5.11.1

INTRUSION DETECTION

(SNORT for Windows)

Objective

At the end of this lab students will be able to configure and use Snort intrusion detection system. Students will understand the purpose of an intrusion detection system.

Information for Laboratory

A. Students will use configure Snort to monitor network traffic.
B. Students will understand how to use Snort to monitor network traffic for intrusion attempts using Snort rules and alerts.
C. Students will utilize Snort as a Network Intrusion Detection System (NIDS)

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

For this lab you will need to have installed WinPcap 3.0 as well as accessing Snort installation files.

Estimated Completion Time

60 Minutes

NIDS - Network Intrusion Detection Systems

A Network based intrusion detection system uses the raw network packets as the data source. A NDIS typically uses a network adapter in promiscuous mode that listens and analyses all traffic in real-time as it travels across the network. Using filters, specific traffic can be sorted, and analyzed in real-time. Using rules, network data is compare against known signs of malicious and suspicious activity such as (DOS)Denial of service attacks. At this level of NDIS, typically rules are used to look for such things as attack signatures, pattern, frequency, or anomalies. Once an attack is detected, a response module can provide options to notify, alert, and/or take action in regards to that attack at hand.

Snort

Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching in order to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plugin architecture.

Snort has three primary functional modes. It can be used as…

1. A straight packet sniffer (like tcpdump)
2. A packet logger (useful for network traffic debugging, etc)
3. A full blown network intrusion detection system

In this laboratory the student will examine each of the functional modes.

Step 1: Installing Snort

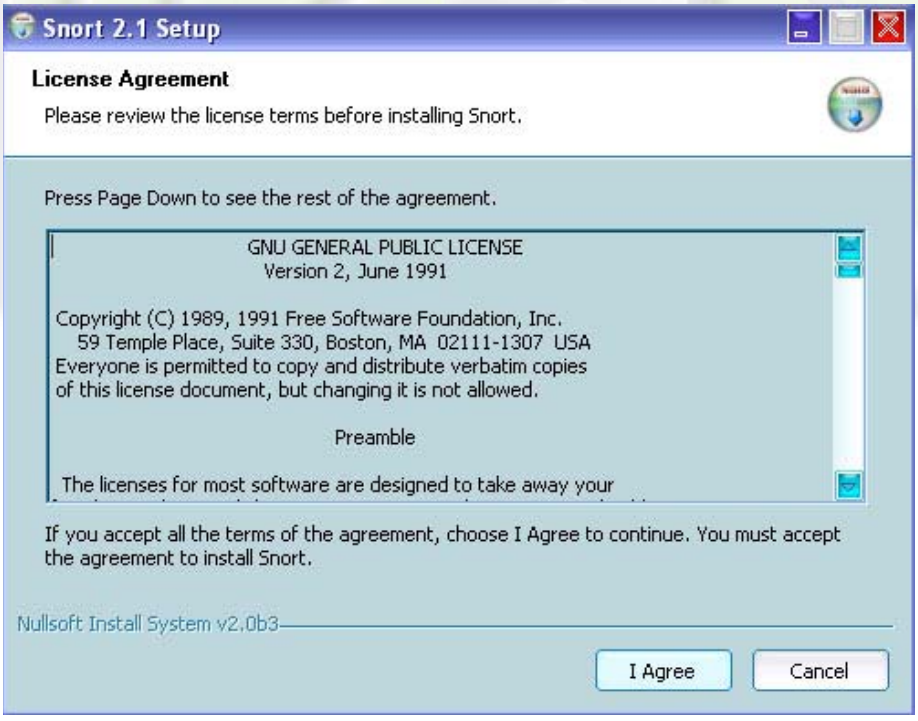
Prior to installing Snort make sure that WinPcap has been installed. Snort is composed of three major subsystems: A Packet Decoder, A Detection Engine and a Logging/Alerting System. All three of these subsystems utilize WinPcap which is a promiscuous packet sniffing library. WinPcap is used on the windows systems while the Libpcap drivers are used on the Unix/Linux systems. WinPcap is a windows port of Libpcap.

After signing onto the Windows and going to the Snort Directory, you should issue the following commands to install Snort.

