there is a bug with relative paths, they are relative to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG 89986
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH C:\Snort\rules
114 var BLACK_LIST_PATH C:\Snort\rules
115
116 ###################################################
117 # Step #2: Configure the decoder.  For more information, see README.decode
118 ###################################################
119
120 # Stop generic decode events:
121 config disable_decode_alerts
122
123 # Stop Alerts on experimental TCP options
124 config disable_tcpopt_experimental_alerts
125
126 # Stop Alerts on obsolete TCP options
127 config disable_tcpopt_obsolete_alerts
128
129 # Stop Alerts on T/TCP alerts
130 config disable_tcpopt_ttcp_alerts
```

Figure 1.10: Configuring Snort.conf File in Notepad++

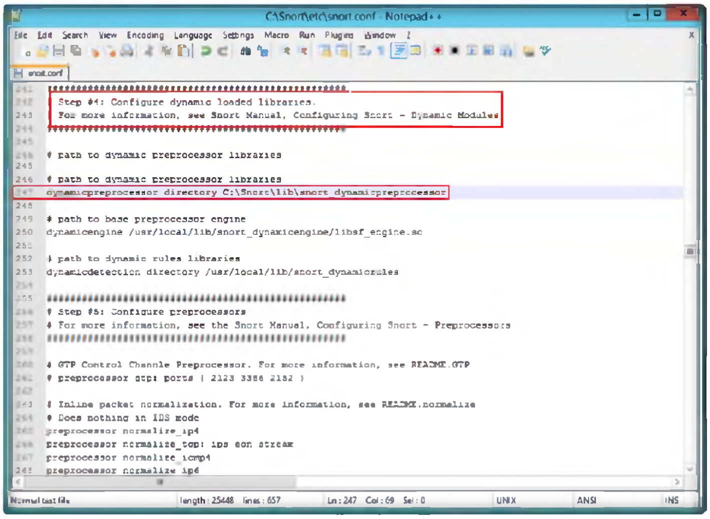
40. Navigate to **C:\Snort\rules** and create two files and name them **white_list.rules** and **black_list.rules** make sure the two files extensions are **.rules**.

41. Scroll down to **Step #4: Configure dynamic loaded libraries** section (Line 242). Configure **dynamic loaded libraries** in this section.

42. At path to dynamic preprocessor libraries (Line 247), replace **/usr/local/lib/snort_dynamicpreprocessor/** with your dynamic preprocessor libraries folder location.

43. In this lab, dynamic preprocessor libraries are located at **C:\Snort\lib\snort_dynamicpreprocessor**.

The include keyword allows other rule files to be included within the rule file indicated on the Snort command line. It works much like an #include from the C programming language, reading the contents of the named file and adding the contents in the place where the include statement appears in the file.

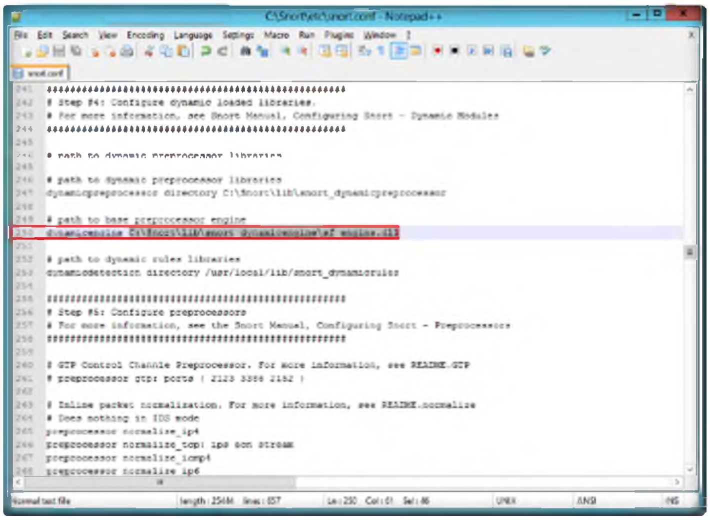


```
###################################################
 Step #4: Configure dynamic loaded libraries.
 For more information, see Snort Manual, Configuring Snort - Dynamic Modules
###################################################

# path to dynamic preprocessor libraries

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so

# path to dynamic rules libraries
dynamicdetection directory /usr/local/lib/snort_dynamicrules

###################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
###################################################

# GTP Control Channle Preprocessor. For more information, see README.GTP
# preprocessor gtp: ports { 2123 3386 2152 }

# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
preprocessor normalize_ip4
preprocessor normalize_tcp: ips ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
```

Figure 1.11: Configuring Snort.conf File in Notepad++

Preprocessors are loaded and configured using the 'preprocessor' keyword. The format of the preprocessor directive in the Snort rules file is: preprocessor <name>: <options>.

44. At path to base preprocessor (or dynamic) engine (Line 250), replace **/usr/local/lib/snort_dynamicengine/libsf_engine.so** with your base preprocessor engine **C:\Snort\lib\snort_dynamicengine\sf_engine.dll**.



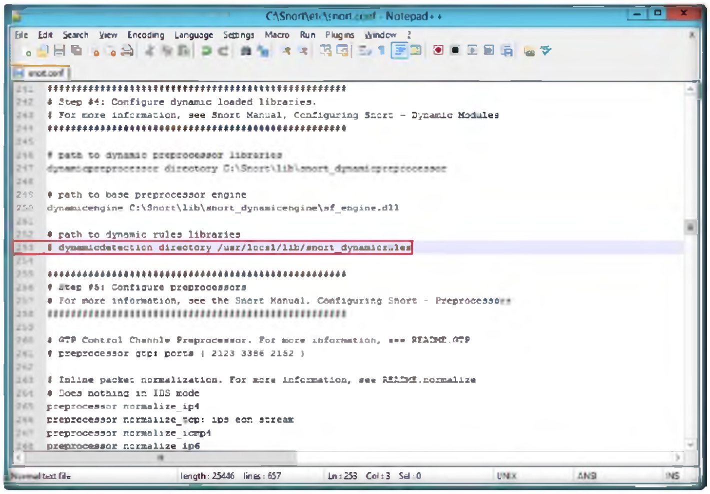
```
###################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
###################################################

# path to dynamic preprocessor libraries

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
dynamicdetection directory /usr/local/lib/snort_dynamicrules

###################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
###################################################

# GTP Control Channle Preprocessor. For more information, see README.GTP
# preprocessor gtp: ports { 2123 3386 2152 }

# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
preprocessor normalize_ip4
preprocessor normalize_tcp: ips ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
```

Figure 1.12: Configuring Snort.conf File in Notepad++

Preprocessors allow the functionality of Snort to be extended by allowing users and programmers to drop modular plug-ins into Snort fairly easily.

45. **Comment** (**#**) the dynamic rules libraries line as you already configured the libraries in dynamic preprocessor libraries (Line 253).

Note: Preprocessor code is run before the detection engine is called, but after the packet has been decoded. The packet can be modified or analyzed in an out-of-band manner using this mechanism.


C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
snort.conf
Normal text file
length : 25446 lines : 657
Ln : 253 Col : 3 Sel : 0
UNIX
ANSI
INS

```
###################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
###################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
# dynamicdetection directory /usr/local/lib/snort_dynamicrules

###################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
###################################################

# GTP Control Channle Preprocessor. For more information, see README.GTP
# preprocessor gtp: ports { 2123 3386 2152 }

# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
preprocessor normalize_ip4
preprocessor normalize_tcp: ips ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
```

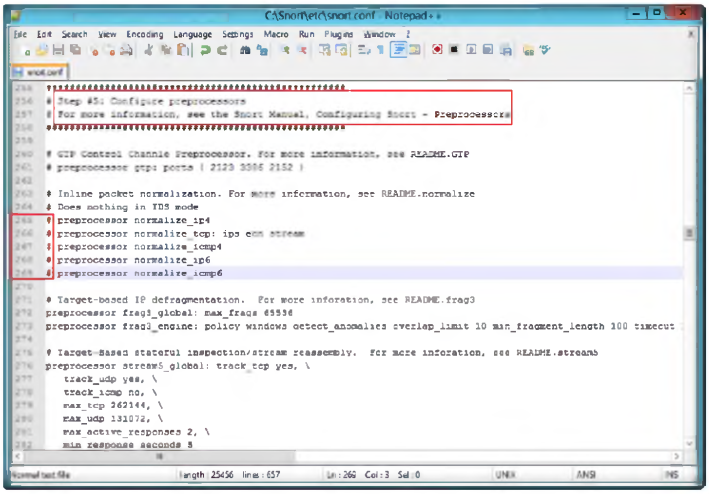
Figure 1.13: Configuring Snort.conf File in Notepad++

46. Scroll down to **Step #5: Configure Preprocessors** section (Line 256), the listed preprocessor. Do nothing in IDS mode, but generate errors at runtime.

IPs may be specified individually, in a list, as a CIDR block, or any combination of the three.

47. Comment all the preprocessors listed in this section by adding **# before** each preprocessors.

Many configuration and command line options of Snort can be specified in the configuration file. Format: config <directive> [: <value>]


C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
snort.conf
Normal text file
length : 25456 lines : 657
Ln : 269 Col : 3 Sel : 0
UNIX
ANSI
INS

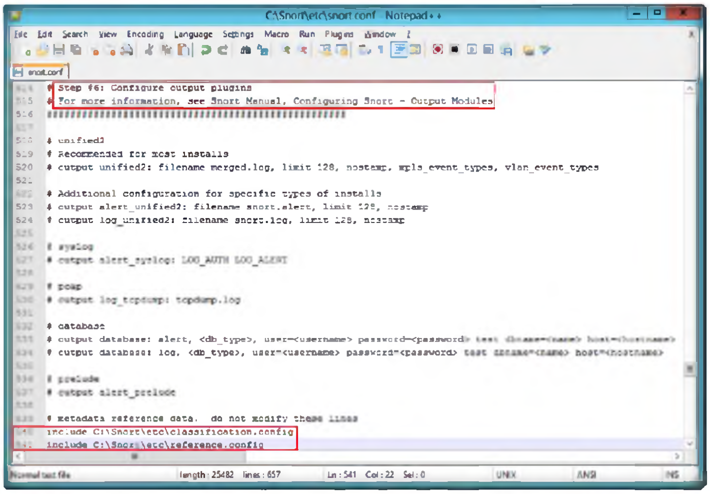
```
###################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
###################################################

# GTP Control Channle Preprocessor. For more information, see README.GTP
# preprocessor gtp: ports { 2123 3386 2152 }

# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
#preprocessor normalize_ip4
#preprocessor normalize_tcp: ips ecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6

# Target-based IP defragmentation.  For more inforation, see README.frag3
preprocessor frag3_global: max_frags 65536
preprocessor frag3_engine: policy windows detect_anomalies overlap_limit 10 min_fragment_length 100 timeout

# Target-Based stateful inspection/stream reassembly.  For more inforation, see README.stream5
preprocessor stream5_global: track_tcp yes, \
   track_udp yes, \
   track_icmp no, \
   max_tcp 262144, \
   max_udp 131072, \
   max_active_responses 2, \
   min_response_seconds 5
```

Figure 1.14: Configuring Snort.conf File in Notepad++

48. Scroll down to **Step #6: Configure output plugins** (Line 514). In this step, provide the location of the **classification.config** and **reference.config** files.

49. These two files are in **C:\Snort\etc**. Provide this location of files in configure output plugins (in Lines 540 and 541).

The frag3 preprocessor is a target-based IP defragmentation module for Snort.


C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
snort.conf

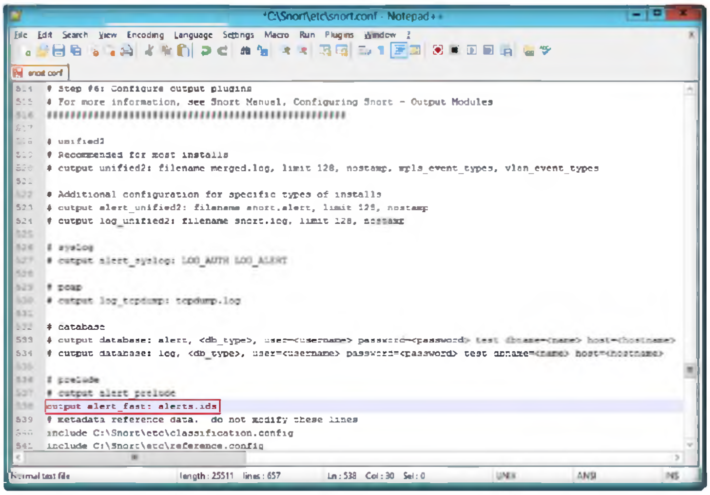
```
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
###################################################

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types

# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
# output alert_syslog: LOG_AUTH LOG_ALERT

# pcap
# output log_tcpdump: tcpdump.log

# database
# output database: alert, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>
# output database: log, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>

# prelude
# output alert_prelude

# metadata reference data.  do not modify these lines
include C:\Snort\etc\classification.config
include C:\Snort\etc\reference.config
```

Figure 1.15: Configuring Snort.conf File in Notepad++

Figure 1.15: Configuring Snort.conf File in Notepad++

50. In this **step #6**, add the line **output alert_fast: alerts.ids**, for Snort to dump all logs in the **alerts.ids** file.

Note: 'ipvar's are enabled only with IPv6 support. Without IPv6 support, use a regular 'var.'


*C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
snort.conf

```
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
###################################################

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types

# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
# output alert_syslog: LOG_AUTH LOG_ALERT

# pcap
# output log_tcpdump: tcpdump.log

# database
# output database: alert, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>
# output database: log, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>

# prelude
# output alert_prelude
output alert_fast: alerts.ids
# metadata reference data.  do not modify these lines
include C:\Snort\etc\classification.config
include C:\Snort\etc\reference.config
```

Figure 1.16: Configuring Snort.conf File in Notepad++

51. By default, the **C:\Snort\log** folder is empty, without any files in it. Go to the **C:\Snort\log** folder, and create a new text file with the name **alerts.ids**.

52. Ensure that extension of that file is **.ids**.

Frag3 is intended as a replacement for the frag2 defragmentation module and was designed with the following goals:

1. Faster execution than frag2 with less complex data management.
2. Target-based host modeling anti-evasion techniques.

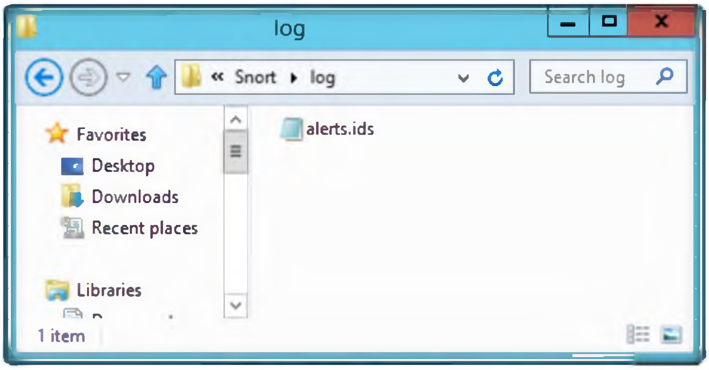


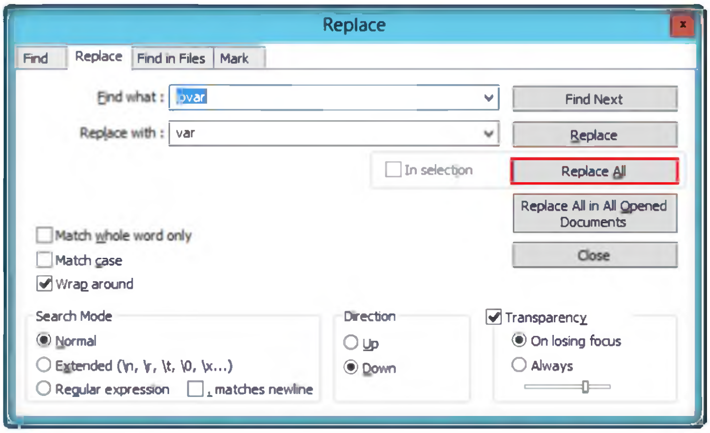
Figure 1.17: Configuring Snort.conf File in Notepad++

53. In the **snort.conf** file, find and replace the **ipvar** string with **var**. By default the string is **ipvar**, which is not recognized by Snort, so replace it with the **var** string.

Note: Snort now supports multiple configurations based on VLAN Id or IP subnet within a single instance of Snort. This allows administrators to specify multiple snort configuration files and bind each configuration to one or more VLANs or subnets rather than running one Snort for each configuration required.

Three types of variables may be defined in Snort:

- Var
- Portvar
- ipvar



Find what : ipvar
Replace with : var
□ In selection
□ Match whole word only
□ Match case
☑ Wrap around
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression □ . matches newline
○ Up
● Down
☑ Transparency
● On losing focus
○ Always

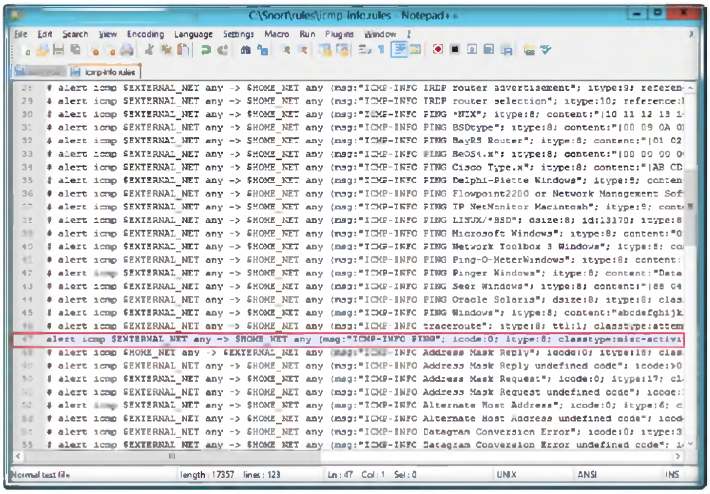
Figure 1.18: Configuring Snort.conf File in Notepad++

54. Save the **snort.conf** file.

55. Before running Snort you need to enable detection rules in the Snort rules file; for this lab we have enabled ICMP rule so that Snort can detect any host discovery ping probes to the system running Snort.

56. Navigate to **C:\Snort\rules** and open the **icmp-info.rules** file with Notepad ++.

57. **Uncomment** the Line number **47** and save and close the file.


C:\Snort\rules\icmp-info.rules - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
icmp-info.rules
Normal text file
length : 17357 lines : 123
Ln : 47 Col : 1 Sel : 0
UNIX
ANSI
INS

