BAB V
IMPLEMENTASI DAN PENGUJIAN

5.1 Instalasi IDS

5.1.1 Instalasi operasi sistem linux pada IDS

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

5.1.2 Instalasi Intrussion 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 tersenit 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

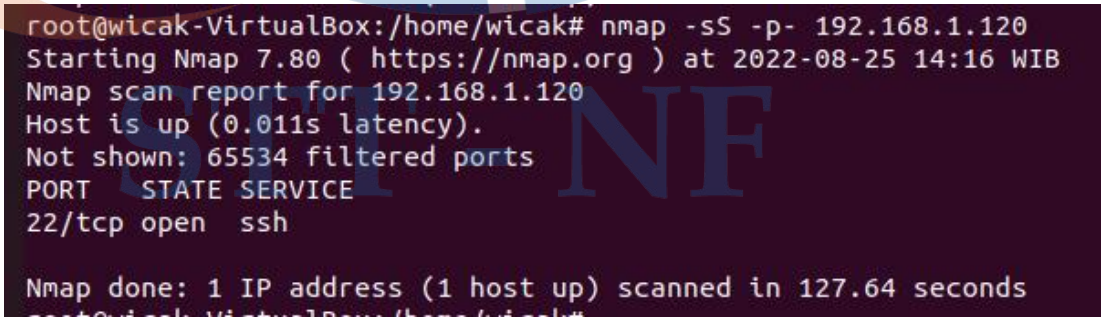
Dapat kita lihat dari hasil scanning bahwa komputer snort menggunakan Nmap yang terdeteksi yaitu komputer snort menggunakan OS ubuntu dan port yang terbuka adalah port 22 dengan membutuhkan waktu selama 23,68 detik scanning.

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.



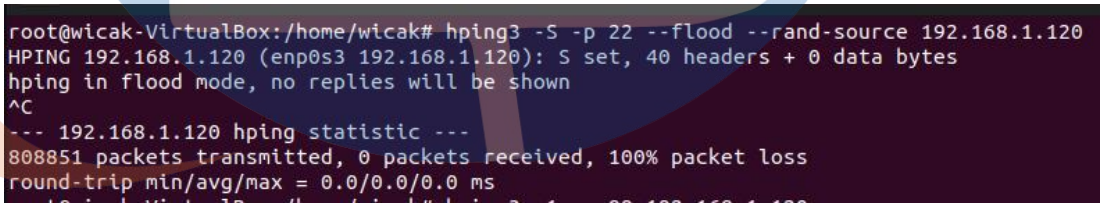
Gambar 19 Alert Snort Nmap #Nmap -sS -p- 192.168.1.120

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.

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

2. DOS

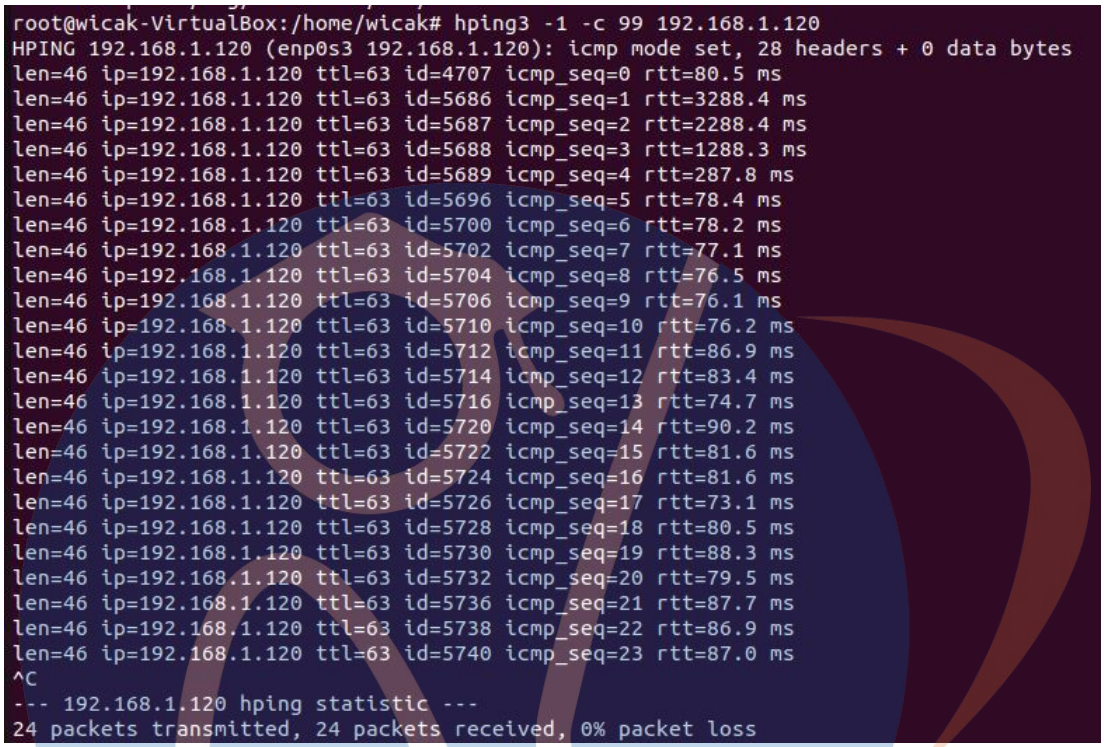
- Hping3 -S -p 22 --flood –rand-source 192.168.1.120



