

Issa Odeh

CS 445

Homework 3

March 24, 2021

Part 1: Using sort

Nmap scan on port 80

```
zsh: suspended nmap -p80 192.168.56.102

(root@kali)-[/home/issa]
# nmap -p80 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-23 15:20 PDT
Nmap scan report for 192.168.56.102
Host is up (0.00034s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:A6:3F:C5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

(root@kali)-[/home/issa]
#
```

```

root@kali: /home/issa/log1

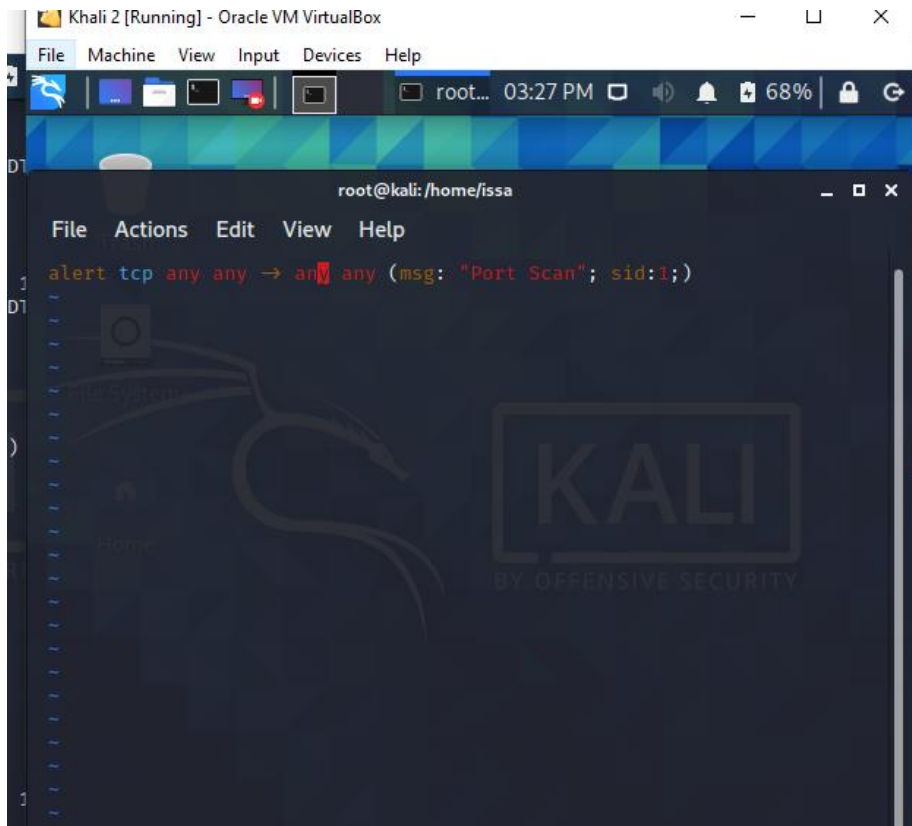
[**] [1:1:0] Port Scan [**]
[Priority: 0]
03/24-19:34:08.029457 08:00:27:A6:3F:C5 → 08:00:27:00:E1:6E type:0x8
len:0x3C
192.168.56.102:47055 → 192.168.56.103:80 TCP TTL:40 TOS:0x0 ID:63815
Len:20 DgmLen:44
*****S* Seq: 0x20DB6FDD Ack: 0x0 Win: 0x400 TcpLen: 24
TCP Options (1) ⇒ MSS: 1460

[**] [1:1:0] Port Scan [**]
[Priority: 0]
03/24-19:34:08.029984 08:00:27:A6:3F:C5 → 08:00:27:00:E1:6E type:0x8
len:0x3C
192.168.56.102:47055 → 192.168.56.103:80 TCP TTL:64 TOS:0x0 ID:0 IpL
20 DgmLen:40 DF
*****R** Seq: 0x20DB6FDE Ack: 0x0 Win: 0x0 TcpLen: 20

~
~
~

```

Snort does indeed detect the port scans. The signature id in this case would be 1 as it is showing in the first line. The signature is important because it will tell us if the scan was detected or not. SID is used to uniquely identify snort rules, and it allows the user to identify which rule is triggered.



snort.log.1616538025

Time	Source	Destination	Protocol	Length	Info
0.000000	PcsCompu_00:e1:6e	Broadcast	ARP	60	Who has 192.1
0.000018	PcsCompu_a6:3f:c5	PcsCompu_00:e1:6e	ARP	42	192.168.56.10
13.031858	192.168.56.103	192.168.56.102	TCP	60	42208 -> 80 [S
13.031891	192.168.56.102	192.168.56.103	TCP	58	80 -> 42208 [S
13.032181	192.168.56.103	192.168.56.102	TCP	60	42208 -> 80 [R

Apply a display filter ... <Ctrl-/>

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: PcsCompu_00:e1:6e (08:00:27:00:e1:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

3.

