UTSA
The University of Texas at San Antonio™

Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

Lab 7 – Firewalls and Intrusion Detection Systems

Lab Description and Instructions

We learn how to setup a basic IDS using Snort. As Kali does not come pre-installed with Snort, we can install it using the following command:

`sudo apt install snort -y` (during the installation, configure 192.168.13.0/24 as local network)

We will first create a rules file for Snort as follows:

```
nano snort-rules.conf
```

Add all the desired Snort rules in snort-rules.conf (using nano or mousepad) and then run Snort as follows:

```
sudo snort -c snort-rules.conf -l ~/
```

In the above command, -c tells Snort to use the following rules file, and -l tells Snort to log all alerts in the user's home directory (/home/student/). We will see some simple Snort rules in operation during the lab.

You can check logged alerts using:

```
cat alert
```

Homework:

Try all the above steps in your VM with varying Snort rules. A quick Snort cheat sheet is on the next page.

Snort Cheat Sheet

comparitech

Output Default Directory	/var/snort/log

Sniffer Mode	
Sniff packets and send to standard output as a dump file	
-v (verbose)	Display output on the screen
-e	Display link layer headers
-d	Display packet data payload
-x	Display full packet with headers in HEX format

Packet Logger Mode	
Input output to a log file	
-r	Use to read back the log file content using snort
-l (directory name)	Log to a directory as a tcpdump file format
-k (ASCII)	Display output as ASCII format

Snort Rules Format

Rule Header + (Rule Options)

Action - Protocol - Source/Destination IP's - Source/Destination Ports - Direction of the flow

Alert Example	alert udp !10.1.1.0/24 any -> 10.2.0.0/24 any
Actions	alert, log, pass, activate, dynamic, drop, reject, sdrop
Protocols	TCP, UDP, ICMP, IP

Snort Rule Example

```
log tcp !10.1.1.0/24 any -> 10.1.1.100 (msg: "ftp access";)
```

NIDS Mode	
Use the specified file as config file and apply rules to process captured packets	
-c	Define configuration file path
-T	Use to test the configuration file including rules

Logger Mode command line options	
-l logdir	Log packets in tcp dump
-K ASCII	Log in ASCII format

NIDS Mode Options	
Define a configuration file	-c (Configuration file name)
Check the rule syntax and format for accuracy	-T -c (Configuration file name)
Alternate alert modes	-A (Mode : Full, Fast, None ,Console)
Alert to syslog	-s
Print alert information	-v
Send SMB alert to PC	-M (PC name or IP address)
ASCII log mode	-K
No logging	-N
Run in Background	-D
Listen to a specific network interface	-i