Gambar 21 DDoS Attack Snort 1

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

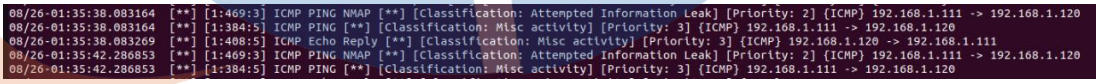
- Hping -1 -c 99 192.168.1.120



Gambar 22 DDoS Attack Snort 2

Berikut percobaan kedua attacker dengan mengirimkan paket sebanyak 99 percobaan.

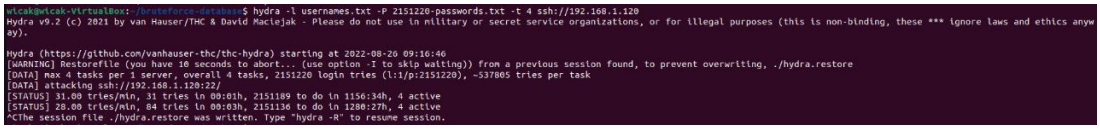
- Allert dari Snort



Gambar 23 Alert Snort DDoS Attack

3. Brute Force

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

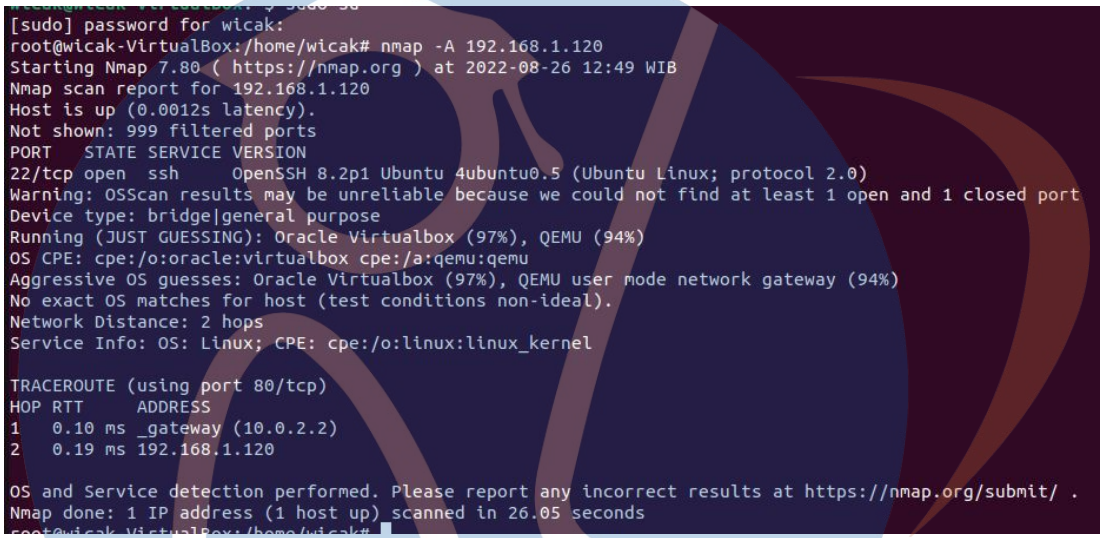


Gambar 24 Brute Force Attack Snort

5.1.2 Suricata Attack

1. Nmap

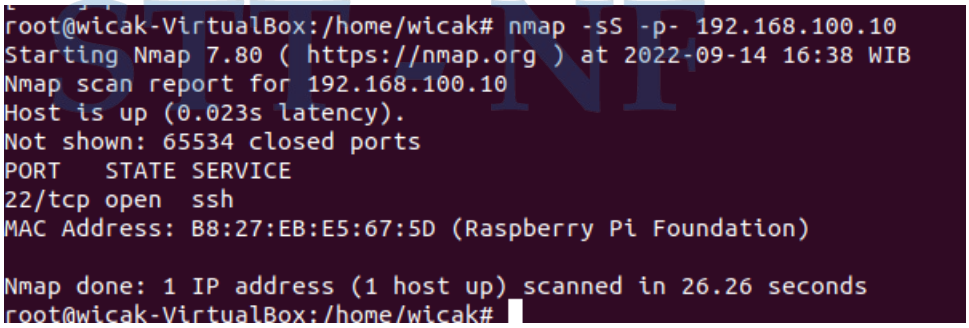