```
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO IRDP router advertisement"; itype:9; referen
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO IRDP router selection"; itype:10; reference:
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING *NIX"; itype:8; content:"|10 11 12 13 1
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING BSDtype"; itype:8; content:"|00 09 0A 0
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING BayRS Router"; itype:8; content:"|01 02
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING BeOS4.x"; itype:8; content:"|00 00 00 0
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Cisco Type.x"; itype:8; content:"|AB CD
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Delphi-Piette Windows"; itype:8; conten
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Flowpoint2200 or Network Management Sof
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING IP NetMonitor Macintosh"; itype:8; cont
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING LINUX/*BSD"; dsize:8; id:13170; itype:8
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Microsoft Windows"; itype:8; content:"0
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Network Toolbox 3 Windows"; itype:8; co
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Ping-O-MeterWindows"; itype:8; content:
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Pinger Windows"; itype:8; content:"Data
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Seer Windows"; itype:8; content:"|88 04
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Oracle Solaris"; dsize:8; itype:8; clas
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Windows"; itype:8; content:"abcdefghijk
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO traceroute"; itype:8; ttl:1; classtype:attem
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING"; icode:0; itype:8; classtype:misc-activi
# alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ICMP-INFO Address Mask Reply"; icode:0; itype:18; clas
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Address Mask Reply undefined code"; icode:>0
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Address Mask Request"; icode:0; itype:17; cl
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Address Mask Request undefined code"; icode:
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Alternate Host Address"; icode:0; itype:6; c
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Alternate Host Address undefined code"; icod
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Datagram Conversion Error"; icode:0; itype:3
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Datagram Conversion Error undefined code"; i
```

Figure 1.19: Configuring Snort.conf File in Notepad++

TASK 4

Validate Configurations

58. Now navigate to **C:\Snort** and right-click folder **bin**, select **CmdHere** from the context menu to open it in the command prompt.

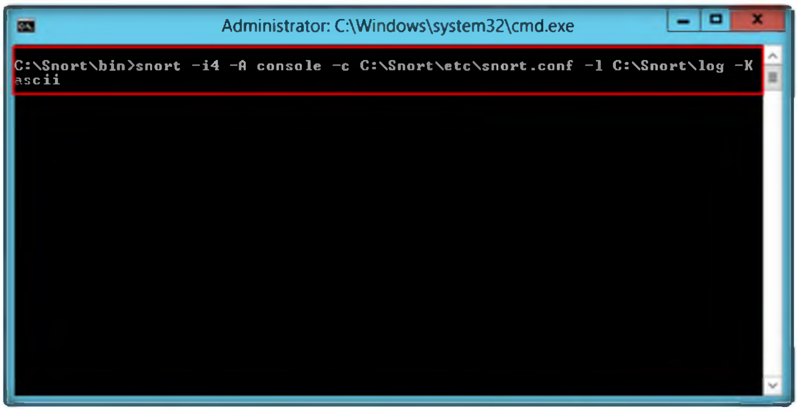
59. Type **snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii** and press **Enter** to start Snort (replace **X** with your device index number; in this lab: **X** is 1).

60. If you enter all the command information **correctly**, you receive a **graceful exit** as shown in the following figure.

61. If you receive a **fatal error**, you should first **verify** that you have typed all modifications correctly into the **snort.conf** file and then search through the file for **entries** matching your fatal error message.

62. If you receive an error stating "**Could not create the registry key**," then run the command prompt as an **Administrator**.

To run Snort as a daemon, add -D switch to any combination. Notice that if you want to be able to restart Snort by sending a SIGHUP signal to the daemon, specify the full path to the Snort binary when you start it, for example: /usr/local/bin/snort -d -h 192.168.1.0/24 \ -l /var/log/snortlogs -c /usr/local/etc/snort.conf -s -D



```
C:\Snort\bin>snort -i4 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K
ascii
```

Figure 2.18: Snort Successfully Validated Configuration Window

TASK 5

Start Snort

63. Start Snort in IDS mode, in the command prompt type **snort –c C:\Snort\etc\snort.conf –l C:\Snort\log –i 2** and then press **Enter**.

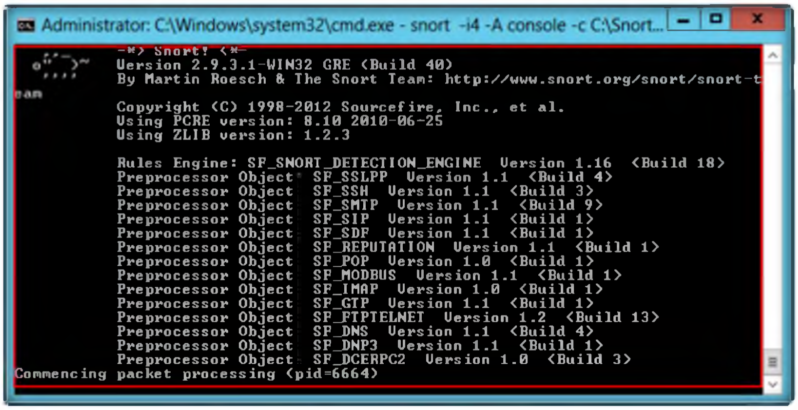
Figure 2.19: Start Snort in IDS Mode Command

64. Snort starts running in IDS mode. It first initializes output plug-ins, preprocessors, plug-ins, load dynamic preprocessors libraries, rule chains of Snort, and then logs all signatures.

65. After initializing interface and logged signatures, Snort starts and waits for an attack and trigger alert when attacks occur on the machine.

C:\Snort\etc\snort.conf is the location of the configuration file

- Option: -l to log the output to C:\Snort\log folder
- Option: -i 2 to specify the interface


Administrator: C:\Windows\system32\cmd.exe - snort -i4 -A console -c C:\Snort...

```
             -*> Snort! <*-
  o"  )~     Version 2.9.3.1-WIN32 GRE (Build 40)
   ''''      By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
             Copyright (C) 1998-2012 Sourcefire, Inc., et al.
             Using PCRE version: 8.10 2010-06-25
             Using ZLIB version: 1.2.3

             Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 1.16  <Build 18>
             Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
             Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
             Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
             Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
             Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
             Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
             Preprocessor Object: SF_POP  Version 1.0  <Build 1>
             Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
             Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
             Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
             Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
             Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
             Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
             Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=6664)
```

Figure 1.20: Initializing Snort Rule Chains Window

Run Snort as a Daemon syntax: /usr/local/bin/snort -d -h 192.168.1.0/24 \ -l /var/log/snortlogs -c /usr/local/etc/snort.conf -s –D.

When Snort is run as a Daemon, the daemon creates a PID file in the log directory.

66. After initializing the interface and logged signatures, Snort starts and waits for an attack and trigger alert when attacks occur on the machine.

67. Leave the Snort command prompt running.

68. Attack your own machine and check whether Snort detects it or not.

TASK 6

Attack Host Machine

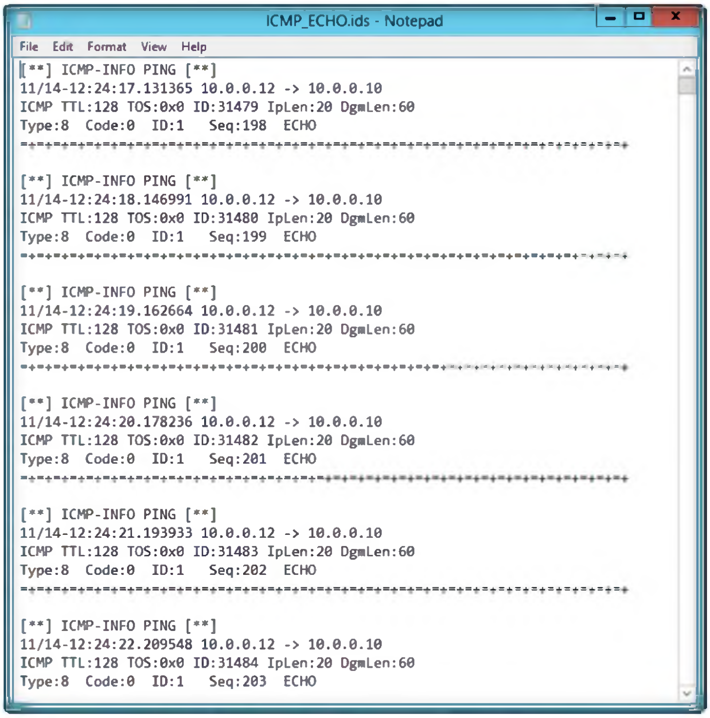
69. Launch your Windows 8 Virtual Machine (**Attacker Machine**).

70. Open the command prompt and type **ping XXX.XXX.XXX.XXX -t** from the **Attacker Machine** (XXX.XXX.XXX.XX is your Windows Server 2012 **IP address**).

71. Go to **Windows Server 2012**, open the Snort command prompt, and press **Ctrl+C** to **stop** Snort. Snort exits.

72. Now go to the **C:\Snort\log\10.0.0.12** folder and open the **ICMP_ECHO.ids** text file.

Note that to view the snort log file, always stop snort and then open snort log file.



