**Intrusion Detection and Prevention Using Snort**

Sumayyah Alahmadi [sfa8135@rit.edu](mailto:sfa8135@rit.edu)

CSEC.744.01

Professor Jonathan Weissman

**Table of contents**

1. Implementation….……………………………………………………………………. 3
2. Conclusion……………………………………………………………………………. 23
3. References ……………………………………………………………………………. 23

**A. Setup**

Download snort 2.9.11.1

For the exercises in this section you need the following information.

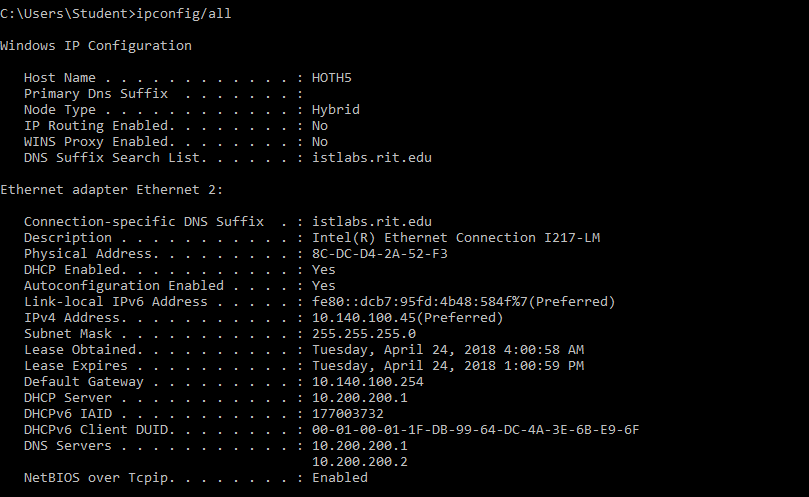
[Network Address]= 10.140.100.0/24

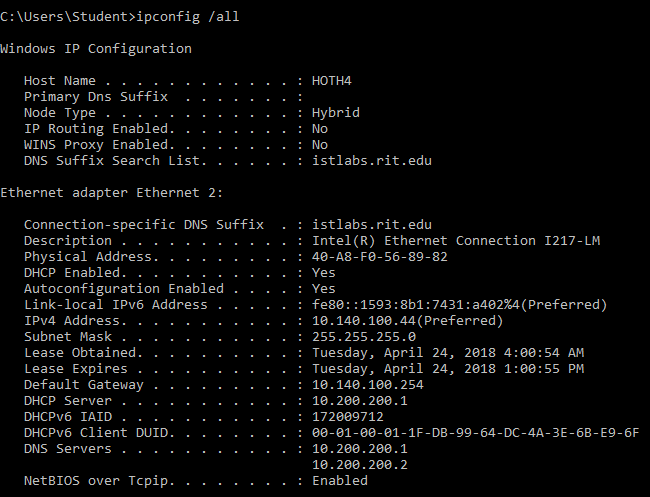
[Computer Name ]= HOTH4

[Your Teammate’s Computer Name ]= HOTH5

[Your IP Address]= 10.140.100.44

[Your Teammate’s IP Address]= 10.140.100.45



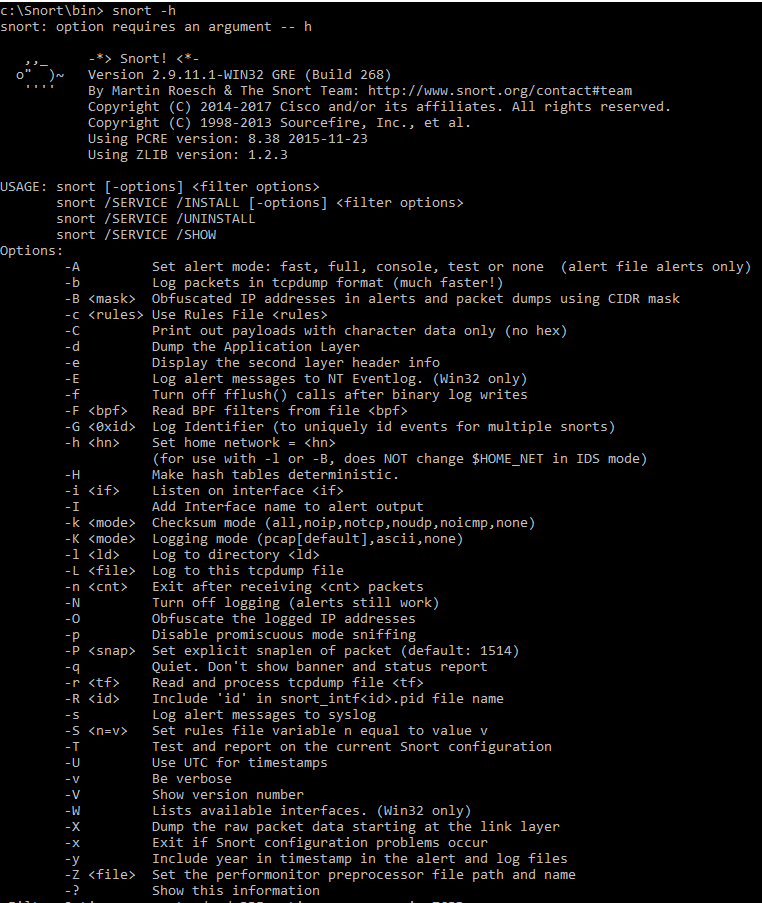


**B. Snort Overview**

In this exercise, you will learn the basics of Snort. Follow the following steps and answer the questions

1. Go to Start > Run > Type “cmd” and press **Enter**.