Nmap Xmas stealthy scan

```
(root@kali)-[/home/issa]
# nmap -sX 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-23 15:36 PDT
Nmap scan report for 192.168.56.102
Host is up (0.00025s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
80/tcp    open|filtered http
MAC Address: 08:00:27:A6:3F:C5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds
```

I did two scans. One above is on all ports and one below is just at port 80.

```
(root@kali)-[/home/issa]
# nmap -sX -p80 192.168.56.102 255 x 1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-24 16:14 PDT
Nmap scan report for 192.168.56.102
Host is up (0.00037s latency).

PORT      STATE      SERVICE
80/tcp    open|filtered http
MAC Address: 08:00:27:A6:3F:C5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

Alert for this screenshot on all ports.

```
File Actions Edit View Help
[Priority: 0]
03/24-15:51:14.409964 08:00:27:00:E1:6E → 08:00:27:A6:3F:C5 type:0x80
0 len:0x3C
192.168.56.103:34901 → 192.168.56.102:8080 TCP TTL:45 TOS:0x0 ID:6207
IpLen:20 DgmLen:40
**U*P**F Seq: 0xD4D6A332 Ack: 0x0 Win: 0x400 TcpLen: 20 UrgPtr: 0x
0

[**] [1:1:0] Xmas Scan [**]
[Priority: 0]
03/24-15:51:14.409985 08:00:27:A6:3F:C5 → 08:00:27:00:E1:6E type:0x80
0 len:0x36
192.168.56.102:25 → 192.168.56.103:84901 TCP TTL:64 TOS:0x0 ID:0 IpLe
n:20 DgmLen:40 DF
**A*R** Seq: 0x0 Ack: 0xD4D6A333 Win: 0x0 TcpLen: 20

[**] [1:1:0] Xmas Scan [**]
[Priority: 0]
03/24-15:51:14.410003 08:00:27:A6:3F:C5 → 08:00:27:00:E1:6E type:0x80
0 len:0x36
192.168.56.102:445 → 192.168.56.103:34901 TCP TTL:64 TOS:0x0 ID:0 IpL
en:20 DgmLen:40 DF
**A*R** Seq: 0x0 Ack: 0xD4D6A333 Win: 0x0 TcpLen: 20

[**] [1:1:0] Xmas Scan [**]
```

When doing the stealthy xmas scanning there was a flag but there is no response coming in. If a RST packet is received, the port is considered closed, while no response means it is open/filtered. It does not manage to evade snort in this case. The signature identified was 1 and the rev is 0. I can clearly see the flags shown above.

This one I only ran the scan on port 80 and this is the results. Same as above. There is no response.

```
File Actions Edit View Help
[**] [1:1:0] Xmas Scan [**]
[Priority: 0]
03/24-16:14:58.827282 08:00:27:00:E1:6E → 08:00:27:A6:3F:C5 type:0x800
len:0x3C
192.168.56.103:40014 → 192.168.56.102:80 TCP TTL:48 TOS:0x0 ID:18983 I
plen:20 DgmLen:40
**U*P**F Seq: 0xB6AB309A Ack: 0x0 Win: 0x400 TcpLen: 20 UrgPtr: 0x0

[**] [1:1:0] Xmas Scan [**]
[Priority: 0]
03/24-16:14:58.927767 08:00:27:00:E1:6E → 08:00:27:A6:3F:C5 type:0x800
len:0x3C
192.168.56.103:40015 → 192.168.56.102:80 TCP TTL:50 TOS:0x0 ID:3203 Ip
Len:20 DgmLen:40
**U*P**F Seq: 0xB6AA309B Ack: 0x0 Win: 0x400 TcpLen: 20 UrgPtr: 0x0