```
[**] ICMP-INFO PING [**]
11/14-12:24:17.131365 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31479 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:198  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP-INFO PING [**]
11/14-12:24:18.146991 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31480 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:199  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP-INFO PING [**]
11/14-12:24:19.162664 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31481 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:200  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP-INFO PING [**]
11/14-12:24:20.178236 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31482 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:201  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP-INFO PING [**]
11/14-12:24:21.193933 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31483 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:202  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP-INFO PING [**]
11/14-12:24:22.209548 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31484 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:203  ECHO
```

Figure 1.21: Snort Alerts.ids Window Listing Snort Alerts

73. You see that all the log entries are saved in the **ICMP_ECHO.ids** file. This means that your Snort is working correctly to trigger alert when attacks occur on your machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Snort	**Output:** victim machine log are captured

Questions

1. Determine and analyze the process to identify and monitor network ports after intrusion detection.

2. Evaluate how you process Snort logs to generate reports.

Internet Connection Required	
□ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

2

Logging Snort Alerts to Kiwi Syslog Server

Snort is an open source network intrusion prevention and detection system (IDS/IPS).

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

Increased connectivity and the use of the Internet have exposed organizations to subversion, thereby necessitating the use of intrusion detection systems to protect information systems and communication networks from malicious attacks and unauthorized access. An intrusion detection system (IDS) is a security system that monitors computer systems and network traffic, analyzes that traffic to identify possible security breaches, and raises alerts. An IDS triggers thousands of alerts per day, making it difficult for human users to analyze them and take appropriate actions. It is important to reduce the redundancy of alerts, intelligently integrate and correlate them, and present high-level view of the detected security issues to the administrator. An IDS is used to inspect data for malicious or anomalous activities and detect attacks or unauthorized use of system, networks, and related resources.

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network intrusion prevention system (IPSes), IDSes, identify network malicious activity, and log information, stop, or block malicious network activity.

Lab Objectives

Tools demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots

The objective of this lab is to help students learn and understand IPSes and IDSes.

In this lab, you need to:

- Install Snort and configure snort.conf file
- Validate configuration settings
- Perform an attack on the Host Machine
- Perform an intrusion detection
- Attempt to stop detected possible incidents

Lab Environment

To carry-out this lab, you need:

- A computer running Windows Server 2012 as a host machine
- Windows 8 running on virtual machine as an attacker machine
- WinPcap drivers installed on the host machine
- Kiwi Syslog Server installed on the host machine
- Administrative privileges to configure settings and run tools

You can also download Kiwi Syslog Server from http://www.kiwisyslog.com

Lab Duration

Time: 10 Minutes

Overview of of IPSes and IDSes

An intrusion detection system (IDS) is a device or **software** application that monitors network and/or system activities for **malicious** activities or policy violations and produces reports to a management station.

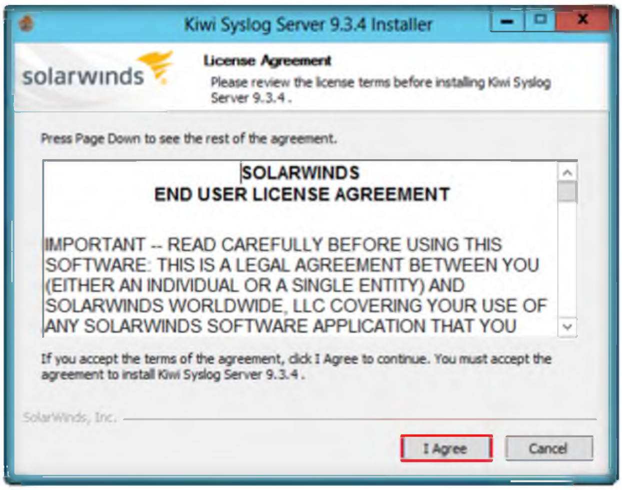
Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible **incidents**, **logging** information about them, attempting to stop them, and reporting them to **security** administrators.

TASK 1

Log Snort Alerts to Syslog Server

Lab Tasks

1. Navigate to **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Kiwi Syslog Server** double click on **Kiwi_Syslog_Server_9.3.4.Eval.setup.exe** and install **Kiwi Syslog Server** on the Windows Server 2012 host machine.
2. The **License Agreement** window appears, Click **I Agree**.



License Agreement

Please review the license terms before installing Kiwi Syslog Server 9.3.4.

Press Page Down to see the rest of the agreement.

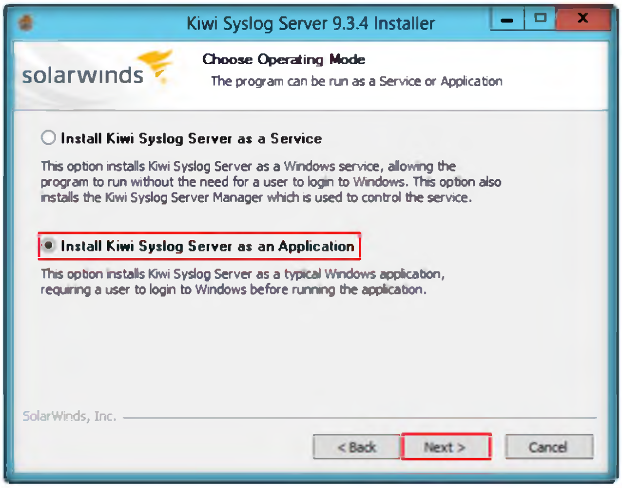
SOLARWINDS
END USER LICENSE AGREEMENT

IMPORTANT -- READ CAREFULLY BEFORE USING THIS SOFTWARE: THIS IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND SOLARWINDS WORLDWIDE, LLC COVERING YOUR USE OF ANY SOLARWINDS SOFTWARE APPLICATION THAT YOU

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Kiwi Syslog Server 9.3.4.

Figure 2.1: kiwi syslog server installation

3. In the **Choose Operating Mode** wizard, check the **Install Kiwi Syslog Server as an Application** check box and click **Next >**.



Kiwi Syslog Server 9.3.4 Installer

Choose Operating Mode

The program can be run as a Service or Application

○ Install Kiwi Syslog Server as a Service

This option installs Kiwi Syslog Server as a Windows service, allowing the program to run without the need for a user to login to Windows. This option also installs the Kiwi Syslog Server Manager which is used to control the service.

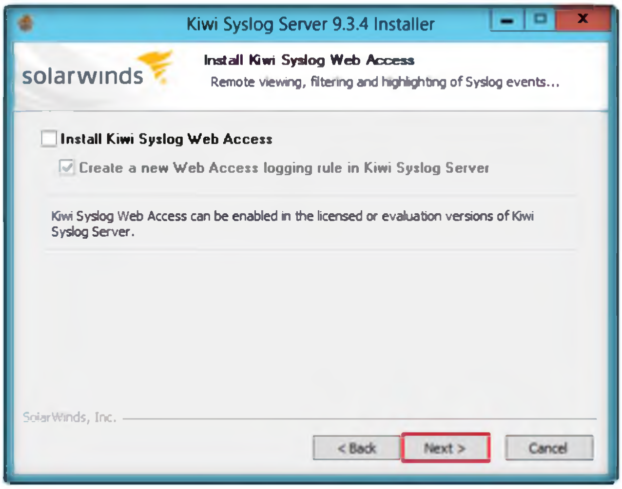
● Install Kiwi Syslog Server as an Application

This option installs Kiwi Syslog Server as a typical Windows application, requiring a user to login to Windows before running the application.

Figure 2.2: Kiwi Syslog server installation

Tools demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots

4. In the **Install Kiwi Syslog Web Access** wizard, uncheck the option selected and click **Next >**.



Kiwi Syslog Server 9.3.4 Installer

Install Kiwi Syslog Web Access

Remote viewing, filtering and highlighting of Syslog events...

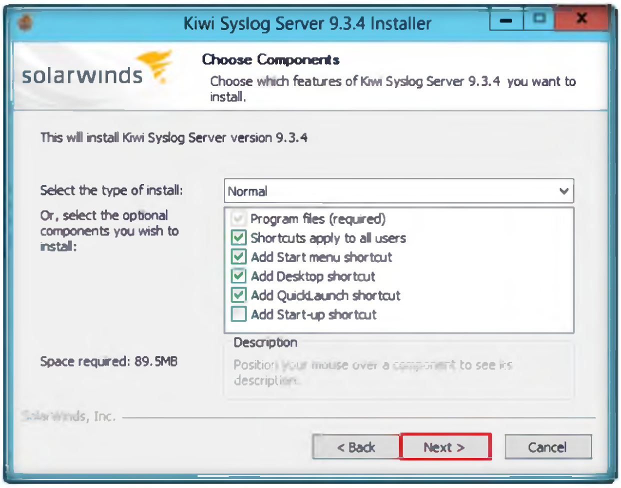
□ Install Kiwi Syslog Web Access

☑ Create a new Web Access logging rule in Kiwi Syslog Server

Kiwi Syslog Web Access can be enabled in the licensed or evaluation versions of Kiwi Syslog Server.

Figure 2.3: kiwi syslog server

5. Leave the settings as their defaults in the **Choose Components** wizard and click **Next >**.



Kiwi Syslog Server 9.3.4 Installer

Choose Components

Choose which features of Kiwi Syslog Server 9.3.4 you want to install.

This will install Kiwi Syslog Server version 9.3.4

Select the type of install: Normal

Or, select the optional components you wish to install:

- ☑ Program files (required)
- ☑ Shortcuts apply to all users
- ☑ Add Start menu shortcut
- ☑ Add Desktop shortcut
- ☑ Add QuickLaunch shortcut
- ☐ Add Start-up shortcut

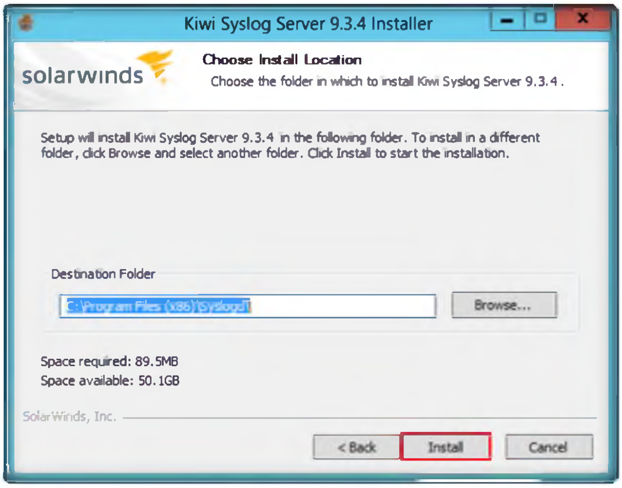
Description

Position your mouse over a component to see its description.

Space required: 89.5MB

Figure 2.4: adding components

6. In the **Choose Install Location** wizard, leave the settings as their defaults and click **Install** to continue.



Kiwi Syslog Server 9.3.4 Installer

Choose Install Location

Choose the folder in which to install Kiwi Syslog Server 9.3.4.

Setup will install Kiwi Syslog Server 9.3.4 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files (x86)\Syslogd\

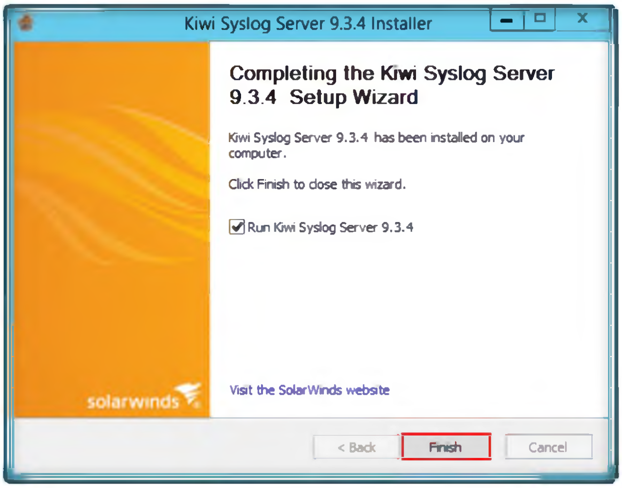
Space required: 89.5MB

Space available: 50.1GB

Figure 2.5: Give destination folder

7. Click **Finish** to complete the installation.

You should see a test message appear, which indicates Kiwi is working.



Kiwi Syslog Server 9.3.4 Installer

Completing the Kiwi Syslog Server 9.3.4 Setup Wizard

Kiwi Syslog Server 9.3.4 has been installed on your computer.

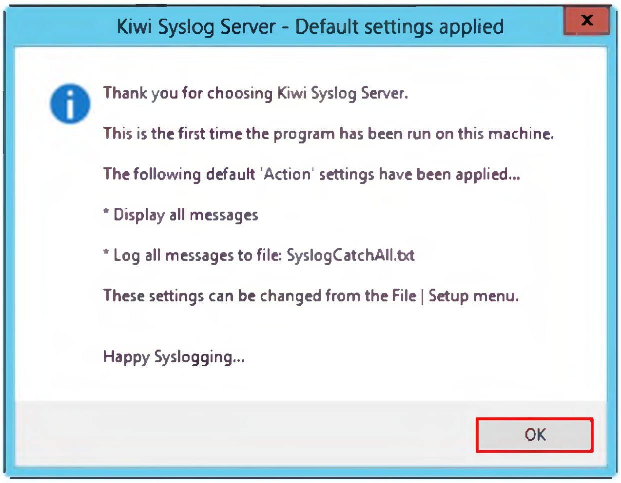
Click Finish to close this wizard.

☑ Run Kiwi Syslog Server 9.3.4

Visit the SolarWinds website

Figure 2.6: kiwi syslog server finish window

8. Click **OK** in the **Kiwi Syslog Server – Default Settings Applied** dialog box.



Kiwi Syslog Server - Default settings applied

Thank you for choosing Kiwi Syslog Server.

This is the first time the program has been run on this machine.

The following default 'Action' settings have been applied...

* Display all messages

* Log all messages to file: SyslogCatchAll.txt

These settings can be changed from the File | Setup menu.

Happy Syslogging...

Figure 2.7: Default setting applied window

9. To launch the **Kiwi Syslog Server Console** move your mouse cursor to lower-left corner of your desktop and click **Start**.

lower-left corner of your desktop and click Start.

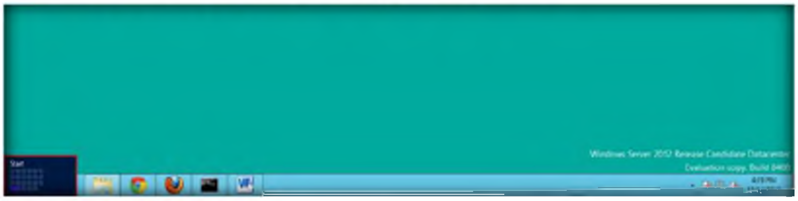


Figure 2.8: starting menu in windows server 2012

10. In the **Start** menu apps click **Kiwi Syslog Server Console** to launch the app.

Kiwi Syslog Server is a free syslog server for Windows. It receives logs, displays and forwards syslog messages from hosts such as routers, switches, UNIX hosts and other syslog-enabled devices.

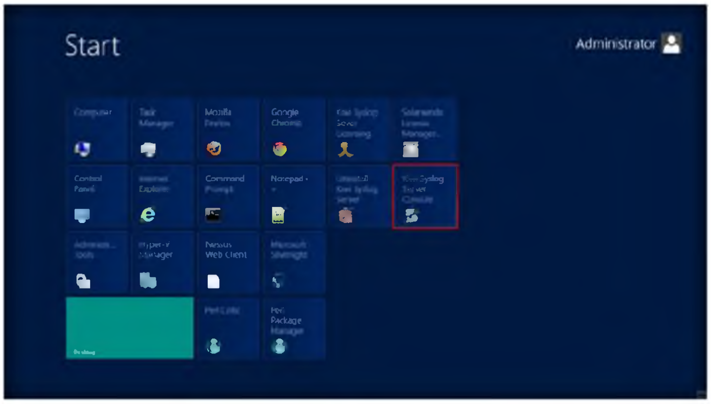


Figure 2.9: click kiwi syslog server application

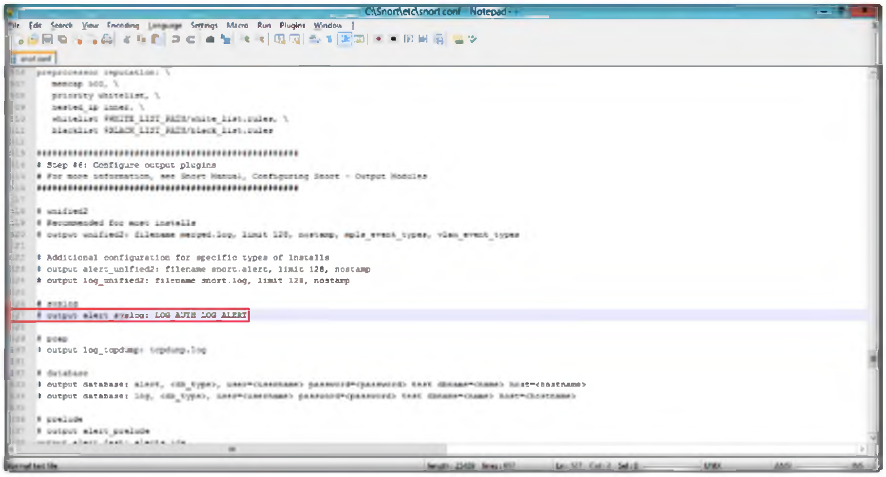
11. Configure Syslog alerts in the **snort.conf** file.

12. To configure **Syslog alerts**, first exit from the Snort command prompt (press **Ctrl+C**).

13. Go to **C:\Snort\etc** and open the **snort.conf** file with **Notepad++**.

14. Scroll down to **Step #6: Configure output plugins**, in the syslog section (Line 527), remove **#** and modify the line to **output alert_syslog: host=127.0.0.1:514, LOG_AUTH LOG_ALERT**.

Snort.conf before modification Syslog

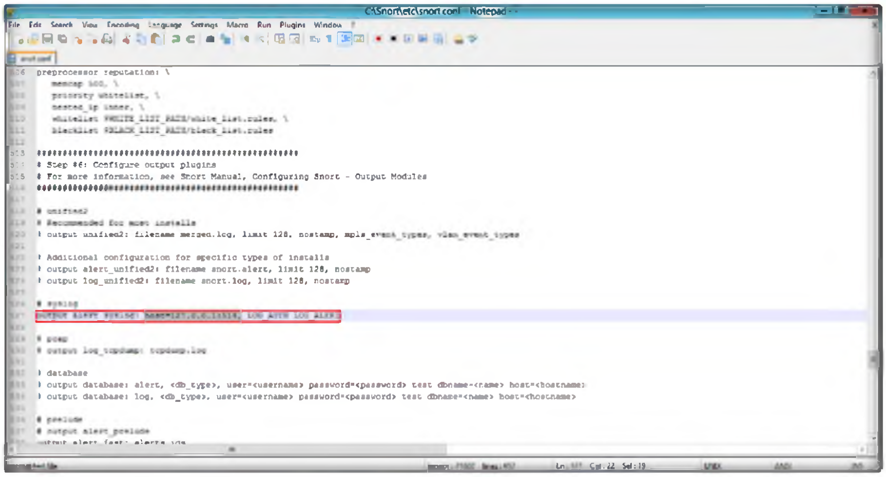

C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
snort.conf

```
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   whitelist $WHITE_LIST_PATH/white_list.rules, \
   blacklist $BLACK_LIST_PATH/black_list.rules

###################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
###################################################

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types

# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
# output alert_syslog: LOG_AUTH LOG_ALERT

# pcap
# output log_tcpdump: tcpdump.log

# database
# output database: alert, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>
# output database: log, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>

# prelude
# output alert_prelude
output alert_fast: alerts.ids
```

Figure 2.10: Snort.config before modification

Snort.conf after modification Syslog

The reason why you have to run snortstart.bat batch file as an administrator is that, in your current configuration, you need to maintain rights to not only output your alerts to Kiwi, but to write them to a log file.



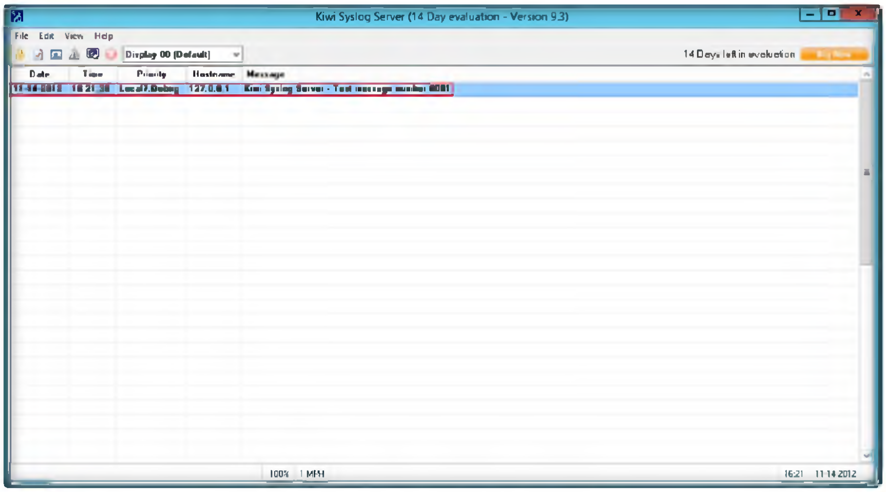
```
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   whitelist $WHITE_LIST_PATH/white_list.rules, \
   blacklist $BLACK_LIST_PATH/black_list.rules

###################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
###################################################

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types

# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
output alert_syslog: host=127.0.0.1:514, LOG_AUTH LOG_ALERT

# pcap
# output log_tcpdump: tcpdump.log

# database
# output database: alert, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>
# output database: log, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>

# prelude
# output alert_prelude
output alert_fast: alerts.ids
```

C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

Figure 2.11: Snort.config after configuration

15. **Save** the file and close it.

16. Open **Kiwi Syslog Server Console** and press **Ctrl+T**. This is to test Kiwi Syslog Server alert logs.



Date	Time	Priority	Hostname	Message
11-14-2012	16:21:38	Local7.Debug	127.0.0.1	Kiwi Syslog Server - Test message number 0001

Kiwi Syslog Server (14 Day evaluation - Version 9.3)
File Edit View Help
Display 00 (Default)
14 Days left in evaluation
100%
1 MPH
16:21 11-14-2012

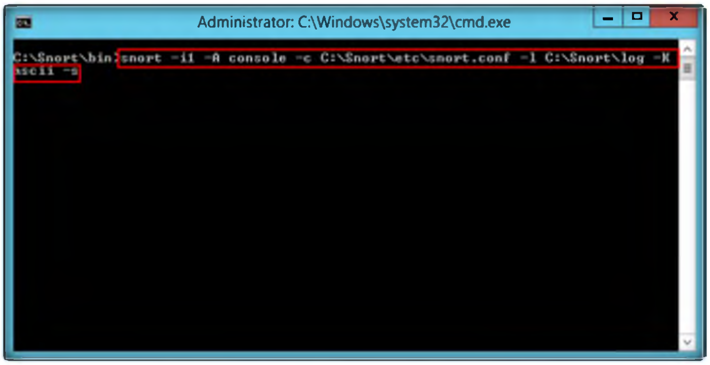
Figure 2.12: Kiwi Syslog Service Manager window

17. Leave the Kiwi Syslog Server Console. Do not close the window.

18. Now open a command prompt with Snort and type this command: **snort –iX –A console –c C:\Snort\etc\snort.conf –l C:\Snort\log –K ascii –s** and press **Enter** (here X is index number of your Ethernet card) .

Kiwi Syslog Server filtering options:

- Filter on IP address, hostname, or message text
- Filter out unwanted host messages or take a different logging action depending on the host name
- Perform an action when a message contains specific keywords.

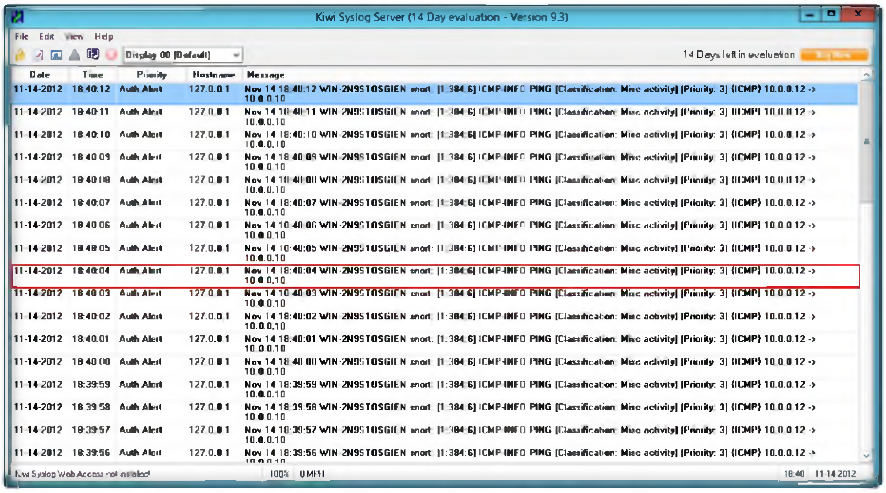


```
C:\Snort\bin>snort -i1 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K
ascii -s
```

Figure 2.13: Snort Alerts.ids Window Listing Snort Alerts

19. Open a command prompt in your Windows 8 virtual machine and type this command: **ping 10.0.0.10** (IP address of your host machine where Kiwi Syslog Server Console is running) .

20. Go to **Kiwi Syslog Service Manager** window (that is already open) and observe the triggered alert logs.


Kiwi Syslog Server (14 Day evaluation - Version 9.3)
File
Edit
View
Help
Display 00 (Default)
14 Days left in evaluation

