

TUGAS
KEAMANAN JARINGAN KOMPUTER
“SNORT”



Devi Purnama
09011281320016

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2017

Domain : telkom.com

IP Address : 176.74.176.187

Hasil scanning yang di lakukan dengan target telkom.com, dengan menggunakan tools Xprobe dan Nmap, dengan melakukan scanning lebih kurang 20 menit. Berikut adalah hasil dari scanning, dan snort dengan menggunakan wireshark. Snort merupakan software yang digunakan untuk mengamati aktivitas dalam sebuah jaringan komputer, snort dapat digunakan dalam suatu NIDS(Network Intrusion Detection System). Wireshark merupakan perangkat lunak yang spesifik untuk melakukan analisa paket data pada jaringan secara real time dan menampilkan hasil analisa paket data tersebut dalam format yang dipahami oleh pengguna. Wireshark dapat melakukan paket filtering, paket color coding, dan fitur-fitur lain yang dapat mengizinkan untuk melihat detail network traffic dan inspeksi paket data secara individu, Wireshark dapat menganalisis paket data secara real time. Artinya, aplikasi wireshark akan mengawasi semua paket data yang keluar masuk melalui antarmuka yang telah ditentukan dan selanjutnya akan menampilkan hasil paket datanya.

1. Lakukan Nmap pada telkom.com untuk mengetahui ip target.

```
devi@devi-Lenovo-Z40-75 ~ $ nmap -sV telkom.com
Starting Nmap 7.01 ( https://nmap.org ) at 2017-02-25 21:42 WIB
Stats: -6:-58:-56 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 85.43% done; ETC: 14:43 (0:00:11 remaining)
Nmap scan report for telkom.com (176.74.176.187)
Host is up (0.22s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    filtered  ssh
80/tcp    open      tcpwrapped
443/tcp   open      ssl/http    Apache httpd 2.2.22
3306/tcp  filtered  mysql
8031/tcp  filtered  unknown
8254/tcp  open      tcpwrapped
Service Info: Host: internettraffic.click

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in -25093.73 seconds
```

```

Terminal - root@devi-Lenovo-Z40-75 /home/devi
File Edit View Terminal Tabs Help
devi-Lenovo-Z40-75 devi # nmap telkom.com

Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-08 21:43 WIB
Nmap scan report for telkom.com (176.74.176.187)
Host is up (0.12s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 37.05 seconds
devi-Lenovo-Z40-75 devi # █

```

2. Lakukan Ping pada Ip Target

```

Terminal - root@devi-Lenovo-Z40-75 /home/devi
File Edit View Terminal Tabs Help
devi-Lenovo-Z40-75 devi # ping 176.74.176.187
PING 176.74.176.187 (176.74.176.187) 56(84) bytes of data:
64 bytes from 176.74.176.187: icmp_seq=1 ttl=49 time=222 ms
64 bytes from 176.74.176.187: icmp_seq=4 ttl=49 time=218 ms
64 bytes from 176.74.176.187: icmp_seq=7 ttl=49 time=225 ms
64 bytes from 176.74.176.187: icmp_seq=9 ttl=49 time=214 ms
64 bytes from 176.74.176.187: icmp_seq=11 ttl=49 time=229 ms
64 bytes from 176.74.176.187: icmp_seq=12 ttl=49 time=215 ms
64 bytes from 176.74.176.187: icmp_seq=13 ttl=49 time=213 ms
64 bytes from 176.74.176.187: icmp_seq=14 ttl=49 time=220 ms
64 bytes from 176.74.176.187: icmp_seq=15 ttl=49 time=236 ms
64 bytes from 176.74.176.187: icmp_seq=17 ttl=49 time=224 ms
64 bytes from 176.74.176.187: icmp_seq=18 ttl=49 time=263 ms
64 bytes from 176.74.176.187: icmp_seq=19 ttl=49 time=267 ms
64 bytes from 176.74.176.187: icmp_seq=20 ttl=49 time=227 ms
64 bytes from 176.74.176.187: icmp_seq=21 ttl=49 time=225 ms

```

3. Hasil dari Wereshark yang dikukan pada saat ping pada ip target, yang berfungsi untuk merekam aktivitas pertukaran data yang di lakukan.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|---------------|----------------|----------------|----------|--------|-------------------------|
| 8602 | 372.451617954 | 10.100.226.100 | 176.74.176.187 | ICMP | 98 | Echo (ping) request ... |
| 8609 | 372.688338115 | 176.74.176.187 | 10.100.226.100 | ICMP | 98 | Echo (ping) reply ... |
| 8625 | 373.193919222 | 10.100.224.1 | 10.100.225.80 | ICMP | 108 | destination unreacha... |
| 8637 | 373.452116875 | 10.100.226.100 | 176.74.176.187 | ICMP | 98 | Echo (ping) request ... |
| 8653 | 374.195938143 | 10.100.224.1 | 10.100.225.80 | ICMP | 98 | destination unreacha... |
| 8676 | 374.452109992 | 10.100.226.100 | 176.74.176.187 | ICMP | 98 | Echo (ping) request ... |
| 8684 | 374.676609602 | 176.74.176.187 | 10.100.226.100 | ICMP | 98 | Echo (ping) reply ... |
| 8704 | 375.194389516 | 10.100.224.1 | 10.100.225.80 | ICMP | 108 | destination unreacha... |
| 8712 | 375.452070443 | 10.100.226.100 | 176.74.176.187 | ICMP | 98 | Echo (ping) request ... |
| 8719 | 375.715856656 | 176.74.176.187 | 10.100.226.100 | ICMP | 98 | Echo (ping) reply ... |
| 8734 | 376.452946299 | 10.100.226.100 | 176.74.176.187 | ICMP | 98 | Echo (ping) request ... |
| 8738 | 376.729324892 | 176.74.176.187 | 10.100.226.100 | ICMP | 98 | Echo (ping) reply ... |
| 8751 | 377.453285841 | 10.100.226.100 | 176.74.176.187 | ICMP | 98 | Echo (ping) request ... |
| 8759 | 377.680385091 | 176.74.176.187 | 10.100.226.100 | ICMP | 98 | Echo (ping) reply ... |
| 8789 | 378.453510493 | 10.100.226.100 | 176.74.176.187 | ICMP | 98 | Echo (ping) request ... |
| 8798 | 378.679302445 | 176.74.176.187 | 10.100.226.100 | ICMP | 98 | Echo (ping) reply ... |

| | | | | | | |
|---|--|--|--|--|--|--|
| ▶ Frame 40792: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0 | | | | | | |
| ▶ Ethernet II, Src: CompexIn_22:cf:fa (00:80:48:22:cf:fa), Dst: AsustekC_cb:b8:62 (ac:9e:17:cb:b8:62) | | | | | | |
| ▶ Internet Protocol Version 4, Src: 10.100.224.1, Dst: 10.100.225.80 | | | | | | |
| ▶ Internet Control Message Protocol | | | | | | |

| | | | |
|------|-------------------------|-------------------------|-------------------|
| 0000 | ac 9e 17 cb b8 62 00 80 | 48 22 cf fa 08 00 45 c0 |b..H"....E. |
| 0010 | 00 68 aa 6c 00 00 40 01 | f9 4e 0a 64 e0 01 0a 64 | .h.l..@. .N.d...d |
| 0020 | e1 50 03 09 83 cc 00 00 | e0 00 45 00 00 4c 1a dc | .P.....E.L.. |
| 0030 | 40 00 3f 11 9a 39 0a 64 | e1 50 67 05 33 d2 bc 5f | @.?.9.d .Pg.3._ |
| 0040 | 00 7b 00 38 ba d4 1b 00 | 00 00 00 00 00 00 00 00 | ..{.8..... |
| 0050 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 0060 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 dc |j |

wireshark_pcapng_wl...170308214033_0LbB5K Packets: 880953 · Displayed: 277 (0.0%) Profile: Default

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|--------------|--------------|----------------|----------|--------|------------------------|
| 40792 | 18.575174507 | 10.100.224.1 | 10.100.225.80 | ICMP | 118 | Destination unreacha.. |
| 76732 | 38.577254866 | 10.100.224.1 | 10.100.225.80 | ICMP | 118 | Destination unreacha.. |
| 78059 | 39.747360774 | 10.100.224.1 | 10.100.225.80 | ICMP | 106 | Destination unreacha.. |
| 79418 | 40.783753186 | 10.100.224.1 | 10.100.225.80 | ICMP | 109 | Destination unreacha.. |
| 81034 | 41.806131502 | 10.100.224.1 | 10.100.225.80 | ICMP | 100 | Destination unreacha.. |
| 82521 | 42.825158461 | 10.100.224.1 | 10.100.225.80 | ICMP | 104 | Destination unreacha.. |
| 83767 | 43.841519979 | 10.100.224.1 | 10.100.225.80 | ICMP | 102 | Destination unreacha.. |
| 86070 | 45.790052349 | 10.100.224.1 | 10.100.225.80 | ICMP | 101 | Destination unreacha.. |
| 87251 | 46.850216657 | 10.100.224.1 | 10.100.225.80 | ICMP | 108 | Destination unreacha.. |
| 90461 | 50.842580376 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 90538 | 50.888062510 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 91583 | 50.726701477 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 92385 | 51.543382290 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 92703 | 51.864345430 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 94577 | 54.025322015 | 10.100.224.1 | 10.100.224.178 | ICMP | 138 | Destination unreacha.. |
| 94600 | 54.064207038 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 94613 | 54.089974104 | 10.100.224.1 | 10.100.224.178 | ICMP | 138 | Destination unreacha.. |

▶ Frame 40792: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
 ▶ Ethernet II, Src: CompexIn_22:cf:fa (00:80:48:22:cf:fa), Dst: AsustekC_cb:b8:62 (ac:9e:17:cb:b8:62)
 ▶ Internet Protocol Version 4, Src: 10.100.224.1, Dst: 10.100.225.80
 ▶ Internet Control Message Protocol

```

0000  ac 9e 17 cb b8 62 00 80 48 22 cf fa 08 00 45 c0  ....b..H"....E.
0010  00 68 aa 6c 00 00 40 01 f9 4e 0a 64 e0 01 0a 64  .h.l.().N.d...d
0020  e1 50 03 09 83 cc 00 00 00 00 45 00 00 4c 1a dc  .P.....E.L..
0030  40 00 3f 11 9a 39 0a 64 e1 50 67 05 33 d2 bc 5f  @.?.9.d.Pg.3...
0040  00 7b 00 38 ba d4 1b 00 00 00 00 00 00 00 00 00  .{.8.....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 dc 6a  .....]
  
```

4. Scanning target dengan menggunakan xprobe

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|---------------|----------------|----------------|----------|--------|------------------------|
| 6086 | 265.621678714 | 10.100.224.1 | 10.100.225.80 | ICMP | 106 | Destination unreacha.. |
| 6193 | 266.281404992 | 10.100.224.1 | 10.100.225.80 | ICMP | 100 | Destination unreacha.. |
| 6147 | 267.284328896 | 10.100.224.1 | 10.100.225.80 | ICMP | 98 | Destination unreacha.. |
| 6184 | 268.431094162 | 10.100.224.1 | 10.100.225.80 | ICMP | 98 | Destination unreacha.. |
| 6234 | 269.344913000 | 10.100.224.1 | 10.100.225.80 | ICMP | 106 | Destination unreacha.. |
| 6445 | 275.654197932 | 10.100.224.1 | 10.100.225.80 | ICMP | 103 | Destination unreacha.. |
| 6462 | 276.742338166 | 10.100.224.1 | 10.100.225.80 | ICMP | 100 | Destination unreacha.. |
| 6878 | 294.764915276 | 10.100.226.100 | 176.74.176.187 | ICMP | 98 | Echo (ping) request .. |
| 6887 | 294.999781556 | 176.74.176.187 | 10.100.226.100 | ICMP | 98 | Echo (ping) reply .. |
| 6901 | 295.316728624 | 10.100.226.100 | 176.74.176.187 | ICMP | 98 | Echo (ping) request .. |
| 6910 | 295.604051887 | 176.74.176.187 | 10.100.226.100 | ICMP | 98 | Echo (ping) reply .. |
| 6911 | 295.616879931 | 10.100.226.100 | 176.74.176.187 | ICMP | 54 | Timestamp request .. |
| 6916 | 295.993354829 | 176.74.176.187 | 10.100.226.100 | ICMP | 54 | Timestamp reply .. |
| 6920 | 296.156977776 | 10.100.226.100 | 176.74.176.187 | ICMP | 46 | Address mask request.. |
| 7216 | 306.484635867 | 10.100.226.100 | 40.118.106.130 | ICMP | 74 | Echo (ping) request .. |
| 7358 | 311.210467813 | 10.100.226.100 | 40.118.106.130 | ICMP | 74 | Echo (ping) request .. |

▶ Frame 40792: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
 ▶ Ethernet II, Src: CompexIn_22:cf:fa (00:80:48:22:cf:fa), Dst: AsustekC_cb:b8:62 (ac:9e:17:cb:b8:62)
 ▶ Internet Protocol Version 4, Src: 10.100.224.1, Dst: 10.100.225.80
 ▶ Internet Control Message Protocol

```

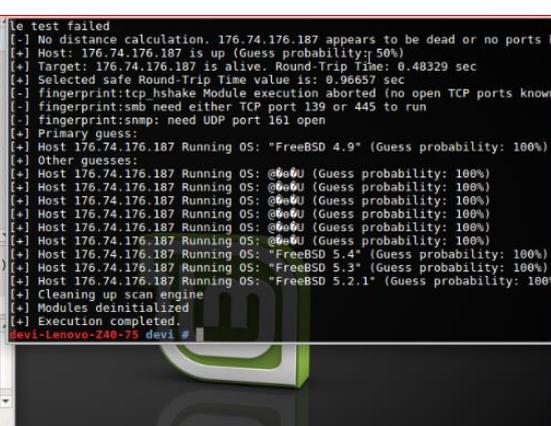
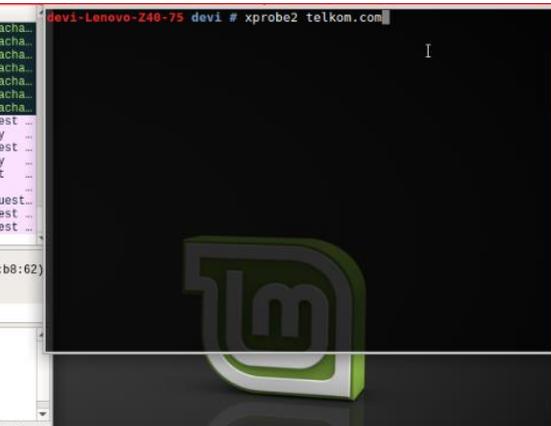
0000  ac 9e 17 cb b8 62 00 80 48 22 cf fa 08 00 45 c0  ....b..H"....E.
0010  00 68 aa 6c 00 00 40 01 f9 4e 0a 64 e0 01 0a 64  .h.l.().N.d...d
0020  e1 50 03 09 83 cc 00 00 00 00 45 00 00 4c 1a dc  .P.....E.L..
0030  40 00 3f 11 9a 39 0a 64 e1 50 67 05 33 d2 bc 5f  @.?.9.d.Pg.3...
0040  00 7b 00 38 ba d4 1b 00 00 00 00 00 00 00 00 00  .{.8.....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 dc 6a  .....]
  
```

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|--------------|--------------|----------------|----------|--------|------------------------|
| 40792 | 18.575174507 | 10.100.224.1 | 10.100.225.80 | ICMP | 118 | Destination unreacha.. |
| 76732 | 38.577254866 | 10.100.224.1 | 10.100.225.80 | ICMP | 118 | Destination unreacha.. |
| 78059 | 39.747360774 | 10.100.224.1 | 10.100.225.80 | ICMP | 106 | Destination unreacha.. |
| 79418 | 40.783753186 | 10.100.224.1 | 10.100.225.80 | ICMP | 109 | Destination unreacha.. |
| 81034 | 41.806131502 | 10.100.224.1 | 10.100.225.80 | ICMP | 100 | Destination unreacha.. |
| 82521 | 42.825158461 | 10.100.224.1 | 10.100.225.80 | ICMP | 104 | Destination unreacha.. |
| 83767 | 43.841519979 | 10.100.224.1 | 10.100.225.80 | ICMP | 102 | Destination unreacha.. |
| 86070 | 45.790052349 | 10.100.224.1 | 10.100.225.80 | ICMP | 101 | Destination unreacha.. |
| 87251 | 46.850216657 | 10.100.224.1 | 10.100.225.80 | ICMP | 108 | Destination unreacha.. |
| 90461 | 50.842580376 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 90538 | 50.888062510 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 91583 | 50.726701477 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 92385 | 51.543382290 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 92703 | 51.864345430 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 94577 | 54.025322015 | 10.100.224.1 | 10.100.224.178 | ICMP | 138 | Destination unreacha.. |
| 94600 | 54.064207038 | 10.100.224.1 | 10.100.224.178 | ICMP | 590 | Destination unreacha.. |
| 94613 | 54.089974104 | 10.100.224.1 | 10.100.224.178 | ICMP | 138 | Destination unreacha.. |

▶ Frame 40792: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
 ▶ Ethernet II, Src: CompexIn_22:cf:fa (00:80:48:22:cf:fa), Dst: AsustekC_cb:b8:62 (ac:9e:17:cb:b8:62)
 ▶ Internet Protocol Version 4, Src: 10.100.224.1, Dst: 10.100.225.80
 ▶ Internet Control Message Protocol

```

0000  ac 9e 17 cb b8 62 00 80 48 22 cf fa 08 00 45 c0  ....b..H"....E.
0010  00 68 aa 6c 00 00 40 01 f9 4e 0a 64 e0 01 0a 64  .h.l.().N.d...d
0020  e1 50 03 09 83 cc 00 00 00 00 45 00 00 4c 1a dc  .P.....E.L..
0030  40 00 3f 11 9a 39 0a 64 e1 50 67 05 33 d2 bc 5f  @.?.9.d.Pg.3...
0040  00 7b 00 38 ba d4 1b 00 00 00 00 00 00 00 00 00  .{.8.....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 dc 6a  .....]
  
```



5. Hasil snort

```
snort -A fast -c /etc/snort/snort.conf -r tugas_snort.pcap
```

```
Max concurrent sessions : 0
-----
dcerpc2 Preprocessor Statistics
  Total sessions: 3
  Total sessions aborted: 2

  Transports
    SMB
      Total sessions: 3
      Packet stats
        Packets: 32
        Ignored bytes: 730
        Maximum outstanding requests: 1
        SMB command requests/responses processed
          Transaction (0x25) : 2/0
          Tree Disconnect (0x71) : 1/1
          Negotiate (0x72) : 3/2
          Session Setup AndX (0x73) : 4/4
          Logoff AndX (0x74) : 1/1
          Tree Connect AndX (0x75) : 2/2
-----

SSL Preprocessor:
  SSL packets decoded: 24119
    Client Hello: 1100
    Server Hello: 619
    Certificate: 552
    Server Done: 1496
  Client Key Exchange: 458
  Server Key Exchange: 230
  Change Cipher: 1319
  Finished: 0
  Client Application: 2872
  Server Application: 468
  Alert: 402
  Unrecognized records: 11848
  Completed handshakes: 0
  Bad handshakes: 146
  Sessions ignored: 393
  Detection disabled: 6987
-----

SIP Preprocessor Statistics
  Total sessions: 0
-----

Snort exiting
devi-Lenovo-Z40-75 Documents #
```

