

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 (IDSe) 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 (IPSe), IDSe, malicious network activity, and log information.

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 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

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

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 IDSe:

- 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.

Module 17 – Evading IDS, Firewalls and Honeypots

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

Tools

**Demonstrated in
this lab are**

located at D:\CEH-

Tools\CEHv8

Module 17

**Evading IDS,
Firewalls, and
Honeypots**

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, IDSe, malicious network activity, and log information.

Lab Objectives

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

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

T A S K 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).

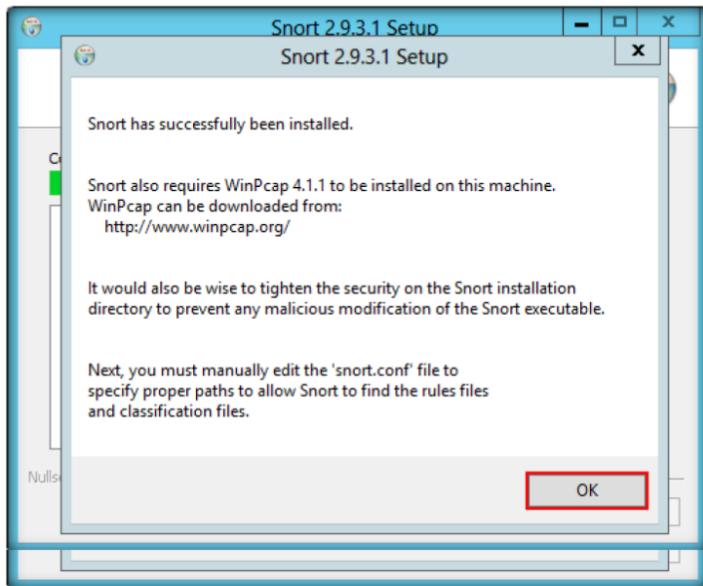


Figure 1.1: Snort Successful Installation Window

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

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 completes 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\snortrules\etc** of the extracted Snort rules, copy the **snort.conf** file, and paste this file in **C:\Snort\etc**.
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**.

Module 17 – Evading IDS, Firewalls and Honeypots

TASK 2

Verify Snort Alert

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

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**.
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**.

```
Administrator: C:\Windows\system32\cmd.exe - snort
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

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.

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-B614-0FC1985DDA25}	
3	00:00:00:00:00:00	disabled	\Device\NPF_{1D13B78A-B411-4325-B216-C98A98F0F2F1}	
4	D4:BE:D9:C3:C3:CC	disabled	\Device\NPF_{2A3EB470-39FB-4880-9A79-77E5AE27E530}	Realtek PCIe GBE Family Controller

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**.

Module 17 – Evading IDS, Firewalls and Honeypots

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

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

```
Administrator: C:\Windows\system32\cmd.exe - 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 ====
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: 8.19 2010-06-25
Using ZLIB version: 1.2.3
Commencing packet processing <pid=2852>
11/14/09 5:49.352079 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**.

```
Administrator: Command Prompt
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 (0x loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 17ms, Average = 16ms

C:\Users\Administrator>
```

Figure 1.5: Ping google.com Command

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

To enable Network Intrusion Detection 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.

```
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
***0P*** Seq: 0x81047C40 Ack: 0xC743C54 Win: 0xFFFF TcpLen: 20
17 03 02 00 32 43 3F 4C 22 B4 01 69 AB 37 FD 34 ...2C7L'..1.7.4
17 03 02 00 32 43 3F 4C 22 B4 01 69 AB 37 FD 34 ...2C7L'..1.7.4
17 03 02 00 32 43 3F 4C 22 F4 B9 6C BD AE E8 0E SA ...101'..1...Z
8D 8A B9 0F C6 3B 5B 22 F4 B9 6C BD AE E8 0E SA ...101'..1...Z
8F F6 7D 55 31 78 EF ...01X.

11/14/09 5:58:16.3724896 D4:BE:D9:C3:C3:CC -> 00:09:5B:AЕ: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 DgmLen:40 DE
***R*** Seq: 0x4C743C54 Ack: 0x81047C77 Win: 0xFB27 TcpLen: 20
=====

11/14/09 5:58:17.496035 ARP who-has 10.0.0.13 tell 10.0.0.10
11/14/09 5:58:18.352315 ARP who-has 10.0.0.13 tell 10.0.0.10
11/14/09 5:58:19.352675 ARP who-has 10.0.0.13 tell 10.0.0.10
```

Figure 1.6: Snort Showing Captured Google Request

Module 17 – Evading IDS, Firewalls and Honeypots

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

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

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

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.

The screenshot shows the Notepad++ application window with the file 'snort.conf' open. The code in the editor is as follows:

```
1  # VRT Rule Packages Snort.conf
2  #
3  # For more information visit us at:
4  #   http://www.snort.org           Snort Website
5  #   https://vt.sourceforge.net/    Sourcefire VRT Blog
6  #
7  #
8  # Mailing list Contact:        snort-signs@lists.sourceforge.net
9  # False Positive reports:      fp@sourcefire.com
10 # Smart bugs:                  bugs@snort.org
11 #
12 # Compatible with Snort Versions:
13 # VERSIONS : 2.9.3.1
14 #
15 # Snort build options:
16 # OPTIONS : --enable-ipv6 --enable-gre --enable-mpls --enable-targetbased --enable-decoder-preprocessor-
17 #
18 # Additional information:
19 # This configuration file enables active response, so run snort in
20 # test mode -T you are required to supply an interface -i <interface>
21 # or test mode will fail to fully validate the configuration and
22 # exit with a FATAL error
23 #
24 #
25 ##### This file contains a sample snort configuration.
26 #
27 # You should take the following steps to create your own custom configuration:
28 #
```

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

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.

The screenshot shows the Notepad++ application window with the file 'snort.conf' open. The code in the editor is as follows, with the 'HOME_NET' line highlighted:

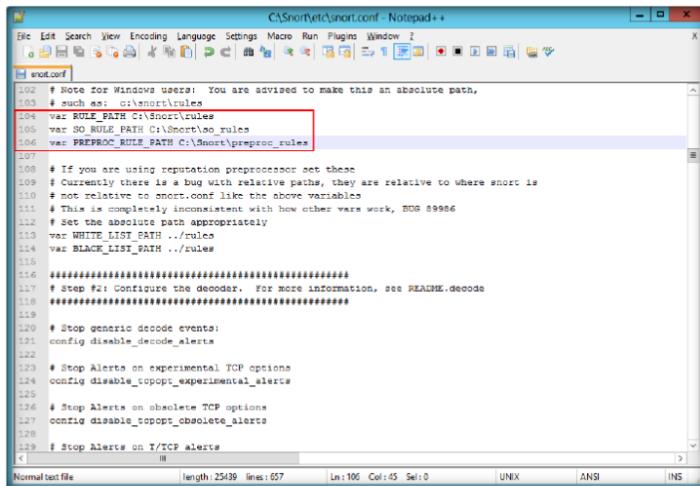
```
39 #
40 # Step #1: Set the network variables. For more information, see README.variables
41 #
42 #
43 #
44 # Set the network addresses you are protecting
45 ipvar HOME_NET 10.0.0.10
46 #
47 # Set up the external network addresses. Leave as "any" in most situations
48 ipvar EXTERNAL_NET any
49 #
50 # 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
67 
```

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**.



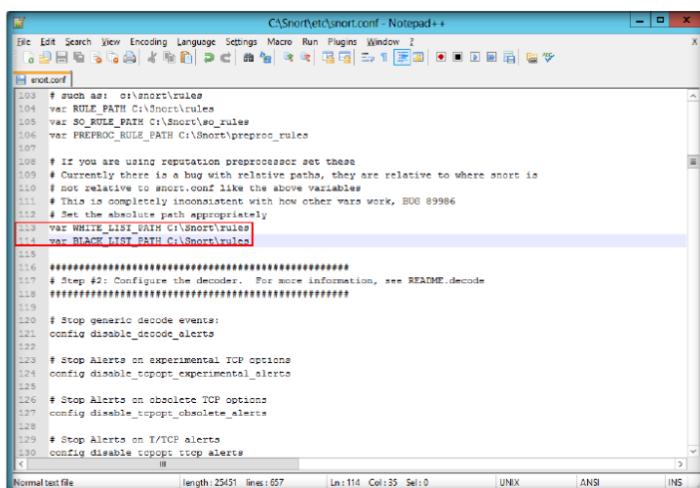
```

C:\Snortetc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window Z
o | A | C | F | G | H | I | L | M | N | P | R | S | T | U | V | W | X | Y | Z | 
[ snort.conf ]
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, EDD 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_tcpoptObsolete_alerts
128
129 # Stop Alerts on T/TCP alerts
130 config disable_tropcp_trop_alerts
< -----
Normal text file | length: 25439 | lines: 657 | ln:106 Col:45 Sel:0 | UNIX | ANSI | INS

```

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

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



```

C:\Snortetc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window Z
o | A | C | F | G | H | I | L | M | N | P | R | S | T | U | V | W | X | Y | Z | 
[ snort.conf ]
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, EDD 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_tcpoptObsolete_alerts
128
129 # Stop Alerts on T/TCP alerts
130 config disable_tropcp_trop_alerts
< -----
Normal text file | length: 25451 | lines: 657 | ln:114 Col:35 Sel:0 | UNIX | ANSI | INS

```

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**.

```

241 #####
242 # Step #4: Configure dynamic loaded libraries.
243 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
244 #####
245 #
246 # path to dynamic preprocessor libraries
247 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
248 #
249 # path to base preprocessor engine
250 dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so
251 #
252 # path to dynamic rules libraries
253 dynamicdetection directory /usr/local/lib/snort_dynamicrules
254 #####
255 #####
256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 #####
259 #
260 # GTP Control Channel Preprocessor. For more information, see README.GTP
261 # preprocessor gtp: ports ( 2123 3386 2182 )
262 #
263 # Inline packet normalization. For more information, see README.normalize
264 # Does nothing in IDS mode
265 preprocessor normalize_ip4
266 preprocessor normalize_ip6
267 preprocessor normalize_icmp
268 preprocessor normalize_ip6
< -----

```

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

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**.

```

241 #####
242 # Step #4: Configure dynamic loaded libraries.
243 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
244 #####
245 #
246 # path to dynamic preprocessor libraries
247 #
248 # path to dynamic preprocessor libraries
249 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
250 #
251 # path to base preprocessor engine
252 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
253 #
254 # path to dynamic rules libraries
255 dynamicdetection directory /usr/local/lib/snort_dynamicrules
256 #####
257 #####
258 # Step #5: Configure preprocessors
259 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
260 #####
261 #
262 # GTP Control Channel Preprocessor. For more information, see README.GTP
263 # preprocessor gtp: ports ( 2123 3386 2182 )
264 #
265 # Inline packet normalization. For more information, see README.normalize
266 # Does nothing in IDS mode
267 preprocessor normalize_ip4
268 preprocessor normalize_ip6
269 preprocessor normalize_icmp
270 preprocessor normalize_ip6
< -----

```

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

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.

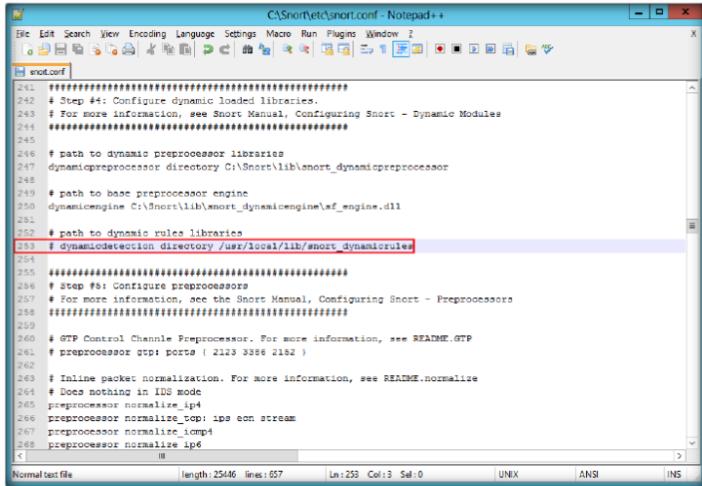
Preprocessors are loaded and configured using the ‘preprocessor’ keyword. The format of the preprocessor directive in the Snort rules file is:
preprocessor <name>:
<options>.