```
Date        Time      Priority    Hostname   Message
11-14-2012  18:40:12  Auth.Alert  127.0.0.1  Nov 14 18:40:12 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:11  Auth.Alert  127.0.0.1  Nov 14 18:40:11 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:10  Auth.Alert  127.0.0.1  Nov 14 18:40:10 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:09  Auth.Alert  127.0.0.1  Nov 14 18:40:09 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:08  Auth.Alert  127.0.0.1  Nov 14 18:40:08 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:07  Auth.Alert  127.0.0.1  Nov 14 18:40:07 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:06  Auth.Alert  127.0.0.1  Nov 14 18:40:06 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:05  Auth.Alert  127.0.0.1  Nov 14 18:40:05 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:04  Auth.Alert  127.0.0.1  Nov 14 18:40:04 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:03  Auth.Alert  127.0.0.1  Nov 14 18:40:03 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:02  Auth.Alert  127.0.0.1  Nov 14 18:40:02 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:01  Auth.Alert  127.0.0.1  Nov 14 18:40:01 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:40:00  Auth.Alert  127.0.0.1  Nov 14 18:40:00 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:39:59  Auth.Alert  127.0.0.1  Nov 14 18:39:59 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:39:58  Auth.Alert  127.0.0.1  Nov 14 18:39:58 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:39:57  Auth.Alert  127.0.0.1  Nov 14 18:39:57 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
11-14-2012  18:39:56  Auth.Alert  127.0.0.1  Nov 14 18:39:56 WIN-2N9STOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.12 ->
                                             10.0.0.10
Kiwi Syslog Web Access not installed    100%    0 MPH                                      18:40    11-14-2012
```

Figure 2.14: Kiwi Syslog Service Manager with Snort Logs

21. In **Kiwi Syslog**, you see the Snort alerts outputs listed in Kiwi Syslog Service Manager.

22. You have successfully output Snort Alerts to two sources.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Kiwi Syslog Server	**Output:** The Snort alerts outputs listed in Kiwi Syslog Service Manager.

Questions

1. Evaluate how you can capture a memory dump to confirm a leak using Kiwi Syslog Server.
2. Determine how you can move Kiwi Syslog Daemon to another machine.
3. Each Syslog message includes a priority value at the beginning of the text. Evaluate the priority of each Kiwi Syslog message and on what basis messages are prioritized.

Internet Connection Required	
□ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

3

Detecting Intruders and Worms Using KFSensor Honeypot IDS

KFSensor is a Windows based honeypot Intrusion Detection System (IDS).

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Intrusion detection systems are designed to search network activity (we are considering both host and network IDS detection) for evidence of malicious abuse. When an IDS algorithm "detects" some sort of activity and the activity is not malicious or suspicious, this detection is known as a false positive. It is important to realize that from the IDS's perspective, it is not doing anything incorrect. Its algorithm is not making a mistake. The algorithm is just not perfect. IDS designers make many assumptions about how to detect network attacks.

An example assumption could be to look for extremely long URLs. Typically, a URL may be only 500 bytes long. Telling an IDS to look for URLs longer than 2000 bytes may indicate a denial of service attack. A false positive could result from some complex e-commerce web sites that store a wide variety of information in the URL and exceed 2000 bytes.

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network intrusion prevention systems (IPSes), intrusion detection systems (IDSes), identify network malicious activity and log information, and stop or block malicious network activity.

Lab Objectives

Tools demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots

The objective of this lab is to make students learn and understand IPSes and IDSes.

In this lab, you need to:

- Detect hackers and worms in a network
- Provide network security

Lab Environment

To carry-out this lab, you need:

- **KF Sensor** located at **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\KFSensor**
- Install KF Sensor in **Windows 8**
- **MegaPing** located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\MegaPing**
- Install Mega ping in **Windows Server 2012**
- If you have decided to download latest of version of these tools, then screen shots would be differ
- Administrative privileges to configure settings and run tools

You can also download KFSensor from http://www.keyfocus.net

Lab Duration

Time: 10 Minutes

Overview of IPSes and IDSes

An intrusion prevention system (IPS) is a **network security** appliance that **monitors** network and system activities for **malicious** activity. The main functions of IPSes are to **identify** malicious activity, **log related information**, attempt to **block/stop** activity, and report activity.

An IDS is a software device or application that **monitors** network and/or system activities for **malicious** activities or **policy violations** and delivers **reports** to a Management Station. It performs intrusion detection and attempts to **stop** detected possible **incidents**.

TASK 1

Configure KFSensor

Lab Tasks

1. Launch **Windows 8** virtual machine and follow the wizard-driven installation steps to install **KFSensor**.
2. After installation it will prompt to reboot the system. **Reboot** the system.
3. In Windows 8 launch KFSensor. To Launch KFSensor move your mouse cursor to the lower-left corner of your desktop and click **Start**.

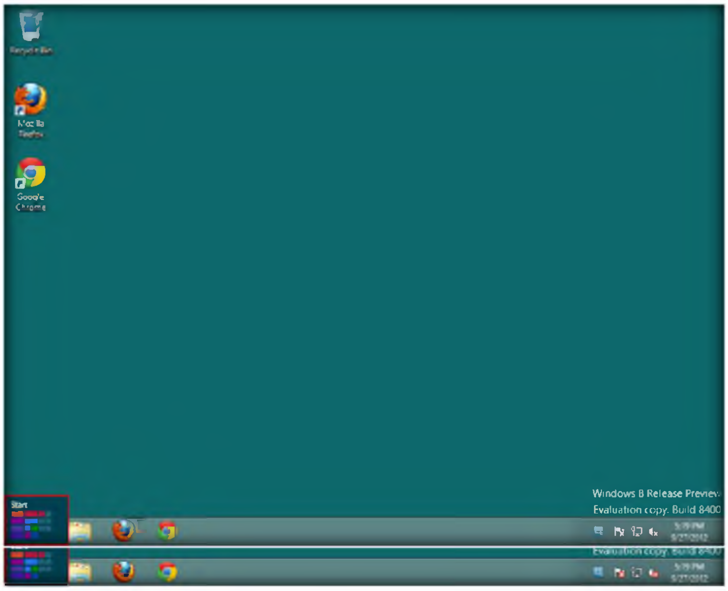


FIGURE 3.1: KFSensor Window with Setup Wizard

To set up common ports KFSensor has a set of pre-defined listen definitions. They are:

- Windows Workstation
- Windows Server
- Windows Internet Services
- Windows Applications
- Linux (services not usually in Windows)
- Trojans and worms

4. In the **Start** menu apps, right click the **KFSensor** app, and click **Run as Administrator** at the bottom.

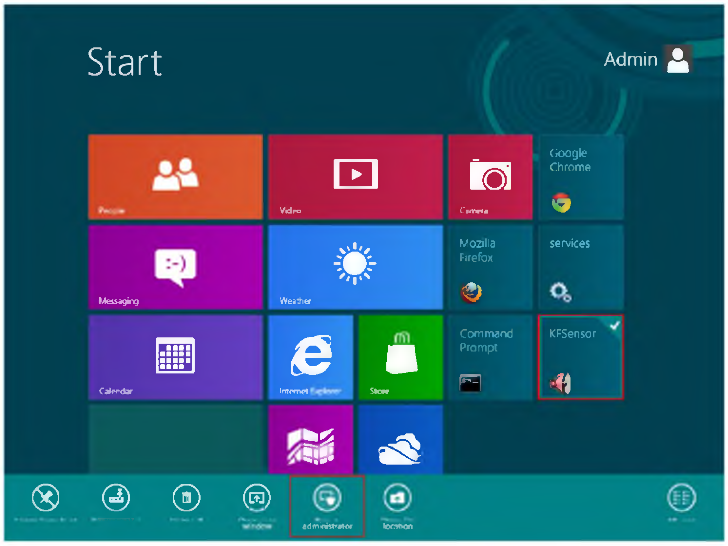
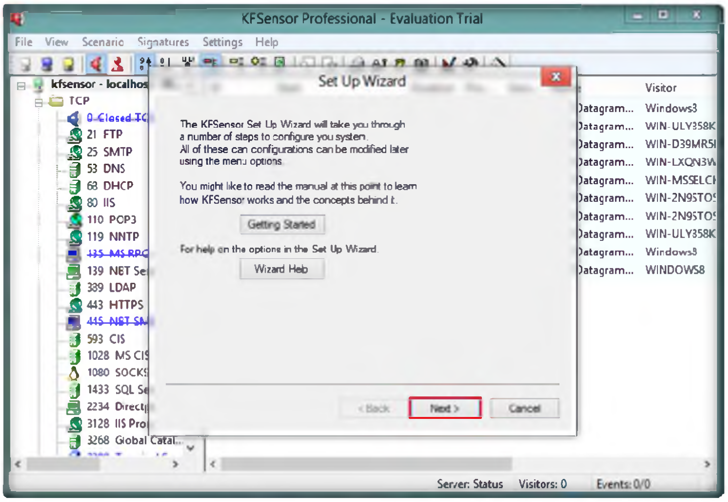


FIGURE 3.2: KFSensor Window with Setup Wizard

5. At the first-time launch of the **KFSensor Set Up Wizard**, click **Next**.

The Set up Wizard is used to perform the initial configuration of KFSensor.



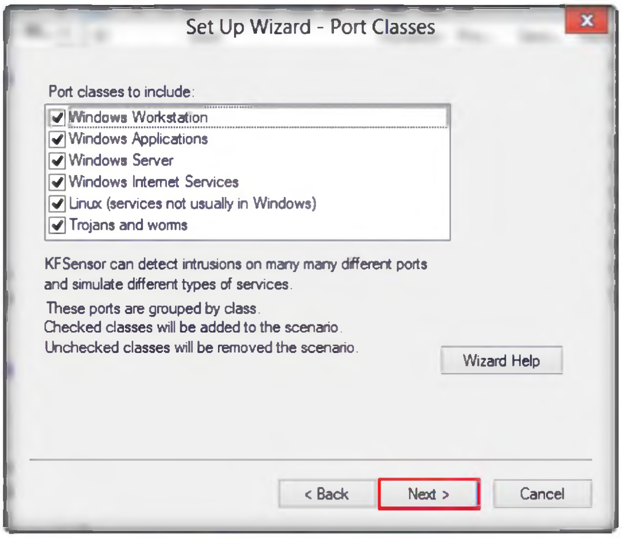
The KFSensor Set Up Wizard will take you through a number of steps to configure you systen.
All of these can configurations can be modified later using the menu options.

You might like to read the manual at this point to learn how KFSensor works and the concepts behind it.

For help on the options in the Set Up Wizard.

FIGURE 3.3: KFSensor main Window

6. Check all the **port classes** to include and click **Next**.



Port classes to include:

☑ Windows Workstation
☑ Windows Applications
☑ Windows Server
☑ Windows Internet Services
☑ Linux (services not usually in Windows)
☑ Trojans and worms

KFSensor can detect intrusions on many many different ports and simulate different types of services.

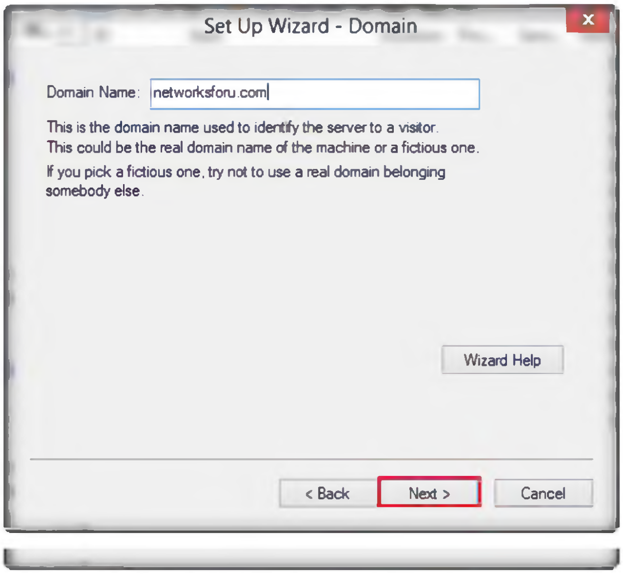
These ports are grouped by class.
Checked classes will be added to the scenario.
Unchecked classes will be removed the scenario.

FIGURE 3.4: KFSensor Window with Setup Wizard

Domain Name is the domain name used to identify the server to a visitor. It is used in several Sim Servers.

7. Live the domain name field as default and click **Next**.

KFSensor can send alerts by email. The settings in the wizard are the minimum needed to enable this feature.



Set Up Wizard - Domain

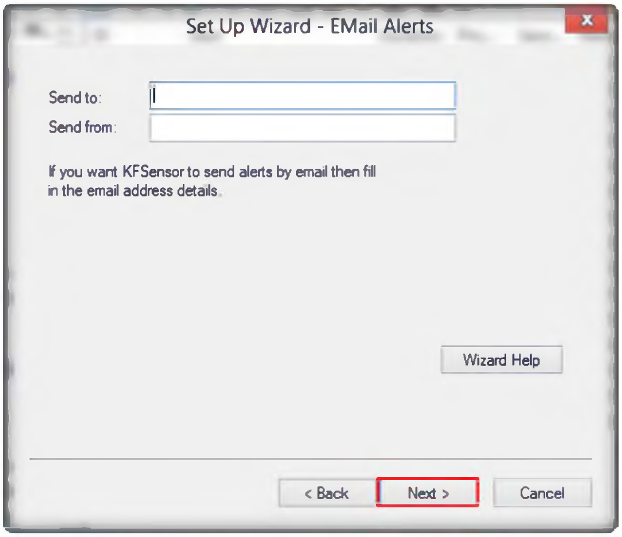
Domain Name: networksforu.com

This is the domain name used to identify the server to a visitor.
This could be the real domain name of the machine or a fictious one.
If you pick a fictious one, try not to use a real domain belonging somebody else.

FIGURE 3.5: KFSensor Window with Setup Wizard

8. If you want to send **KFSensor alerts** by email and then specify the email address details and click **Next**.

A systems service is a special type of application that Windows runs in the background and is similar in concept to a UNIX daemon.



Set Up Wizard - EMail Alerts

Send to:

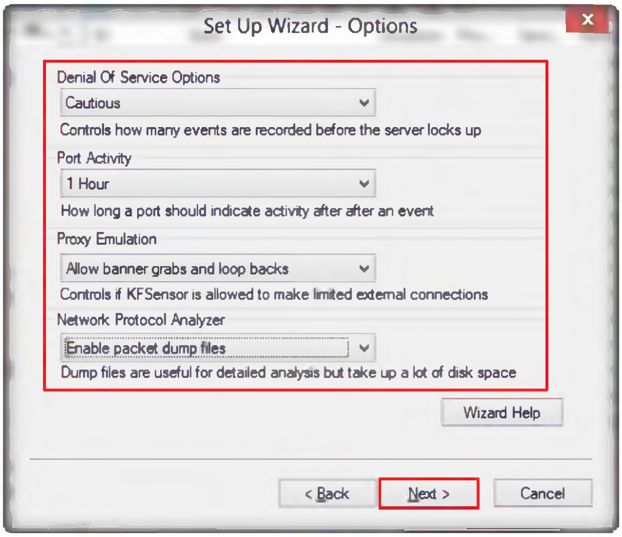
Send from:

If you want KFSensor to send alerts by email then fill in the email address details.

FIGURE 3.6: KFSensor Window with Setup Wizard-email alerts

9. Choose options for **Denial of Service**, **Port activity**, **Proxy Emulation**, and **Network Protocol Analyzer** and click **Next**.

The KFSensor Server becomes independent of the logged on user, so the user can log off and another person can log on without affecting the server.



Set Up Wizard - Options

Denial Of Service Options

Cautious

Controls how many events are recorded before the server locks up

Port Activity

1 Hour

How long a port should indicate activity after after an event

Proxy Emulation

Allow banner grabs and loop backs

Controls if KFSensor is allowed to make limited external connections

Network Protocol Analyzer

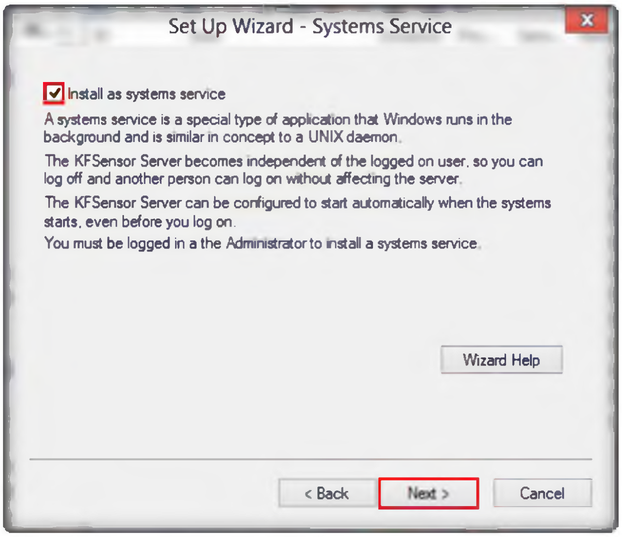
Enable packet dump files

Dump files are useful for detailed analysis but take up a lot of disk space

FIGURE 3.7: KFSensor Window with Setup Wizard-options

The KFSensor Monitor is a module that provides the user interface to the KFSensor system. With it you can configure the KFSensor Server and examine the events that it generates.

10. Check the **Install as system service** option and click **Next**.



Set Up Wizard - Systems Service

☑ Install as systems service

A systems service is a special type of application that Windows runs in the background and is similar in concept to a UNIX daemon.

The KFSensor Server becomes independent of the logged on user, so you can log off and another person can log on without affecting the server.

The KFSensor Server can be configured to start automatically when the systems starts, even before you log on.

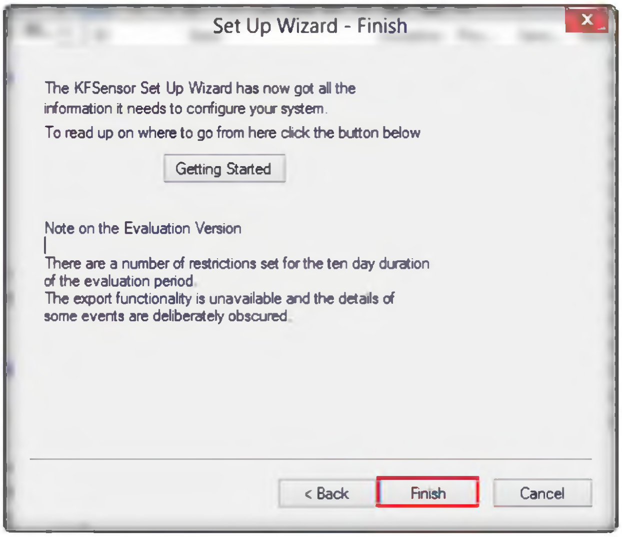
You must be logged in a the Administrator to install a systems service.

FIGURE 3.8: KFSensor Window with Setup Wizard-system service

The Ports View is displayed on the left panel of the main window. It comprises of a tree structure that displays the name and status of the KFSensor Server and the ports on which it is listening.

11. Click **Finish** to complete the **Set Up wizard**.

The Ports View can be displayed by selecting the Ports option from the View menu.



The KFSensor Set Up Wizard has now got all the information it needs to configure your system.

To read up on where to go from here click the button below

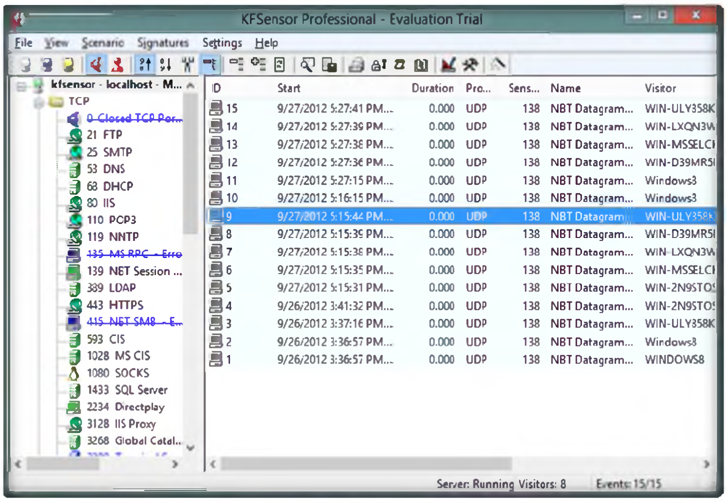
Note on the Evaluation Version

There are a number of restrictions set for the ten day duration of the evaluation period.

The export functionality is unavailable and the details of some events are deliberately obscured.

FIGURE 3.9: KFSensor finish installation

12. The **KFSensor** main window appears. It displays list of **ID protocols**, **Visitor**, and **Received** automatically when it starts. In the following window, all the nodes in the left block crossed out with **blue lines** are the **ports** that are being used.

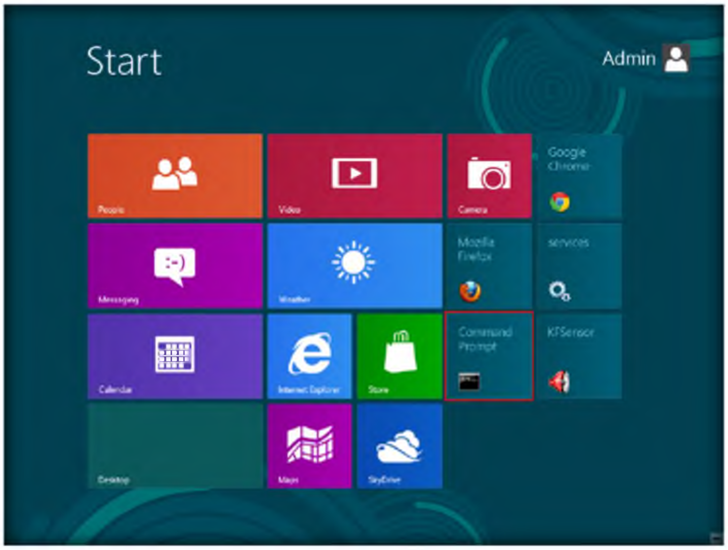


ID	Start	Duration	Pro...	Sens...	Name	Visitor
15	9/27/2012 5:27:41 PM...	0.000	UDP	138	NBT Datagram...	WIN-ULY358K
14	9/27/2012 5:27:39 PM...	0.000	UDP	138	NBT Datagram...	WIN-LXQN3W
13	9/27/2012 5:27:38 PM...	0.000	UDP	138	NBT Datagram...	WIN-MSSELCI
12	9/27/2012 5:27:36 PM...	0.000	UDP	138	NBT Datagram...	WIN-D39MR5I
11	9/27/2012 5:27:15 PM...	0.000	UDP	138	NBT Datagram...	Windows8
10	9/27/2012 5:16:15 PM...	0.000	UDP	138	NBT Datagram...	Windows8
9	9/27/2012 5:15:44 PM...	0.000	UDP	138	NBT Datagram...	WIN-ULY358K
8	9/27/2012 5:15:39 PM...	0.000	UDP	138	NBT Datagram...	WIN-D39MR5I
7	9/27/2012 5:15:38 PM...	0.000	UDP	138	NBT Datagram...	WIN-LXQN3W
6	9/27/2012 5:15:35 PM...	0.000	UDP	138	NBT Datagram...	WIN-MSSELCI
5	9/27/2012 5:15:31 PM...	0.000	UDP	138	NBT Datagram...	WIN-2N9STOS
4	9/26/2012 3:41:32 PM...	0.000	UDP	138	NBT Datagram...	WIN-2N9STOS
3	9/26/2012 3:37:16 PM...	0.000	UDP	138	NBT Datagram...	WIN-ULY358K
2	9/26/2012 3:36:57 PM...	0.000	UDP	138	NBT Datagram...	Windows8
1	9/26/2012 3:36:57 PM...	0.000	UDP	138	NBT Datagram...	WINDOWS8

Server: Running Visitors: 8 Events: 15/15

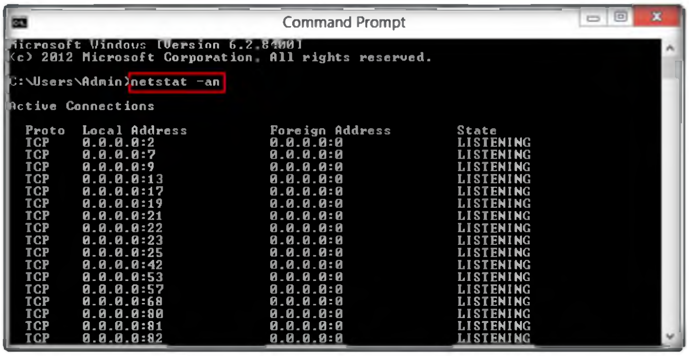
FIGURE 3.10: KFSensor Main Window

13. Open a command prompt from the **Start** menu apps.



The top level item is the server. The IP address of the KFSensor Server and the name of the currently active Scenario are displayed. The server icon indicates the state of the server.

14. In the command prompt window, type **netstat -an**.

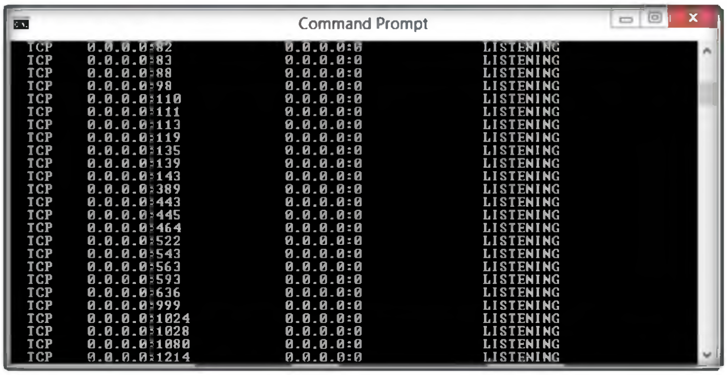


