

BAB V

IMPLEMENTASI DAN PENGUJIAN

5.1 Instalasi IDS

5.1.1 Instalasi operasi sistem linux pada IDS

Proses awal dalam implementasi IDS adalah *Operating System* (OS), Instalasi OS dianggap proses yang sudah umum, untuk mempersingkat langkah ini, maka penulis menjabarkan proses instalasi pada lampiran 1 Proses install Ubuntu-server.

5.1.2 Instalasi Intrusion Detection System (IDS)

5.2 Pengujian

1. Skenario Pertama

Seorang attacker melakukan serangan kepada jaringan server yang menggunakan *tools* nmap yang bertujuan untuk menentukan *port* yang terbuka, *sistem operasi* yang digunakan dan mengetahui alamat *mac address* dari target. Dari sisi *attacker* melakukan *scanning port* menggunakan *tools* nmap dengan perintah berikut;

- # nmap -A 192.168.100.10
-A digunakan untuk mendeteksi keseluruhan mulai dari OS maupun versi *tools* yang berada pada target tujuan *scanning*.
- # nmap -sS -p- 192.168.100.10
-sS Merupakan Teknik *scanning* dengan *port* dengan cepat. Teknik ini dapat membedakan status *port* Open, closed dan filtered. Cara kerjanya adalah dengan mengirimkan sebuah paket SYN, kemudian menunggu jawaban dari sistem target. Bila kita mendapat jawaban paket SYN/ACK berarti *port* tersebut open, apabila kita mendapat paket RST berarti *port* closed.

1. Skenario Kedua

Seorang attacker melakukan serangan menggunakan *Disrtribute Of Services (DOS)* dengan menggunakan *tools hping3* yang bertujuan untuk menghabiskan sumber (resouces) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut dengan cara membanjiri lalu lintas jaringan dengan banyak data.

Attacker melakukan *DOS* yang bertujuan untuk membanjiri lalu lintas data sehingga layanan server tidak dapat berjalan, dengan menjalankan perintah berikut:

2. Skenario Ketiga

Seorang *attacker* melakukan serangan menggunakan *Brute Force* dengan menggunakan *tools hydra* yang bertujuan untuk mendapatkan sebuah username dan password yang dimiliki oleh komputer tersebut dengan memasukan username dan password yang berpotensi sering dipakai.

Dengan menjalankan perintah berikut:

5.1.1 Snort Attack

1. Nmap

- # Nmap -A 192.168.1.120

```
root@wicak-VirtualBox:/home/wicak# nmap -A 192.168.1.120
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-25 11:02 WIB
Nmap scan report for 192.168.1.120
Host is up (0.0033s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge[general purpose]
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
 1  0.20 ms  _gateway (10.0.2.2)
 2  0.25 ms  192.168.1.120

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.68 seconds
root@wicak-VirtualBox:/home/wicak#
```