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

Module 17 – Evading IDS, Firewalls and Honeypots

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.

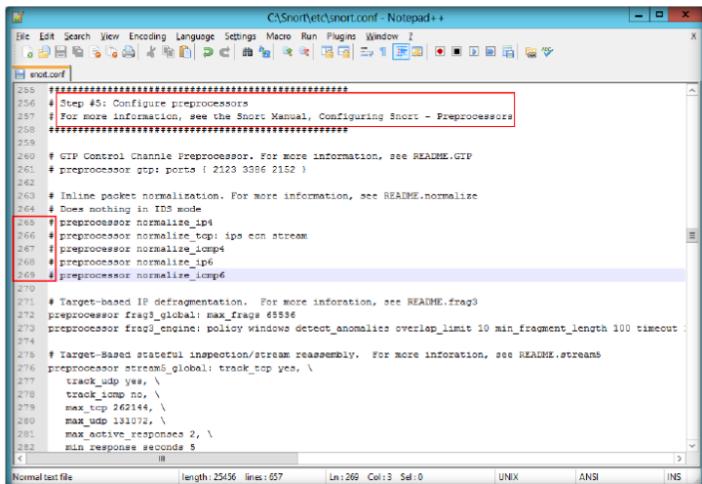


```
C:\Snort\etc\snort.conf - Notepad++  
File Edit Search View Encoding Language Settings Macro Run Plugins Window I  
[snort.conf]  
241 ##### Step #4: Configure Dynamic Loadable Libraries.  
242 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules  
243 #####  
244  
245 # path to dynamic preprocessor libraries  
246 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor  
247  
248 # path to base preprocessor engine  
249 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll  
250  
251 # path to dynamic rules libraries  
252 # dynamicdetection directory /usr/local/lib/snort_dynamicrules  
253 #####  
254  
255 ##### Step #5: Configure preprocessors  
256 # For more information, see the Snort Manual, Configuring Snort - Preprocessors  
257 #####  
258  
259 # GTP Control Channel Preprocessor. For more information, see README.GTP  
260 # preprocessor gtp: ports { 2123 3386 2152 }  
261  
262 # Inline packet normalization. For more information, see README.normalize  
263 # Does nothing in IDS mode  
264 preprocessor normalize_ip4  
265 preprocessor normalize_ip6: ips ecn stream  
266 preprocessor normalize_icmp4  
267 preprocessor normalize_ip6  
268  
< ... >  
Normal text file | length: 25466 lines: 657 | Ln:253 Col:3 Sel:0 | UNIX | ANSI | INS
```

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

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



```
C:\Snort\etc\snort.conf - Notepad++  
File Edit Search View Encoding Language Settings Macro Run Plugins Window I  
[snort.conf]  
255 #####  
256 # Step #5: Configure preprocessors  
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors  
258 #####  
259  
260 # GTP Control Channel Preprocessor. For more information, see README.GTP  
261 # preprocessor gtp: ports { 2123 3386 2152 }  
262  
263 # Inline packet normalization. For more information, see README.normalize  
264 # Does nothing in IDS mode  
265 # preprocessor normalize_ip4  
266 # preprocessor normalize_ip6: ips ecn stream  
267 # preprocessor normalize_icmp4  
268 # preprocessor normalize_ip6  
269  
270 # Target-based IP fragmentation. For more information, see README.frag3  
271 preprocessor frag_global: max frags 65536  
272 preprocessor fragd_engine: policy windows detect anomalies overlap_limit 10 min_fragment_length 100 timeout  
273  
274  
275 # Target-Based stateful inspection/stream reassembly. For more information, see README.streams  
276 preprocessor streams_global track_top yes, \  
277 track_udp yes, \  
278 track_icmp no, \  
279 max_tcp 262144, \  
280 max_udp 131072, \  
281 max_active_responses 2, \  
282 min_response_seconds 5  
< ... >  
Normal text file | length: 25456 lines: 657 | Ln:269 Col:3 Sel:0 | UNIX | ANSI | INS
```

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).

```

C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window I
[snort.conf]
514 # Step #6: Configure output plugins
515 # For more information, see Snort Manual, Configuring Snort - Output Modules
516 #####
517
518 # unified2
519 # Recommended for most installs
520 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types
521
522 # Additional configuration for specific types of installs
523 # output alert_unified2: filename snort.alert, limit 128, nostamp
524 # output log_unified2: filename snort.log, limit 128, nostamp
525
526 # syslog
527 # output alert_syslog: LOG_AUTH LOG_ALERT
528
529 # pcap
530 # output log_tcpdump: tcpdump.log
531
532 # database
533 # output database: alert, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>
534 # output database: log, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>
535
536 # prelude
537 # output alert_prelude
538
539 # metadata reference data, do not modify these lines
540 include C:\Snort\etc\classification.config
541 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.

```

C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window I
[snort.conf]
514 # Step #6: Configure output plugins
515 # For more information, see Snort Manual, Configuring Snort - Output Modules
516 #####
517
518 # unified2
519 # Recommended for most installs
520 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types
521
522 # Additional configuration for specific types of installs
523 # output alert_unified2: filename snort.alert, limit 128, nostamp
524 # output log_unified2: filename snort.log, limit 128, nostamp
525
526 # syslog
527 # output alert_syslog: LOG_AUTH LOG_ALERT
528
529 # pcap
530 # output log_tcpdump: tcpdump.log
531
532 # database
533 # output database: alert, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>
534 # output database: log, <db_type>, user=<username> password=<password> test dbname=<name> host=<hostname>
535
536 # prelude
537 # output alert_prelude
538 # output alert_fast: alerts.ids
539 # metadata reference data, do not modify these lines
540 include C:\Snort\etc\classification.config
541 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.

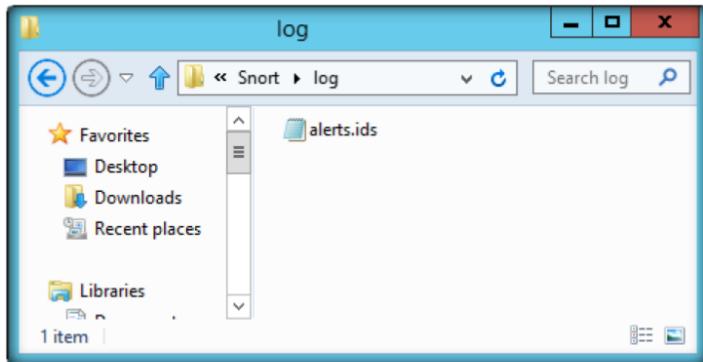


Figure 1.17: Configuring Snort.conf File in Notepad++

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.

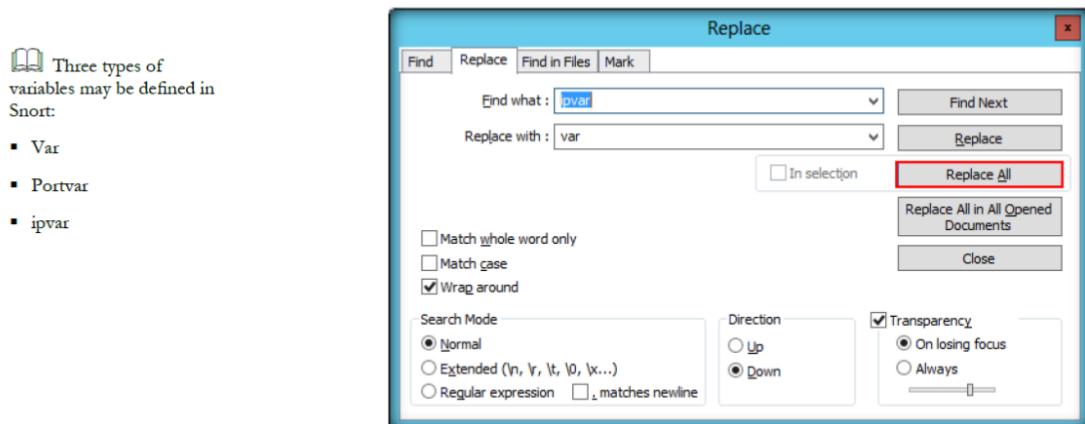
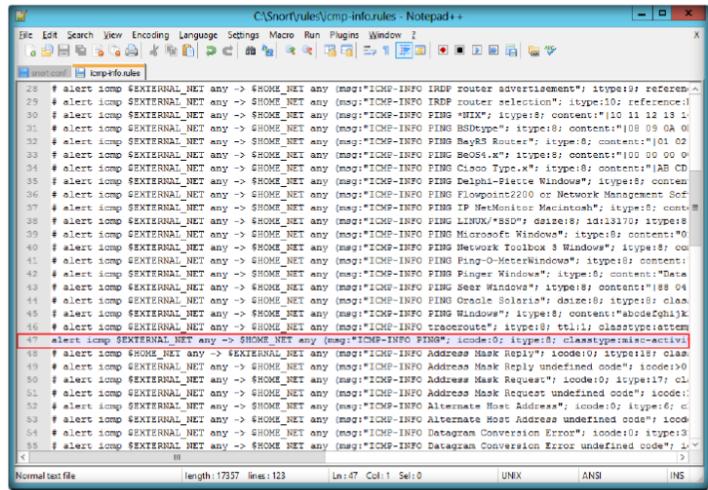


Figure 1.18: Configuring Snort.conf File in Notepad++

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.

Module 17 – Evading IDS, Firewalls and Honeypots



```
C:\Snort\Rules\icmp-info.rules - Notepad++  
File Edit Search View Encoding Language Settings Macro Run Plugins Window Z  
Snort.conf icmp-info.rules  
28 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO IRDP router advertisement"; type:9; reference:  
29 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO IRDP router selection"; type:10; reference:  
30 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING 'WINS'"; type:8; content:"10 11 12 13 1"  
31 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING BS/Dejy"; type:8; content:"10 09 0A 01"  
32 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING BayR Router"; type:8; content:"10 0B 0C 0D"  
33 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Cisco Router"; type:8; content:"10 0E 0F 00 0"  
34 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Cisco Router"; type:8; content:"10 0E 0F 00 0"  
35 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Delphi-Plastic Windows"; type:8; content:  
36 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Flowpoint2200 or Network Management Soft"  
37 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING IP NetMonitor Macintosh"; type:8; content:  
38 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING LINUX/*BSD"; daiseis: id:131370; type:8;  
39 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Microsoft Windows"; type:8; content:"0"  
40 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Network Toolkit 3 Windows"; type:8; content:  
41 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Ping-O-MeterWindows"; type:8; content:  
42 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Pinger Windows"; type:8; content:"Date"  
43 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING See Windows"; type:8; content:"10 04"  
44 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Oracle Solaris"; daiseis: id:131370; type:8; clas:  
45 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING Windows"; type:8; content:"abdeqzhik"  
46 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO traceroute"; type:8; ttl:1; class:type:attack  
47 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO PING"; code:0; type:8; class:type:active  
48 # alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ICMP-INFO Address Mask Reply"; code:0; type:8; clas:  
49 # alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ICMP-INFO Address Mask Request"; code:0; type:8; clas:  
50 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Address Mask Request"; code:0; type:8; clas:  
51 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Address Mask Request undefined code"; acce:  
52 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Alternate Host Address"; code:0; type:6; clas:  
53 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Alternate Host Address undefined code"; code:  
54 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Datagram Conversion Error"; code:0; type:3;  
55 # alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP-INFO Datagram Conversion Error undefined code"; code:  
< >
```

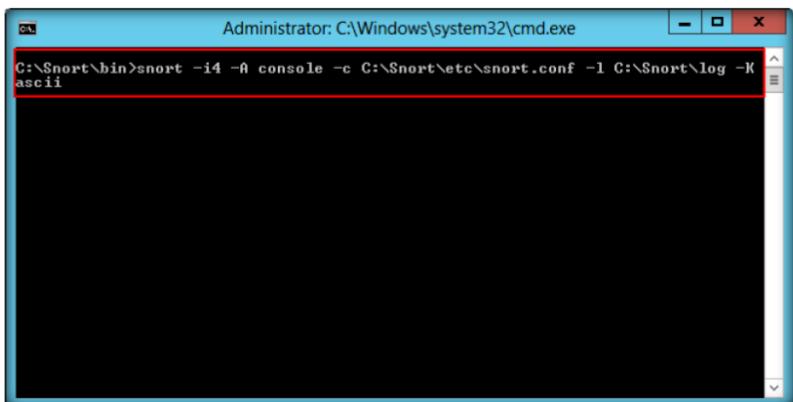
Figure 1.19: Configuring Snort.conf File in Notepad++

Validate Configurations

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
```

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**.