2. At the command prompt type “**cd c:\snort\bin**” and press **Enter**.
3. Type “**snort –h**” and press Enter to see the snort help. Answer the following questions

|  |  |
| --- | --- |
| snort ‐parameter | Function |
| snort –i <if> Listen to interface <if> | |
| snort –v Be verbose | |
| snort –l <ld> Log to directory <ld> | |
| snort ‐W Lists available interface | |



**C. Snort Sniffer Mode**

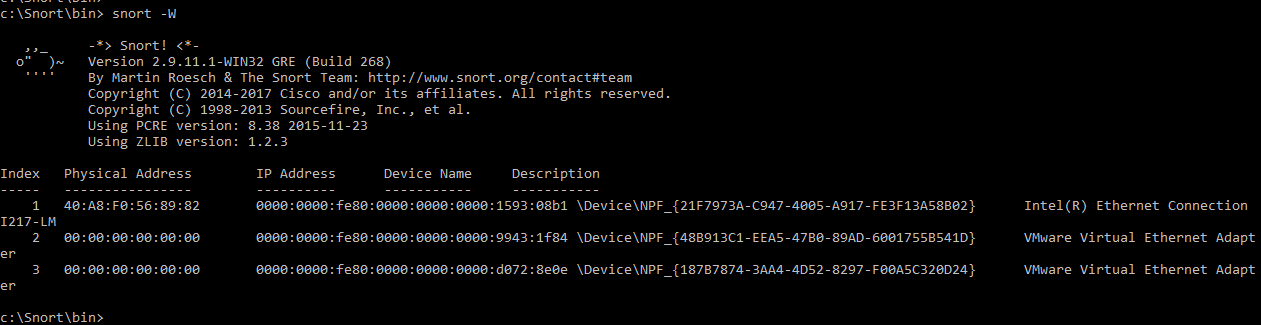
In this exercise, you will use Snort to capture packets from the network (sniffer mode) and print out the TCP/IP packet headers to the screen.

While snort is still running you will notice that the incorrect network adapter is selected by looking at “Initializing Network Interface.” We will need to change this.

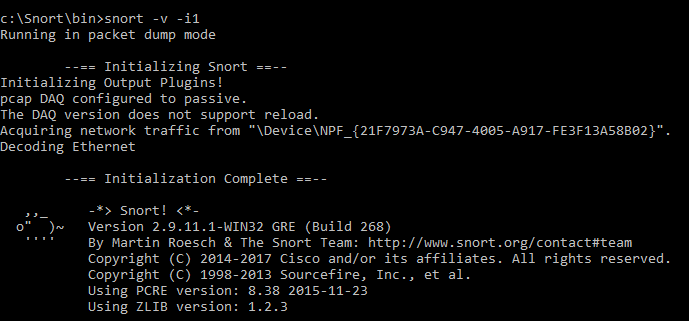
**1)** At the command prompt, type “**cd c:\snort\bin**” and press **Enter**.