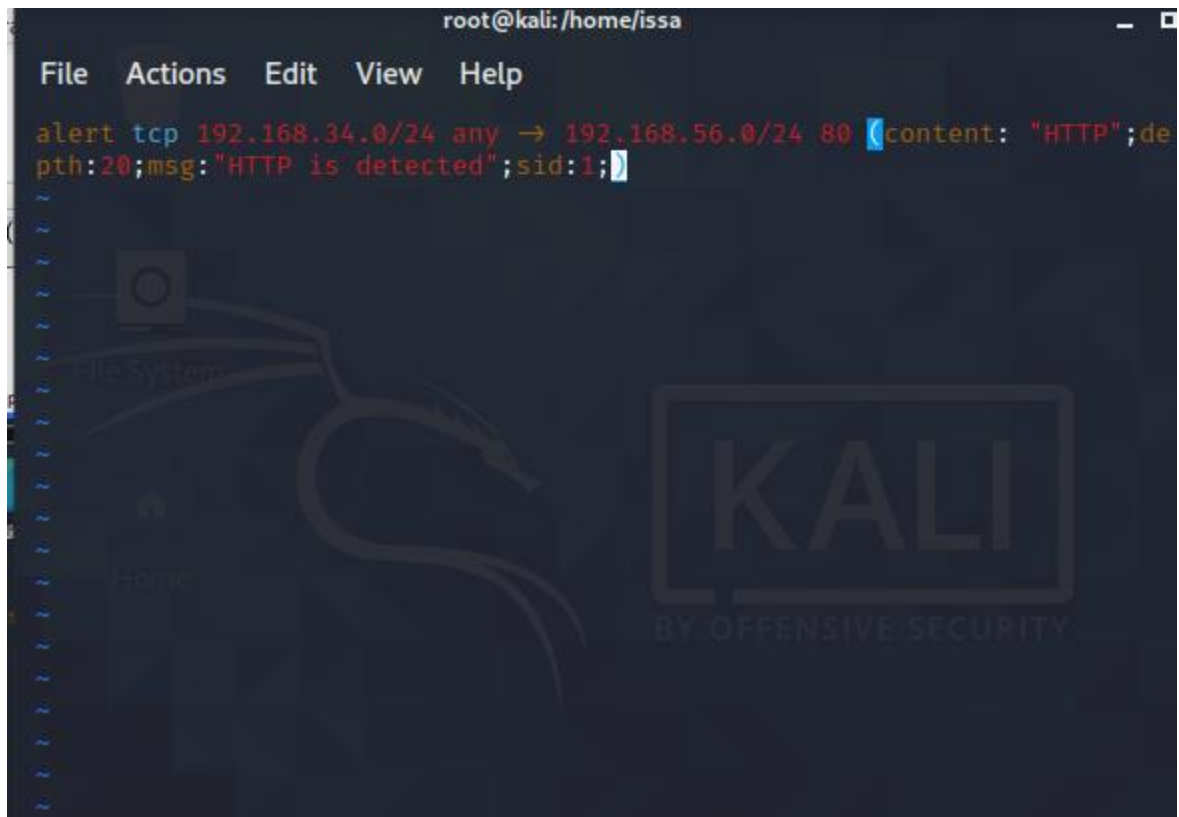
~
~
~
~
```

Used tcp dump for this screenshot

```
15:51:15.544990 IP 192.168.56.102.625 > 192.168.56.103.34901: Flags [R
.], seq 0, ack 3570836275, win 0, length 0
15:51:15.545173 IP 192.168.56.103.34901 > 192.168.56.102.15000: Flags
[FPU], seq 3570836274, win 1024, urg 0, length 0
15:51:15.545175 IP 192.168.56.103.34901 > 192.168.56.102.2035: Flags [
FPU], seq 3570836274, win 1024, urg 0, length 0
15:51:15.545176 IP 192.168.56.103.34901 > 192.168.56.102.zebra: Flags
[FPU], seq 3570836274, win 1024, urg 0, length 0
15:51:15.545191 IP 192.168.56.102.15000 > 192.168.56.103.34901: Flags
[R.], seq 0, ack 3570836275, win 0, length 0
15:51:15.545215 IP 192.168.56.102.2035 > 192.168.56.103.34901: Flags [
R.], seq 0, ack 3570836275, win 0, length 0
15:51:15.545230 IP 192.168.56.102.zebra > 192.168.56.103.34901: Flags
[R.], seq 0, ack 3570836275, win 0, length 0
15:51:15.545711 IP 192.168.56.103.34901 > 192.168.56.102.7435: Flags [
FPU], seq 3570836274, win 1024, urg 0, length 0
15:51:15.545714 IP 192.168.56.103.34901 > 192.168.56.102.32778: Flags
[FPU], seq 3570836274, win 1024, urg 0, length 0
15:51:15.545715 IP 192.168.56.103.34901 > 192.168.56.102.1201: Flags [
FPU], seq 3570836274, win 1024, urg 0, length 0
15:51:15.545717 IP 192.168.56.103.34901 > 192.168.56.102.9099: Flags [
FPU], seq 3570836274, win 1024, urg 0, length 0
15:51:15.545739 IP 192.168.56.102.7435 > 192.168.56.103.34901: Flags [
R.], seq 0, ack 3570836275, win 0, length 0
15:51:15.545773 IP 192.168.56.102.32778 > 192.168.56.103.34901: Flags
[R.], seq 0, ack 3570836275, win 0, length 0
15:51:15.545797 IP 192.168.56.102.1201 > 192.168.56.103.34901: Flags [
R.], seq 0, ack 3570836275, win 0, length 0
15:51:15.545821 IP 192.168.56.102.9099 > 192.168.56.103.34901: Flags [
R.], seq 0, ack 3570836275, win 0, length 0
```

```
(root@kali)-[/home/issa/log2]
```

Part 2:



I tried to use this alert and the one below. This one didn't quite work.

```
root@kali: /home/issa
File Actions Edit View Help
alert tcp 192.168.56.102 80 → any any (content: "www.Facebook.com";msg
:"GET OFF FACEBOOK";sid:1;)
```

This alert worked when I opened Facebook browser.

[illegible]

Used tcpdump to open information. Was not quite sure where else I can get the message. I tried wireshark but my computer did not have the best time running it.

```
# tcpdump -r snort.log.1616629807
reading from file snort.log.1616629807, link-type EN10MB (Ethernet)
16:50:18.651985 IP edge-star-mini-shv-01-dfw5.facebook.com.http > 10.0.2.7.44806: Flags [P.], seq 6859:7225,
Moved Permanently
```