```
Microsoft Windows [Version 6.2.8400]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Admin>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:2              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:13             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:17             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:19             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:22             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:23             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:42             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:53             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:57             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:68             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:81             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:82             0.0.0.0:0              LISTENING
```

FIGURE 3.11: Command Prompt with netstat -an

15. This will display a list of listening ports.

The protocol level of KFSensor is used to group the ports based on their protocol; either TCP or UDP.



```
  TCP    0.0.0.0:82             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:83             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:88             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:98             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:110            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:111            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:113            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:119            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:139            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:143            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:389            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:464            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:522            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:543            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:563            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:593            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:636            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:999            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1024           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1080           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1214           0.0.0.0:0              LISTENING
```

FIGURE 3.12: Command Prompt with netstat -an

The Visitors View is displayed on the left panel of the main window. It comprises of a tree structure that displays the name and status of the KFSensor Server and the visitors who have connected to the server.

16. Leave the **KF Sensor** tool running.

17. Follow the wizard-driven installation steps to install MegaPing in **Windows Server 2012 (Host Machine)**.

18. To launch **MegaPing** move your mouse cursor to the lower-left corner of your desktop and click **Start**.

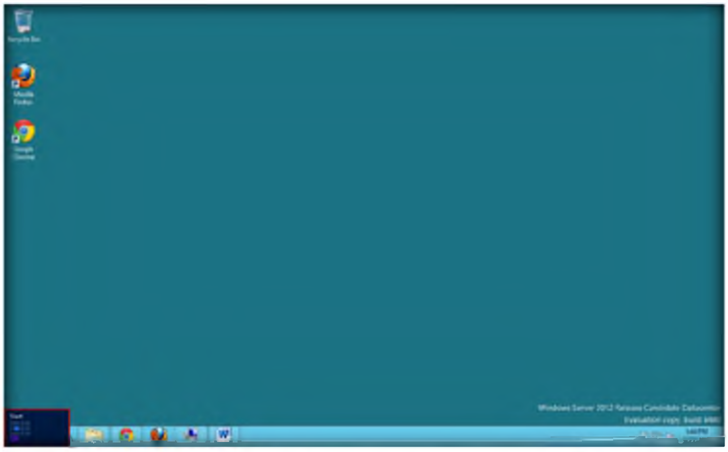


FIGURE 3.13: starting windows in windows server 2012

19. Click the **MegaPing** app in the **Start** menu apps.

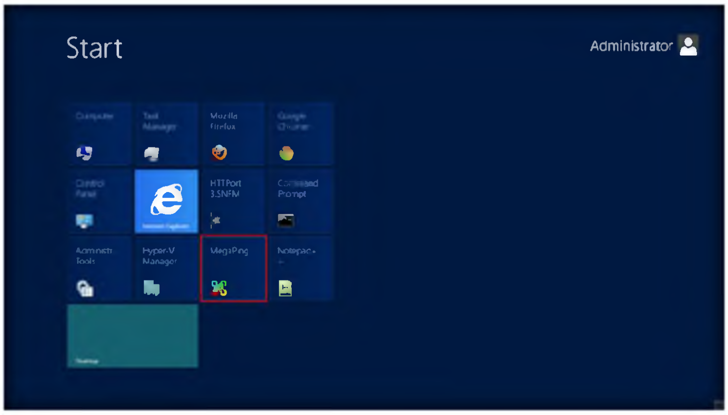
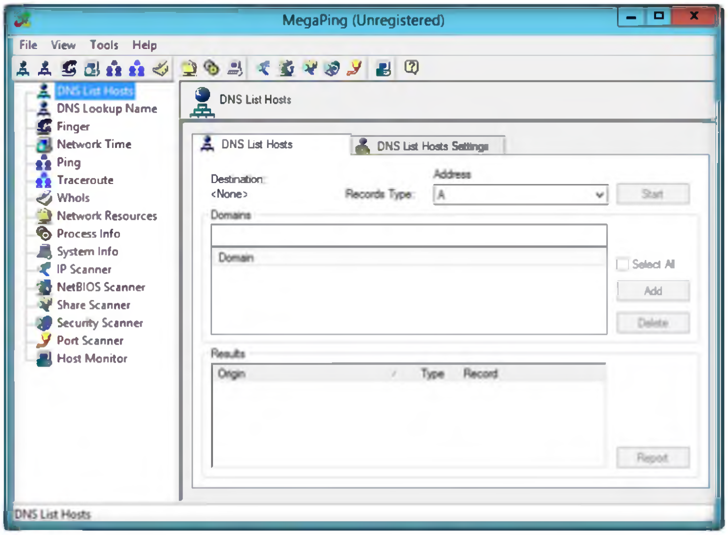


FIGURE 3.14: click on megaping

Each visitor detected by the KFSensor Server is listed. The visitor's IP address and domain name are displayed.

20. The main window of **MegaPing** appears as shown in the following screenshot.



Destination: <None>

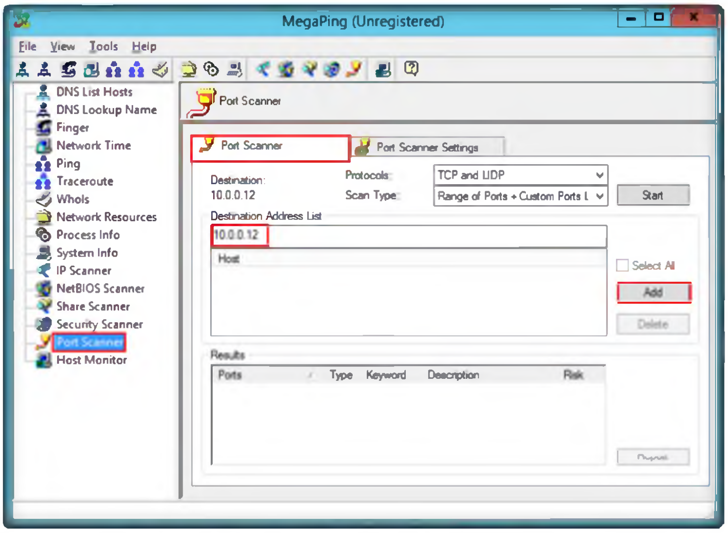
Records Type: A

FIGURE 3.15: MegaPing on Windows Server 2012

The Visitors View can be displayed by selecting the Visitors option from the View menu.

21. Select **Port Scanner** from left side of the list.

22. Enter the IP address of **Windows 8** (in this lab IP address is **10.0.0.12**) machine in which KFSensor is running in Destination Address List and click **Add**.



Destination: 10.0.0.12

Protocols: TCP and UDP

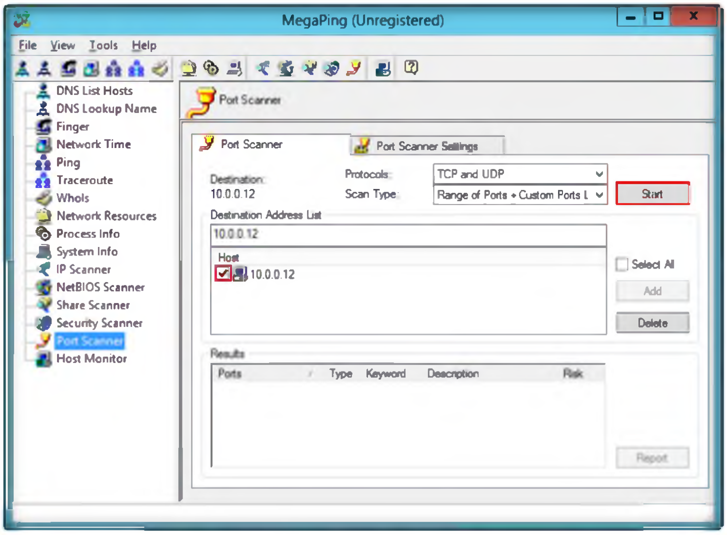
Scan Type: Range of Ports + Custom Ports L

Destination Address List: 10.0.0.12

FIGURE 3.16: MegaPing: Select 10.0.0.12 from Host, Press Start button

23. Check the IP address and click the **Start** button to start listening to the traffic on **10.0.0.12**.

Visitor is obtained by a reverse DNS lookup on the visitor's IP address. An icon is displayed indicating the last time the visitor connected to the server:



Destination: 10.0.0.12

Protocols: TCP and UDP

Scan Type: Range of Ports + Custom Ports L

Destination Address List: 10.0.0.12

Host: ☑ 10.0.0.12

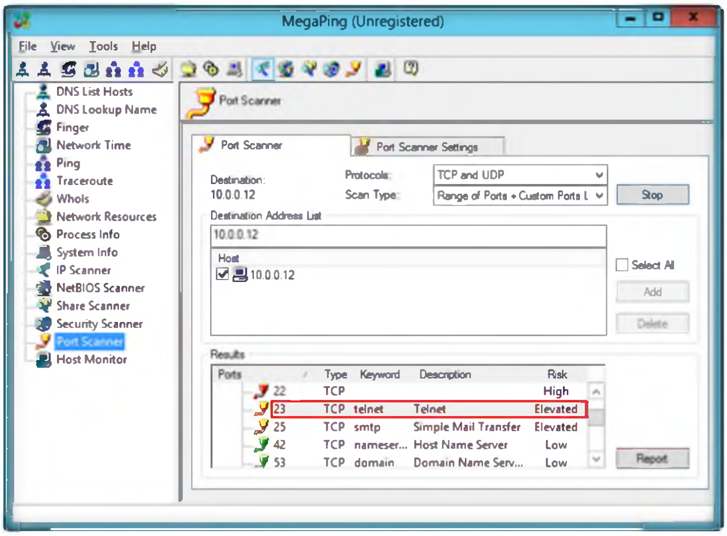
Results

Ports	Type	Keyword	Description	Risk

FIGURE 3.17: MegaPing: Data of the packets recieved

24. The following image displays the identification of Telnet on port 23.

The Visitors View is linked to the Events View and acts as a filter to it. If you select a visitor then only those events related to that visitor will be displayed in the Events View.



Destination: 10.0.0.12

Protocols: TCP and UDP

Scan Type: Range of Ports + Custom Ports L

Destination Address List: 10.0.0.12

Host: ☑ 10.0.0.12

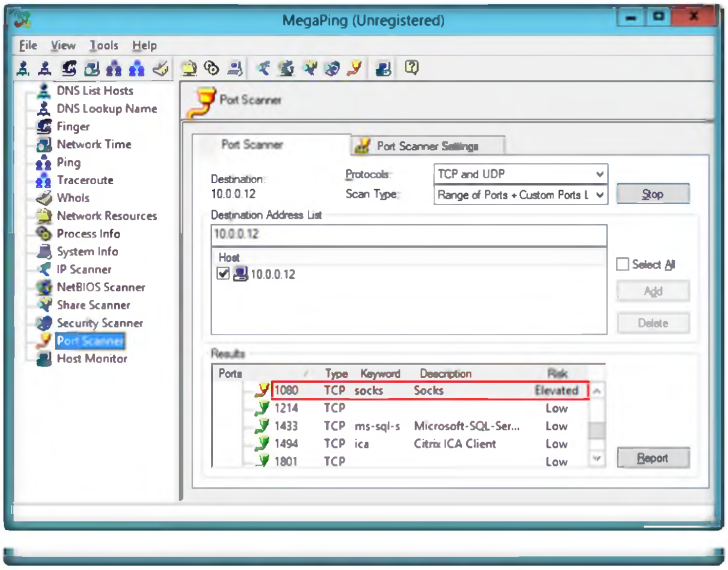
Results

Ports	Type	Keyword	Description	Risk
22	TCP			High
23	TCP	telnet	Telnet	Elevated
25	TCP	smtp	Simple Mail Transfer	Elevated
42	TCP	nameser...	Host Name Server	Low
53	TCP	domain	Domain Name Serv...	Low

FIGURE 3.18: MegaPing: Telnet port data

25. The following image displays the identification of Socks on port 1080.

The events are sorted in either ascending or descending chronological order. This is controlled by options on the View Menu.



Destination: 10.0.0.12

Protocols: TCP and UDP

Scan Type: Range of Ports + Custom Ports L

Destination Address List: 10.0.0.12

Host: ☑ 10.0.0.12

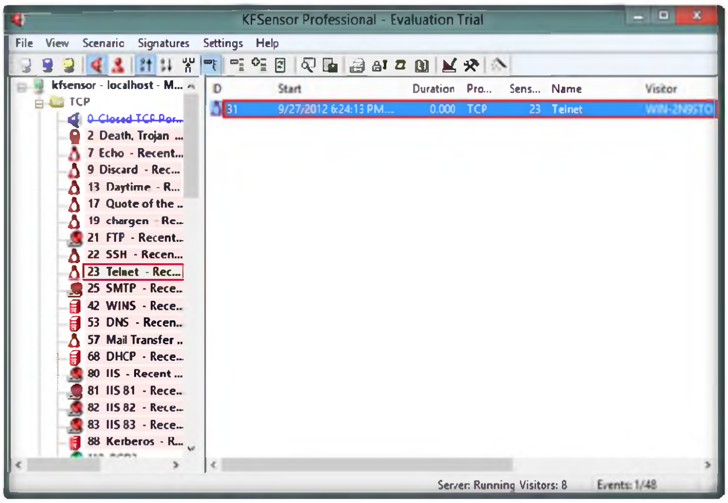
Results

Ports	Type	Keyword	Description	Risk
1080	TCP	socks	Socks	Elevated
1214	TCP			Low
1433	TCP	ms-sql-s	Microsoft-SQL-Ser...	Low
1494	TCP	ica	Citrix ICA Client	Low
1801	TCP			Low

FIGURE 3.19: MegaPing: Blackjack virus

26. Now come back to **Windows 8** virtual machine and look for Telnet data.

The events that are displayed are filtered by the currently selected item in the Ports View or the Visitors View.

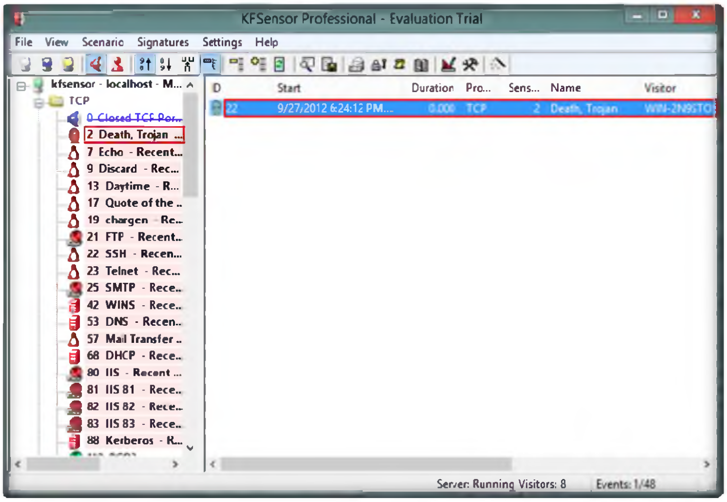


ID	Start	Duration	Pro...	Sens...	Name	Visitor
31	9/27/2012 6:24:13 PM...	0.000	TCP	23	Telnet	WIN-2N9STO

Server: Running Visitors: 8 Events: 1/48

FIGURE 3.20: Telnet data on KFSensor

27. The following image displays the data of a Death Trojan.



kfsensor - localhost - M...
TCP
~~0 Closed TCP Por...~~
2 Death, Trojan ...
7 Echo - Recent...
9 Discard - Rec...
13 Daytime - R...
17 Quote of the ..
19 chargen - Re...
21 FTP - Recent...
22 SSH - Recen...
23 Telnet - Rec...
25 SMTP - Rece...
42 WINS - Rece...
53 DNS - Recen...
57 Mail Transfer ..
68 DHCP - Rece...
80 IIS - Recent ...
81 IIS 81 - Rece...
82 IIS 82 - Rece...
83 IIS 83 - Rece...
88 Kerberos - R...

D	Start	Duration	Pro...	Sens...	Name	Visitor
22	9/27/2012 6:24:12 PM...	0.000	TCP	2	Death, Trojan	WIN-2N9STO

Server: Running Visitors: 8 Events: 1/48

FIGURE 3.21: Death Trojan data on KFSensor

Exit: Shuts down the KFSensor Monitor. If the KFSensor Server if not installed as a systems service then it will be shut down as well.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
KFSensor Honeypot IDS	**Output:** Infected Port number: 1080 Number of Detected Trojans: 2

Internet Connection Required	
□ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab
4

HTTP Tunneling Using HTTPort

HTTPort is a program from HTTHost that creates a transparent tunnel through a proxy server or firewall.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers are always in a hunt for clients that can be easily compromised and they can enter your network by IP spoofing to damage or steal your data. The attacker can get packets through a firewall by spoofing the IP address. If attackers are able to capture network traffic as you have learned to do in the previous lab, they can perform Trojan attacks, registry attacks, password hijacking attacks, etc., which can prove to be disastrous for an organization's network. An attacker may use a network probe to capture raw packet data and then use this raw packet data to retrieve packet information such as source and destination IP address, source and destination ports, flags, header length, checksum, Time to Live (TTL), and protocol type.