Gambar 17 Nmap Attack Snort #Nmap -A 192.168.1.120

Dapat kita lihat dari hasil scanning bahwa komputer snort menggunakan Nmap yang terdeteksi yaitu komputer snort menggunakan OS ubuntu dan port yang terbuka adalah port 22 dengan membutuhkan waktu selama 23,68 detik scanning.

```
08/25-04:02:24.313309 ** [1:1421:11] SNMP AgentX/tcp request ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59430 -> 192.168.1.120:705
08/25-04:02:24.406304 ** [1:1421:11] SNMP AgentX/tcp request ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59473 -> 192.168.1.120:705
08/25-04:02:24.826513 ** [1:1421:11] SNMP AgentX/tcp request ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59430 -> 192.168.1.120:705
08/25-04:02:24.926506 ** [1:1421:11] SNMP AgentX/tcp request ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59473 -> 192.168.1.120:705
08/25-04:02:24.990327 ** [1:1418:11] SNMP request tcp ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:60109 -> 192.168.1.120:161
08/25-04:02:25.102766 ** [1:1418:11] SNMP request tcp ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:60156 -> 192.168.1.120:161
08/25-04:02:25.332026 ** [1:1421:11] SNMP AgentX/tcp request ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59430 -> 192.168.1.120:705
08/25-04:02:25.422112 ** [1:1421:11] SNMP AgentX/tcp request ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59473 -> 192.168.1.120:705
08/25-04:02:25.495380 ** [1:1418:11] SNMP request tcp ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:60109 -> 192.168.1.120:161
08/25-04:02:25.662590 ** [1:1418:11] SNMP request tcp ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:60156 -> 192.168.1.120:161
08/25-04:02:25.834334 ** [1:1421:11] SNMP AgentX/tcp request ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59430 -> 192.168.1.120:705
08/25-04:02:25.935599 ** [1:1421:11] SNMP AgentX/tcp request ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59473 -> 192.168.1.120:705
08/25-04:02:25.999397 ** [1:1418:11] SNMP request tcp ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:60109 -> 192.168.1.120:161
08/25-04:02:26.167714 ** [1:1418:11] SNMP request tcp ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:60156 -> 192.168.1.120:161
08/25-04:02:26.506225 ** [1:1418:11] SNMP request tcp ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:60109 -> 192.168.1.120:161
08/25-04:02:26.696734 ** [1:1418:11] SNMP request tcp ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:60156 -> 192.168.1.120:161
08/25-04:02:27.018603 ** [1:1418:11] SNMP request tcp ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:60109 -> 192.168.1.120:161
08/25-04:02:27.201538 ** [1:1418:11] SNMP request tcp ** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:60156 -> 192.168.1.120:161
08/25-04:02:27.781217 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.111 -> 192.168.1.120
08/25-04:02:27.781290 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:27.819960 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.111 -> 192.168.1.120
08/25-04:02:27.820001 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:27.856702 ** [1:402:7] ICMP Destination Unreachable Port Unreachable ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:28.121816 ** [1:402:7] ICMP Destination Unreachable Port Unreachable ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:28.330513 ** [1:402:7] ICMP Destination Unreachable Port Unreachable ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:28.536099 ** [1:402:7] ICMP Destination Unreachable Port Unreachable ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:28.572786 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.111 -> 192.168.1.120
08/25-04:02:30.572779 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:30.608926 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.111 -> 192.168.1.120
08/25-04:02:30.608990 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:30.649982 ** [1:402:7] ICMP Destination Unreachable Port Unreachable ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:30.752730 ** [1:402:7] ICMP Destination Unreachable Port Unreachable ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:30.853823 ** [1:402:7] ICMP Destination Unreachable Port Unreachable ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-04:02:30.954830 ** [1:402:7] ICMP Destination Unreachable Port Unreachable ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.120 -> 192.168.1.111
```

Gambar 18 Alert Snort Nmap #Nmap -A 192.168.1.120

Berikut merupakan alert dari snort ketika ada attacker yang melakukan Scanning kedalam jaringan snort.

- Nmap -sS -p- 192.168.1.120

Berikut merupakan port-port yang berhasil discanning oleh Nmap.

```
root@wicak-VirtualBox:/home/wicak# nmap -sS -p- 192.168.1.120
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-25 14:16 WIB
Nmap scan report for 192.168.1.120
Host is up (0.011s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 127.64 seconds
```

