

IDS (Intrusion Detection System)



**Northeastern
University**

Name: Davindernain Singh Sehgal



Due to some policies at my academic institute,
I am unable to share the entire document.

The following pages give the results of most of the rules I have
talked about and give a general idea of my proficiency with the tool.

Currently, I share my router and internet services with someone
which is why I am unable to reveal the IP address in the following
pages.

4. Wrote a rule to Detect any image/ media downloads (can require multiple rules)

5. Carried out the following Nmaps Scans and wrote a rule to detect the following Nmap network scans:

- Nmap FIN Scan

```
nmap done. 1 IP address (1 host up) scanned in 0.1s
securityonion@securityonion:~$ sudo nmap -sF -p22
```

```
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Commencing packet processing (pid=1321)
12/01-19:45:30.558498  [**] [1:1000008:1] Nmap FIN Scan detected [**] [Priority: 0] {TCP}
12/01-19:45:30.558498  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Gathering] {TCP}
12/01-19:45:30.660236  [**] [1:1000008:1] Nmap FIN Scan detected [**] [Priority: 0] {TCP}
12/01-19:45:30.660236  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Gathering] {TCP}
```

- TCP Ping scan

```
nmap done. 1 IP address (1 host up) scanned in 0.1s
securityonion@securityonion:~$ sudo nmap -sT -p22
```

```
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Commencing packet processing (pid=1346)
12/01-19:49:35.263344  [**] [1:1829291:2] NMAP TCP scan detected [**] [Priority: 0] {TCP}
```

- Null Scan

```
nmap done. 1 IP address (1 host up) scanned in 0.17s
securityonion@securityonion:~$ sudo nmap -sN -p22
```

```
Commencing packet processing (pid=1363)
12/01-19:50:31.574511  [**] [1:1000009:1] Nmap NULL Scan detected [**] [Priority: 0] {TCP}
12/01-19:50:31.674724  [**] [1:1000009:1] Nmap NULL Scan detected [**] [Priority: 0] {TCP}
```

- SYN-FIN Scan

```
Preprocessor Object: SF_DNS Version 1.1 (built 4/11/07)
Commencing packet processing (pid=1406)
12/01-19:53:09.839856  [**] [1:1413297417:1] "Nmap SYN-FIN Scan" [**] [Priority: 0] {TCP}
12/01-19:53:09.839856  [**] [1:624:7] SCAN SYN FIN [**] [Classification: Attempted Informa
12/01-19:53:09.941550  [**] [1:1413297417:1] "Nmap SYN-FIN Scan" [**] [Priority: 0] {TCP}
12/01-19:53:09.941550  [**] [1:624:7] SCAN SYN FIN [**] [Classification: Attempted Informa
```

QUITTING!

```
securityonion@securityonion:~$ sudo nmap -sS --scanflags SYNFIN -p22
1.77
```

- XMAS Scans

```
nmap done. 1 IP address (1 host up) scanned in 0.17s
securityonion@securityonion:~$ sudo nmap -sX -p22
```

```
Preprocessor Object: SF_DNS Version 1.1 (built 4/11/07)
Commencing packet processing (pid=1386)
12/01-19:51:51.682398  [**] [1:1000006:1] Nmap XMAS Scan detected [**] [Priority: 0] {TCP}
12/01-19:51:51.682398  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Infor
12/01-19:51:51.784053  [**] [1:1000006:1] Nmap XMAS Scan detected [**] [Priority: 0] {TCP}
12/01-19:51:51.784053  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Infor
```

- URG Scan

```
Commencing packet processing (pid=1441)
12/01-19:54:41.552169  [**] [1:130003232:1] "Nmap URG Scan" [**] [Priority: 0] {TCP}
12/01-19:54:41.654025  [**] [1:130003232:1] "Nmap URG Scan" [**] [Priority: 0] {TCP}
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
securityonion@securityonion:~$ sudo nmap --scanflags URG -p22
```

6. Wrote a rule to detect pings from devices on the same subnet

```
Commencing packet processing (pid=1547)
12/01-20:03:00.409614  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:00.409669  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:01.411945  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:01.412148  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:02.413415  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:02.413479  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:03.415370  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:03.415412  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:04.417502  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:04.417565  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:05.419977  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:05.420040  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:06.421605  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:06.421635  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:07.428414  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:07.428475  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:08.431508  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:08.431575  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:09.433047  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:09.433117  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:10.434883  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
12/01-20:03:10.434929  [**] [1:128343214:1] Ping Detected from same SUBNET [**] [Priority: 0] {ICMP}
```

7. Wrote a rule to detect user browsing "http://info.cern.ch/"

```
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Commencing packet processing (pid=1684)
12/01-20:16:55.255346  [**] [1:228332:2] Connection to info cern detected [**] [Priority: 0] {TCP}
```

8. Detected SNMP Traffic

- 1) Wrote a script to run a TCP syn flood against your system (which has the IDS)
- 2) Created a rule to detect incoming syn attacks.
- 3) Detected when a TCP syn flood is occurring

```
securityunion@securityunion:~/Desktop$ sudo python syn.py :
```

[illegible]

References:

- <https://www.thepythoncode.com/article/syn-flooding-attack-using-scapy-in-python>
- <https://www.opensourceforu.com/2011/10/syn-flooding-using-scapy-and-prevention-using-iptables/>
- <http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node29.html>
- <https://stackoverflow.com/>
- https://paginas.fe.up.pt/~mgi98020/pgr/writing_snort_rules.htm
- <https://www.hackingarticles.in/detect-nmap-scan-using-snort/>

-X-