```
Administrator: C:\Windows\system32\cmd.exe  
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

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**.

Module 17 – Evading IDS, Firewalls and Honeypots

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



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.

```
--> Snort! (*-)
Version 2.9.3.1-WIN32 GRE (Build 40)
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
ban
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_SDP 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

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.
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.

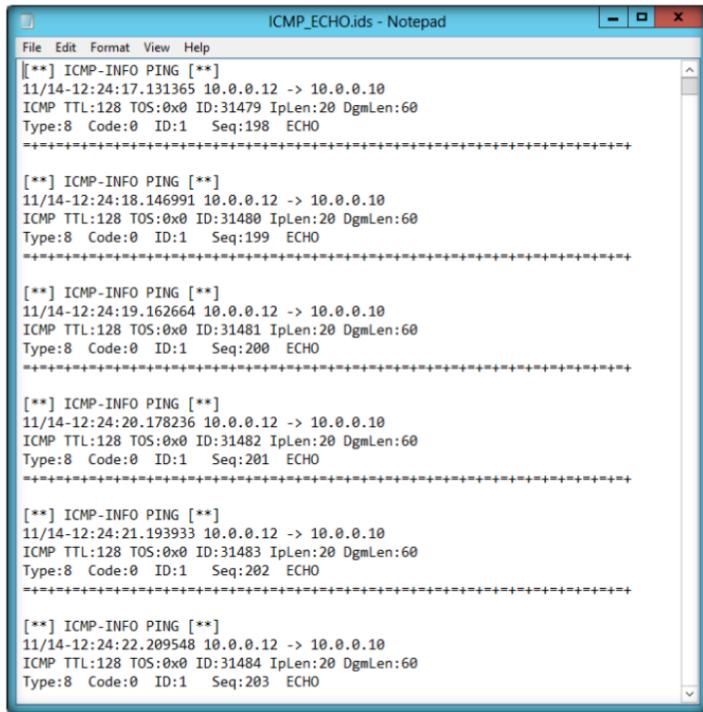
T A S K 6

Attack Host Machine



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

Module 17 – Evading IDS, Firewalls and Honeypots



The screenshot shows a Windows Notepad window titled "ICMP_ECHO.ids - Notepad". The content of the window is a log of Snort alerts, specifically ICMP ECHO requests, captured over several days. The log entries are as follows:

- [**] 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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



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:

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

- 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

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**.

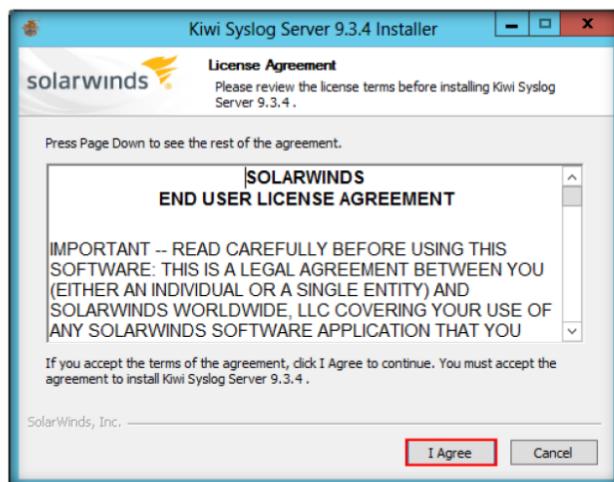


Figure 2.1: kiwi syslog server installation

Module 17 – Evading IDS, Firewalls and Honeypots

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



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 >**.



Figure 2.3: kiwi syslog server

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

Module 17 – Evading IDS, Firewalls and Honeypots

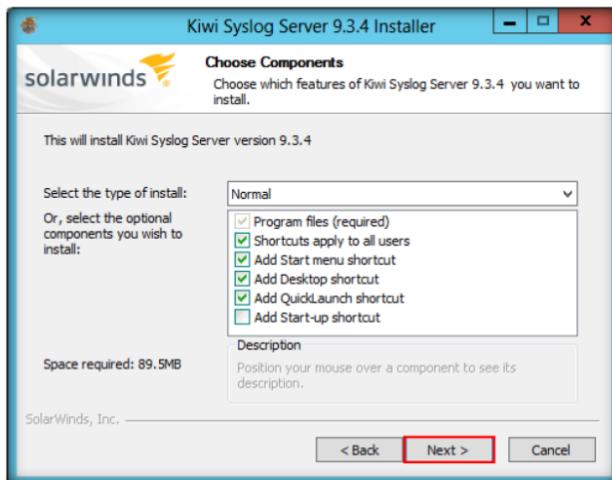


Figure 2.4: adding components

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

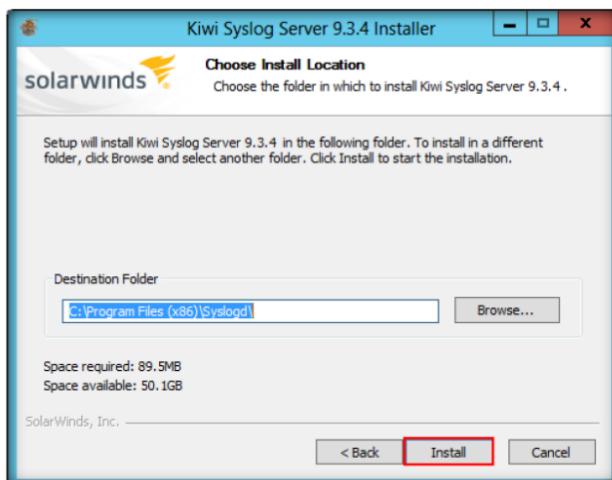


Figure 2.5: Give destination folder

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

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



Figure 2.6: kiwi syslog server finish window

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

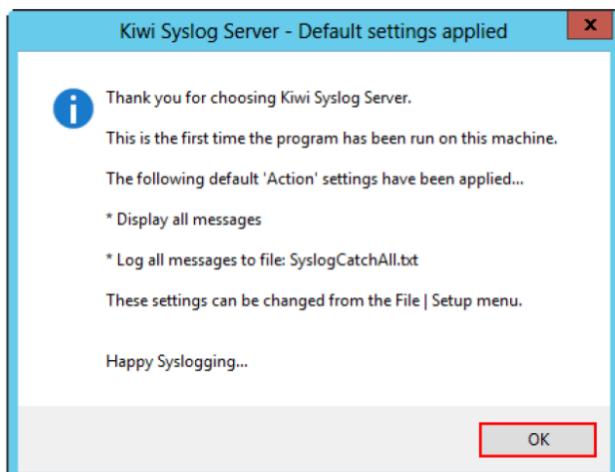


Figure 2.7: Default setting applied window

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.

Module 17 – Evading IDS, Firewalls and Honeypots

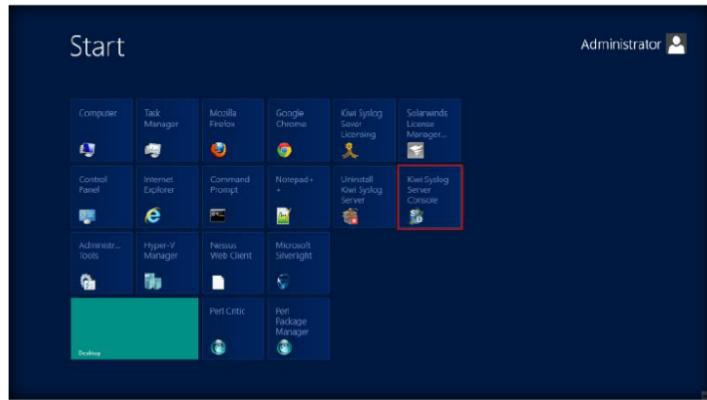


Figure 2.9: click kiwi syslog server application

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

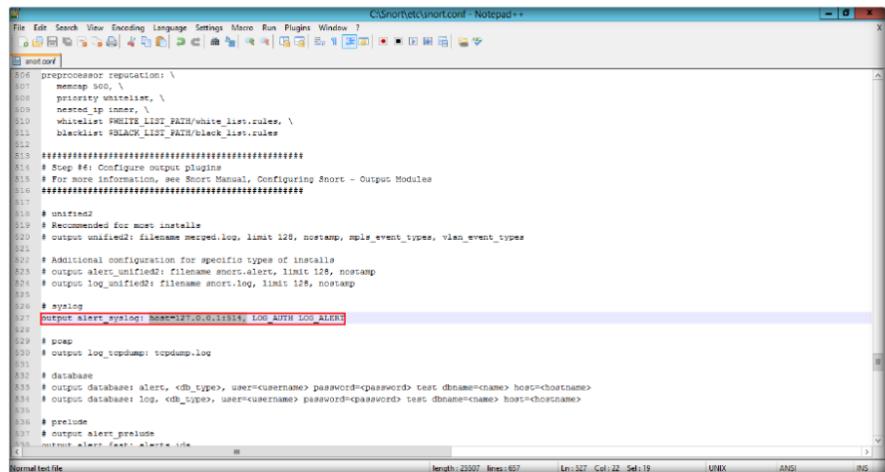
```
File Edit Search View Encoding Language Settings Macro Run Plugins Window ]  
C:\Snort\etc\snort.conf - Notepad++  
Normal text file  
length: 25459 lines: 657 Ln:527 Col: 2 Sel: 0 MRX ANSI INS  
106 preprocessor reputation: \  
107     memcap 500, \  
108     priority whitelist, \  
109     nested_ip inner, \  
110     whitelists RWHITE_LIST_PATH/white_list.rules, \  
111     blacklists RBLACK_LIST_PATH/black_list.rules  
112 #####  
113 # Step #6: Configure output plugins  
114 # For more information, see Snort Manual, Configuring Snort - Output Modules  
115 #####  
116 # unified2  
117 # Recommended for snort installs  
118 # output unified2: filename merged.log, limit 128, nostamp, nplus_event_types, vlan_event_types  
119 #  
120 # Additional configuration for specific types of installs  
121 # output alert_unified2: filename snort.alert, limit 128, nostamp  
122 # output log_unified2: filename snort.log, limit 128, nostamp  
123 #  
124 # syslog  
125 # output alert_syslog: LOG_AUTH LOG_ALERT  
126 #  
127 # pcre  
128 # output log_todump: todump.log  
129 #  
130 # database  
131 # output database: alert, <db_type>, user=<username>, password=<password> test dbname=<name> host=<hostname>  
132 # output database: log, <db_type>, user=<username>, password=<password> test dbname=<name> host=<hostname>  
133 #  
134 # prelude  
135 # output alert_prelude  
136 #  
137 #
```

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.

Module 17 – Evading IDS, Firewalls and Honeypots