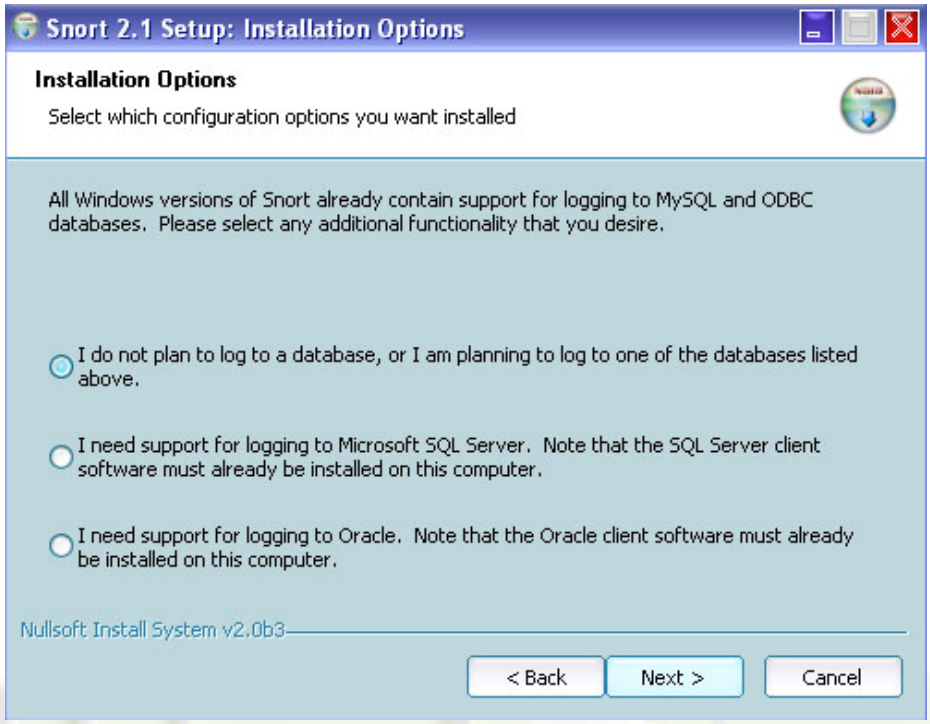
(1) Activate the Windows Explorer and navigate to the Snort Directory.

(2) Double click Snort-2_1_2.exe.

(3) The following screen should appear.

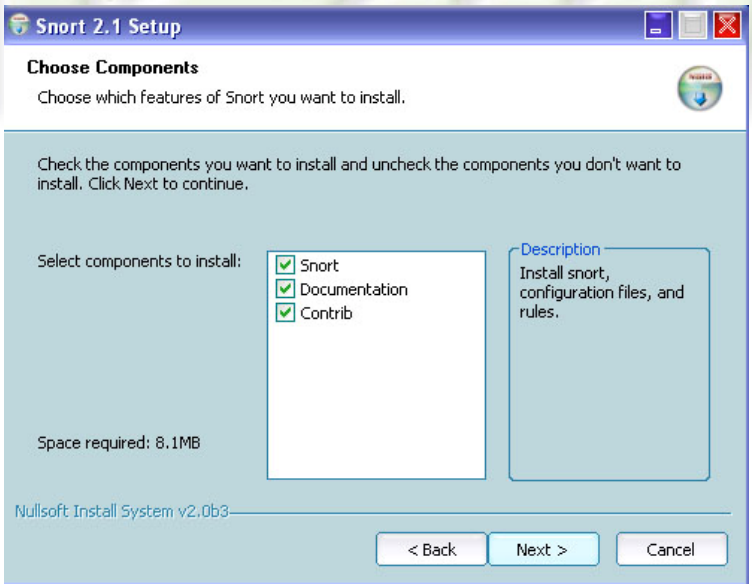


Click I Agree. The following screen should appear.

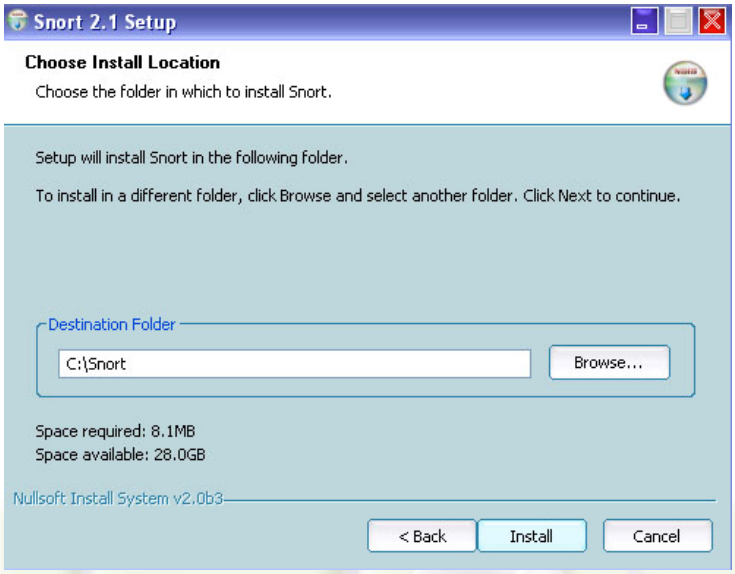


Choose the top option: I do not plan to log to a database, or I am planning to log to one of the databases listed above. Snort has built in support for MySQL and ODBC databases.