Hence, as a network administrator you should be able to identify attacks by extracting information from captured traffic such as source and destination IP addresses, protocol type, header length, source and destination ports, etc. and compare these details with modeled attack signatures to determine if an attack has occurred. You can also check the attack logs for the list of attacks and take evasive actions.

Also, you should be familiar with the HTTP tunneling technique by which you can identify additional security risks that may not be readily visible by conducting simple network and vulnerability scanning and determine the extent to which a network IDS can identify malicious traffic within a communication channel. In this lab, you will learn HTTP tunneling using HTTPort.

Lab Objectives

This lab will show you how networks can be scanned and how to use **HTTPort** and **HTTHost**.

Lab Environment

In the lab, you need the HTTPort tool.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots

- **HTTPort** is located at **D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots\HTTPort**
- You can also download the latest version of **HTTPort** from the link http://www.targeted.org
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Install HTTHost on **Windows 8** Virtual Machine
- Install HTTPort on **Windows Server 2012** Host Machine
- Follow the wizard-driven installation steps and **install it**
- **Administrative privileges** are required to run this tool

Lab Duration

Time: 20 Minutes

Overview of HTTPort

HTTPort creates a transparent tunnel through a proxy server or firewall. HTTPort allows using all sorts of Internet software from behind the proxy. It bypasses **HTTP proxies** and **HTTP**, **firewalls**, and **transparent accelerators**.

TASK 1

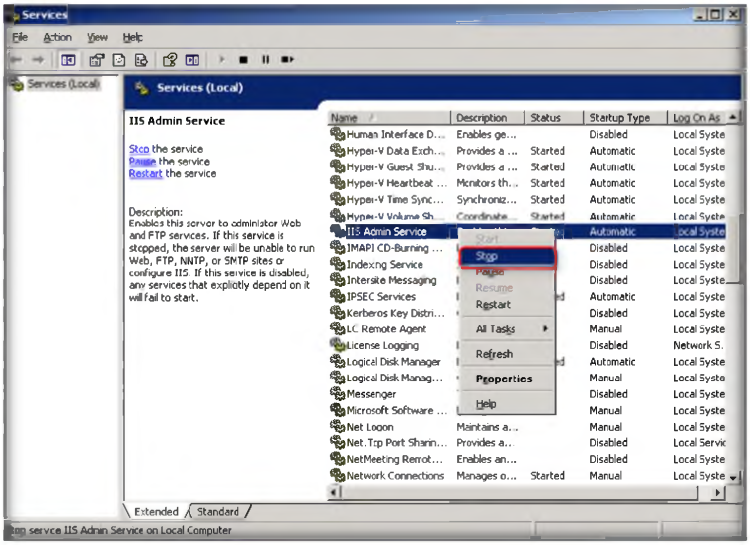
Stopping IIS Services

Lab Tasks

1. Before running tool you need to stop **IIS Admin Service** and **World Wide Web services** on **Windows Server 2008 virtual machine**.

2. Select **Administrative Privileges → Services → IIS Admin Service**, right-click and select **Stop**.

HTTPort creates a transparent tunnel through a proxy server or firewall. This allows you to use all sorts of Internet software from behind the proxy.



IIS Admin Service

Stop the service
Pause the service
Restart the service

Description:
Enables this server to administer Web and FTP services. If this service is stopped, the server will be unable to run Web, FTP, NNTP, or SMTP sites or configure IIS. If this service is disabled, any services that explicitly depend on it will fail to start.

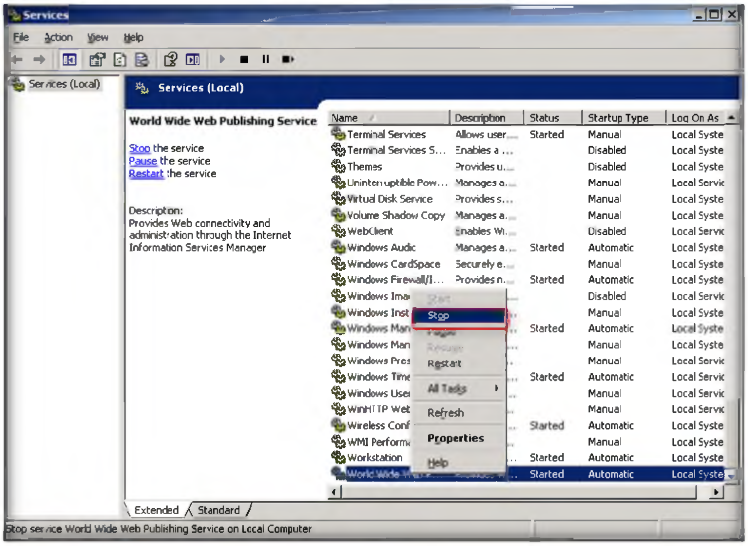
Name	Description	Status	Startup Type	Log On As
Human Interface D...	Enables ge...		Disabled	Local Syste
Hyper-V Data Exch...	Provides a ...	Started	Automatic	Local Syste
Hyper-V Guest Shu...	Provides a ...	Started	Automatic	Local Syste
Hyper-V Heartbeat ...	Monitors th...	Started	Automatic	Local Syste
Hyper-V Time Sync...	Synchroniz...	Started	Automatic	Local Syste
Hyper-V Volume Sh...	Coordinate...	Started	Automatic	Local Syste
IIS Admin Service			Automatic	Local Syste
IMAPI CD-Burning ...			Disabled	Local Syste
Indexing Service			Disabled	Local Syste
Intersite Messaging			Disabled	Local Syste
IPSEC Services			Automatic	Local Syste
Kerberos Key Distri...			Disabled	Local Syste
LC Remote Agent			Manual	Local Syste
License Logging			Disabled	Network S.
Logical Disk Manager			Automatic	Local Syste
Logical Disk Manag...			Manual	Local Syste
Messenger			Disabled	Local Syste
Microsoft Software ...			Manual	Local Syste
Net Logon	Maintains a...		Manual	Local Syste
Net.Tcp Port Sharin...	Provides a...		Disabled	Local Servic
NetMeeting Remot...	Enables an...		Disabled	Local Syste
Network Connections	Manages o...	Started	Manual	Local Syste

Stop service IIS Admin Service on Local Computer

FIGURE 4.1: Stopping IIS Admin Service in Windows Server 2008

It bypasses HTTPS and HTTP proxies, transparent accelerators, and firewalls. It has a built-in SOCKS4 server.

3. Select **Administrative Privileges → Services → World Wide Web Services**, right-click and select **Stop**.



World Wide Web Publishing Service

Stop the service
Pause the service
Restart the service

Description:
Provides Web connectivity and administration through the Internet Information Services Manager

Name	Description	Status	Startup Type	Log On As
Terminal Services	Allows user...	Started	Manual	Local Syste
Terminal Services S...	Enables a ...		Disabled	Local Syste
Themes	Provides u...		Disabled	Local Syste
Uninterruptible Pow...	Manages a...		Manual	Local Servic
Virtual Disk Service	Provides s...		Manual	Local Syste
Volume Shadow Copy	Manages a...		Manual	Local Syste
WebClient	Enables Wi...		Disabled	Local Servic
Windows Audio	Manages a...	Started	Automatic	Local Syste
Windows CardSpace	Securely e...		Manual	Local Syste
Windows Firewall/I...	Provides n...	Started	Automatic	Local Syste
Windows Ima	...		Disabled	Local Servic
Windows Inst	...		Manual	Local Syste
Windows Man	...	Started	Automatic	Local Syste
Windows Man	...		Manual	Local Syste
Windows Pres	...		Manual	Local Servic
Windows Time	...	Started	Automatic	Local Servic
Windows User	...		Manual	Local Servic
WinHTTP Wet	...		Manual	Local Servic
Wireless Conf	...	Started	Automatic	Local Syste
WMI Performa	...		Manual	Local Syste
Workstation	...	Started	Automatic	Local Syste
World Wide W...	...	Started	Automatic	Local Syste

Stop service World Wide Web Publishing Service on Local Computer

FIGURE 4.2: Stopping World Wide Web Services in Windows Server 2008

4. Log in to **Windows Server 2008** virtual machine.

5. Open Mapped Network Drive **CEH-Tools** at **Z:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots**.

It supports strong traffic encryption, which makes proxy logging useless, and supports NTLM and other authentication schemes.

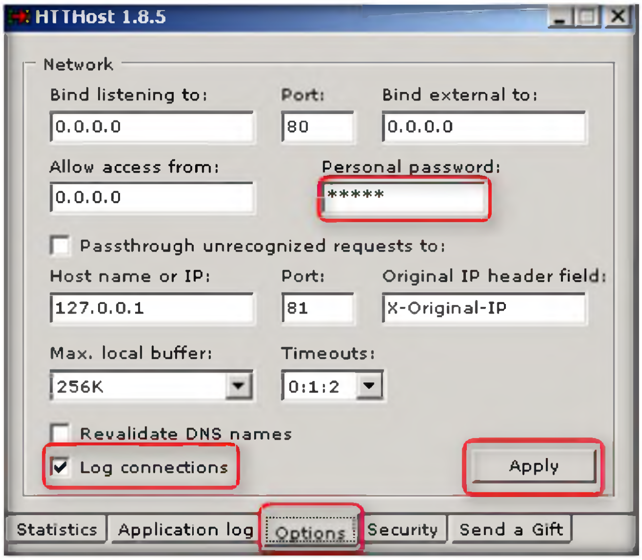
6. Open the **HTTHost** folder and double-click **htthost.exe**.

7. A **HTTHost** wizard will open; select the **Options** tab.

8. On the **Options** tab leave all the settings as their defaults except the **Personal Password** field, which should be filled with any other password. In this Lab the Personal Password is "**magic**."

9. Check the **Log Connections** option and click **Apply**.

Tools demonstrated in this lab are available in Z:\ Mapped Network Drive



Network

Bind listening to: 0.0.0.0 Port: 80 Bind external to: 0.0.0.0

Allow access from: 0.0.0.0 Personal password: *****

□ Passthrough unrecognized requests to:

Host name or IP: 127.0.0.1 Port: 81 Original IP header field: X-Original-IP

Max. local buffer: 256K Timeouts: 0:1:2

□ Revalidate DNS names

☑ Log connections

FIGURE 4.3: HTTHost Options tab

10. Now leave **HTTHost** intact, and don't turn off **Windows Server 2008** Virtual Machine.

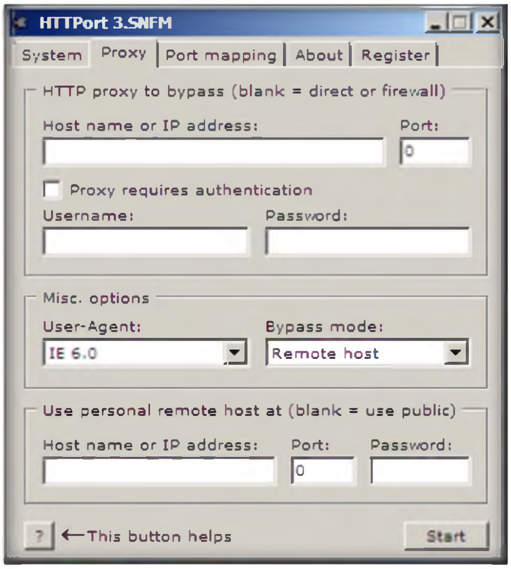
11. Now switch to **Windows Server 2008 Host Machine**, and install HTTPort from **D:\CEH-Tools\CEHv7 Module 16 Evading IDS, Firewalls and Honeypots**.

12. Follow the wizard-driven installation steps.

13. Now open **HTTPort** from **Start → All Programs → HTTPort 35NFM → HTTPort 35NFM**.

14. The **HTTPort** window appears as shown in the following figure.

To set up HTTPort need to point your browser to 127.0.0.1



HTTP proxy to bypass (blank = direct or firewall)

Host name or IP address: Port: 0

□ Proxy requires authentication

Username: Password:

Misc. options

User-Agent: IE 6.0 Bypass mode: Remote host

Use personal remote host at (blank = use public)

Host name or IP address: Port: 0 Password:

FIGURE 4.4: HTTPort Main Window

15. Select the **Proxy** tab and enter the **Host name** or **IP address** of the targeted machine.

HTTPort goes with the predefined mapping "External HTTP proxy" of local port

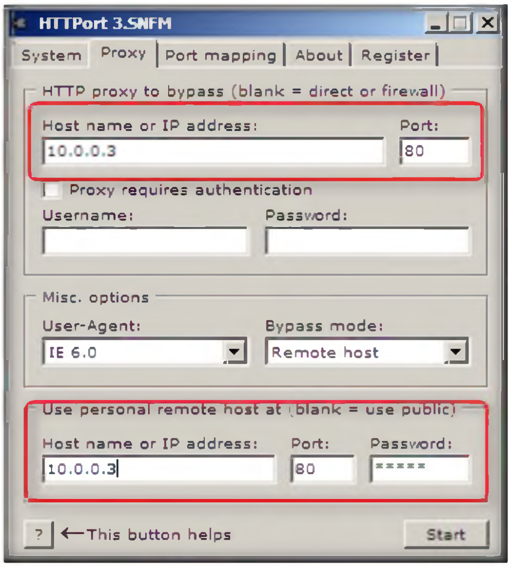
16. Here, as an example, enter the **Windows Server 2008** virtual machine **IP address**, and enter **Port number 80**.

17. You cannot set the **Username** and **Password** fields.

18. In **User personal remote host at section**, enter the targeted **Host machine IP address** and the port should be **80**.

19. Here any password could be chosen. Here as an example the password is **magic**.

For each software to create custom, given all the addresses from which it operates. For applications that are dynamically changing the ports there Socks4-proxy mode, in which the software will create a local server Socks (127.0.0.1)



HTTPort 3.SNFM

HTTP proxy to bypass (blank = direct or firewall)

Host name or IP address: 10.0.0.3

Port: 80

□ Proxy requires authentication

Username:

Password:

Misc. options

User-Agent: IE 6.0

Bypass mode: Remote host

Use personal remote host at (blank = use public)

Host name or IP address: 10.0.0.3