```
File Edit Search View Encoding Language Settings Macro Run Plugins Windows ?  
File Edit Search View Encoding Language Settings Macro Run Plugins Windows ?  
and.conf  
506 preprocessor reputation: \  
507 processor wod: \  
508 processor untrusted: \  
509 needed_ip inner, \  
510 whitelist $WHITE_LIST_PATH/white_list.rules, \  
511 blacklist $BLACK_LIST_PATH/black_list.rules  
512  
*****  
513 # Step #4: Configure output plugins  
514 # For more information, see Snort Manual, Configuring Snort - Output Modules  
515 #####  
516  
517 # unified2  
518 # Recommended for most installs  
519 # output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, vlan_event_types  
520  
521 # Additional configuration for specific types of installs  
522 # output alert-unified2: filename snort.alert, limit 128, nostamp  
523 # output log-unified2: filename snort.log, limit 128, nostamp  
524  
525 # syslog  
526 output alert_syslog: host=127.0.0.1;syslog; LOG_AUTH LOG_ALERT  
527  
528 # pcap  
529 # output log_tcpdump: tcpdump.log  
530  
531 # database  
532 # output database: alert, <db_type>, user=<username>, password=<password>, test dbname=<name>, host=<hostname>  
533 # output database: log, <db_type>, user=<username>, password=<password>, test dbname=<name>, host=<hostname>  
534  
535 # prelude  
536 # output alert_prelude  
537 #output alert_fast_alerts_idx  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206  
2207  
2208  
2209  
2209  
2210  
2211  
2212  
2213  
2214  
2215  
2216  
2217  
2218  
2219  
2219  
2220  
2221  
2222  
2223  
2224  
2225  
2226  
2227  
2228  
2229  
2229  
2230  
2231  
2232  
2233  
2234  
2235  
2236  
2237  
2238  
2239  
2239  
2240  
2241  
2242  
2243  
2244  
2245  
2246  
2247  
2248  
2249  
2249  
2250  
2251  
2252  
2253  
2254  
2255  
2256  
2257  
2258  
2259  
2259  
2260  
2261  
2262  
2263  
2264  
2265  
2266  
2267  
2268  
2269  
2269  
2270  
2271  
2272  
2273  
2274  
2275  
2276  
2277  
2278  
2279  
2279  
2280  
2281  
2282  
2283  
2284  
2285  
2286  
2287  
2288  
2289  
2289  
2290  
2291  
2292  
2293  
2294  
2295  
2296  
2297  
2298  
2299  
2299  
2300  
2301  
2302  
2303  
2304  
2305  
2306  
2307  
2308  
2309  
2309  
2310  
2311  
2312  
2313  
2314  
2315  
2316  
2317  
2318  
2319  
2319  
2320  
2321  
2322  
2323  
2324  
2325  
2326  
2327  
2328  
2329  
2329  
2330  
2331  
2332  
2333  
2334  
2335  
2336  
2337  
2338  
2339  
2339  
2340  
2341  
2342  
2343  
2344  
2345  
2346  
2347  
2348  
2349  
2349  
2350  
2351  
2352  
2353  
2354  
2355  
2356  
2357  
2358  
2359  
2
```

Module 17 – Evading IDS, Firewalls and Honeypots

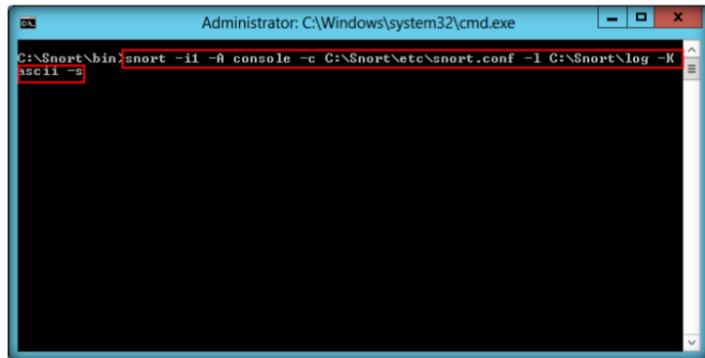
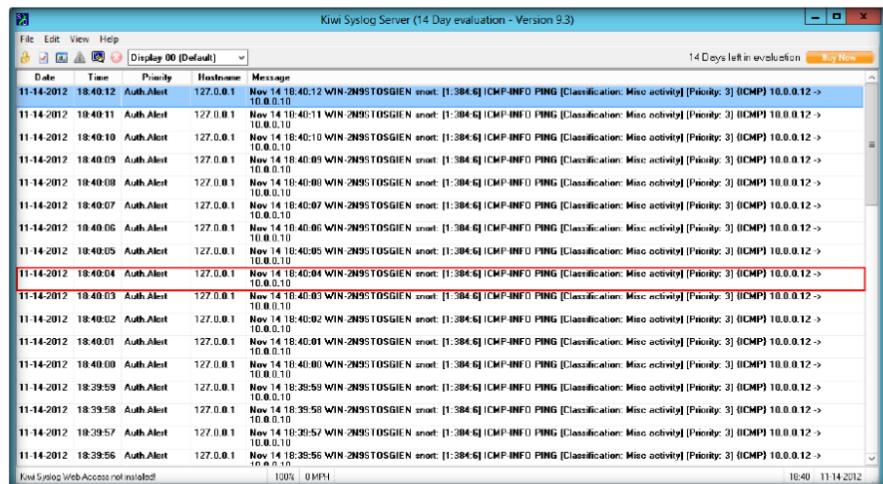


Figure 2.13: Snort Alerts.ids Window Listing Snort Alerts

- BOOK 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.

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.



Date	Time	Priority	Hostname	Message
11-14-2012	18:40:12	Auth.Alert	127.0.0.1	Nov 14 18:40:12 WIN-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN 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-2N95TOSGIEN snort: [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



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 (IDSe), 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 IDSe.

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 IDSe

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**.



T A S K 1

Configure KFSensor

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**.

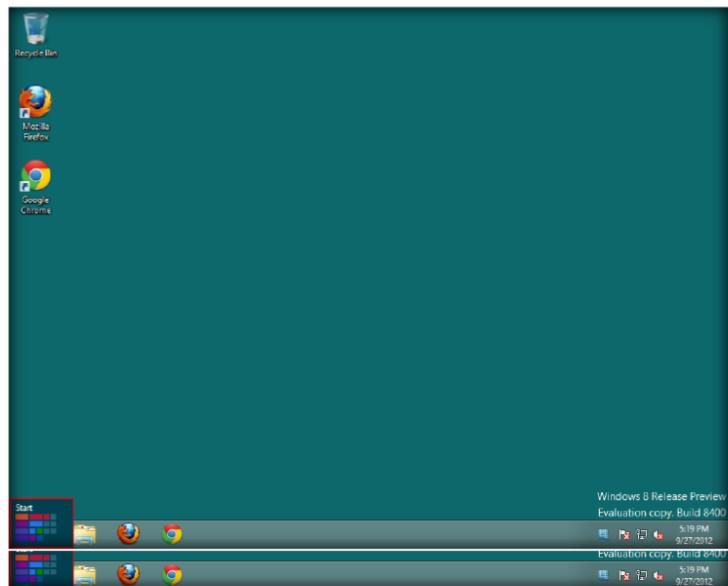


FIGURE 3.1: KFSensor Window with Setup Wizard

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**.

Module 17 – Evading IDS, Firewalls and Honeypots

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

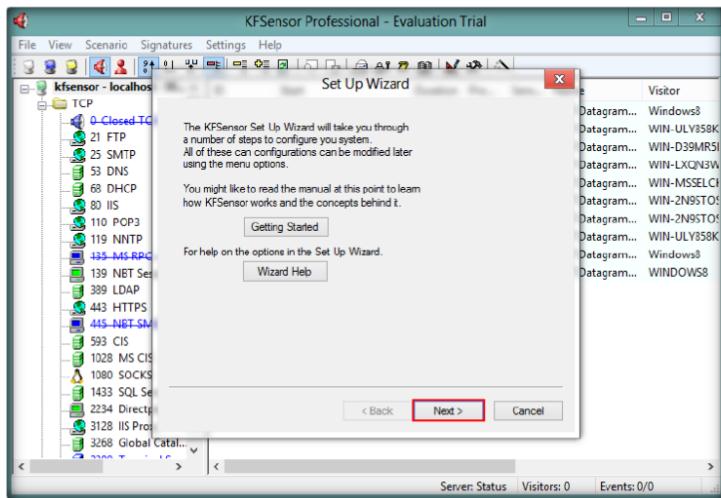


FIGURE 3.3: KFSensor main Window

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

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

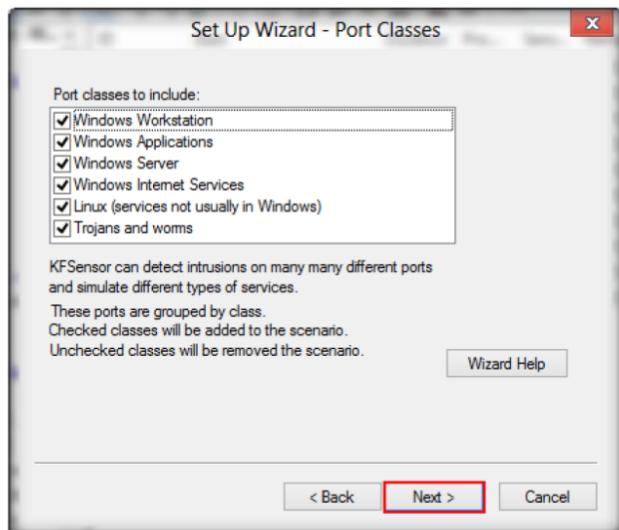


FIGURE 3.4: KFSensor Window with Setup Wizard

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

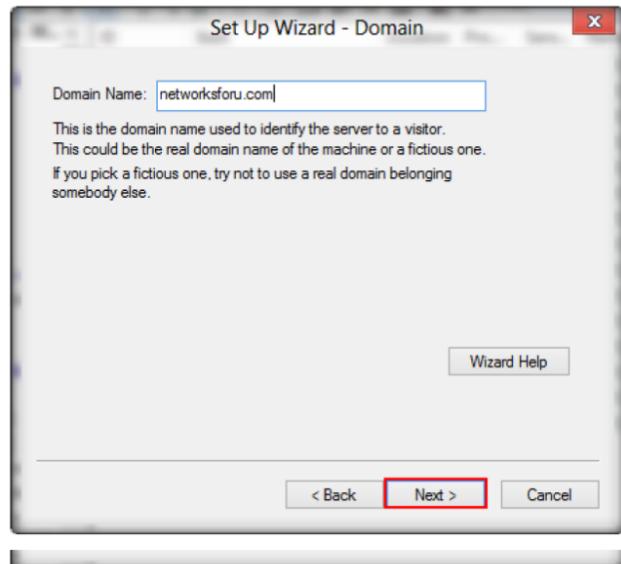


FIGURE 3.5: KFSensor Window with Setup Wizard

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

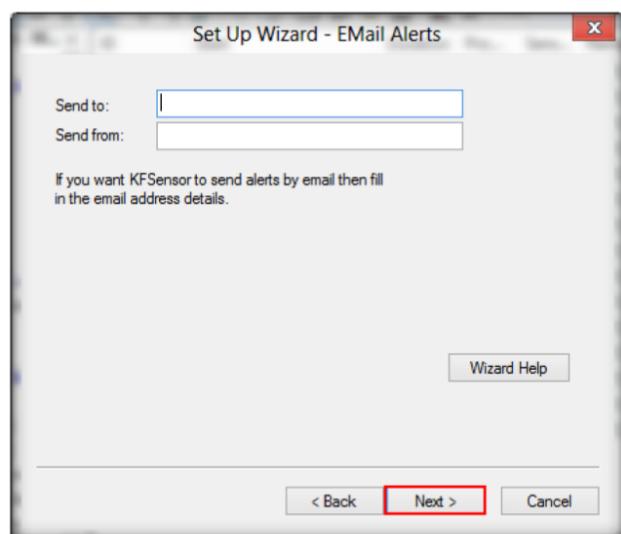


FIGURE 3.6: KFSensor Window with Setup Wizard-email alerts

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.

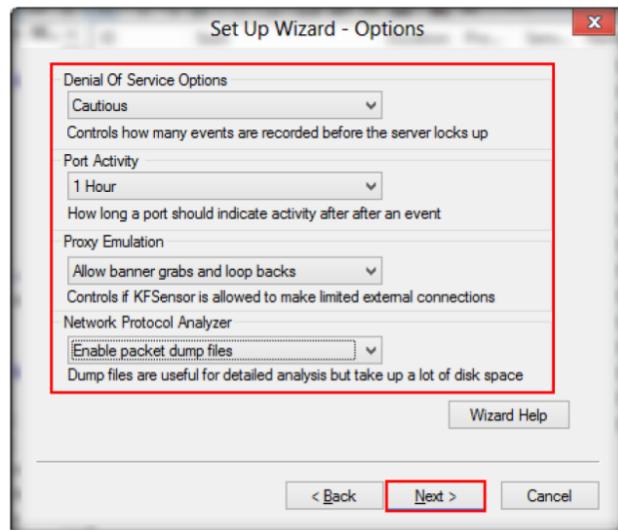


FIGURE 3.7: KFSensor Window with Setup Wizard-options

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**.

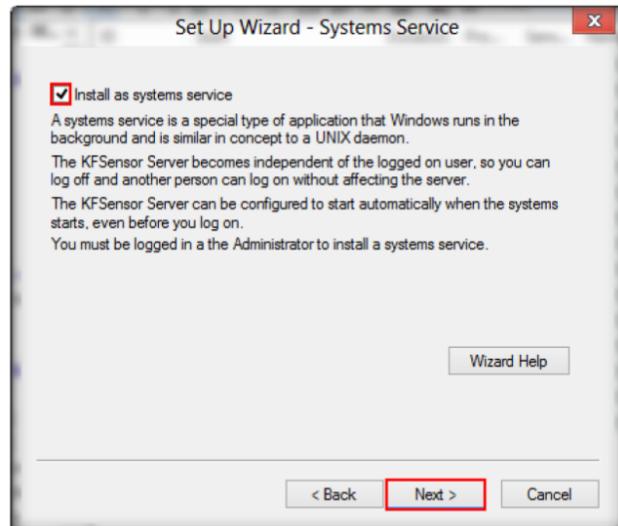
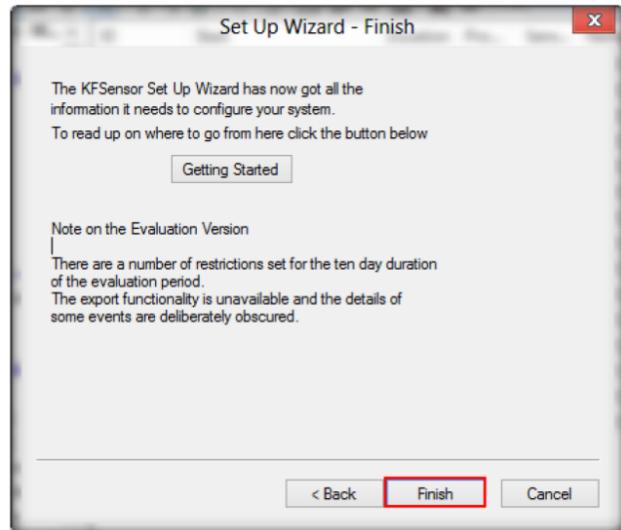


FIGURE 3.8: KFSensor Window with Setup Wizard-system service

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**.

Module 17 – Evading IDS, Firewalls and Honeypots



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

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.

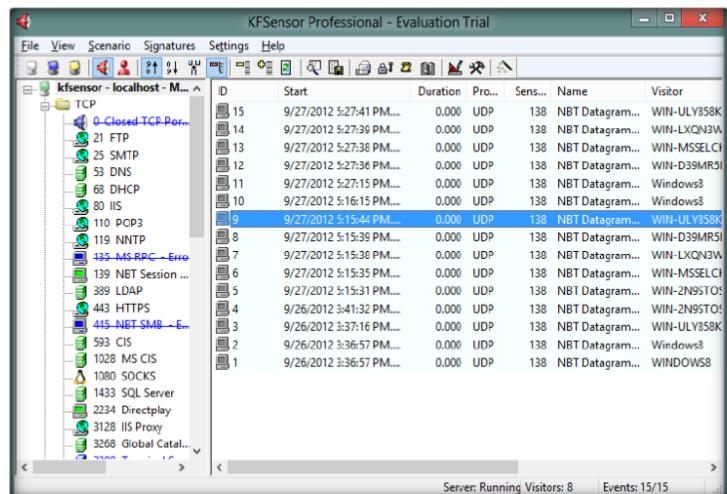
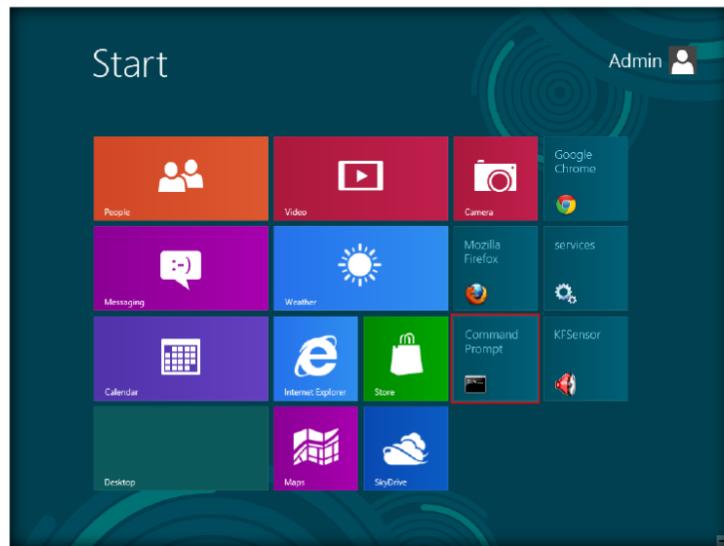


FIGURE 3.10: KFSensor Main Window

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.