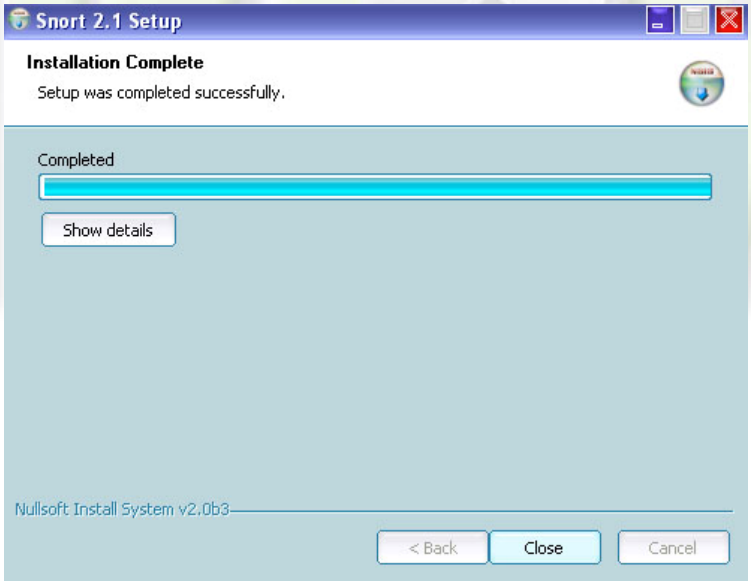
(4) Click Next. The following screen should appear. Select all components to be installed.



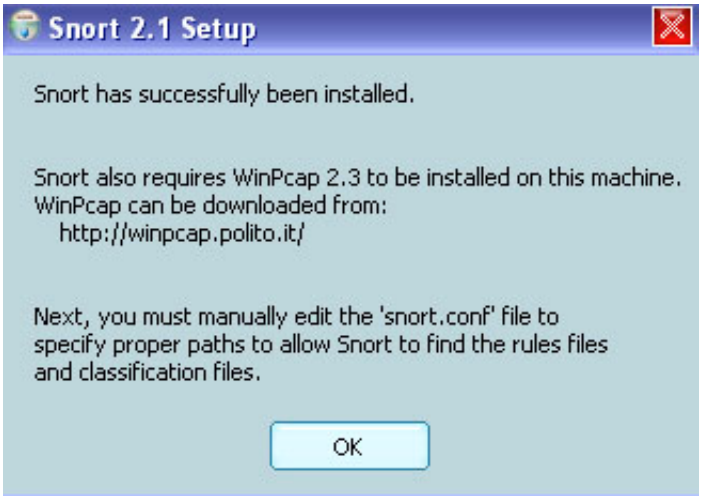
(5) Click Next. The following screen should appear. Do not make any changes to the default path which should be C:\Snort.



(6) Click Install. The Installation Complete screen should appear.

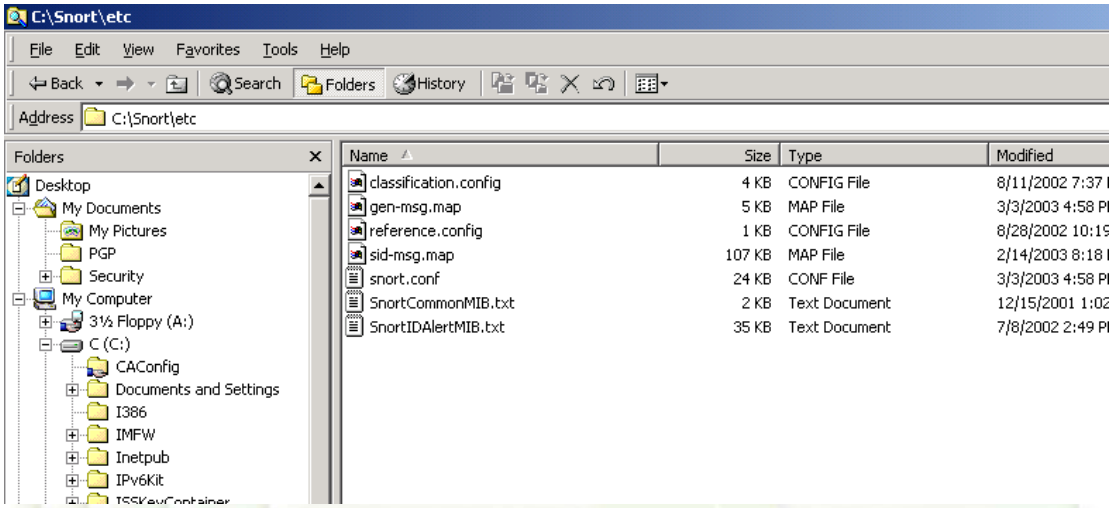


(7) Click Close. This completes the Snort installation.