**2)** If snort is running, press Crtl+c to stop snort.

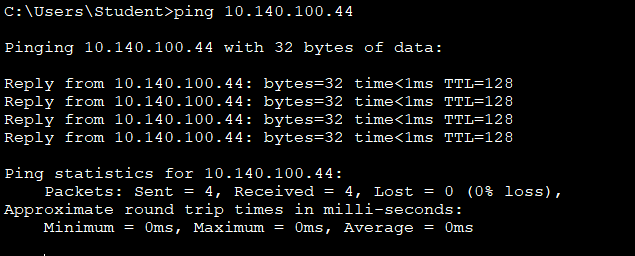
**3)** Type “**snort –W**” and press **Enter** to see a list of adapters to choose from. Choose the correct adapter. If it’s 3, continue with a “3” after the –i in the instructions below. If not, use the actual number you see. We choose adapter 1

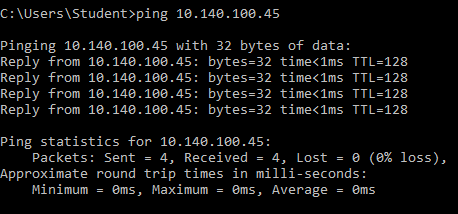


**4)** At the command prompt type “**snort –v –i3**” and press enter. Snort is now running from the network adapter 3 and listens to the network traffic.



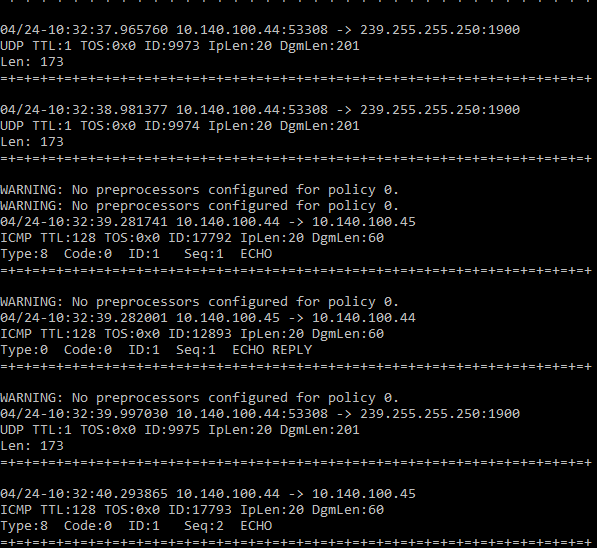
**5)** Keep the snort command prompt window open and open another command prompt.

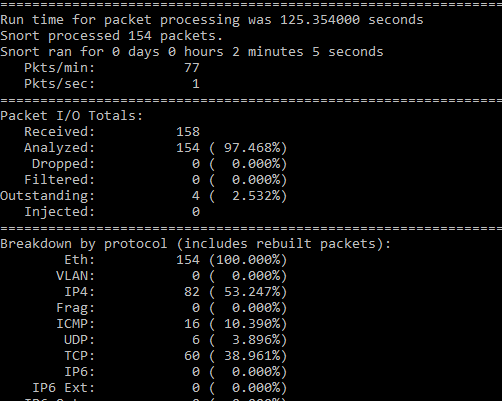
**6)** At the new command prompt window type “**ping [Teammate’s Computer IP Address]**” and ask your teammate to ping your computer as well. 



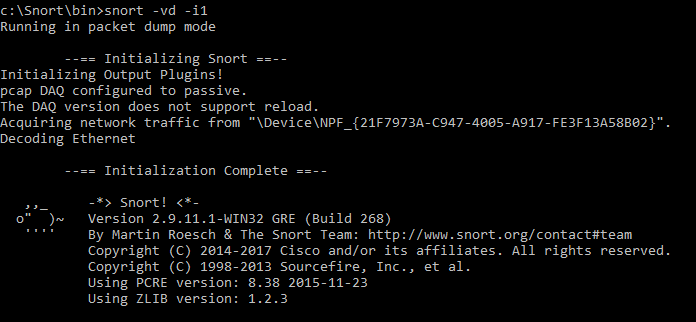
**7)** Observe the captured packets at the snort window. What is happening? Press “Crtl+c” to stop snort and analyze the results.

