UTSA
The University of Texas at San Antonio™

Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

Lab 8 – 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 update & sudo apt install snort -y
```

We will first specify the local and external networks in the /etc/snort/snort.lua config file as follows:

```
sudo nano /etc/snort/snort.lua
```

In the snort.lua file, change HOME_NET = 'any' to HOME_NET = '192.168.13.0/24' and change EXTERNAL_NET = '!$HOME_NET'.

Also, add this under "configure outputs" of snort.lua

```
alert_full = { file = true, limit = 1000000000 }
```

Exit nano saving changes.

Next, create a rules file for Snort as follows:

```
nano ~/mysnort.rules
```

Example alert rules for outgoing ICMP pings and incoming SSH connections:

```
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ICMP Ping Detected";
itype:8; icode:0; sid:1000001; rev:1;)

alert tcp any any -> $HOME_NET 22 (msg:"Incoming SSH traffic detected";
flags:S; sid:1000002; rev:1;)
```

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

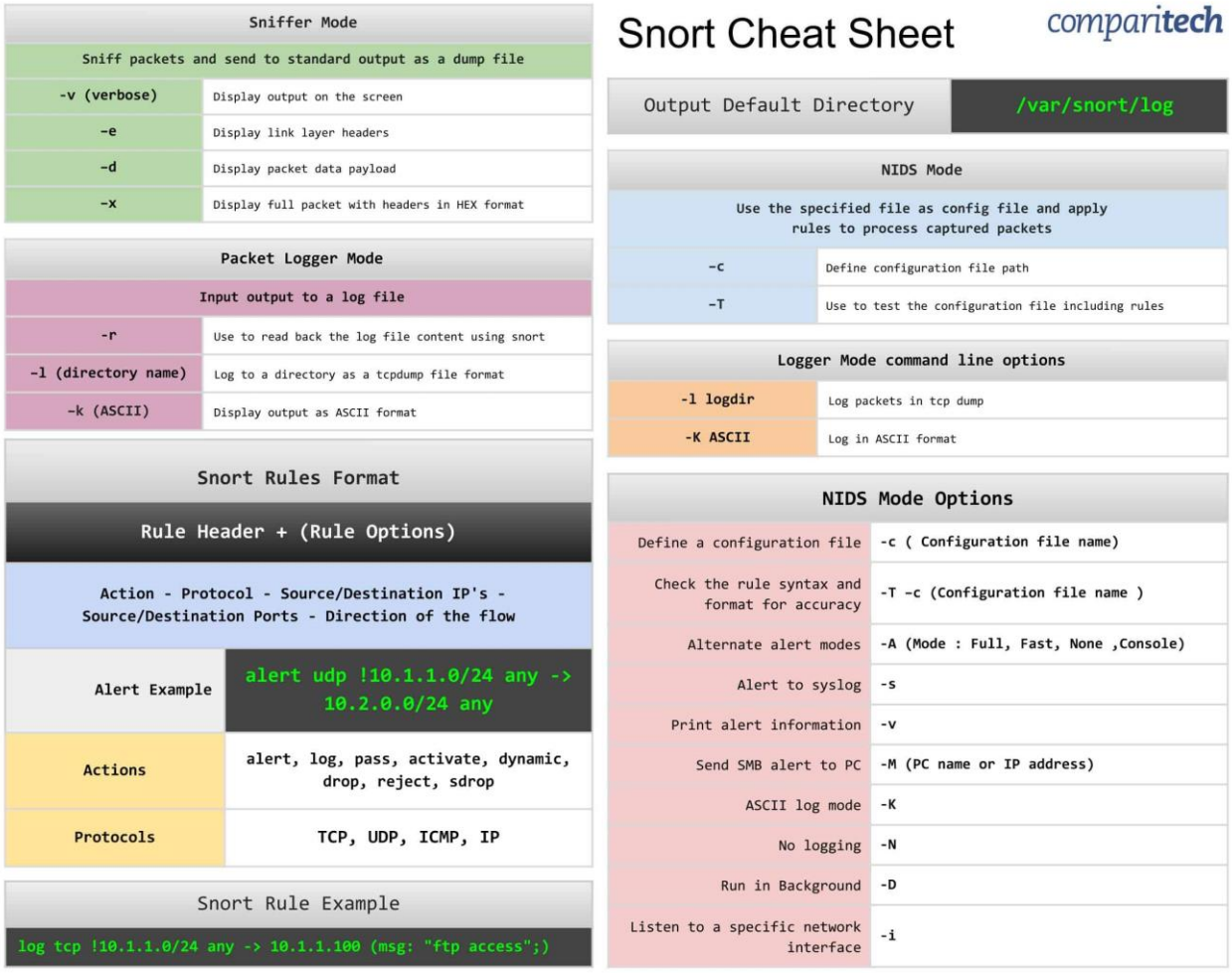
```
sudo snort -c /etc/snort/snort.lua -R ~/mysnort.rules -l /var/log/snort
-i eth0
```

In the above command, -c tells Snort to use the following config file, -R tells Snort to use the following rules file, and -l tells Snort to log all alerts in the system log directory (/var/log/snort/). We will see some simple Snort rules in operation during the lab.

You can check logged alerts using:

```
sudo cat /var/log/snort/alert_full.txt
```

Homework:
Try all the above steps in your VM with varying Snort rules. A quick Snort cheat sheet is on the next page. No submission required.



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";)

Snort Cheat Sheet

comparitech

Output Default Directory	/var/snort/log

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