Snort 2.1 Setup
Snort has successfully been installed.
Snort also requires WinPcap 2.3 to be installed on this machine.
WinPcap can be downloaded from:
http://winpcap.polito.it/
Next, you must manually edit the 'snort.conf' file to
specify proper paths to allow Snort to find the rules files
and classification files.
OK

Step 2: Configuring Snort

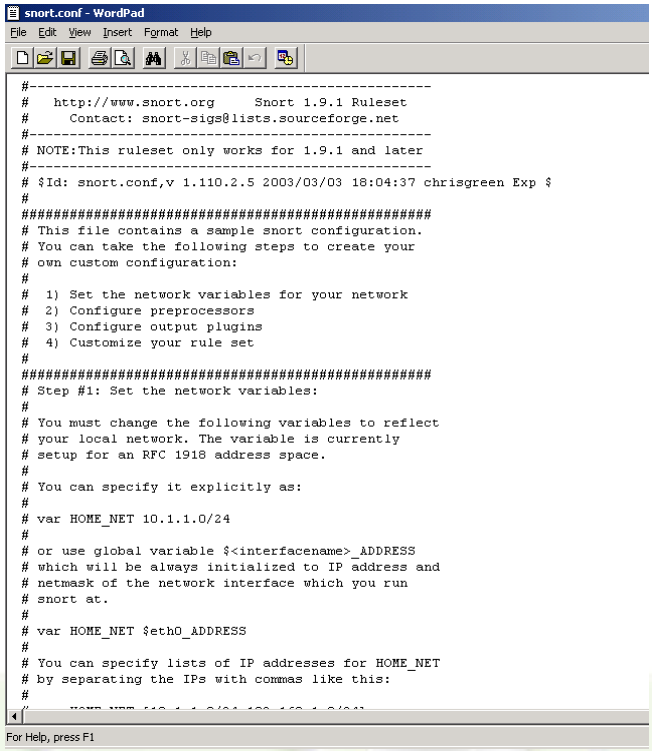
Snort is configured via the snort.conf file utilizing Wordpad.



(1) Activate the Windows Explorer and navigate to the Snort Directory. Double click the etc directory. The following screen should be present.

(2) Highlight the snort.conf file and rename it snort.old. Open snort.old with Wordpad and save it as snort.conf Remember to use “snort.conf” (in quotation marks) when you save the file. After editing the snort.conf file, check the directory for the correct file names. Snort.conf may be saved as snort.conf.txt if you left out the quotes. If so, right click and rename the file snort.conf.

Under the guidance of the Instructor browse the snort.conf file. (below)



(3) Locate the var $HOME_NET any line. This is used to specify the range of IP addresses to be monitored. Leave 'any' for the IP addresses.

```
#
# MAKE SURE YOU DON'T PLACE ANY SPACES IN YOUR LIST!
#
# or you can specify the variable to be any IP address
# like this:

var HOME_NET any

# Set up the external network addresses as well.
# A good start may be "any"

var EXTERNAL_NET any

# Configure your server lists.  This allows snort to only look for attacks
# to systems that have a service up.  Why look for HTTP attacks if you are
# not running a web server?  This allows quick filtering based on IP addresses
# These configurations MUST follow the same configuration scheme as defined
# above for $HOME_NET.

# List of DNS servers on your network
var DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
var SMTP_SERVERS $HOME_NET
```

(4) Next locate the RULE_PATH line which is used to specify the location of the Snort rules. Change this line to read var RULE_PATH c:/snort/rules (or a location specified by the instructor) as shown in the following screen.