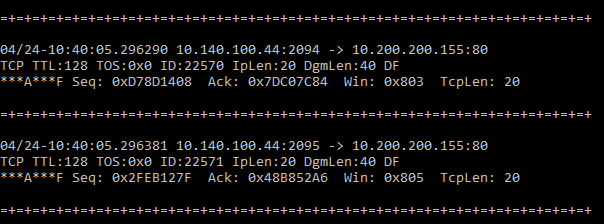
We use -v -i1 which is a basic sniffer mode that shows ICMP packet transferring inside the networks. In the next screenshot, we can see that ICMP packet coming from 10.140.100.44 with TTL:128 and an ECHO replay. Also, another echo ICMP coming from 10.140.100.45 with TTL:128 and echo replay

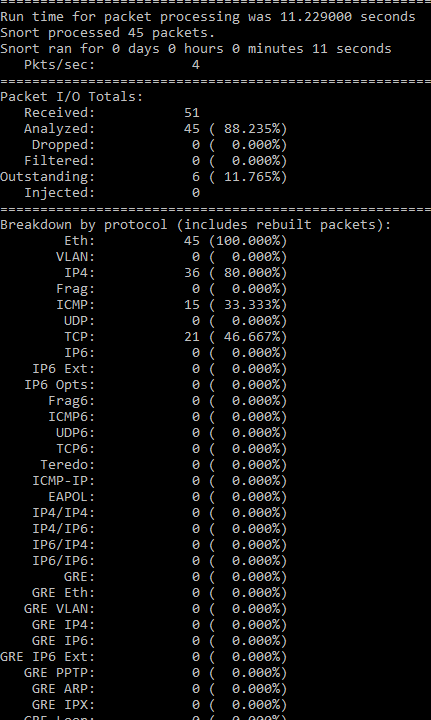




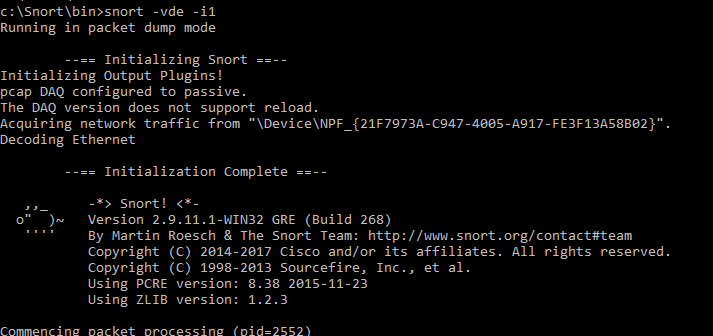
Repeat the same exercise, but this time type “**snort –vd –i3**” or “**snort –v –d –i3**” at the command prompt.