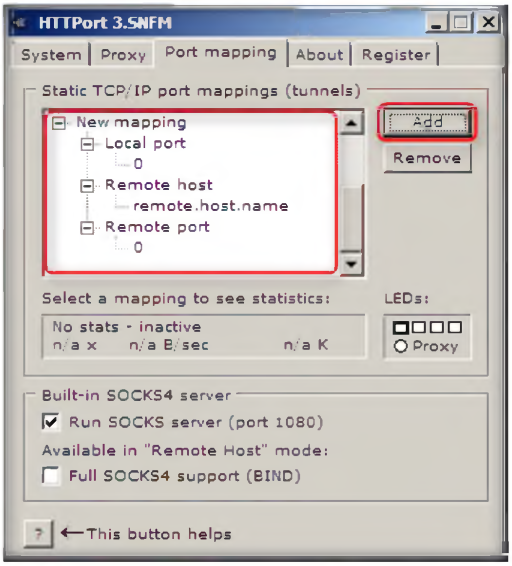
Port: 80

Password: *****

FIGURE 4.5: HTTPort Proxy settings window

20. Select the **Port Mapping** tab and click **Add** to create **New Mapping**.

In real world environment, people sometimes use password protected proxy to make company employees to access the Internet.



Static TCP/IP port mappings (tunnels)

New mapping
Local port
0
Remote host
remote.host.name
Remote port
0

Select a mapping to see statistics:

No stats - inactive
n/a x n/a B/sec n/a K

○ Proxy

Built-in SOCKS4 server

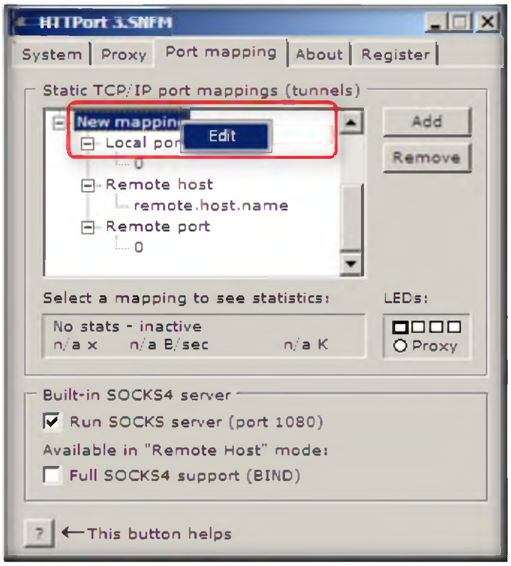
☑ Run SOCKS server (port 1080)

Available in "Remote Host" mode:

□ Full SOCKS4 support (BIND)

FIGURE 4.6: HTTPort creating a New Mapping

21. Select **New Mapping Node**, and right-click **New Mapping**, and select **Edit**.



Static TCP/IP port mappings (tunnels)

New mappin
Local por
0
Remote host
remote.host.name
Remote port
0

Select a mapping to see statistics:

No stats - inactive
n/a x n/a B/sec n/a K

○ Proxy

Built-in SOCKS4 server

☑ Run SOCKS server (port 1080)

Available in "Remote Host" mode:

□ Full SOCKS4 support (BIND)

FIGURE 4.7: HTTPort Editing to assign a mapping

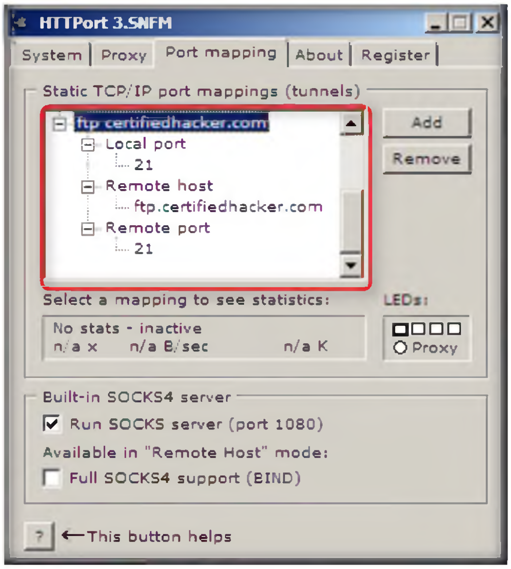
HTTHost supports the registration, but it is free and password-free - you will be issued a unique ID, which you can contact the support team and ask your questions.

22. Rename it to **ftp certified hacker**, and select **Local port node**, right-click to **Edit** and enter a **Port value** to **80**.

23. Now right-click **Remote host node** to **Edit** and rename it as **ftp.certifiedhacker.com**.

24. Now right click **Remote port** node to **Edit** and enter the port value of **21**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots


HTTPort 3.SNFM

Static TCP/IP port mappings (tunnels)

- ftp certifiedhacker.com
  - Local port
    - 21
  - Remote host
    - ftp.certifiedhacker.com
  - Remote port
    - 21

Select a mapping to see statistics:

No stats - inactive
n/a x n/a B/sec n/a K

LEDs:
□□□□
○ Proxy

Built-in SOCKS4 server

☑ Run SOCKS server (port 1080)

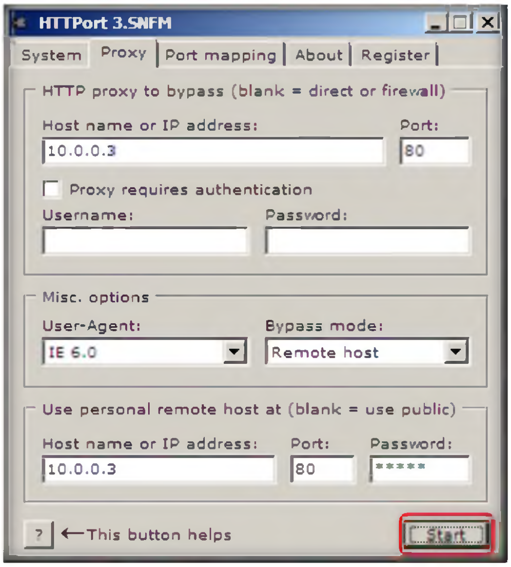
Available in "Remote Host" mode:

□ Full SOCKS4 support (BIND)

FIGURE 4.8: HTTPort Static TCP/IP port mapping

25. Click **Start** on the **Proxy** tab of HTTPort to run the HTTP tunneling.

In this kind of environment, the federated search webpart of Microsoft Search Server 2008 will not work out-of-the-box because we only support non-password protected proxy.


HTTPort 3.SNFM

HTTP proxy to bypass (blank = direct or firewall)

Host name or IP address: 10.0.0.3
Port: 80

□ Proxy requires authentication

Username:
Password:

Misc. options

User-Agent: IE 6.0
Bypass mode: Remote host

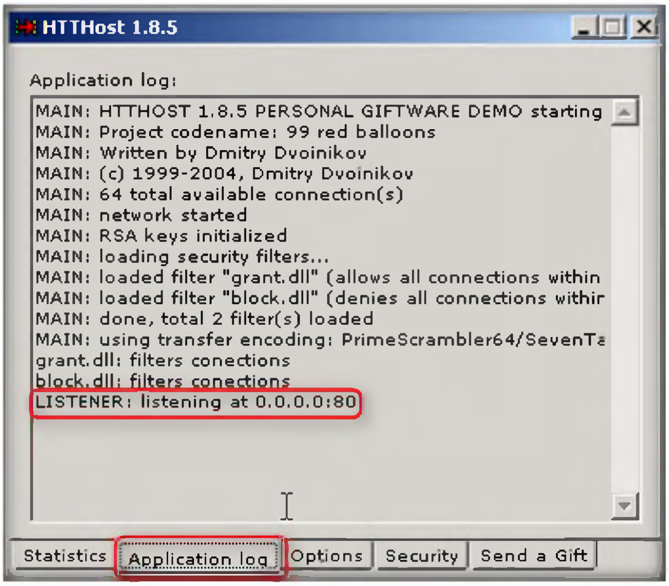
Use personal remote host at (blank = use public)

Host name or IP address: 10.0.0.3
Port: 80
Password: *****

FIGURE 4.9: HTTPort to start tunneling

26. Now switch to **Windows Server 2008** virtual machine and click the **Applications log** tab.

27. Check the last line. If **Listener: listening at 0.0.0.0:80**, then it is running properly.



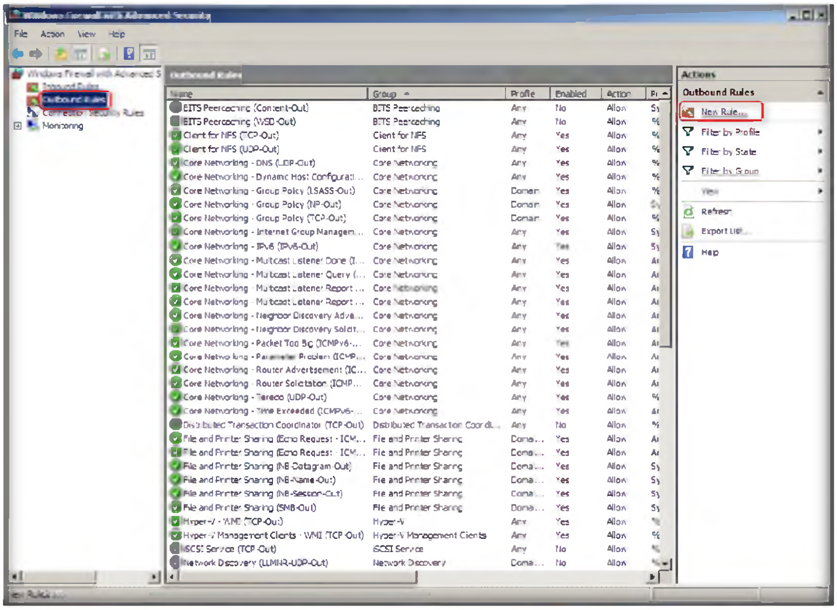
```
MAIN: HTTHOST 1.8.5 PERSONAL GIFTWARE DEMO starting
MAIN: Project codename: 99 red balloons
MAIN: Written by Dmitry Dvoinikov
MAIN: (c) 1999-2004, Dmitry Dvoinikov
MAIN: 64 total available connection(s)
MAIN: network started
MAIN: RSA keys initialized
MAIN: loading security filters...
MAIN: loaded filter "grant.dll" (allows all connections within
MAIN: loaded filter "block.dll" (denies all connections withir
MAIN: done, total 2 filter(s) loaded
MAIN: using transfer encoding: PrimeScrambler64/SevenTa
grant.dll: filters conections
block.dll: filters conections
LISTENER: listening at 0.0.0.0:80
```

FIGURE 4.10: HTTHost Application log section

28. Now switch to **Windows Server 2008** host machine and turn **ON** the **Windows Firewall**.

29. Go to **Windows Firewall with Advanced Security**.

30. Select **Outbound rules** from the left pane of the window, then click **New Rule** in the right pane of the window.



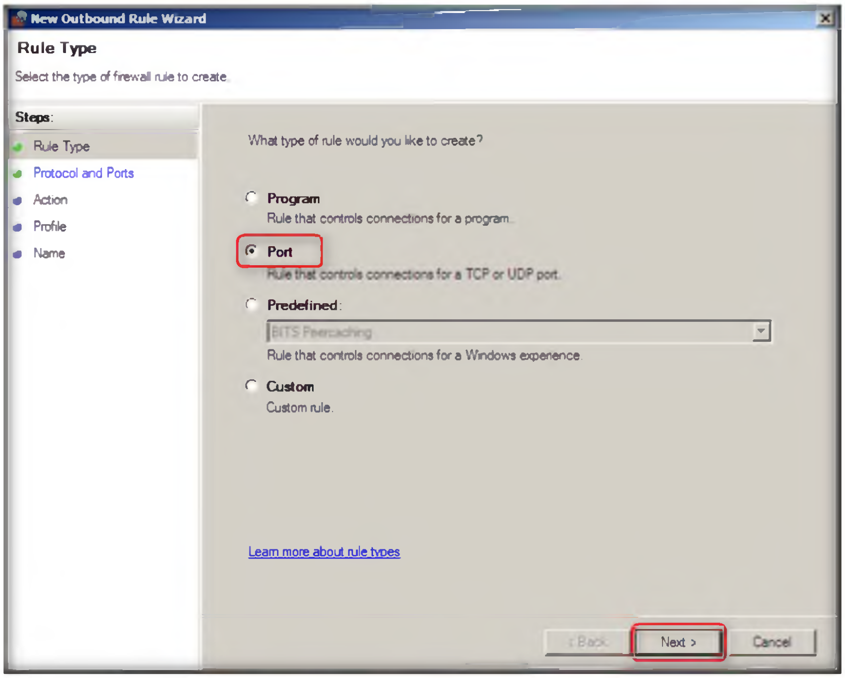
Name	Group	Profile	Enabled	Action	Pı
BITS Peercaching (Content-Out)	BITS Peercaching	Any	No	Allow	Sy
BITS Peercaching (WSD-Out)	BITS Peercaching	Any	No	Allow	%
Client for NFS (TCP-Out)	Client for NFS	Any	Yes	Allow	%
Client for NFS (UDP-Out)	Client for NFS	Any	Yes	Allow	%
Core Networking - DNS (UDP-Out)	Core Networking	Any	Yes	Allow	%
Core Networking - Dynamic Host Configurati...	Core Networking	Any	Yes	Allow	%
Core Networking - Group Policy (LSASS-Out)	Core Networking	Domain	Yes	Allow	%
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	Sy
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	%
Core Networking - Internet Group Managem...	Core Networking	Any	Yes	Allow	Sy
Core Networking - IPv6 (IPv6-Out)	Core Networking	Any	Yes	Allow	Sy
Core Networking - Multicast Listener Done (I...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Multicast Listener Query (...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Multicast Listener Report ...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Multicast Listener Report ...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Neighbor Discovery Adve...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Neighbor Discovery Solicit...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Packet Too Big (ICMPv6-...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Parameter Problem (ICMP...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Router Advertisement (IC...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Router Solicitation (ICMP...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Teredo (UDP-Out)	Core Networking	Any	Yes	Allow	%
Core Networking - Time Exceeded (ICMPv6-...	Core Networking	Any	Yes	Allow	Ar
Distributed Transaction Coordinator (TCP-Out)	Distributed Transaction Coordi...	Any	No	Allow	%
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Doma...	Yes	Allow	Ar
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Doma...	Yes	Allow	Ar
File and Printer Sharing (NB-Datagram-Out)	File and Printer Sharing	Doma...	Yes	Allow	Sy
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	Doma...	Yes	Allow	Sy
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	Doma...	Yes	Allow	Sy
File and Printer Sharing (SMB-Out)	File and Printer Sharing	Doma...	Yes	Allow	Sy
Hyper-V - WMI (TCP-Out)	Hyper-V	Any	Yes	Allow	%
Hyper-V Management Clients - WMI (TCP-Out)	Hyper-V Management Clients	Any	Yes	Allow	%
iSCSI Service (TCP-Out)	iSCSI Service	Any	No	Allow	%
Network Discovery (LLMNR-UDP-Out)	Network Discovery	Doma...	No	Allow	%

FIGURE 4.11: Windows Firewall with Advanced Security window in Windows Server 2008

Tools demonstrated in this lab are available in Z:\ Mapped Network Drive in Virtual Machines

31. In the **New Outbound Rule Wizard**, check the **Port** option in the **Rule Type** section and click **Next**.

HTTPort doesn't really care for the proxy as such, it works perfectly with firewalls, transparent accelerators, NATs and basically anything that lets HTTP protocol through.



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

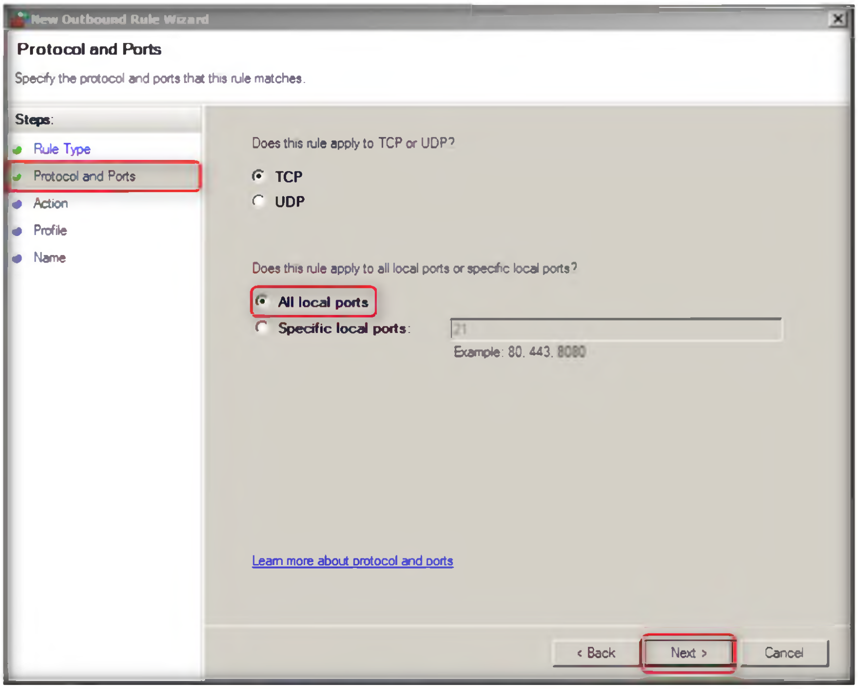
○ **Predefined**:
BITS Peercaching
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

FIGURE 4.12: Windows Firewall selecting a Rule Type

32. Now select **All local ports** in the **Protocol and Ports** section.

You need to install htthost on a PC, who is generally accessible on the Internet - typically your "home" PC. This means that if you started a webserver on the home PC, everyone else must be able to connect to it. There are two showstoppers for htthost on home PCs



New Outbound Rule Wizard

Protocol and Ports

Specify the protocol and ports that this rule matches.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

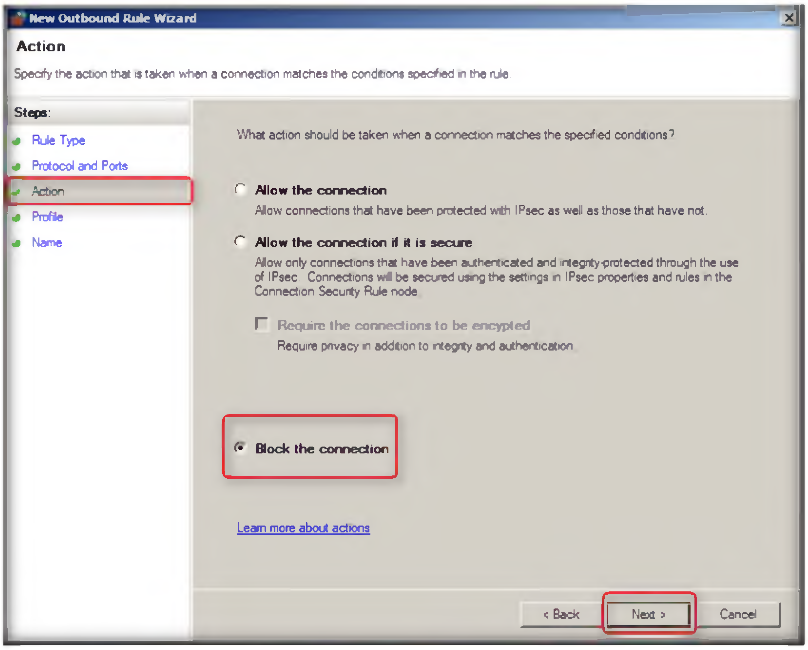
Does this rule apply to all local ports or specific local ports?

● **All local ports**
○ **Specific local ports**: 21
Example: 80, 443, 8080

FIGURE 4.13: Windows Firewall assigning Protocols and Ports

33. In the **Action** section, select **Block the connection** and click **Next**.

NAT/firewall issues: You need to enable an incoming port. For HTThost it will typically be 80(http) or 443(https), but any port can be used - IF the HTTP proxy at work supports it - some proxy's are configured to allow only 80 and 443.



Action

Specify the action that is taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

○ Allow the connection

Allow connections that have been protected with IPsec as well as those that have not.

○ Allow the connection if it is secure

Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

□ Require the connections to be encrypted

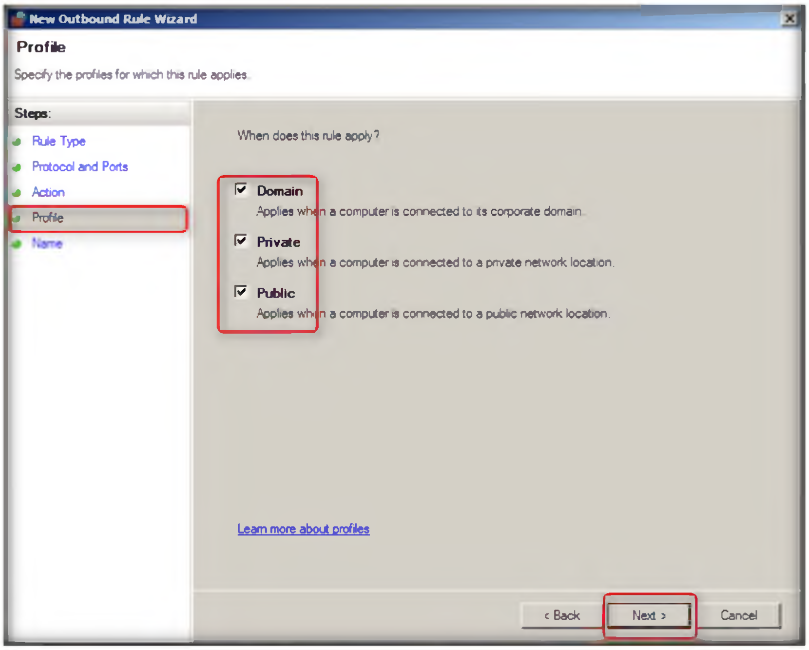
Require privacy in addition to integrity and authentication

● Block the connection

Learn more about actions

FIGURE 4.14: Windows Firewall setting an Action

34. In the **Profile** section, select all the three options. The rule will apply to: **Domain**, **Public**, **Private** and click **Next**.



Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ Domain

Applies when a computer is connected to its corporate domain.

☑ Private

Applies when a computer is connected to a private network location.

☑ Public

Applies when a computer is connected to a public network location.

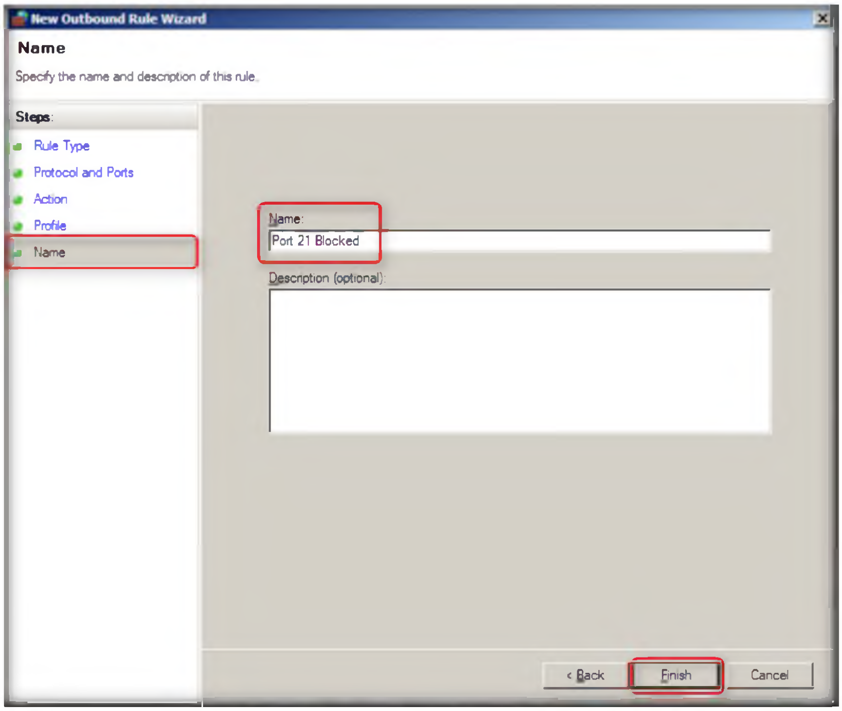
Learn more about profiles

FIGURE 4.15: Windows Firewall Profile settings

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots

35. Type **Port 21 Blocked** in the **Name** field, and click **Finish**.

The default TCP port for FTP connection is port 21. Sometimes the local Internet Service Provider blocks this port and this will result in FTP connection issues.



Name: Port 21 Blocked

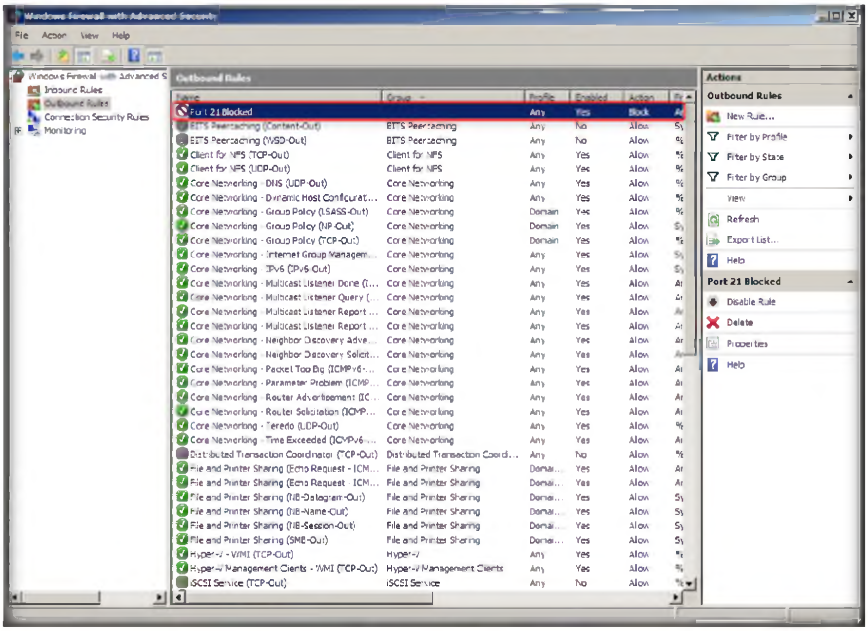
Description (optional):

FIGURE 4.16: Windows Firewall assigning a name to Port

36. New Rule **Port 21 Blocked** is created as shown in the following figure.

HTTPort doesn't really care for the proxy as such: it works perfectly with firewalls, transparent accelerators, NATs and basically anything that lets the HTTP protocol through.

HTTP is the basis for Web surfing, so if you can freely surf the Web from where you are, HTTPort will bring you the rest of the Internet applications.

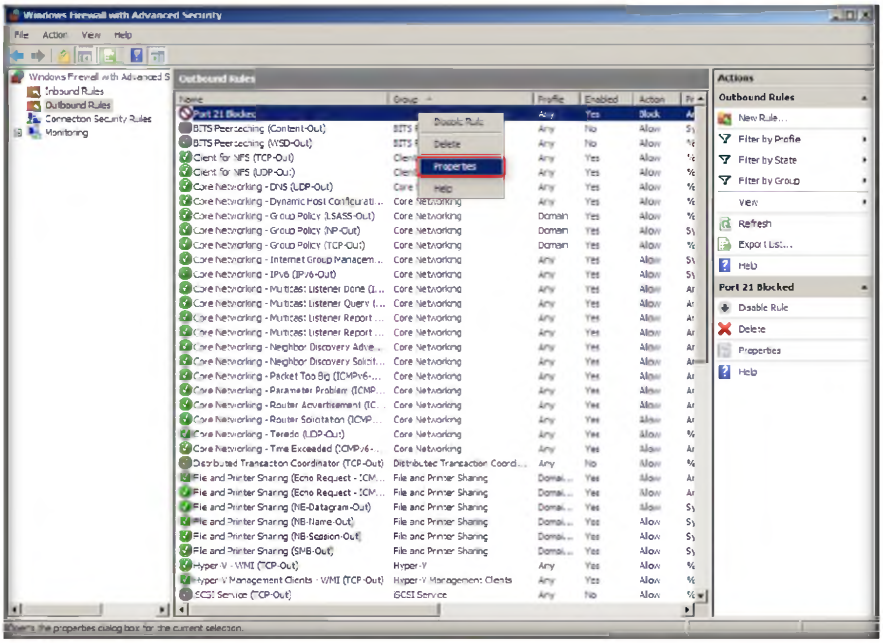


Name	Group	Profile	Enabled	Action
Port 21 Blocked		Any	Yes	Block
BITS Peercaching (Content-Out)	BITS Peercaching	Any	No	Allow
BITS Peercaching (WSD-Out)	BITS Peercaching	Any	No	Allow
Client for NFS (TCP-Out)	Client for NFS	Any	Yes	Allow
Client for NFS (UDP-Out)	Client for NFS	Any	Yes	Allow
Core Networking - DNS (UDP-Out)	Core Networking	Any	Yes	Allow
Core Networking - Dynamic Host Configurat...	Core Networking	Any	Yes	Allow
Core Networking - Group Policy (LSASS-Out)	Core Networking	Domain	Yes	Allow
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow
Core Networking - Internet Group Managem...	Core Networking	Any	Yes	Allow
Core Networking - IPv6 (IPv6-Out)	Core Networking	Any	Yes	Allow
Core Networking - Multicast Listener Done (I...	Core Networking	Any	Yes	Allow
Core Networking - Multicast Listener Query (...	Core Networking	Any	Yes	Allow
Core Networking - Multicast Listener Report ...	Core Networking	Any	Yes	Allow
Core Networking - Multicast Listener Report ...	Core Networking	Any	Yes	Allow
Core Networking - Neighbor Discovery Adve...	Core Networking	Any	Yes	Allow
Core Networking - Neighbor Discovery Solicit...	Core Networking	Any	Yes	Allow
Core Networking - Packet Too Big (ICMPv6-...	Core Networking	Any	Yes	Allow
Core Networking - Parameter Problem (ICMP...	Core Networking	Any	Yes	Allow
Core Networking - Router Advertisement (IC...	Core Networking	Any	Yes	Allow
Core Networking - Router Solicitation (ICMP...	Core Networking	Any	Yes	Allow
Core Networking - Teredo (UDP-Out)	Core Networking	Any	Yes	Allow
Core Networking - Time Exceeded (ICMPv6-...	Core Networking	Any	Yes	Allow
Distributed Transaction Coordinator (TCP-Out)	Distributed Transaction Coord...	Any	No	Allow
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (NB-Datagram-Out)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (SMB-Out)	File and Printer Sharing	Domai...	Yes	Allow
Hyper-V - WMI (TCP-Out)	Hyper-V	Any	Yes	Allow
Hyper-V Management Clients - WMI (TCP-Out)	Hyper-V Management Clients	Any	Yes	Allow
iSCSI Service (TCP-Out)	iSCSI Service	Any	No	Allow

FIGURE 4.17: Windows Firewall New rule

37. Right-click the newly created rule and select **Properties**.

HTTPort then intercepts that connection and runs it through a tunnel through the proxy.



Name	Group	Profile	Enabled	Action	Pr
Port 21 Blocked		Any	Yes	Block	A
BITS Peercaching (Content-Out)	BITS	Any	No	Allow	Sy
BITS Peercaching (WSD-Out)	BITS	Any	No	Allow	%
Client for NFS (TCP-Out)	Clien	Any	Yes	Allow	%
Client for NFS (UDP-Out)	Clien	Any	Yes	Allow	%
Core Networking - DNS (UDP-Out)	Core	Any	Yes	Allow	%
Core Networking - Dynamic Host Configurati...	Core Networking	Any	Yes	Allow	%
Core Networking - Group Policy (LSASS-Out)	Core Networking	Domain	Yes	Allow	%
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	Sy
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	%
Core Networking - Internet Group Managem...	Core Networking	Any	Yes	Allow	Sy
Core Networking - IPv6 (IPv6-Out)	Core Networking	Any	Yes	Allow	Sy
Core Networking - Multicast Listener Done (I...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Multicast Listener Query (I...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Multicast Listener Report ...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Multicast Listener Report ...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Neighbor Discovery Adve...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Neighbor Discovery Solicit...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Packet Too Big (ICMPv6-...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Parameter Problem (ICMP...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Router Advertisement (IC...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Router Solicitation (ICMP...	Core Networking	Any	Yes	Allow	Ar
Core Networking - Teredo (UDP-Out)	Core Networking	Any	Yes	Allow	%
Core Networking - Time Exceeded (ICMPv6-...	Core Networking	Any	Yes	Allow	Ar
Distributed Transaction Coordinator (TCP-Out)	Distributed Transaction Coordi...	Any	No	Allow	%
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Domai...	Yes	Allow	Ar
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Domai...	Yes	Allow	Ar
File and Printer Sharing (NB-Datagram-Out)	File and Printer Sharing	Domai...	Yes	Allow	Sy
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	Domai...	Yes	Allow	Sy
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	Domai...	Yes	Allow	Sy
File and Printer Sharing (SMB-Out)	File and Printer Sharing	Domai...	Yes	Allow	Sy
Hyper-V - WMI (TCP-Out)	Hyper-V	Any	Yes	Allow	%
Hyper-V Management Clients - WMI (TCP-Out)	Hyper-V Management Clients	Any	Yes	Allow	%
iSCSI Service (TCP-Out)	iSCSI Service	Any	No	Allow	%

Opens the properties dialog box for the current selection.

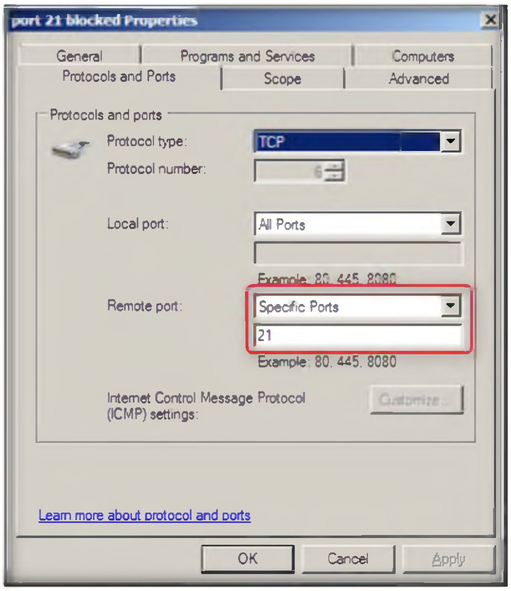
FIGURE 4.18: Windows Firewall new rule properties

Enables you to bypass your HTTP proxy in case it blocks you from the Internet

38. Select the **Protocols and Ports** tab. Change the **Remote Port** option to **Specific Ports** and enter the **Port number** as **21**.

39. Leave the other settings as their defaults and Select **Apply → OK**.

With HTTPort, you can use various Internet software from behind the proxy, e.g., e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC etc. The basic idea is that you set up your Internet software



Protocol type: TCP

Protocol number: 6

Local port: All Ports

Example: 80, 445, 8080

Remote port: Specific Ports

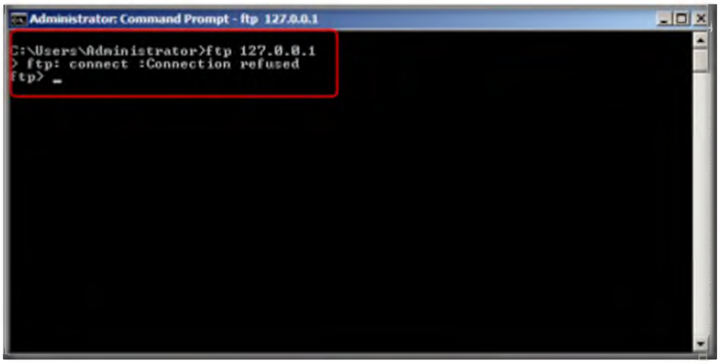
21

Example: 80, 445, 8080

Internet Control Message Protocol (ICMP) settings:

FIGURE 4.19: Firewall Port 21 Blocked Properties

40. Type **ftp 127.0.0.1** in the command prompt and press **Enter**. The connection is blocked at the local host in **Windows Server 2008**.

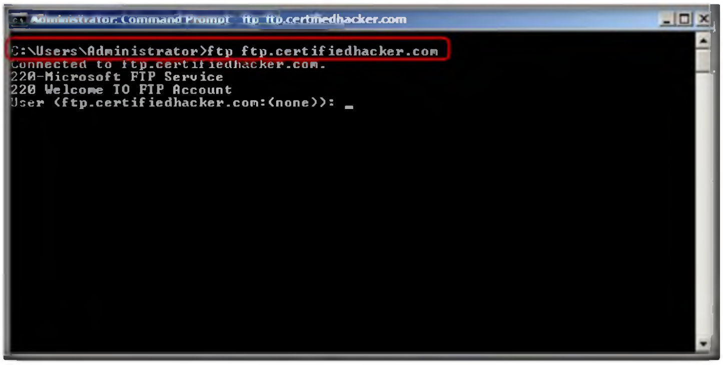


```
C:\Users\Administrator>ftp 127.0.0.1
> ftp: connect :Connection refused
ftp> _
```

FIGURE 4.20: ftp connection is blocked

HTTPort does neither freeze nor hang. What you are experiencing is known as "blocking operations"

41. Now open a command prompt in **Windows Server 2008** host machine and type **ftp ftp.certifiedhacker.com** and Press **Enter**



```
C:\Users\Administrator>ftp ftp.certifiedhacker.com
Connected to ftp.certifiedhacker.com.
220-Microsoft FTP Service
220 Welcome TO FTP Account
User (ftp.certifiedhacker.com:(none)): _
```

FIGURE 4.21: Executing ftp command

HTTPort makes it possible to open a client side of a TCP/IP connection and provide it to any software. The keywords here are: "client" and "any software".

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
HTTPort	**Proxy server Used:** 10.0.0.4
	Port scanned: 80
	Result: ftp 127.0.0.1 connected to 127.0.0.1

Questions

1. How would you set up an HTTPort to use an email client (Outlook, Messenger, etc.)?
2. Examine if the software does not allow editing the address to connect to.

Internet Connection Required	
☑ Yes	□No
Platform Supported	
☑ Classroom	□ iLabs