Gambar 19 Alert Snort Nmap #Nmap -sS -p- 192.168.1.120

Berdasarkan hasil scanning #nmap -sS -p- 192.168.1.120 terdapat 65.534 port yang filtered terdapat 65.534 ports dan port yang terbuka hanya port 22 dengan membutuhkan waktu 127,64 detik untuk melakukan scanning.

```
08/25-07:16:01.126774 *** [1527:0] BAD-TRAFFIC same SRC/DST *** [Classification: Potentially Bad Traffic] [Priority: 2] [IPv6-ICMP] !! -> ff02::16
08/25-07:16:02.088281 *** [1527:0] BAD-TRAFFIC same SRC/DST *** [Classification: Potentially Bad Traffic] [Priority: 2] [IPv6-ICMP] !! -> ff02::16
08/25-07:16:27.079417 *** [1469:3] ICMP PING NMAP *** [Classification: Attempted Information Leak] [Priority: 2] [ICMP] 192.168.1.111 -> 192.168.1.120
08/25-07:16:27.079417 *** [1384:5] ICMP PING *** [Classification: Misc activity] [Priority: 2] [ICMP] 192.168.1.111 -> 192.168.1.120
08/25-07:16:27.079537 *** [1400:5] ICMP Echo Reply *** [Classification: Misc activity] [Priority: 2] [ICMP] 192.168.1.120 -> 192.168.1.111
08/25-07:16:30.216213 *** [1527:0] BAD-TRAFFIC same SRC/DST *** [Classification: Potentially Bad Traffic] [Priority: 2] [IPv6-ICMP] !! -> ff02::16
08/25-07:17:23.776074 *** [1418:1] SNMP request tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:50192 -> 192.168.1.120:161
08/25-07:17:23.782498 *** [1418:1] SNMP request tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:50192 -> 192.168.1.120:161
08/25-07:17:23.507071 *** [1418:1] SNMP request tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:50198 -> 192.168.1.120:161
08/25-07:17:23.782498 *** [1418:1] SNMP request tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:50192 -> 192.168.1.120:161
08/25-07:17:24.089188 *** [1418:1] SNMP request tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:50198 -> 192.168.1.120:161
08/25-07:17:24.510874 *** [1418:1] SNMP request tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:50198 -> 192.168.1.120:161
08/25-07:17:24.788053 *** [1418:1] SNMP request tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:50192 -> 192.168.1.120:161
08/25-07:17:25.011085 *** [1418:1] SNMP request tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:50198 -> 192.168.1.120:161
08/25-07:17:44.660943 *** [1421:1] SNMP AgentX/tcp request *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:57775 -> 192.168.1.120:765
08/25-07:17:44.622402 *** [1421:1] SNMP AgentX/tcp request *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:57775 -> 192.168.1.120:765
08/25-07:17:45.125495 *** [1421:1] SNMP AgentX/tcp request *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:57775 -> 192.168.1.120:765
08/25-07:17:45.474671 *** [1421:1] SNMP AgentX/tcp request *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:57775 -> 192.168.1.120:765
08/25-07:17:45.626885 *** [1421:1] SNMP AgentX/tcp request *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:57775 -> 192.168.1.120:765
08/25-07:17:45.996466 *** [1421:1] SNMP AgentX/tcp request *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:57775 -> 192.168.1.120:765
08/25-07:17:46.134447 *** [1421:1] SNMP AgentX/tcp request *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:57775 -> 192.168.1.120:765
08/25-07:17:46.602783 *** [1421:1] SNMP AgentX/tcp request *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:57775 -> 192.168.1.120:765