```

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    0.0.0.0:82             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    0.0.0.0:656             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

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**.

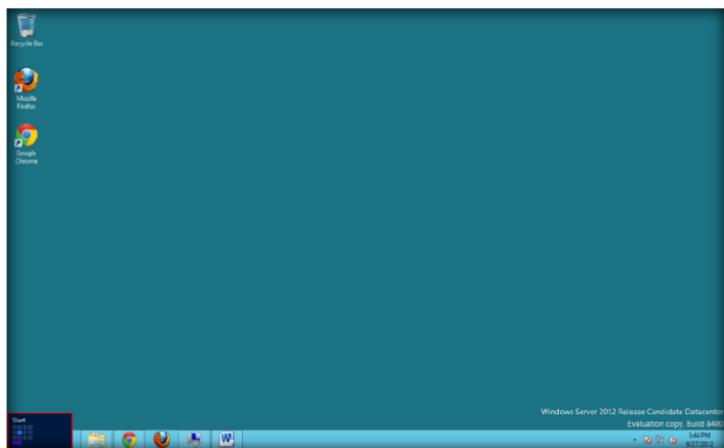


FIGURE 3.13: starting windows in windows server 2012

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

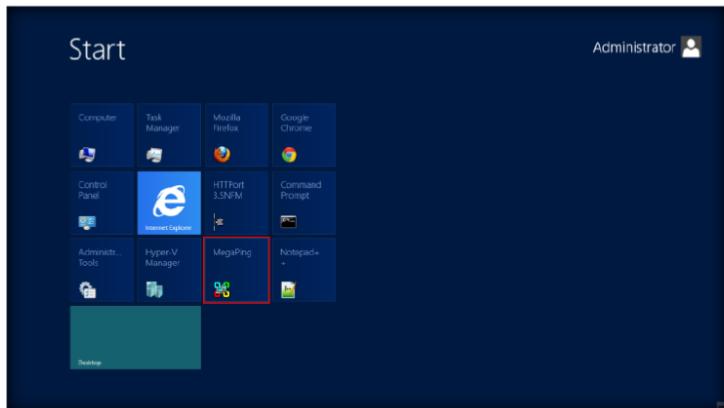


FIGURE 3.14: click on megaping

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

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.

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

Module 17 – Evading IDS, Firewalls and Honeypots

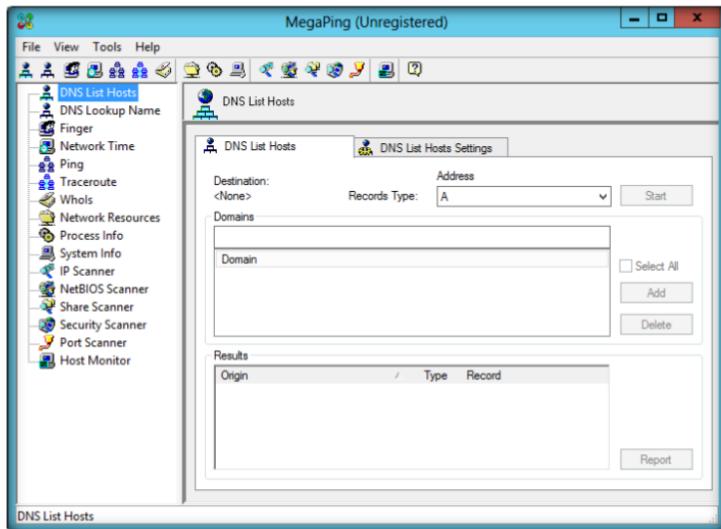


FIGURE 3.15: MegaPing on Windows Server 2012

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**.

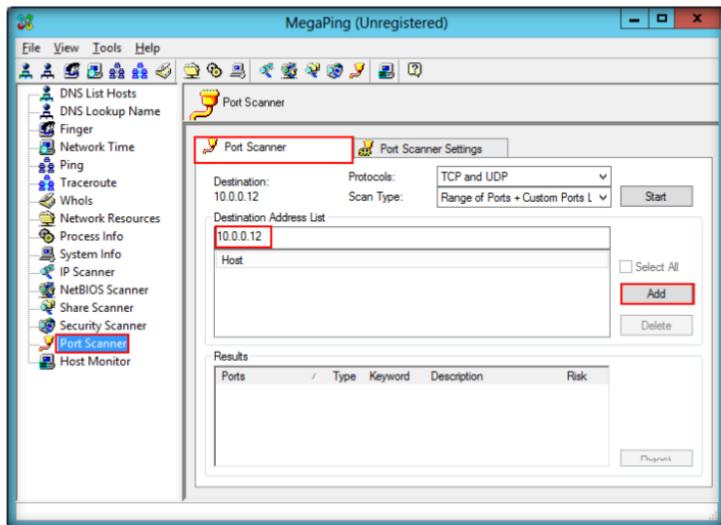


FIGURE 3.16: MegaPing: Select 10.0.0.12 from Host, Press Start button

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

Module 17 – Evading IDS, Firewalls and Honeypots

 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:

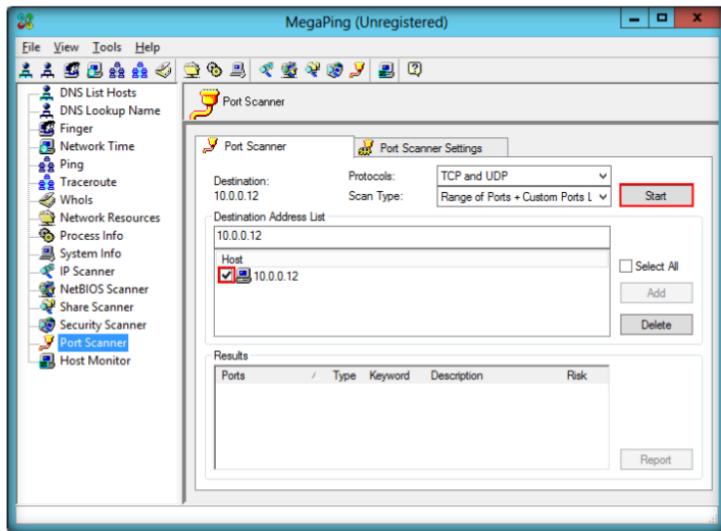


FIGURE 3.17: MegaPing: Data of the packets received

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.