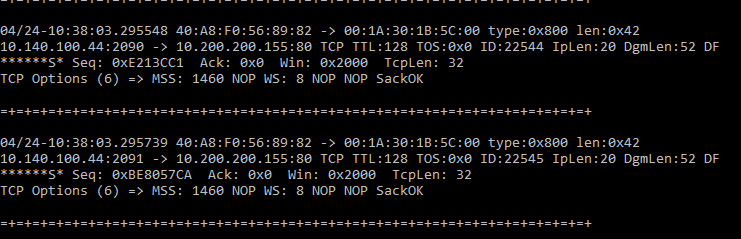


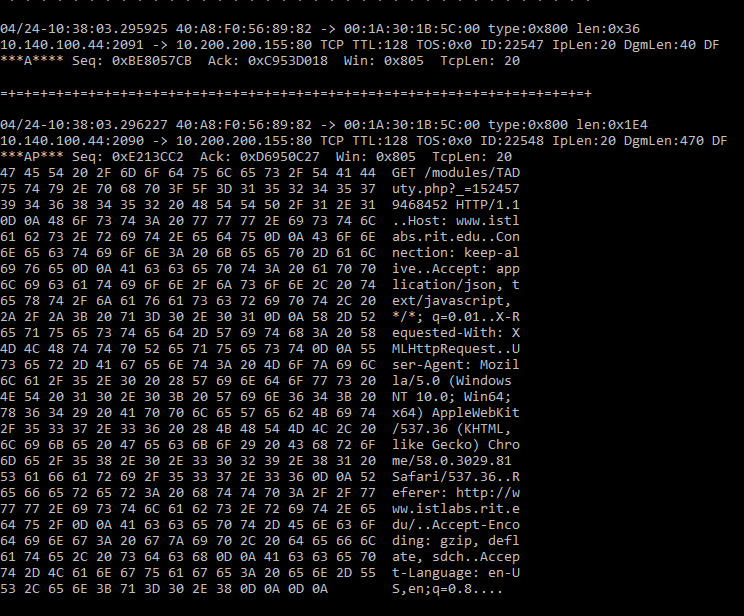


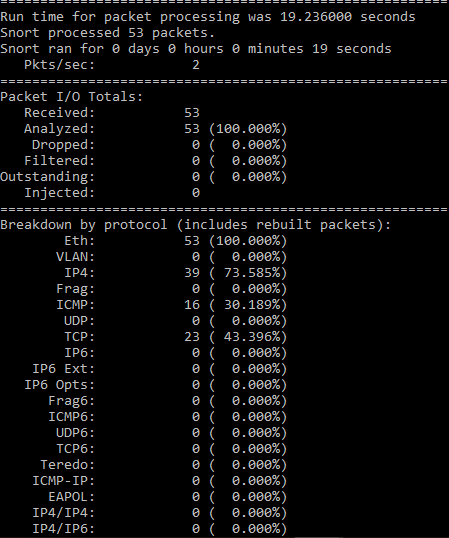


Repeat the same exercise, but type “**snort –vde –i3**” or “**snort –v –d –e –i3**” at the command prompt. What happens when the **–e** switch is used? We repeat the last step with an extra command -e which is used to show the second layed header data as ICMP packet have IP address, TCP/IP header, application layer with ASCII , second layer header with MAC address for source and destination.









**D. Packet Logger Mode**

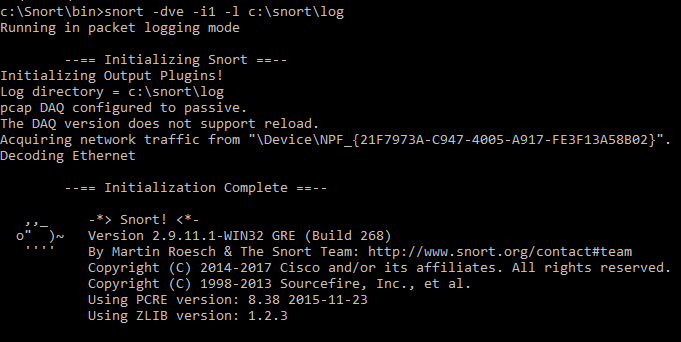
You can use Snort to record packets in a file by specifying a log directory using the –l switch.

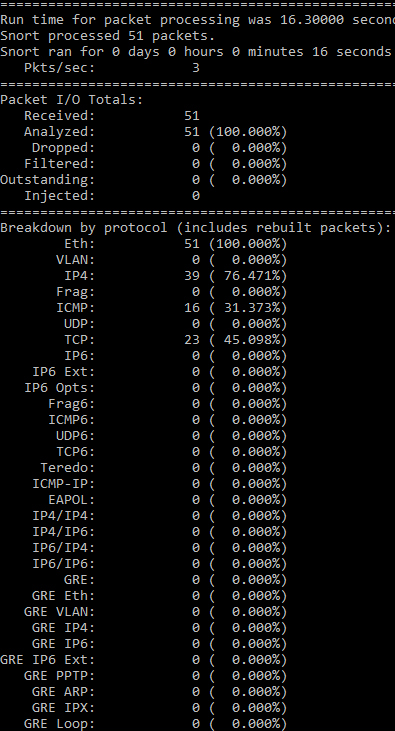
**1)** At the command prompt, type “**cd c:\snort\bin**”and press enter.