08/25-07:17:46.602364 *** [1421:1] SNMP AgentX/tcp request *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:57775 -> 192.168.1.120:765
08/25-07:18:01.116431 *** [1249:0] DDoS nstream client to handler *** [Classification: Attempted Denial of Service] [Priority: 2] [TCP] 192.168.1.111:83976 -> 192.168.1.120:15104
08/25-07:18:01.059508 *** [1249:0] DDoS nstream client to handler *** [Classification: Attempted Denial of Service] [Priority: 2] [TCP] 192.168.1.111:84063 -> 192.168.1.120:15104
08/25-07:18:02.021642 *** [1249:0] DDoS nstream client to handler *** [Classification: Attempted Denial of Service] [Priority: 2] [TCP] 192.168.1.111:83976 -> 192.168.1.120:15104
08/25-07:18:02.162460 *** [1249:0] DDoS nstream client to handler *** [Classification: Attempted Denial of Service] [Priority: 2] [TCP] 192.168.1.111:84063 -> 192.168.1.120:15104
08/25-07:18:02.065117 *** [1249:0] DDoS nstream client to handler *** [Classification: Attempted Denial of Service] [Priority: 2] [TCP] 192.168.1.111:83976 -> 192.168.1.120:15104
08/25-07:18:03.032555 *** [1249:0] DDoS nstream client to handler *** [Classification: Attempted Denial of Service] [Priority: 2] [TCP] 192.168.1.111:83976 -> 192.168.1.120:15104
08/25-07:18:03.113834 *** [1249:0] DDoS nstream client to handler *** [Classification: Attempted Denial of Service] [Priority: 2] [TCP] 192.168.1.111:84063 -> 192.168.1.120:15104
08/25-07:18:03.138810 *** [1249:0] DDoS nstream client to handler *** [Classification: Attempted Denial of Service] [Priority: 2] [TCP] 192.168.1.111:83976 -> 192.168.1.120:15104
08/25-07:18:03.017981 *** [1249:0] DDoS nstream client to handler *** [Classification: Attempted Denial of Service] [Priority: 2] [TCP] 192.168.1.111:84063 -> 192.168.1.120:15104
08/25-07:18:21.666551 *** [1420:1] SNMP trap tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59761 -> 192.168.1.120:162
08/25-07:18:21.857375 *** [1420:1] SNMP trap tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59562 -> 192.168.1.120:162
08/25-07:18:22.869041 *** [1420:1] SNMP trap tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59761 -> 192.168.1.120:162
08/25-07:18:22.869041 *** [1420:1] SNMP trap tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59761 -> 192.168.1.120:162
08/25-07:18:22.672597 *** [1420:1] SNMP trap tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59761 -> 192.168.1.120:162
08/25-07:18:23.032555 *** [1420:1] SNMP trap tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59562 -> 192.168.1.120:162
08/25-07:18:23.074990 *** [1420:1] SNMP trap tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59761 -> 192.168.1.120:162
08/25-07:18:23.065896 *** [1420:1] SNMP trap tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59562 -> 192.168.1.120:162
08/25-07:18:23.579207 *** [1420:1] SNMP trap tcp *** [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.111:59761 -> 192.168.1.120:162
08/25-07:19:17.759636 *** [1527:0] BAD-TRAFFIC same SRC/DST *** [Classification: Potentially Bad Traffic] [Priority: 2] [IPv6-ICMP] !! -> ff02::16
08/25-07:19:17.769887 *** [1527:0] BAD-TRAFFIC same SRC/DST *** [Classification: Potentially Bad Traffic] [Priority: 2] [IPv6-ICMP] !! -> ff02::16
08/25-07:19:18.442020 *** [1527:0] BAD-TRAFFIC same SRC/DST *** [Classification: Potentially Bad Traffic] [Priority: 2] [IPv6-ICMP] !! -> ff02::16
```