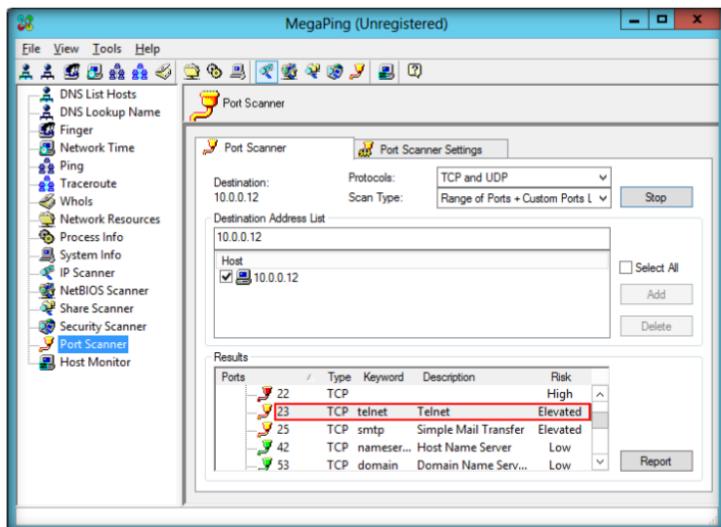


FIGURE 3.18: MegaPing: Telnet port data

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

Module 17 – Evading IDS, Firewalls and Honeypots

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

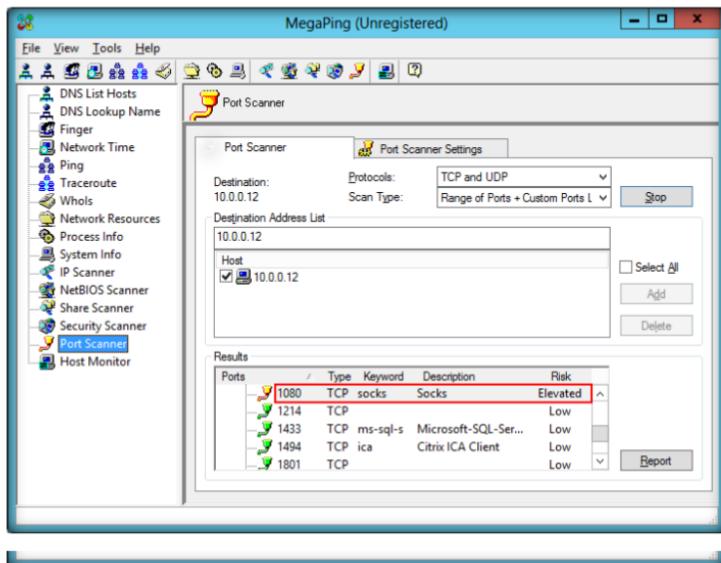


FIGURE 3.19: MegaPing: Blackjack virus

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.

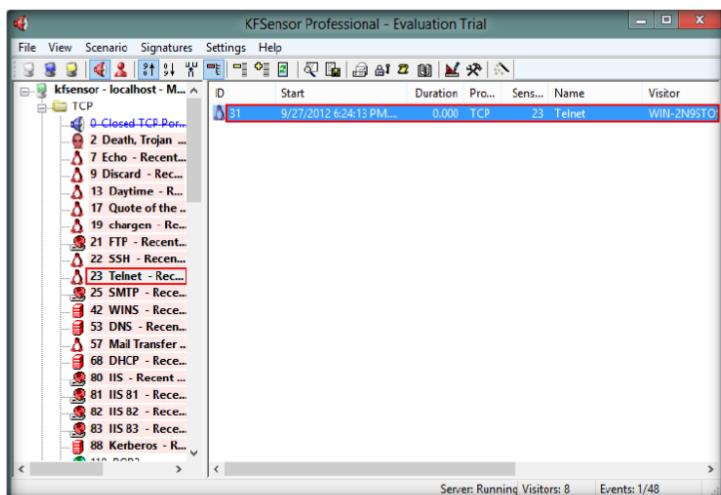


FIGURE 3.20: Telnet data on KFSensor

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

Module 17 – Evading IDS, Firewalls and Honeypots

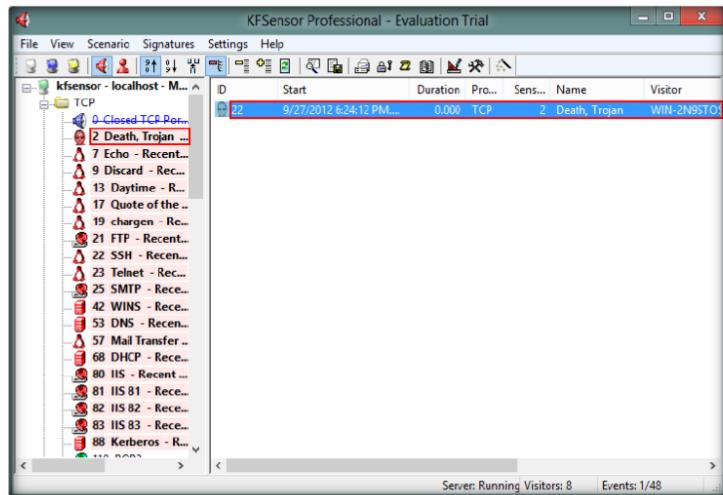


FIGURE 3.21: Death Trojan data on KFSensor

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	<p>Output:</p> <p>Infected Port number: 1080</p> <p>Number of Detected Trojans: 2</p>

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



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

- **HTTPPort** is located at **D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots\HTTPPort**
- You can also download the latest version of **HTTPPort** 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 HTTPPort 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 HTTPPort

HTTPPort creates a transparent tunnel through a proxy server or firewall. HTTPPort 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**.

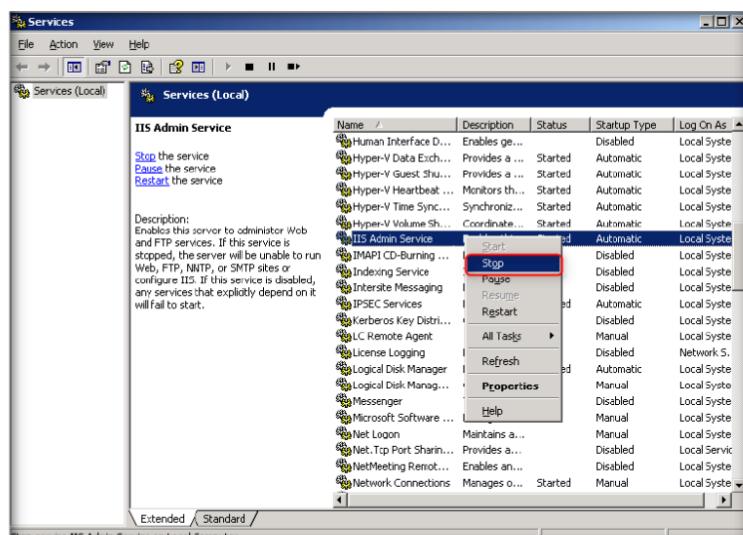


FIGURE 4.1: Stopping IIS Admin Service in Windows Server 2008

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

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

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

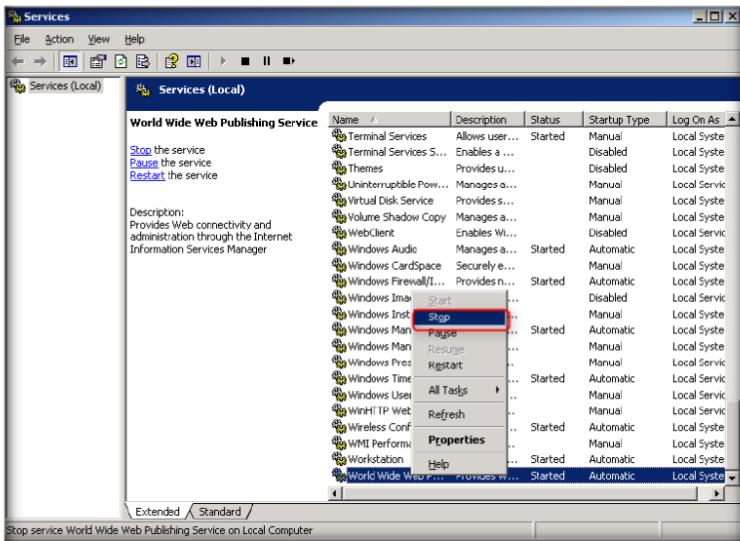


FIGURE 4.2: Stopping World Wide Web Services in Windows Server 2008

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**.
6. Open the **HTTHost** folder and double-click **httphost.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**.

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

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

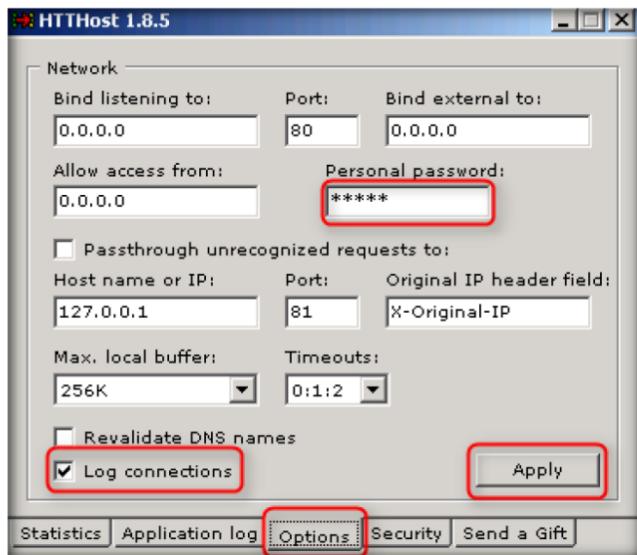


FIGURE 4.3: HTTHost Options tab

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

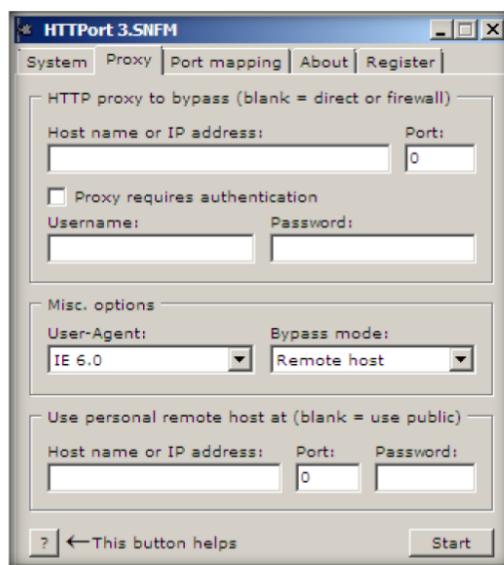


FIGURE 4.4: HTTPort Main Window

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

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

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)

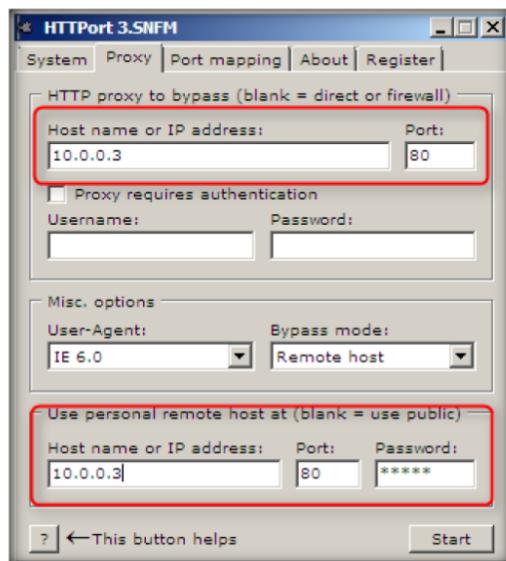


FIGURE 4.5: HTTPPort Proxy settings window

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.