**2)** At the command prompt, type “**snort –dev –i3 –l c:\snort\log**” to log every packet into a log file.

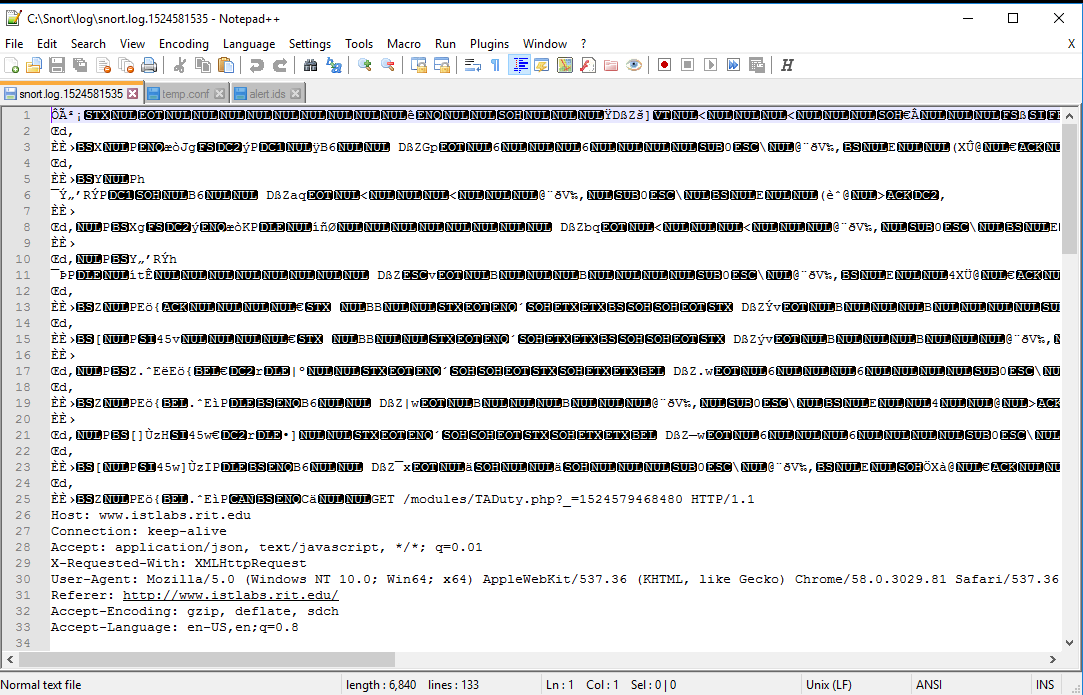
**3)** Ping [Your Teammate Computer’s IP]

**4)** Stop Snort by CRTL+C





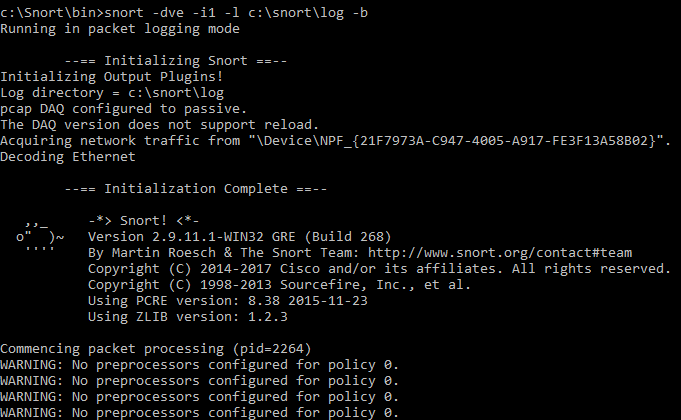
**5)** Start My Computer and browse to C:\snort\log directory. You should see a log file in this directory. Open this file log file using WordPad.