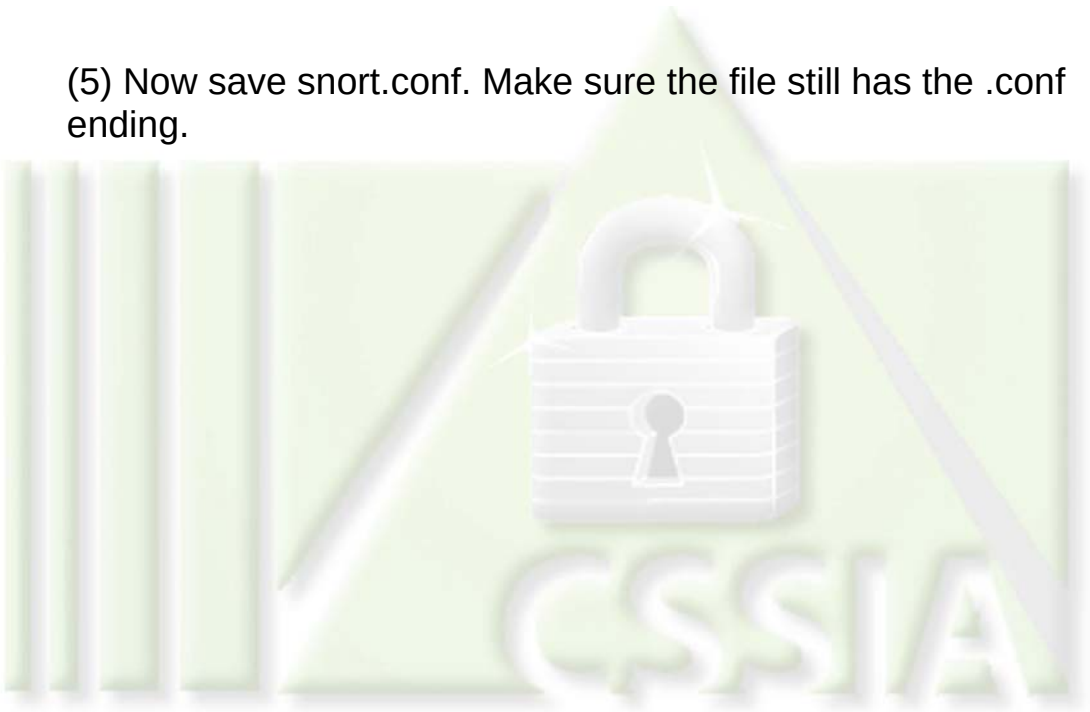
```
# other variables
#
# AIM servers.  AOL has a habit of adding new AIM servers, so instead of
# modifying the signatures when they do, we add them to this list of
# servers.
var AIM_SERVERS [64.12.24.0/24,64.12.25.0/24,64.12.26.14/24,64.12.28.0/24,64.12.29.

# Path to your rules files (this can be a relative path)
var RULE_PATH C:/snort/rules/rules

##################################################
# Step #2: Configure preprocessors
#
# General configuration for preprocessors is of
# the form
# preprocessor <name_of_processor>: <configuration_options>

# frag2: IP defragmentation support
# ------------------------------
# This preprocessor performs IP defragmentation.  This plugin will also detect
# people launching fragmentation attacks (usually DoS) against hosts.  No
```

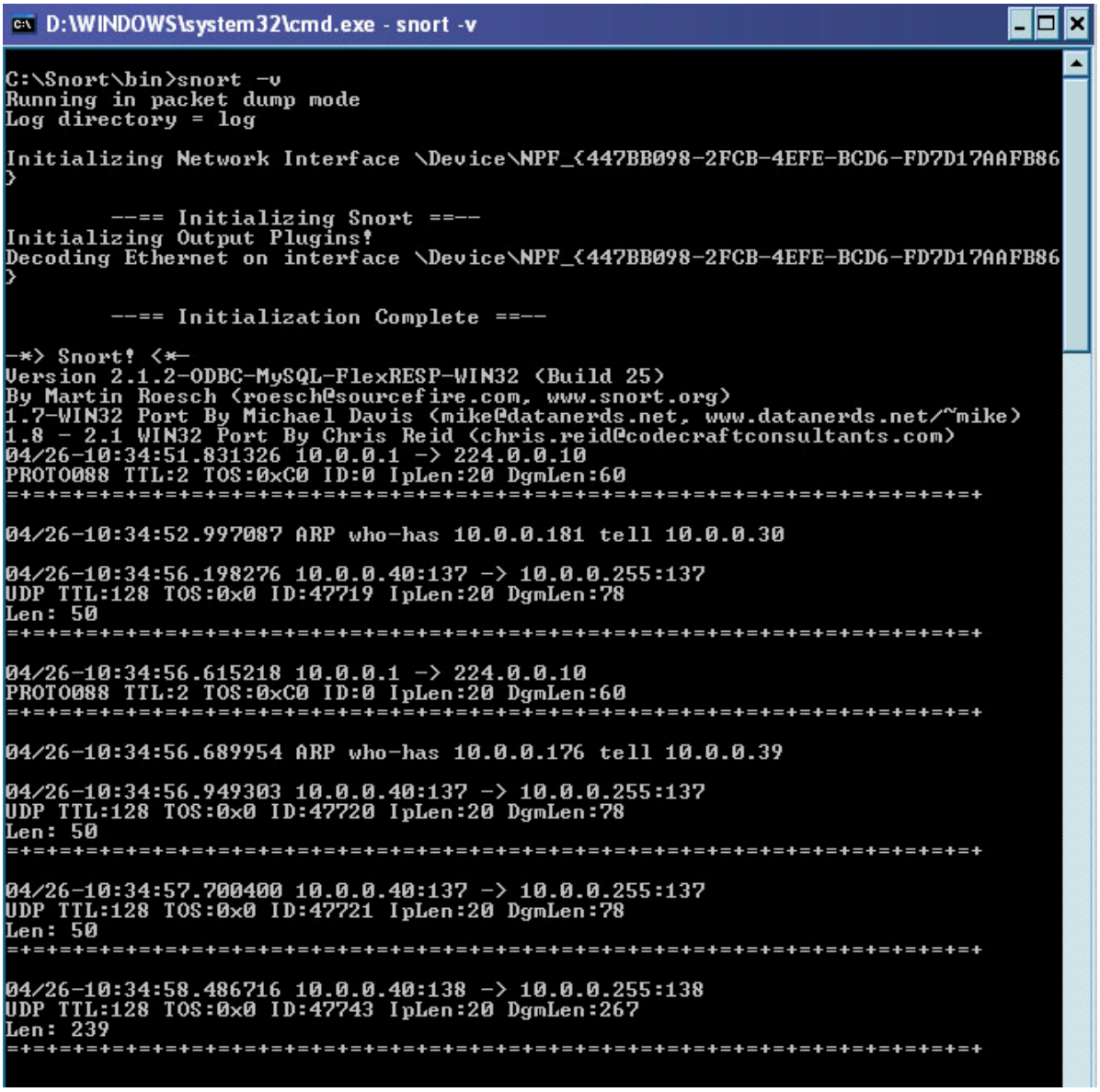
(5) Now save snort.conf. Make sure the file still has the .conf ending.