Gambar 20 Nmap Attack Snort #Nmap -sS -p- 192.168.1.120

2. DOS

- Hping3 -S -p 22 --flood --rand-source 192.168.1.120

```
root@wicak-VirtualBox:/home/wicak# hping3 -S -p 22 --flood --rand-source 192.168.1.120
HPING 192.168.1.120 (enp0s3 192.168.1.120): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.120 hping statistic ---
808851 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Gambar 21 DDoS Attack Snort 1

Disini attacker mencoba menyerang dengan mengirimkan paket SYN ke port 22 dengan bertujuan mengacaukan lalu lintas jaringan terhadap defender dan berhasil membuat lalu lintas jaringan defender kacau hingga terjadinya hang terhadap pc defender.

- Hping -1 -c 99 192.168.1.120

```

root@wicak-VirtualBox:/home/wicak# hping3 -1 -c 99 192.168.1.120
HPING 192.168.1.120 (enp0s3 192.168.1.120): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.120 ttl=63 id=4707 icmp_seq=0 rtt=80.5 ms
len=46 ip=192.168.1.120 ttl=63 id=5686 icmp_seq=1 rtt=3288.4 ms
len=46 ip=192.168.1.120 ttl=63 id=5687 icmp_seq=2 rtt=2288.4 ms
len=46 ip=192.168.1.120 ttl=63 id=5688 icmp_seq=3 rtt=1288.3 ms
len=46 ip=192.168.1.120 ttl=63 id=5689 icmp_seq=4 rtt=287.8 ms
len=46 ip=192.168.1.120 ttl=63 id=5696 icmp_seq=5 rtt=78.4 ms
len=46 ip=192.168.1.120 ttl=63 id=5700 icmp_seq=6 rtt=78.2 ms
len=46 ip=192.168.1.120 ttl=63 id=5702 icmp_seq=7 rtt=77.1 ms
len=46 ip=192.168.1.120 ttl=63 id=5704 icmp_seq=8 rtt=76.5 ms
len=46 ip=192.168.1.120 ttl=63 id=5706 icmp_seq=9 rtt=76.1 ms
len=46 ip=192.168.1.120 ttl=63 id=5710 icmp_seq=10 rtt=76.2 ms
len=46 ip=192.168.1.120 ttl=63 id=5712 icmp_seq=11 rtt=86.9 ms
len=46 ip=192.168.1.120 ttl=63 id=5714 icmp_seq=12 rtt=83.4 ms
len=46 ip=192.168.1.120 ttl=63 id=5716 icmp_seq=13 rtt=74.7 ms
len=46 ip=192.168.1.120 ttl=63 id=5720 icmp_seq=14 rtt=90.2 ms
len=46 ip=192.168.1.120 ttl=63 id=5722 icmp_seq=15 rtt=81.6 ms
len=46 ip=192.168.1.120 ttl=63 id=5724 icmp_seq=16 rtt=81.6 ms
len=46 ip=192.168.1.120 ttl=63 id=5726 icmp_seq=17 rtt=73.1 ms
len=46 ip=192.168.1.120 ttl=63 id=5728 icmp_seq=18 rtt=80.5 ms
len=46 ip=192.168.1.120 ttl=63 id=5730 icmp_seq=19 rtt=88.3 ms
len=46 ip=192.168.1.120 ttl=63 id=5732 icmp_seq=20 rtt=79.5 ms
len=46 ip=192.168.1.120 ttl=63 id=5736 icmp_seq=21 rtt=87.7 ms
len=46 ip=192.168.1.120 ttl=63 id=5738 icmp_seq=22 rtt=86.9 ms
len=46 ip=192.168.1.120 ttl=63 id=5740 icmp_seq=23 rtt=87.0 ms
^C
--- 192.168.1.120 hping statistic ---
24 packets transmitted, 24 packets received, 0% packet loss

```

Gambar 22 DDoS Attack Snort 2

Berikut percobaan kedua attacker dengan mengirimkan paket sebanyak 99 percobaan.

- Allert dari Snort

```

08/26-01:35:38.083164  [**] [1:469:3] ICMP PING NMAP [**] [classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.111 -> 192.168.1.120
08/26-01:35:38.083164  [**] [1:384:5] ICMP PING [**] [classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.111 -> 192.168.1.120
08/26-01:35:38.083209  [**] [1:408:5] ICMP Echo Reply [**] [classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.120 -> 192.168.1.111
08/26-01:35:42.286853  [**] [1:469:3] ICMP PING NMAP [**] [classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.111 -> 192.168.1.120
08/26-01:35:42.286853  [**] [1:384:5] ICMP PING [**] [classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.111 -> 192.168.1.120

```

Gambar 23 Alert Snort DDoS Attack

STT NF

3. Brute Force

- Hydra -l username.txt -p password.txt -t 4 ssh://192.168.1.120

```

wicak@wicak-VirtualBox:~/brute-force$ hydra -l usernames.txt -P 2151220-passwords.txt -t 4 ssh://192.168.1.120
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-20 09:16:40
[WARNING] Restorefile (you have 58 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2151220 login tries (l1/p:2151220), -537805 tries per task
[DATA] attacking ssh://192.168.1.120:22/
[STATUS] 31.00 tries/min, 31 tries in 00:01h, 2151189 to do in 1156:34h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 2151134 to do in 1200:27h, 4 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

```

Gambar 24 Brute Force Attack Snort

5.1.2 Suricata Attack

1. Nmap

- # Nmap -A 192.168.1.120

```
[sudo] password for wicak:
root@wicak-VirtualBox:/home/wicak# nmap -A 192.168.1.120
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-26 12:49 WIB
Nmap scan report for 192.168.1.120
Host is up (0.0012s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.10 ms  _gateway (10.0.2.2)
2   0.19 ms  192.168.1.120

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.05 seconds
root@wicak-VirtualBox:/home/wicak#
```

Gambar 25 Nmap attack Suricata #Nmap -A 192.168.1.120

Attacker melakukan percobaan Nmap terhadap suricata dengan melakukan nmap kepada defender, disini terlihat bahwa nmap sukses melancarkan serangannya namun suricata tidak dapat mendeteksi serangan tersebut.

- # nmap -sS -p- 192.168.100.10

```
root@wicak-VirtualBox:/home/wicak# nmap -sS -p- 192.168.100.10
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-14 16:38 WIB
Nmap scan report for 192.168.100.10
Host is up (0.023s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: B8:27:EB:E5:67:5D (Raspberry Pi Foundation)