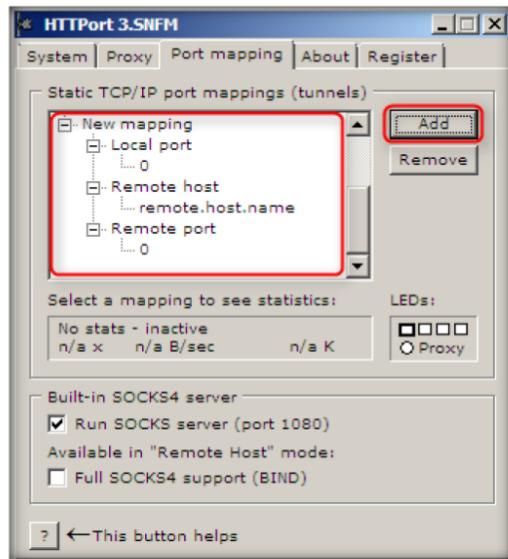


FIGURE 4.6: HTTPort creating a New Mapping

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

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.

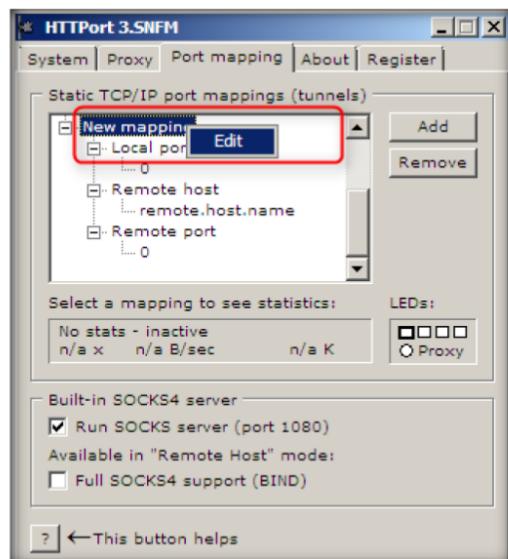


FIGURE 4.7: HTTPort Editing to assign a mapping

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**.

Module 17 – Evading IDS, Firewalls and Honeypots

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

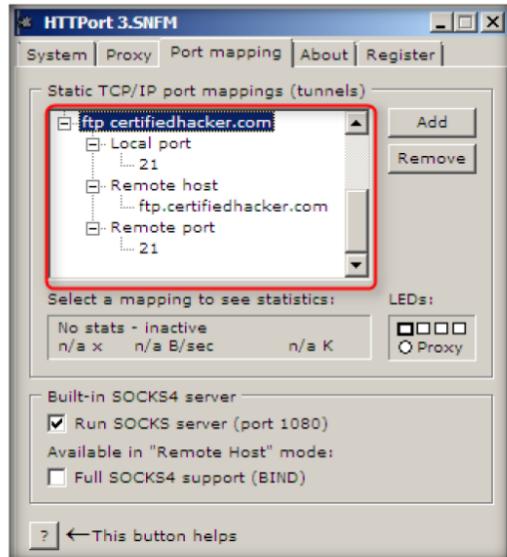


FIGURE 4.8: HTTPPort Static TCP/IP port mapping

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.

- Click **Start** on the **Proxy** tab of HTTPPort to run the HTTP tunneling.

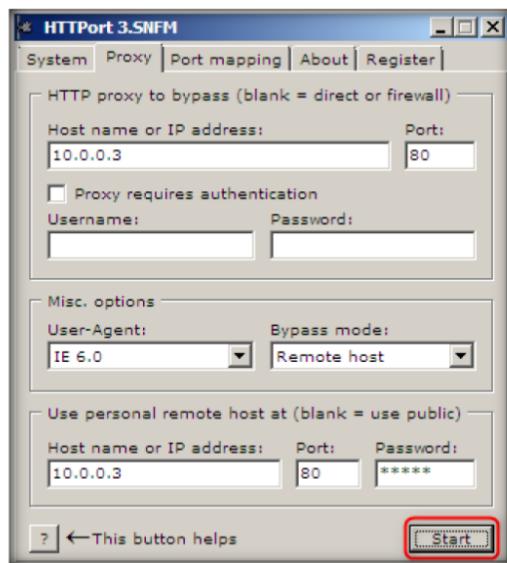


FIGURE 4.9: HTTPPort to start tunneling

- Now switch to **Windows Server 2008** virtual machine and click the **Applications log** tab.
- Check the last line. If **Listener: listening at 0.0.0.0:80**, then it is running properly.

Module 17 – Evading IDS, Firewalls and Honeypots

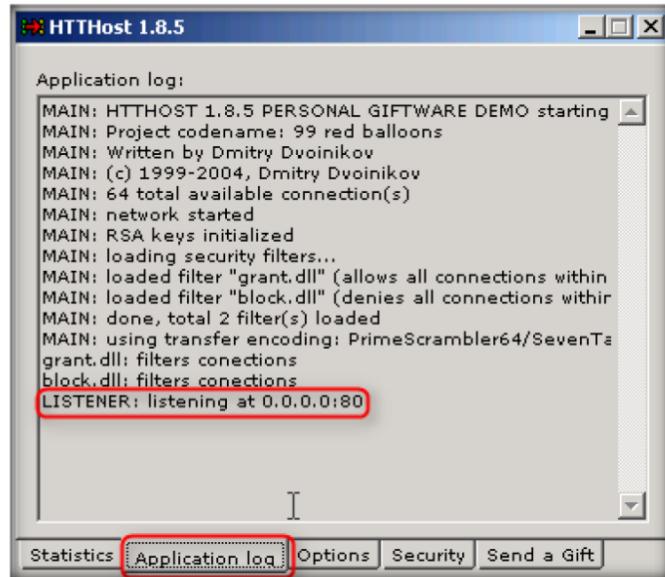


FIGURE 4.10: HTTHost Application log section

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.

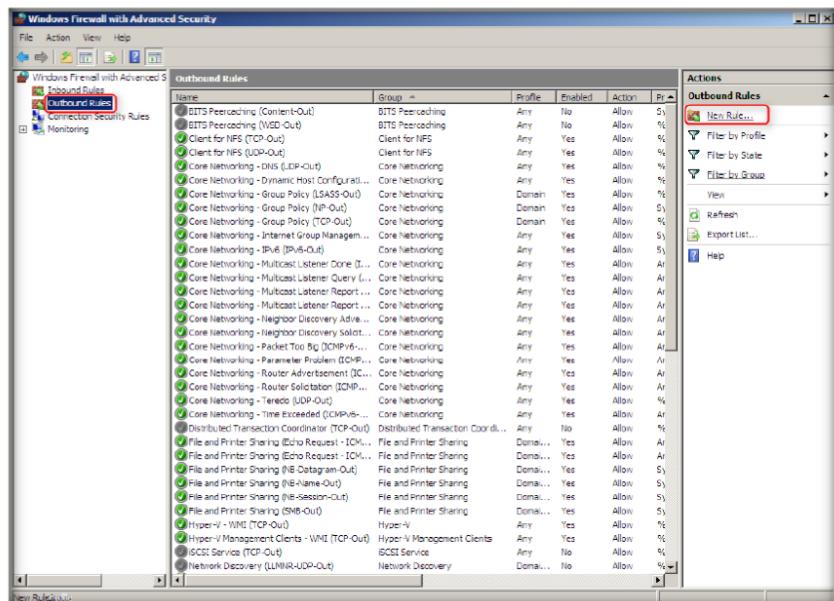


FIGURE 4.11: Windows Firewall with Advanced Security window in Windows Server 2008

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

Module 17 – Evading IDS, Firewalls and Honeypots

HTTP port 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.

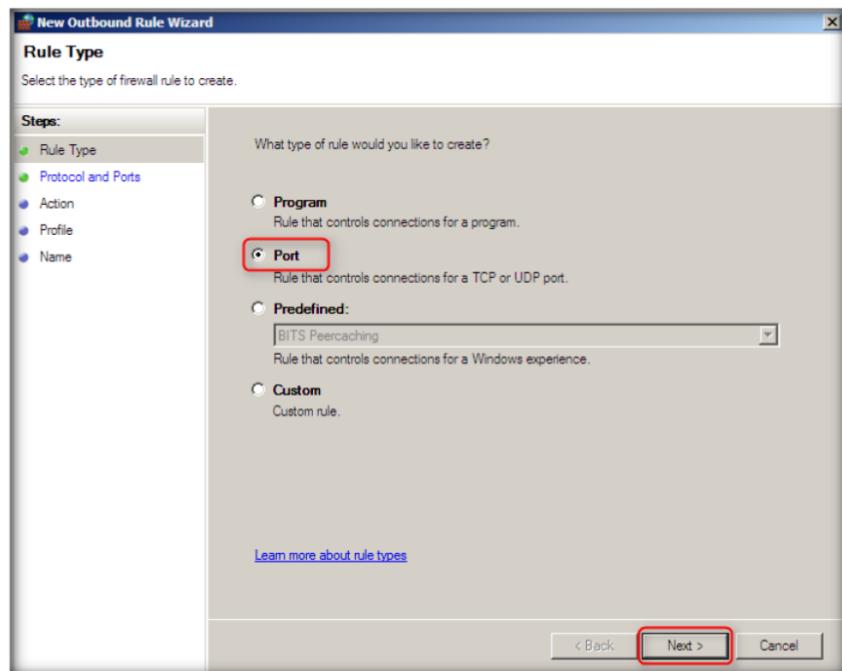


FIGURE 4.12: Windows Firewall selecting a Rule Type

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

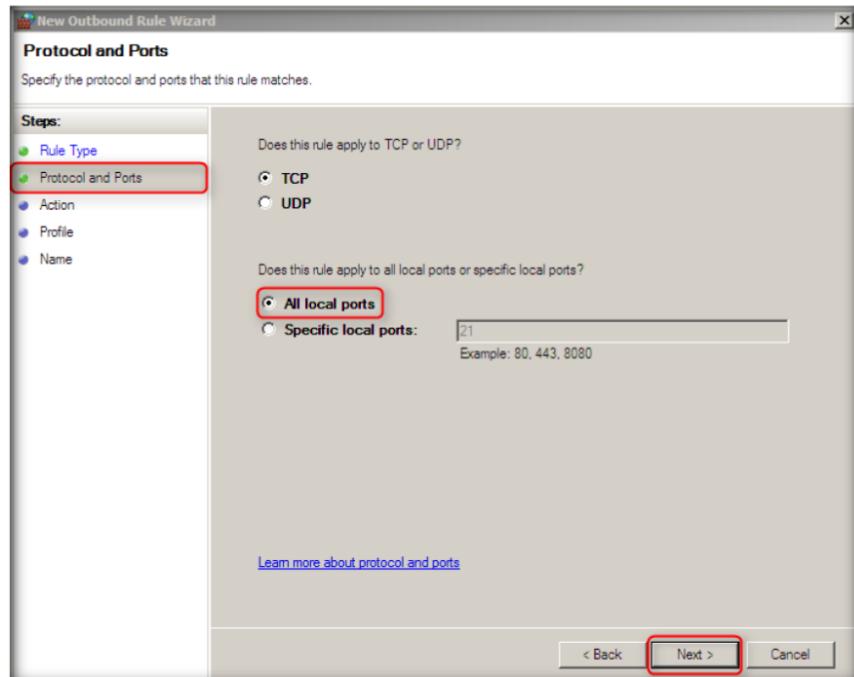


FIGURE 4.13: Windows Firewall assigning Protocols and Ports

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

Module 17 – Evading IDS, Firewalls and Honeypots

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.