Step 3: Capturing packets

You have now successfully installed and configured Snort. You will now capture and display packets from your partner's workstation.

(1). At the Command Prompt change directory to the Snort Directory C:\Snort\bin. This is where the snort.exe executable file is. At the snort\bin directory issue the following command 'snort –v'
The –v parameter displays the packet headings



(2) Your lab partner should now ping your station. After you have captured several pings then issue a ctrl-c to stop Snort. A screen similar to the one shown below should be displayed. This display will be analyzed in coordination with your instructor.

(3) The lab partners should new reverse roles and repeat the procedure.

Step 4: Logging

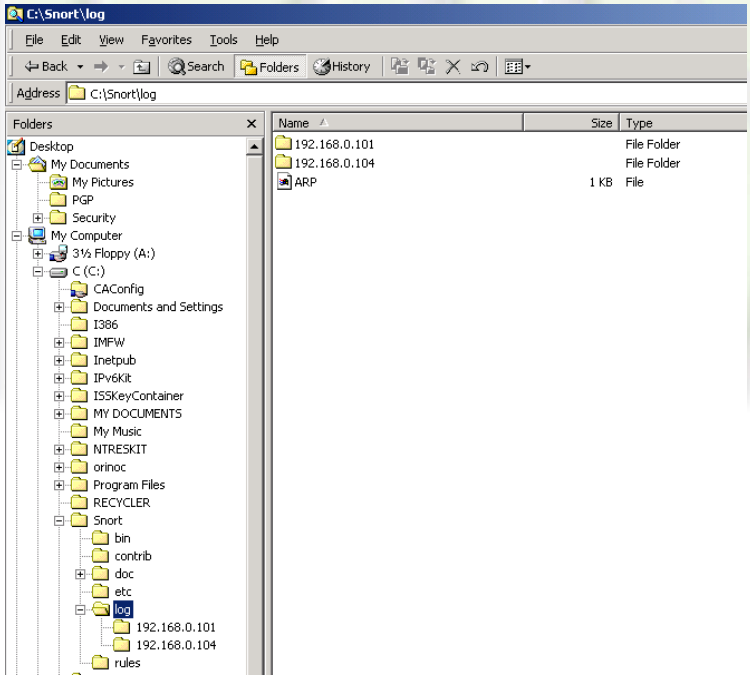
You have now successfully installed, configured, captured and displayed packets. You will now capture and save packets to a file.

(1) Issue the following command
snort –dev –l \snort\log

This command will capture and save the packets to the log file for later viewing.

(2) Your partner should now ping your workstation. After your partner has pinged your workstation stop Snort with a cntrl-c.

(3) Navigate to the /log file in the Snort directory. Use Wordpad to open and examine the captured packets in coordination with your instructor.



(4) After examining the packets reverse roles and repeat the process.

(5) As a final exercise delete the contents of /log.

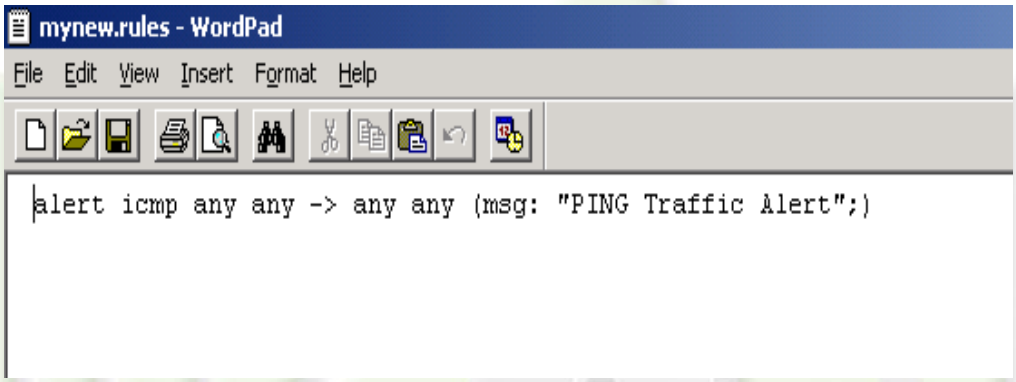
Step 5: Creating a Simple Rule

A Rule allows Snort to inspect the contents of a packet and map the contents against known attack signatures. A Rule is composed of two basic elements.