Nmap done: 1 IP address (1 host up) scanned in 26.26 seconds
root@wicak-VirtualBox:/home/wicak#
```

Gambar 26 nmap -sS -p- 192.168.100.10

Attacker melakukan percobaan ke dua dengan melakukan scanning port kepada defender dengan waktu 26,26 detik. Dan pada percobaan ke dua ini Suricata belum berhasil mendeteksi adanya serangan.

2. DOS

- # hping3 -l -c 5 192.168.1.120

```
root@wicak-VirtualBox:/home/wicak# hping3 -l -c 5 192.168.1.120
HPING 192.168.1.120 (enp0s3 192.168.1.120): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.120 ttl=63 id=22319 icmp_seq=0 rtt=83.4 ms
len=46 ip=192.168.1.120 ttl=63 id=22320 icmp_seq=1 rtt=87.0 ms
len=46 ip=192.168.1.120 ttl=63 id=22321 icmp_seq=2 rtt=77.2 ms
len=46 ip=192.168.1.120 ttl=63 id=22322 icmp_seq=3 rtt=84.0 ms
len=46 ip=192.168.1.120 ttl=63 id=22382 icmp_seq=4 rtt=79.2 ms

--- 192.168.1.120 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 77.2/82.1/87.0 ms
```

Gambar 27 DDoS Attack Suricata

Attacker mencoba melakukan serangan berikutnya yaitu DDoS yaitu dengan mengirimkan 5 paket, dengan percobaan DDoS suricata belum berhasil untuk mendeteksi serangan tersebut.

3. Brute Force

- # hydra -L user.txt -P password.txt 192.168.1.120 -t 4 ssh -V

```
root@wicak-VirtualBox:/home/wicak# hydra -L user.txt -P password.txt 192.168.1.120 -t 4 ssh -V
Hydra v0.2 (c) 2001 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-26 11:16:06
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 867785343100 login tries (1:463355/p;2151220), ~216926335775 tries per task
[DATA] attacking ssh://192.168.1.120:22/
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!" - 1 of 867785343100 [child 0] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "I love you" - 2 of 867785343100 [child 1] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!" - 3 of 867785343100 [child 2] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!" - 4 of 867785343100 [child 3] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!!" - 5 of 867785343100 [child 0] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!!" - 6 of 867785343100 [child 1] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!!" - 7 of 867785343100 [child 2] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!!" - 8 of 867785343100 [child 3] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!!" - 9 of 867785343100 [child 0] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!!" - 10 of 867785343100 [child 1] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!1888888" - 11 of 867785343100 [child 2] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!112" - 12 of 867785343100 [child 3] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!11111" - 13 of 867785343100 [child 0] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!1123" - 14 of 867785343100 [child 1] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!123ps" - 15 of 867785343100 [child 2] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!145ylltlanxlan" - 16 of 867785343100 [child 3] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!521268" - 17 of 867785343100 [child 0] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!5205420" - 18 of 867785343100 [child 1] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!6666661!" - 19 of 867785343100 [child 2] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!5LMD0D4T6" - 20 of 867785343100 [child 3] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!778322" - 21 of 867785343100 [child 0] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!7891!" - 22 of 867785343100 [child 1] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!789456123111" - 23 of 867785343100 [child 2] (0/0)
[ATTENPT] target 192.168.1.120 login "Aaren" - pass "!!!!890" - 24 of 867785343100 [child 3] (0/0)
<The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Gambar 28 Brute Force Attack Suricata

Attacker melakukan percobaan ke tiga dengan melakukan penyerangan dengan menggunakan BruteForce, tapi suricata tidak dapat mendeteksi serangan tersebut.