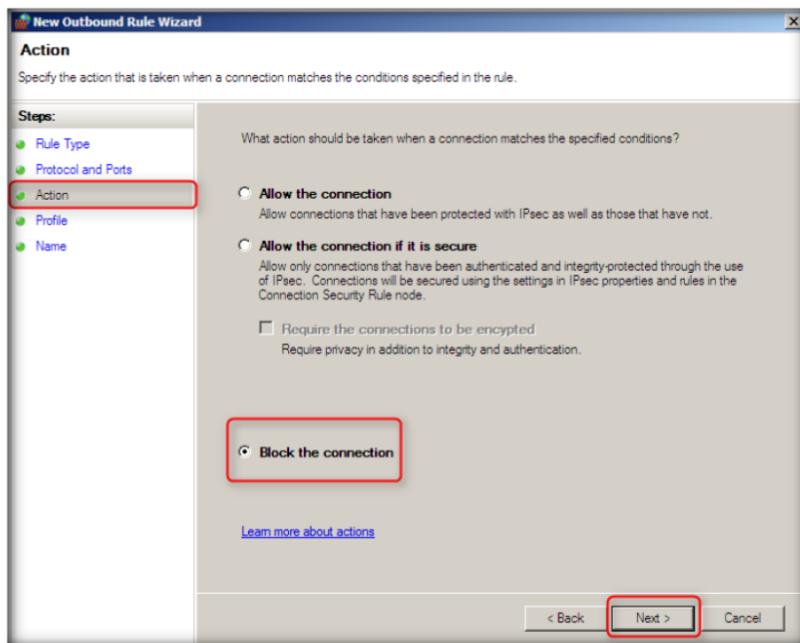


FIGURE 4.14: Windows Firewall setting an Action

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

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

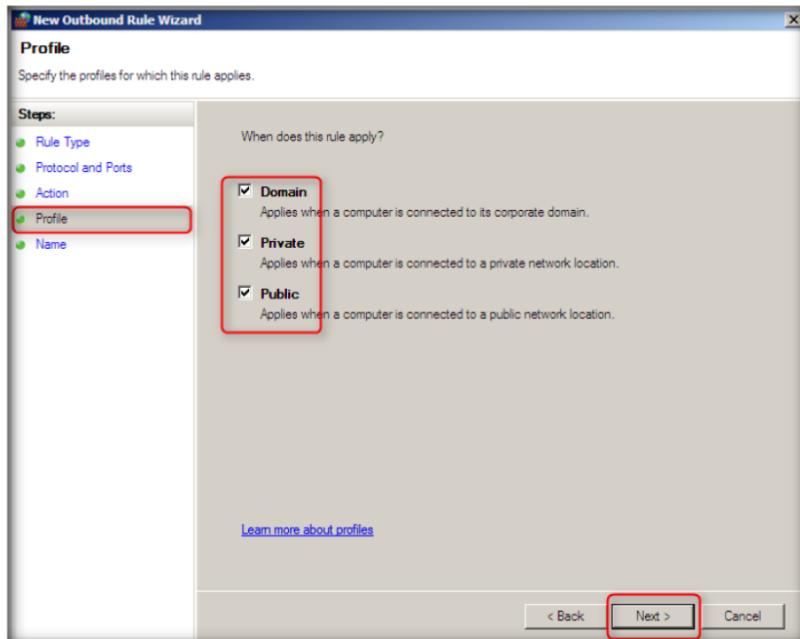


FIGURE 4.15: Windows Firewall Profile settings

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

Module 17 – Evading IDS, Firewalls and Honeypots

 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.

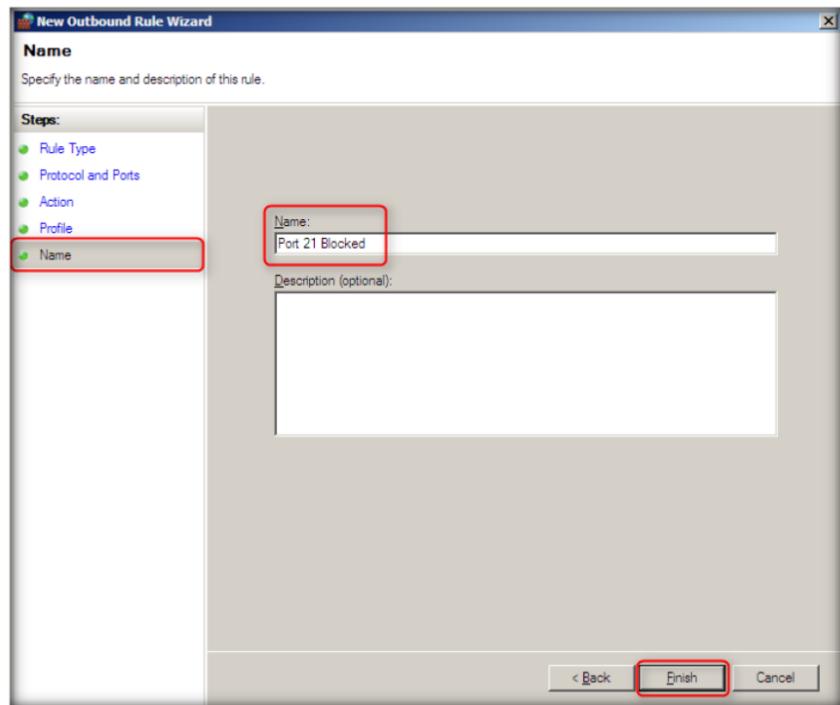


FIGURE 4.16: Windows Firewall assigning a name to Port

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

 HTTP port 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, HTTP port will bring you the rest of the Internet applications.

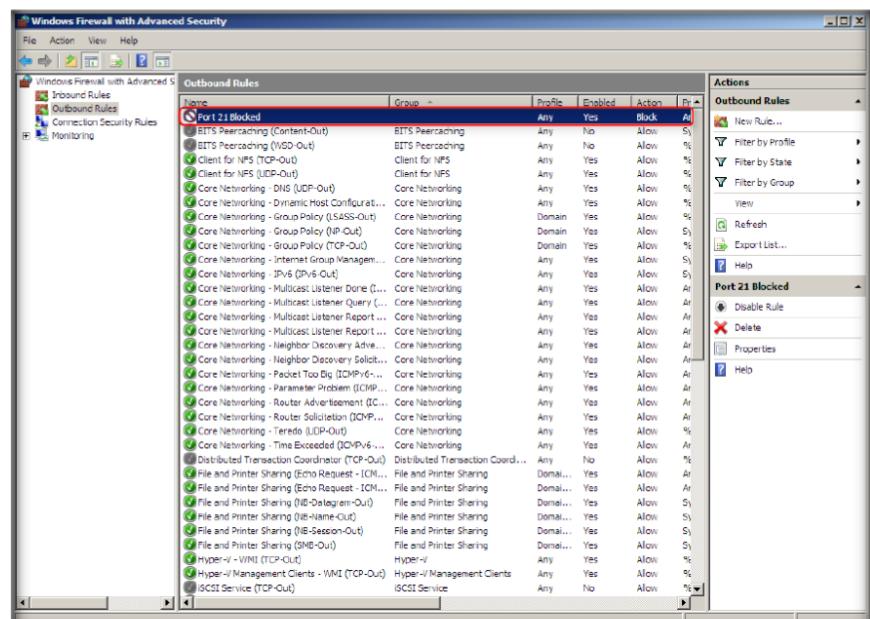


FIGURE 4.17: Windows Firewall New rule

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

Module 17 – Evading IDS, Firewalls and Honeypots

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

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

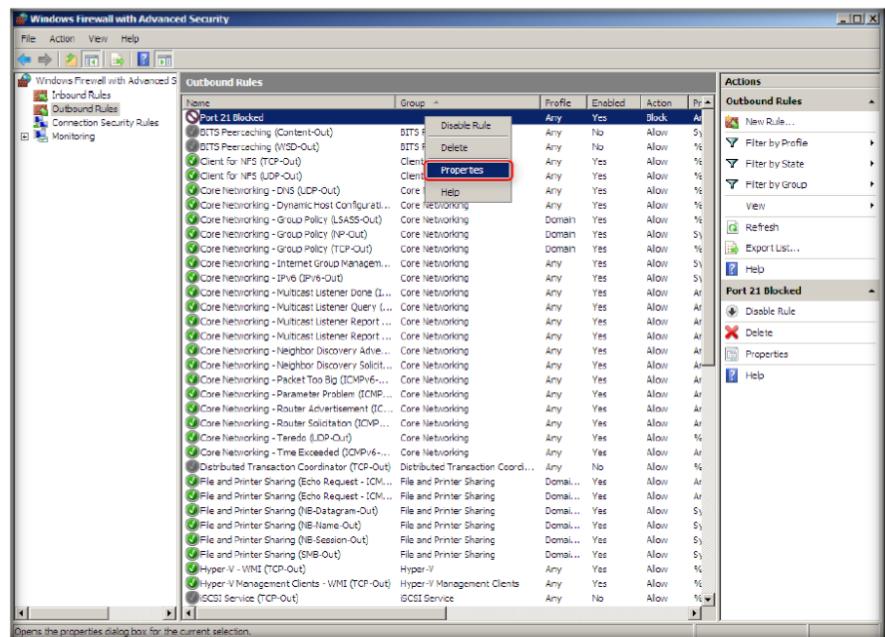


FIGURE 4.18: Windows Firewall new rule properties

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 HTTPPort, 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

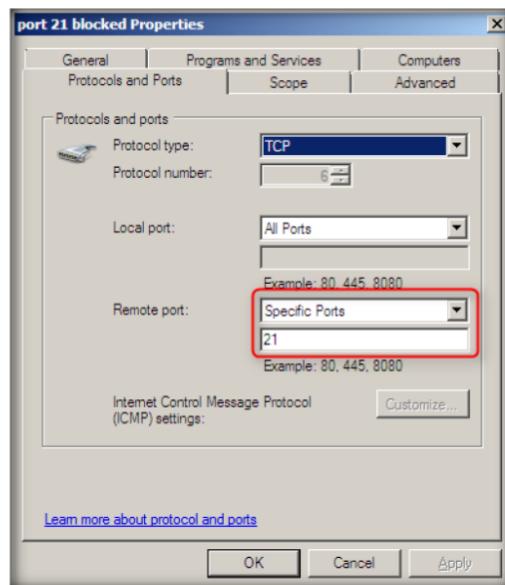


FIGURE 4.19: Firewall Port 21 Blocked Properties

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**.

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

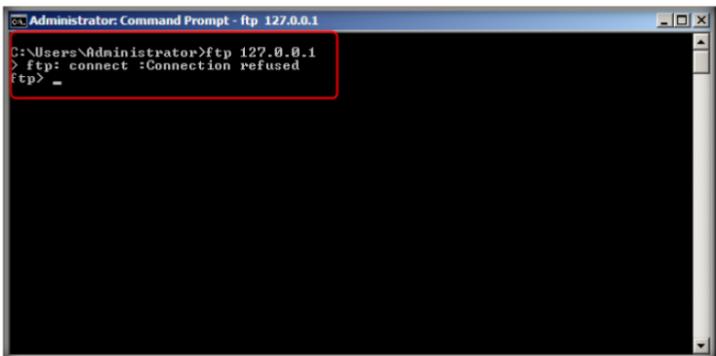


FIGURE 4.20: ftp connection is blocked

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

 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".

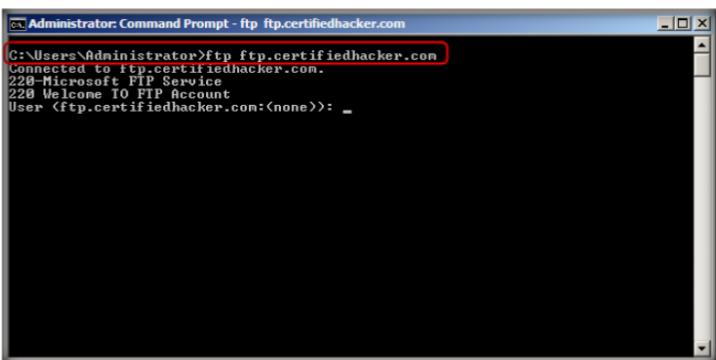


FIGURE 4.21: Executing ftp command

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 HTTPPort 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	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs