

Snort Lab

Purpose:

In this lab, we will explore a common free Intrusion Detection System called Snort. Snort was written initially for Linux/Unix, but most functionality is now available in Windows. In this lab, we will use the windows version, but there is an extra credit section to setup and use Snort on Linux (See Extra Credit Section).

Software Requirements:

WinIDS AIO Software Pack which mainly includes the following:

1. Snort
2. Active Perl
3. Oinkmaster

The package will be provided you; you may also download it from:

<http://www.winsnort.com/modules.php?op=modload&name=Downloads&file=index&req=viewsdownload&sid=22>

2. WinPcap. If you already installed Wireshark on the Windows XP machine, then you probably already have it. To verify go to Start > Control Panel > Add Remove Programs to check. If not, then download it from here: <http://www.winpcap.org/install/default.htm>

3. Wireshark. Download from: http://sourceforge.net/project/downloading.php?groupname=wireshark&filename=wireshark-setup-0.99.6a.exe&use_mirror=superb-west

References:

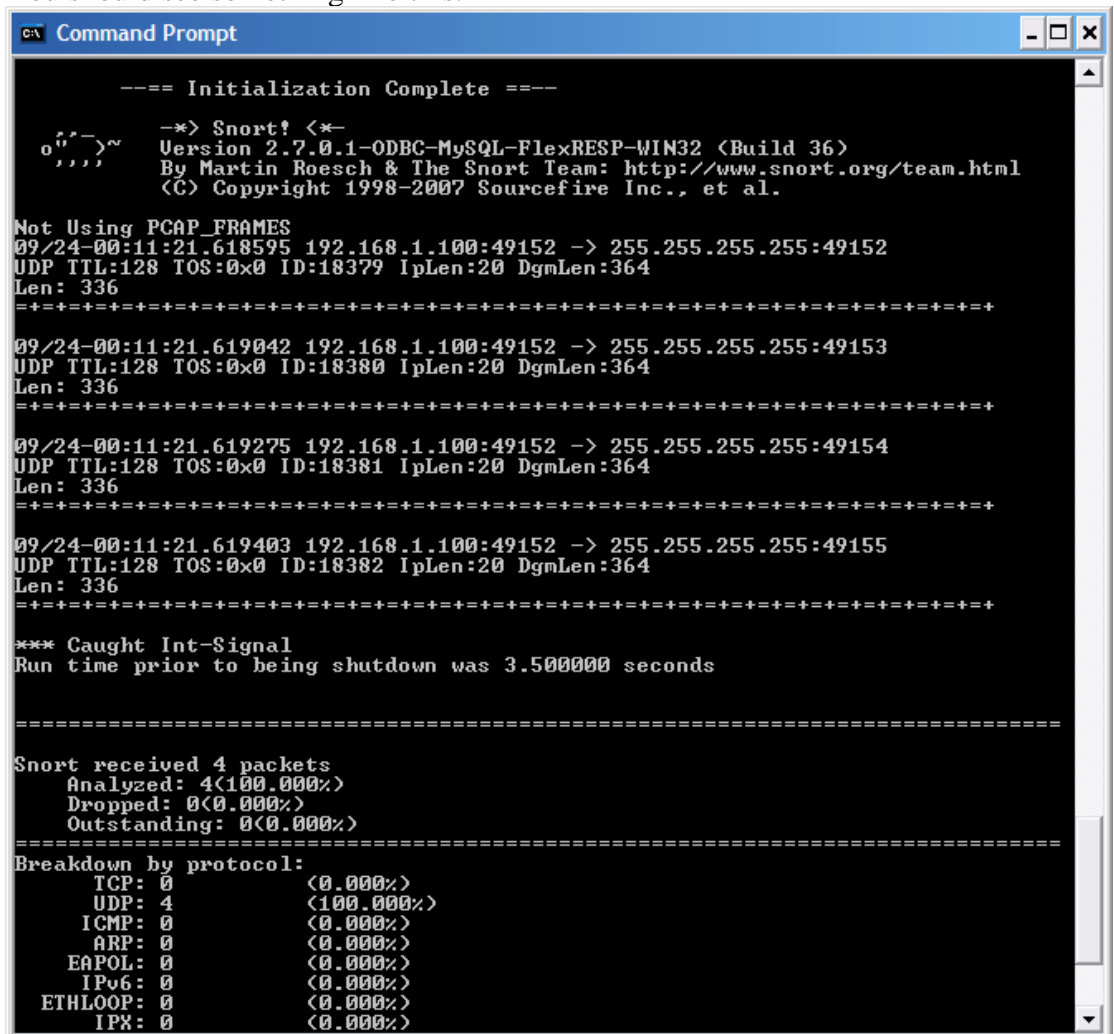
1. <http://www.winsnort.com>
2. <http://www.wireshark.org/download.html>
3. <http://elc.fhda.edu>
4. <http://www.winsnort.com/index.php?name=Sections&req=viewarticle&artid=39&allpages=1&theme=Printer>
5. www.snort.com
6. http://www.snort.org/docs/snort_manual/
7. http://ussrback.com/docs/papers/IDS/snort_rules.htm.html
8. http://www.internetsecurityguru.com/documents/Snort_Base_Minimal_CentOS_5.pdf

Lab Exercise:

1. In your WinIDS_Support_Pack folder, install Snort by double-clicking on the Snort Installer file. Keep defaults values.
2. Snort has three main modes of operations. The sniffer mode, the packet logger mode, and the Network Intrusion Detection mode. Do some reading on these modes (http://www.snort.org/docs/snort_manual/node2.html)
3. **Snort Modes:**
 - a. **Sniffer Mode:**

1. In a command prompt, cd to c:\snort
2. .\bin\snort help >>> View different options for snort.
3. Use the appropriate flag to list available interfaces. (What flag did you use? _____)
4. Run snort in the sniffer mode by typing
.\bin\snort -v -i2

Important: Note that you need to replace the i2 with whichever your network interface is (see point 3 above). Also note that this lab assumes that you are not using a wireless interface. If you want to use a wireless NIC card, then you need to install a Pcap for wireless traffic like AirPcap. You should see something like this:



```

C:\> Command Prompt

----- Initialization Complete -----

o''''~  -*> Snort! <*-
        Version 2.7.0.1-ODBC-MySQL-FlexRESP-WIN32 (Build 36)
        By Martin Roesch & The Snort Team: http://www.snort.org/team.html
        (C) Copyright 1998-2007 Sourcefire Inc., et al.

Not Using PCAP_FRAMES
09/24-00:11:21.618595 192.168.1.100:49152 -> 255.255.255.255:49152
UDP TTL:128 TOS:0x0 ID:18379 Iplen:20 Dgmlen:364
Len: 336
=====
09/24-00:11:21.619042 192.168.1.100:49152 -> 255.255.255.255:49153
UDP TTL:128 TOS:0x0 ID:18380 Iplen:20 Dgmlen:364
Len: 336
=====
09/24-00:11:21.619275 192.168.1.100:49152 -> 255.255.255.255:49154
UDP TTL:128 TOS:0x0 ID:18381 Iplen:20 Dgmlen:364
Len: 336
=====
09/24-00:11:21.619403 192.168.1.100:49152 -> 255.255.255.255:49155
UDP TTL:128 TOS:0x0 ID:18382 Iplen:20 Dgmlen:364
Len: 336
=====

*** Caught Int-Signal
Run time prior to being shutdown was 3.500000 seconds

=====

Snort received 4 packets
Analyzed: 4(100.000%)
Dropped: 0(0.000%)
Outstanding: 0(0.000%)
=====

Breakdown by protocol:
TCP: 0 (0.000%)
UDP: 4 (100.000%)
ICMP: 0 (0.000%)
ARP: 0 (0.000%)
EAPOL: 0 (0.000%)
IPv6: 0 (0.000%)
ETHLOOP: 0 (0.000%)
IPX: 0 (0.000%)

```

5. Ctrl c will stop the capture. Notice that no data-link headers are being displayed. Find the flag that will also display data-link headers as well as the raw packets in HEX/ASCII. What command/flags did you use?
-

b. Packet Logger Mode:

1. In this mode, Snort will log some activities to a log directory. If you look at the c:\snort\log directory, it should be empty. Type a snort command that will start snort in the Logger mode. (don't forget to specify the output directory .\log after the appropriate flag; also don't forget to specify the right interface). What command did you type?
-

2. To get some logs, open up a browser and go to www.gmu.edu.
3. Ctrl + c to stop Snort. Now look at the \log directory, you should see some Snort. log files. These files are Capture files and you can import them into Wireshark to view details. Open up Wireshark and import the log file that was just created. Can you see the page request to www.gmu.edu? Provide a snap shot.

c. IDS Mode:

1. In the Snort Network Intrusion Detection Mode, Snort uses some configuration files and a set of Rule's files. The configuration files will help configure different options in Snort. The Rule's files are files that include signatures against which Snort is comparing all captured traffic. We will be writing some of these signatures. If some traffic pattern matches some signature, a Snort "alert" will be fired. Snort also has Preprocessors also. Preprocessors will check flow of traffic as well. For example if an attacker sends a packet that has "user:" and then later sends another one that has "root". If there is a Snort signature to trigger on text content: "user: root". It will not catch this attempt of remotely trying to access resources with root privileges. The 'Preprocessor' will try to process the stream of data, and reassemble it before it goes into the detection engine, so it detects such tricks of evading the IDS. As a matter of fact, there is an excellent paper that discusses IDS evasion. Read this article that summarizes it:

<http://www.securityfocus.com/infocus/1852>

2. Look at the main Snort configuration file under c:\snort\etc\snort.conf. There is a line that specifies the Rule's path:

```
var RULE_PATH ../rules.
```

Change this line to read:

```
var RULE_PATH c:\snort\rules
```

This tells the Snort engine where to find the Rules files. If you look at the rules folder now, it should be empty. You can populate it by using a Perl script called Oinkmaster. This script automatically goes to the Snort website to get more rules. We will take the time here to get Oinkmaster up and running to load the rules files. To do this, follow the following steps:

- A) Install Active Perl. Note that Active Perl is part of the package that you have already downloaded. Also install Oinkmaster which is also part of that package. (Hint: a very useful document is the README.win32 under the following directory (WinIDS_Support_Pak-081007\oinkmaster-2.0\oinkmaster).
- B) You need to make a change on the "oinkmaster.conf" file. To specify the URL from which you will download the rules. But to be able to do this, you need to be registered (with a snort username and password). Go ahead and create an account for yourself in the snort website www.snort.com. Once you create the account and login to it, you can scroll to the bottom of the page and click on get Oink Code. This will give you the Oink Code that you will use in your "oinkmaster.conf" file. Once you have this code, replace the <oinkcode> on the line shown below with the new code you just got:

```
# Example for Snort-current ("current" means cvs snapshots).  
# url = http://www.snort.org/pub-  
bin/oinkmaster.cgi/<oinkcode>/snortrules-snapshot-CURRENT.tar.gz
```

- C) Now you can execute the Oinkmaster script to go out and get the rules by executing the following line (Note, the path might be different for you): (Format is: [Perl] [Source Perl script] [output])

```
c:\perl\bin\perl c:\WinIDS_Support_Pak-081007\oinkmaster-  
2.0\oinkmaster.pl -o c:\Snort\rules.
```

Please note that if some folder names have spaces, you need to include the path in double quotes, like: "My documents".

This should start installing the Snort rules and the rules file should be populated.

3. There are some minor changes that need to take place in the "Snort.conf" file. To make it simple, just delete the entire file and create the one provided.
4. Now run snort in the Network IDS mode by typing the following:

```
.\bin\snort -c .\etc\snort.conf
```

5. Keep snort running as an IDS and let's trigger an alert. An easy trick to trigger an alert is to open up your browser and type:

www.gmu.edu/readme.eml

The following signature from the web-client.rules file should trigger:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"WEB-CLIENT
readme.eml download attempt"; flow:from_client,established;
uricontent:"/readme.eml"; nocase;
reference:url,www.cert.org/advisories/CA-2001-26.html;
classtype:attempted-user; sid:1284; rev:10;)
```

Go ahead and stop Snort (Ctrl + c). No go to the Log directory and you should see "alert.ids" file. Open the file and you should see more details on the alert.

Extra Credit:

Use the following document to install Snort on Linux in a VMware. Get it up and running and save the VMware image. Turn in your VMware image.

http://www.internetsecurityguru.com/documents/Snort_Base_Minimal_CentOS_5.pdf

Wireshark Lab

Purpose:

In this lab, we will explore a tool called Wireshark (a new version of Ethereal), to capture traffic and identify packet headers and data information.

Software Requirements:

Wireshark for windows:

http://sourceforge.net/project/downloading.php?groupname=wireshark&filename=wirshark-setup-0.99.6a.exe&use_mirror=superb-west

References:

<http://www.wireshark.org/download.html>

Part 1:

4. Download and install Wireshark for windows on your windows XP machine.
5. Wireshark will capture raw traffic from the network interface card.
6. Run the program, and under the 'Capture' Menu, go to Options. Under "Display Options", make sure that "Update list of packets in real time" and "Automatic scrolling in live capture" are both checked.
7. Under the "Capture" menu, choose "Interfaces". (You might see some Vmware virtual interfaces). You want to choose your host's Interface card.
8. Now we are ready to capture traffic as soon we click on the start button. We will capture some web traffic and try to analyze the packet captures.
9. Note: Try to do the following steps consecutively and quickly so you can minimize the noise in the desired traffic capture.
10. Click on start in Wireshark to start capturing traffic.
11. Open up an internet browser and go to www.mail.com.
12. Sign in at the right side of the page with username: gmu@hotmail.com, and password "testing"
13. After the page loads up, stop the capture by clicking on "stop" under the 'Capture' menu.

Part 2: Data Analysis

1. Take a look at the Captured traffic in Wireshark. Notice three sections that show traffic summary, packet headers, and raw data. In the traffic summary section, identify different colors that correspond to different protocols being used.
2. Now you want to search for the username and password that were entered when you logged in. You will be looking at the bottom section where it displays the raw data. To make this easier, click on one of the green-colored

captured packets. Then click on the 'Analyze' menu, and choose 'Follow TCP Stream'. Perform a find for the username and password.

Part 3: Questions

1. Provide a screen shot for the TCP Stream where it shows the username and password.
2. Under the menu bar, you will see the word 'Filter'. That's where you place filters to the packet captures. (You will see a filter that you have placed when you chose to follow the TCP stream). Click on 'clear' to see all traffic again. Now look for the DNS query response corresponding to the query for mail.com. What is answer returned? Provide a screen shot that shows the DNS header with the returned answer.
3. Now you need to perform another packet capture. Go to 'mail.gmu.edu'. Then start your capture. Sign in to your GMU mail account, and then stop the capture. Go back and perform another 'Follow TCP stream' from under the 'Analyze' menu. Can you find your username or password? Why or why not?
4. Do some reading on SSL, and provide a good definition of SSL and a short explanation on how it works.