6. Hasil Snort yang telah dilakukan pada target, maka kita dapat mengetahui daftar dari Alert yang telah di rekam pada wireshark.

```

1 03/08-21:40:38.590480 ** [1:1917:6] SCAN UPnP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] (UDP) 10.100.226.136:58
2 03/08-21:40:39.718508 ** [1:1917:6] SCAN UPnP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] (UDP) 10.100.226.136:58
3 03/08-21:40:41.591424 ** [1:1917:6] SCAN UPnP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] (UDP) 10.100.226.136:58
4 03/08-21:40:42.754232 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
5 03/08-21:40:43.781573 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
6 03/08-21:40:49.315350 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (ICMP) 0.0.0.0:68 -> 255.255.255.255:67
7 03/08-21:40:52.034095 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.225.80
8 03/08-21:40:54.329009 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
9 03/08-21:40:54.429177 ** [1:1917:6] SCAN UPnP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] (UDP) 10.100.226.0:6085
10 03/08-21:40:55.436183 ** [1:1917:6] SCAN UPnP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] (UDP) 10.100.226.0:6085
11 03/08-21:40:59.344155 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
12 03/08-21:41:00.602560 ** [1:2570:7] WEB-MISC Invalid HTTP Version String ** [Classification: Detection of a non-standard protocol or event] [Priority: 2] (TC
13 03/08-21:41:03.623814 ** [1:100000122:1] SCAN UPnP service discover attempt ** [Classification: Web Application Attack] [Priority: 1] (TCP) 10.100.224.231:60
14 03/08-21:41:05.701459 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
15 03/08-21:41:07.638339 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
16 03/08-21:41:11.094787 ** [1:2570:7] WEB-MISC Invalid HTTP Version String ** [Classification: Detection of a non-standard protocol or event] [Priority: 2] (TC
17 03/08-21:41:11.119166 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
18 03/08-21:41:12.032575 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.225.80
19 03/08-21:41:13.202681 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.225.80
20 03/08-21:41:14.239074 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.225.80
21 03/08-21:41:14.916366 ** [1:100000122:1] SCAN UPnP service discover attempt ** [Classification: Web Application Attack] [Priority: 1] (TCP) 10.100.224.231:45
22 03/08-21:41:15.261452 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.225.80
23 03/08-21:41:16.280479 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.225.80
24 03/08-21:41:17.296841 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.225.80
25 03/08-21:41:17.979913 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
26 03/08-21:41:19.245373 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.225.80
27 03/08-21:41:19.413631 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
28 03/08-21:41:19.618444 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
29 03/08-21:41:20.305537 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.225.80
30 03/08-21:41:20.766243 ** [1:1917:6] SCAN UPnP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] (UDP) 10.100.224.178:64
31 03/08-21:41:22.636685 ** [1:2570:7] WEB-MISC Invalid HTTP Version String ** [Classification: Detection of a non-standard protocol or event] [Priority: 2] (TC
32 03/08-21:41:23.497901 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.224.178
33 03/08-21:41:23.543383 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.224.178
34 03/08-21:41:23.808061 ** [1:1917:6] SCAN UPnP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] (UDP) 10.100.224.178:64
35 03/08-21:41:24.182022 ** [1:487:4] SCAN UPnP service discover attempt ** [Classification: Misc activity] [Priority: 3] (ICMP) 10.100.224.1 -> 10.100.224.178
36 03/08-21:41:24.229478 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
37 03/08-21:41:24.233185 ** [1:527:8] BAD-TRAFFIC same SRC/DST ** [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255.255.255.255:67

```

7. TABEL HASIL SNORT ALERT PADA WIRESHARK

| No | Alert | Jumlah |
|----|--|--------|
| 1 | BAD-TRAFFIC same SRC/DST | 199 |
| 2 | ICMP Destination Unreachable Communication with Destination Network is Administratively Prohibited | 147 |
| 3 | ICMP PING | 143 |
| 4 | ICMP PING *NIX | 73 |
| 5 | ICMP Echo Reply | 54 |
| 6 | SCAN UPnP service discover attempt | 51 |
| 7 | COMMUNITY WEB-MISC mod_jrun overflow attempt | 37 |
| 8 | WEB-MISC Invalid HTTP Version String | 22 |
| 9 | INFO web bug 0x0 gif attempt | 16 |
| 10 | Timestamp Request | 3 |
| 11 | SNMP AgentX/tcp request | 2 |
| 12 | Address Mask Request | 2 |

GRAFIK HASIL SNORT