5.1.3 FAIL2BAN ATTACK

1. Nmap

- # Nmap -A 192.168.1.120

```
wicak@wicak-VirtualBox:~$ nmap -A 192.168.100.10
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-14 14:39 WIB
Nmap scan report for 192.168.100.10
Host is up (0.012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.99 seconds
```

Gambar 29 Nmap Attack F2ban

Attacker melakukan percobaan penyerangan pertama ke fail2ban dengan menggunakan nmap dan hasilnya fail2ban dapat mendeteksi adanya percobaan attack nmap.

```
2022-09-14 07:34:45,045 fail2ban.filter [702]: INFO [sshd] Found 192.168.100.21 - 2022-09-14 07:34:44
```

Gambar 30 Alert Nmap F2ban

- # Nmap -sS -p- 192.168.100.10

```
root@wicak-VirtualBox:/home/wicak# nmap -sS -p- 192.168.100.10
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-14 14:46 WIB
Nmap scan report for 192.168.100.10
Host is up (0.024s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: B8:27:EB:E5:67:5D (Raspberry Pi Foundation)

Nmap done: 1 IP address (1 host up) scanned in 34.16 seconds
```

Gambar 31 Nmap Attack f2ban 2

Attacker melakukan percobaan ke dua dengan melakukan scanning port terhadap Fail2ban dengan membutuhkan waktu selama 34,16 detik. Dan dengan percobaan ke dua ini fail2ban belum dapat mendeteksi serangan tersebut.

2. DDos Attack

- # hping3 -I -c 99 192.168.1.120

```
root@wicak-VirtualBox:/home/wicak# hping3 -I -c 99 192.168.100.10
HPING 192.168.100.10 (enp0s3 192.168.100.10): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.100.10 ttl=64 id=405 icmp_seq=0 rtt=8.8 ms
len=46 ip=192.168.100.10 ttl=64 id=449 icmp_seq=1 rtt=50.1 ms
len=46 ip=192.168.100.10 ttl=64 id=459 icmp_seq=2 rtt=6.7 ms
len=46 ip=192.168.100.10 ttl=64 id=545 icmp_seq=3 rtt=8.6 ms
len=46 ip=192.168.100.10 ttl=64 id=583 icmp_seq=4 rtt=7.4 ms
len=46 ip=192.168.100.10 ttl=64 id=698 icmp_seq=5 rtt=6.0 ms
len=46 ip=192.168.100.10 ttl=64 id=702 icmp_seq=6 rtt=7.7 ms
len=46 ip=192.168.100.10 ttl=64 id=871 icmp_seq=7 rtt=8.4 ms
len=46 ip=192.168.100.10 ttl=64 id=1020 icmp_seq=8 rtt=7.1 ms
```

Gambar 32 DDos Attack Fail2ban

Attacker melakukan percobaan penyerangan ke tiga dengan menyerang menggunakan DDos yang bertujuan menyibukkan lalulintas jaringan defender. Dalam percobaan ke tiga ini Fail2ban belum dapat mendeteksi serangan DDos.

3. Brute Force

- # hydra -L user.txt -P password.txt 192.168.1.120 -t 4 ssh -V

```
wicak@wicak-VirtualBox:~/bruteforce-database$ hydra -l usernames.txt -P 2151220-
passwords.txt -t 4 ssh://192.168.1.120
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-14 14:18:
06
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa
iting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2151220 login tries (l:1/p:215
1220), ~537805 tries per task
[DATA] attacking ssh://192.168.1.120:22/
```

Gambar 33 Brute Force Attack F2ban

Attacker melakukan percobaan ke empat dengan melakukan serangan BruteForce yaitu mencoba berbagai kemungkinan untuk mendapatkan sebuah username dan sandi defender. Dan pada percobaan keempat ini Fail2ban berhasil mendeteksi adanya sebuah serangan.

```

2022-09-14 07:18:38,629 fail2ban.filter [702]: INFO [sshd] Found 192.168.100.21 - 2022-09-14 07:18:38
2022-09-14 07:18:38,979 fail2ban.filter [702]: INFO [sshd] Found 192.168.100.21 - 2022-09-14 07:18:38
2022-09-14 07:18:38,986 fail2ban.filter [702]: INFO [sshd] Found 192.168.100.21 - 2022-09-14 07:18:38
2022-09-14 07:18:38,993 fail2ban.filter [702]: INFO [sshd] Found 192.168.100.21 - 2022-09-14 07:18:38
2022-09-14 07:18:38,998 fail2ban.filter [702]: INFO [sshd] Found 192.168.100.21 - 2022-09-14 07:18:38
2022-09-14 07:18:39,702 fail2ban.actions [702]: NOTICE [sshd] Ban 192.168.100.21
2022-09-14 07:18:41,045 fail2ban.filter [702]: INFO [sshd] Found 192.168.100.21 - 2022-09-14 07:18:41
2022-09-14 07:18:41,048 fail2ban.filter [702]: INFO [sshd] Found 192.168.100.21 - 2022-09-14 07:18:41
2022-09-14 07:18:41,050 fail2ban.filter [702]: INFO [sshd] Found 192.168.100.21 - 2022-09-14 07:18:41
2022-09-14 07:18:41,055 fail2ban.filter [702]: INFO [sshd] Found 192.168.100.21 - 2022-09-14 07:18:41
2022-09-14 07:28:38,857 fail2ban.actions [702]: NOTICE [sshd] Unban 192.168.100.21

