

## Homework 5 – Snort

Ryan Foster -CIS 480

### Task 1. Start and stop Snort (sec 4.1 & 4.2)

- Follow the instructions in sec 4.2 and perform an nmap scan of [www.example.com](http://www.example.com) from the remote workstation. Take a screenshot of the output on the snort terminal.

The screenshot shows two terminal windows side-by-side. The left window, titled 'tom@snort: ~', displays the command 'ls -l' followed by the contents of 'start\_snort.sh'. The right window, titled 'tom@snort: ~', shows the output of running the script, which includes several ICMP and SNMP logs indicating network activity.

```
tom@snort:~$ ls -l
total 4
-rwxrwxr-x 1 tom tom 78 Jan 20 2018 start_snort.sh
tom@snort:~$ cat start_snort.sh
#!/bin/bash
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0 -k none
tom@snort:~$ ./start_snort.sh
10/29-20:14:31.185199 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 203.0.113.20 -> 203.0.113.10
10/29-20:14:31.185199 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 203.0.113.20 -> 203.0.113.10
10/29-20:14:31.185424 [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 203.0.113.20 -> 203.0.113.10
10/29-20:14:32.504548 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 203.0.113.20:50559 -> 203.0.113.10:161
10/29-20:14:32.547170 [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 203.0.113.20:50559 -> 203.0.113.10:705
```

The screenshot shows two terminal windows side-by-side. The left window, titled 'hank@remote\_ws: ~', displays the Nmap help menu with various options like --datadir, --send-eth, and examples. The right window, titled 'admin@remote\_gw: ~', shows the output of an Nmap scan of 'www.example.com', reporting port 22/tcp as open (ssh), 53/tcp as open (domain), 80/tcp as open (http), and 443/tcp as open (https). The scan took 1.51 seconds.

```
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
hank@remote_ws:~$ sudo nmap www.example.com

Starting Nmap 7.01 ( https://nmap.org ) at 2022-10-29 20:14 UTC
Nmap scan report for www.example.com (203.0.113.10)
Host is up (0.000046s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
hank@remote_ws:~$
```

## Task 2. Write a sample bad rule (sec 4.3)

- Open the local.rules file with nano editor. Add a rule following the instructions in sec 4.3.  
Take a screenshot of the rule you created.

•

The screenshot shows a terminal window titled "GNU nano 2.5.3" with the file "local.rules" open. The content of the file is:

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# alert tcp xxxxx

# -----
# This file intentionally does not come with signatures. Put your local
# additions here.
```

At the bottom of the terminal window, there is a menu bar with various keyboard shortcuts for nano editor commands like "Get Help", "Write Out", "Where Is", etc.

- Restart snort and test this rule following the instructions. Report the output displayed on the snort terminal in a screenshot.

•

The screenshot displays several terminal windows and a browser window. The terminal windows show the following command and its output:

```
tom@snort:~$ ./start_snort.sh
[...]
Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
hank@remote_ws:~$ sudo nmap www.example.com
Starting Nmap 7.01 ( https://nmap.org ) at 2022-10-29 20:42 UTC
Failed to resolve "firefox".
Nmap scan report for www.example.com (203.0.113.10)
Host is up (0.000046s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
```

Another terminal window shows the user trying to run the script again:

```
tom@snort:~$ ./start_snort.sh
[...]
Nmap done: 1 IP address (1 host up) scanned in 11.51 seconds
hank@remote_ws:~$ firefox www.example.com
```

A Firefox browser window titled "Hunderblunder and Thunder Turkey Ranch" is open, displaying the website "www.example.com". The URL bar shows "www.example.com".

### Task 3. Create a custom rule for confidential traffic (sec 4.4)

- Open the local.rules file with nano editor. Add a rule following the instructions in sec 4.4. Confirm that this rule is working and [take a screenshot of the rule you created](#).

•

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# alert tcp xxxxx
# alert ip any any -> any any (msg: "IP Packet Detected" ; )
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.
```

- Restart snort and test this rule following the instructions. [Report the output displayed on the snort terminal in a screenshot](#).