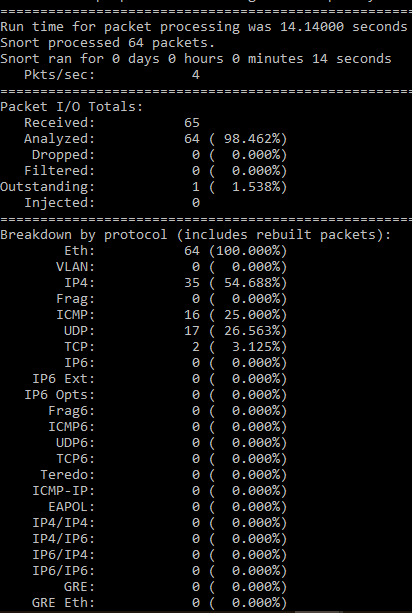


If you are on a high speed network, you should consider using logging in binary mode. The binary mode creates a compact binary file that can be opened with a protocol analyzer such as Wireshark.

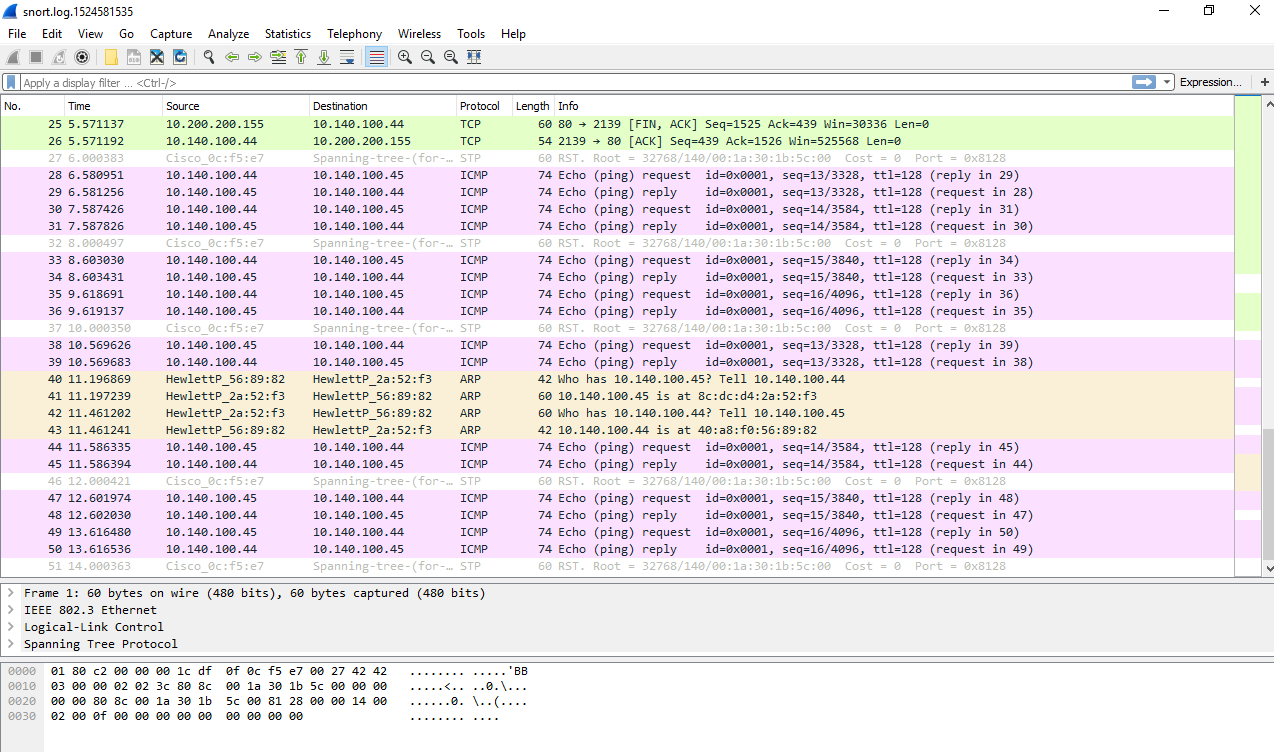
Repeat the same exercise, but this timer start snort as

“**snort –dev –i3 –l c:\snort\log –b**”.





The –b switches indicates a binary format. Open the log file from Wireshark.