```

Gambar 34 Log Attack Fail2ban

5.2 Hasil

Dari hasil pengujian yang dilakukan terhadap IDS dibagi menjadi 3 skenario pengujian, sebagai berikut;

Table 2 Hasil Pengujian

No	Jenis IDS	Script Attack	Percobaan Attack										Keterangan	
			1	2	3	4	5	6	7	8	9	10		
1	Snort	# nmap -A 192.168.1.120	√	×	×	×	×	×	×	×	×	×	×	Dari 9 Percobaan ScanningPort - ASnort hanya mendeteksi 1
		# nmap -sS -p- 192.168.1.120	√	×	×	×	×	×	×	×	×	×	×	Dari 9 Percobaan Scanning Port -sS -p- 22 Snort hanya mendeteksi 1
		# hping3 -1 -c 1000 192.168.1.120	√	×	×	×	×	×	×	×	×	×	×	Dari 9 Percobaan Snort hanya mendeteksi 1
		Hydra -L user.txt -p	√	×	×	×	×	×	×	×	×	×	×	Dari 9 Percobaan

		password.txt 192.168.1.120 -t 4 ssh -V																		Snort hanya mendeteksi 1
2	Suricata	# nmap -A 192.168.1.120	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	Suricata berhasil mendeteksi seluruh percobaan scanning port parameter -A
		# nmap -sS 192.168.1.120	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	Suricata gagal mendeteksi percobaan Scanning Port -sS -p- 22
		# hping3 -1 -c 1000 192.168.1.120	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	Suricata gagal mendeteksi percobaan serangan DDoS
		Hydra -L user.txt -p password.txt 192.168.1.120 -t 4 ssh -V	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	Suricata gagal mendeteksi percobaan serangan BruteForce
3	Fail2ban	# nmap -A 192.168.1.120	√	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	Dari 10 percobaan Scanning port parameter -A Fail2ban

																	berhasil mendeteksi 1 buah serangan
		# nmap -sS 192.168.1.120	×	×	×	×	×	×	×	×	×	×	×	×	×	×	Fail2ban gagal mendeteksi percobaan Scanning Port parameter -sS -p- 22
		# hping3 -1 -c 1000 192.168.1.120	×	×	×	×	×	×	×	×	×	×	×	×	×	×	Fail2ban gagal mendeteksi percobaan DDoS
		Hydra -L user.txt -p password.txt 192.168.1.120 -t 4 ssh -V	√	√	√	√	√	√	√	√	√	√	√	√	√	√	Fail2ban berhasil mendeteksi seluruh percobaan BruteForce

Catatan : √ merupakan arti dari terdeteksi, dan × merupakan arti dari tidak terdeteksi.

Berdasarkan pengujian serangan pertama Snort berhasil mendeteksi seluruh serangan, tetapi ketika uji coba tersebut diulang Snort gagal mendeteksi serangan-serangan tersebut. Suricata berhasil mendeteksi seluruh percobaan Scanning Port menggunakan parameter -A, tetapi gagal dalam mendeteksi serangan-serangan yang lain. Fail2ban berhasil mendeteksi percobaan Scanning Port parameter -A, tetapi setelah fail2ban membolkir IP penyerang dan dalam waktu 10 menit membuka

kembali IP penyerang tersebut Fail2ban gagal dalam mendeteksi percobaan berikutnya, kecuali percobaan penyerangan BruteForce, Fail2ban berhasil mendeteksi seluruh percobaan penyerangan Fail2ban.



STT - NF