•

```
Failed to resolve 'firefox'.
Nmap scan timing for www.example.com (203.0.113.10)
Host is up (0.00001s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 11.51 seconds
hank@remote_ws:~$ firefox www.example.com
^[[A^[[GFX1:]: Receive IPC close with reason=AbnormalShutdown
[Child 428, Chrome ChildThread] WARNING: pipe error (3): Connection reset by peer: file /ox-QrVfEH/firefox-61.0+build3/IPC/chromium/src/chrome/common/lpc_channel_posix.cc, line 3
[GFX1:]: Receive IPC close with reason=AbnormalShutdown
[Child 386, Chrome ChildThread] WARNING: pipe error (3): Connection reset by peer: file /ox-QrVfEH/firefox-61.0+build3/IPC/chromium/src/chrome/common/lpc_channel_posix.cc, line 3
hank@remote_ws:~$ firefox www.example.com
hank@remote_ws:~$ firefox www.example.com
ExceptionHandler::GenerateDump cloned child 670
ExceptionHandler::SendContinueSignalToChild sent continue signal to child
ExceptionHandler::WaitForContinueSignal waiting for continue signal...
hank@remote_ws:~$ 
```

  

```
File Edit View Search Terminal Tabs Help
File: rc.local
GNU nano 2.5.3
#!/bin/bash
route delete default
route add default gw 203.0.113.1
#
# get ethernet device names for the two lans and the wan interfaces
lan1=$(ifconfig | grep -B1 "inet addr:192.168.1.10" | awk '$1!="inet" && $1!="-" {print $1}')
lan2=$(ifconfig | grep -B1 "inet addr:192.168.2.10" | awk '$1!="inet" && $1!="-" {print $1}')
wan=$(ifconfig | grep -B1 "inet addr:203.0.113.10" | awk '$1!="inet" && $1!="-" {print $1}')
#
# flush and delete all chains
#
iptables --flush
iptables -t nat --flush
iptables -t mangle --flush
iptable --delete-chain
[ Read 52 lines (Warning: No write permission) ]
```

#### Task 4. Watch internet traffic (sec 4.6)

- Go to the ws2 (mary) terminal and run nmap: “sudo nmap [www.example.com](http://www.example.com)”.
- Explain why the output does not include the ICMP PING NMAP alerts that you saw when the remote workstation ran nmap.
- Now restart snort and again run nmap from mary’s ws2 computer. Report the output on the snort terminal in a screenshot. Explain why you now can see the ICMP PING NMAP alerts.
- 

```
# flush and delete all chains
#
iptables --flush
iptables -t nat --flush
iptables -t mangle --flush
iptables --delete-chain
iptables -t nat --delete-chain
iptables -t mangle --delete-chain
#
# mirror incoming wan traffic to snort
#
iptables -t mangle -A PREROUTING -i $wan -j TEE --gateway 192.168.3.1
iptables -t mangle -A PREROUTING -i $lan1 -j TEE --gateway 192.168.3.1
iptables -t mangle -A PREROUTING -i $lan2 -j TEE --gateway 192.168.3.1
#
[ Error writing rc.local: Permission denied ]
```

The terminal window shows the following details:  
File Edit View Search Terminal Tabs Help  
admin@web\_server:~ x ubuntu@gateway:/etc Modified  
GNU nano 2.5.3 File: rc.local  
The rc.local file contains configuration for iptables to flush and mirror traffic to snort. An error message at the bottom indicates a permission denied issue when writing the file.  
Bottom menu: Get Help, Write Out, Where Is, Cut Text, Justify, Cur Pos, Exit, Read File, Replace, Uncut Text, To Listener, Go To Line

```
File Edit View Search Terminal Tabs Help
mary@ws2:~                                         x
Nmap scan report for www.example.com (192.168.1.2)
Host is up (0.000032s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
mary@ws2:~$ ^C
mary@ws2:~$ sudo nmap www.example.com

Starting Nmap 7.01 ( https://nmap.org ) at 2022-10-29 21:06 UTC
Nmap scan report for www.example.com (192.168.1.2)
Host is up (0.000030s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
mary@ws2:~$ █
ubuntu@gateway: /etc
File Edit View Search Terminal Tabs Help
```