1. A Rule Header which defines WHO must be involved for the rule to be considered.

2. A Rule Option which specifies WHAT must be involved.

(1) Click Start, Run and enter Notepad. Click OK. Enter the following rule into Notepad as shown on the following screen.

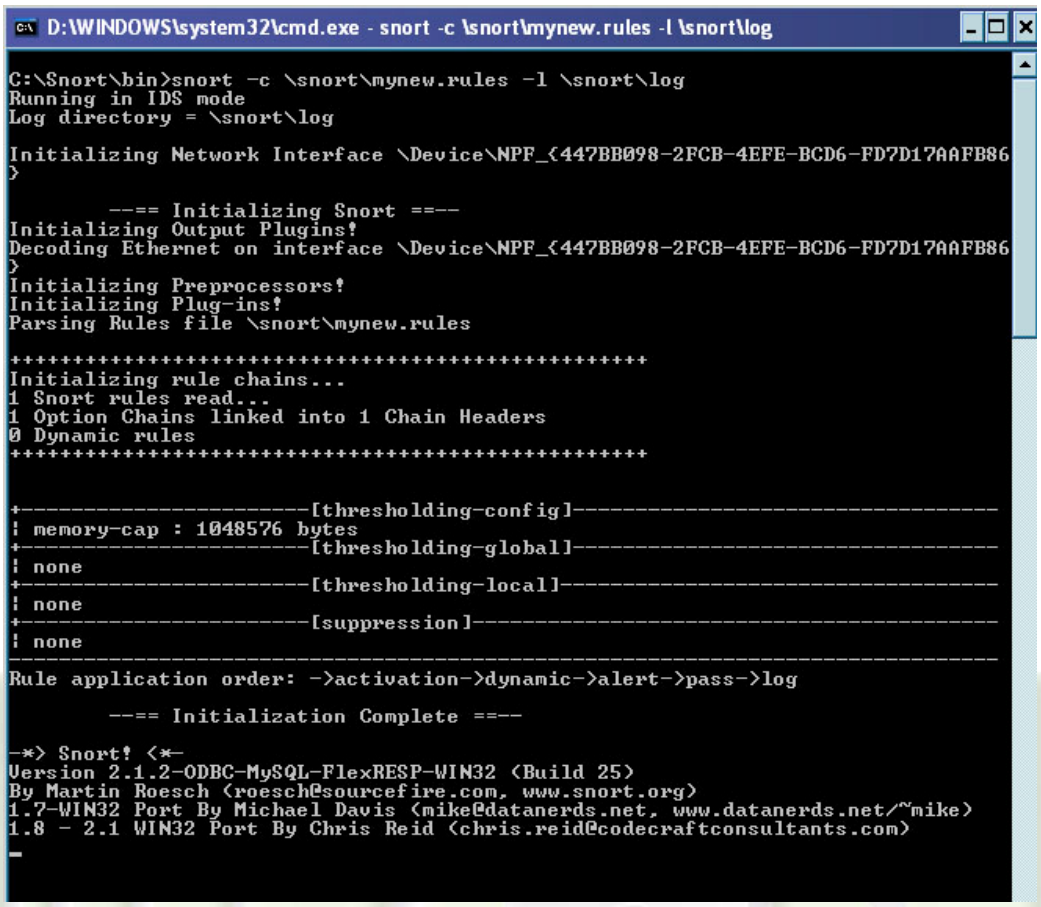


(2) Save this file under c:\snort as mynew.rules. Remember to include the quotation marks, “mynew.rules” to retain the .rules ending.

(3) Now go to the Command Prompt, change directory to c:\snort\bin and enter the following command:

snort –c \snort\mynew.rules –l \snort\log

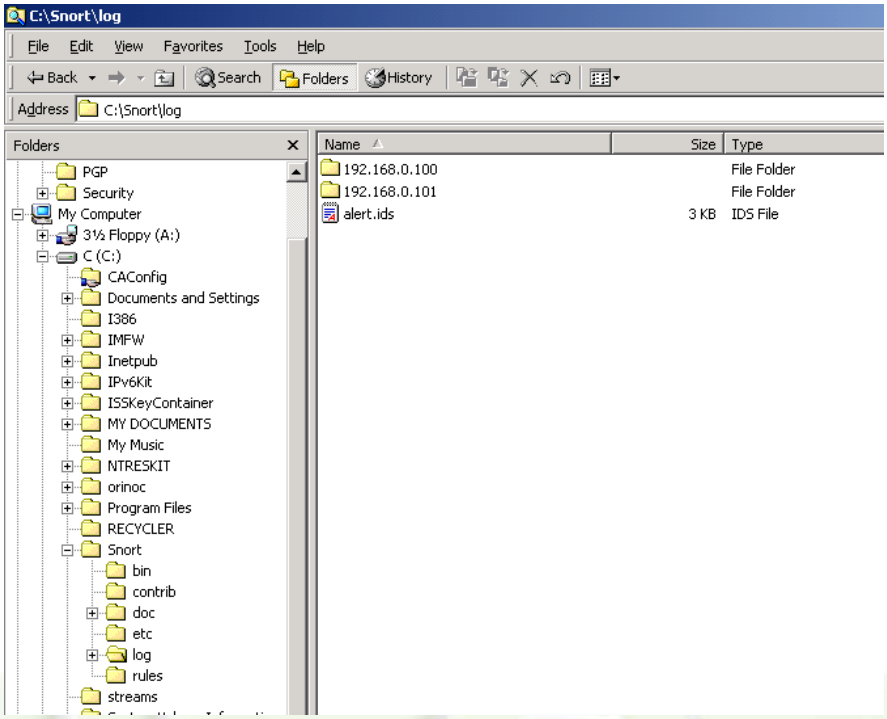
With the above command, snort will not display any information to the screen, all output will be logged to the log file.



(4) Your lab partner should now Ping your IP address.

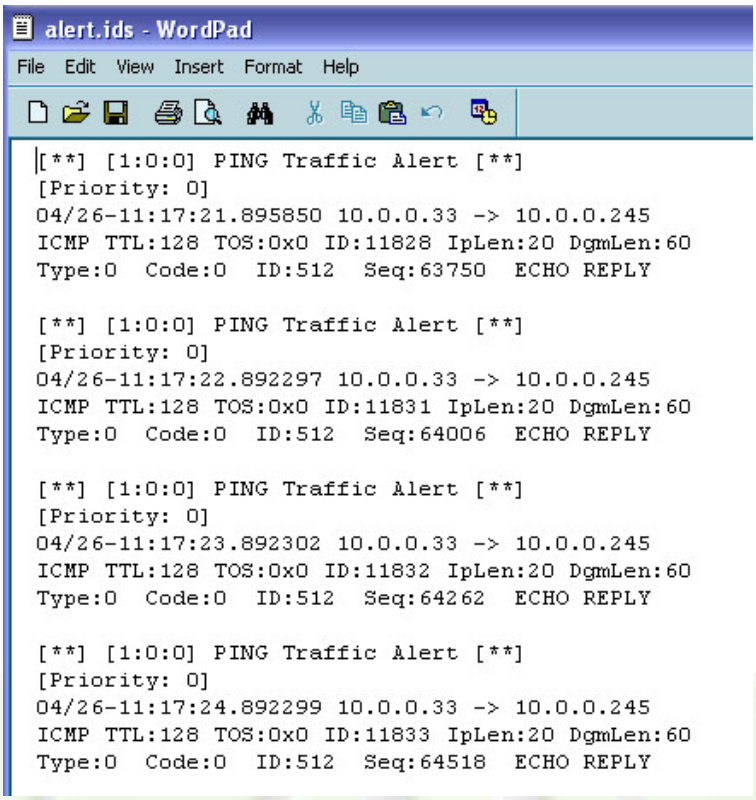
(5) Now stop Snort by entering ctrl-c.

(6) Open Windows Explorer and examine the contents of the c:\snort\log file. The contents should be similar to the following screen.



(7) Now examine each of the files using Wordpad.

(8) After examining each file then delete each file under the log directory. Be sure to open and check the contents of the alert.ids file. This is where your newly created rule logs the alerts to. If your rule was entered correctly, your alert.ids file should look like the example below. Notice the “PING Traffic Alert” lines. This is the msg: or message from your rule.



Analysis

1) For which applications is Snort best suited?

2) After working with Snort, what about packet sniffing, and or network intrusion detection systems do you feel you should study further? Why?

3) Why would you use Snort to monitor your network?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

Instructors Appendix

WinPcap

WinPcap must be utilized with windows version of Snort. WinPcap 3.0 was utilized in this exercise. Note that WinPcap 3.1 produced the error “Packet.dll not found” when used with Snort. WinPcap may be downloaded from http://winpcap.polito.it. Double click WinPcap to start the installation procedure. The system will need to be rebooted after installation of WinPcap.

Snort

Snort 2.3.0 was utilized with this exercise. The current version can be downloaded from www.winsnort.org. After downloading, double click the Snort-2_1_1.exe executable and follow the installation instructions. Typical settings no modifications are necessary for the lab.

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).