**E. Intrusion Detection Mode**

In the intrusion detection mode, Snort records only packets defined by a set of **rules.** Rules are stored in a configuration file. In this exercise, you will create a basic snort configuration file with an alert to capture web traffic in your network, and then analyze the captured log file.

***E.1 Create Snort Configuration File***

**1)** At the command prompt, type “**notepad c:\snort\etc\temp.conf**” and press **Enter**.

**2)** Click yes to create file and in Notepad type the following lines:

var HOME\_NET 192.168.1.0/24

var EXTERNAL\_NET any

var RULE\_PATH c:\snort\rules

alert tcp any any -> any [80] (msg:"Alert! Web connection"; sid:1;)

**3)** When you are done, save the file and minimize Notepad.

***E.2 Start Snort with the Configuration File.***

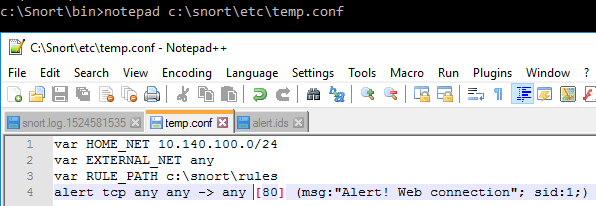
**1)** Start a new command prompt and type “**cd c:\snort\bin**”.

**2)** At the command prompt, type

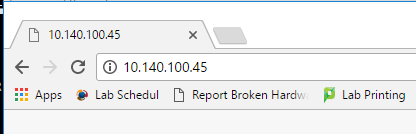
**“snort ‐i3 –l c:\snort\log –c c:\snort\etc\temp.conf”**

and keep Snort running.

If you don’t have a mistake in the configuration file, Snort starts monitoring the network. If you have a mistake in the configuration file, edit the file and try step 2. The –c is to identify the location of the configuration file.



**3)** Open a browser and type **“http://[Your Teammate’s IP Address]”** in the address window and ask your teammate to enter your website address.

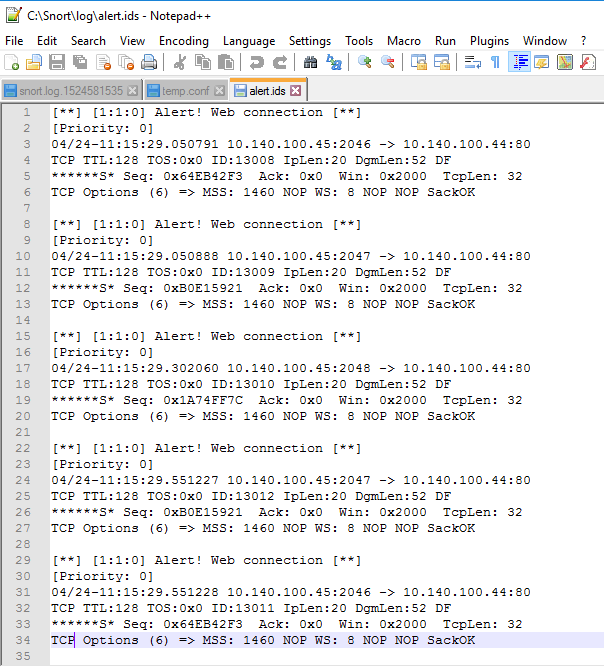


**4)** Ping your teammate computer.

**5)** On the Command Prompt window where Snort is running, press Crtl+C to stop snort.

**6)** Using Windows Explorer, go to “**C:\snort\log**” directory and find **alert.ids** file. Right‐click **alert.ids** file and open with WordPad.

**7)** Scroll down to see all alerts generated by the rule.



**Review Questions:**

How many alerts were generated? 5 alert from the same file is generated which is web connection

Identify the source and destination IP addresses and port number of the alerts. 10.140.100.45, 10.140.11.44. port 2046,2047,2048 for source and port 80 for destination

Why are there no entities for ping traffic? There was an alert for http ant not ICMP from pinging because in the rules we specified the alert for TCP traffic which comping through port 80 for http.

Conclusion

For this lab we implement what we learn and from the intrusion detecting and preventive system using snort software by setting up two hosts and sniff the traffic between them. Also, we become more familiar with snort and its useful functionality.

Reference:

Lecture notes