- # Nmap -A 192.168.1.120



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

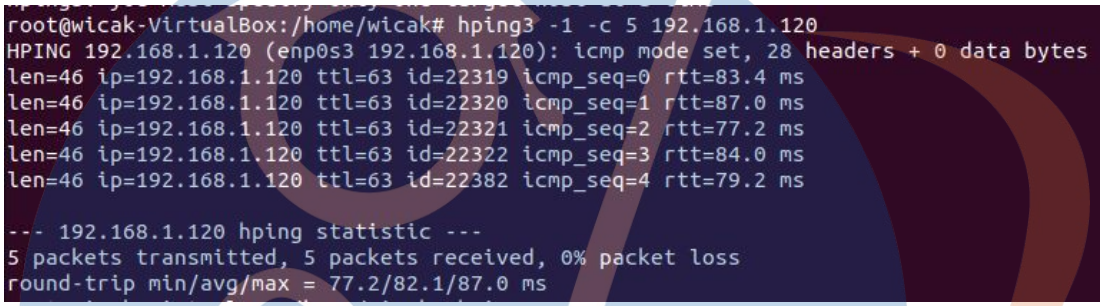


Gambar 26 nmap -sS -p- 192.168.100.10

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 -1 -c 5 192.168.1.120

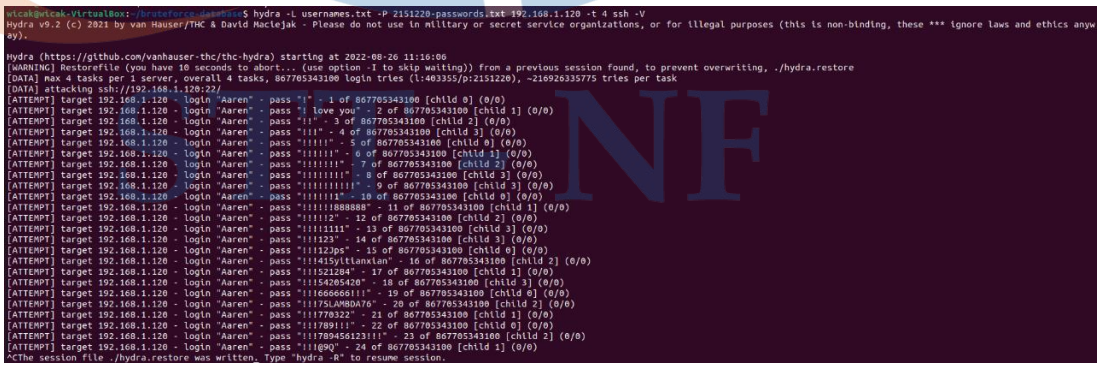


Gambar 27 DDoS Attack Suricata

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



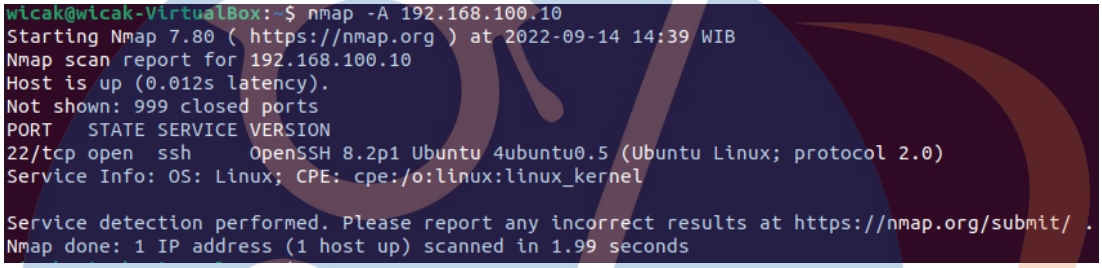
Gambar 28 Brute Force Attack Suricata

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

5.1.3 FAIL2BAN ATTACK

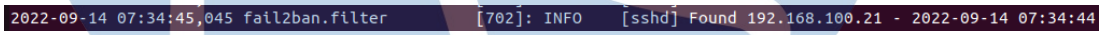
1. Nmap

- # Nmap -A 192.168.1.120



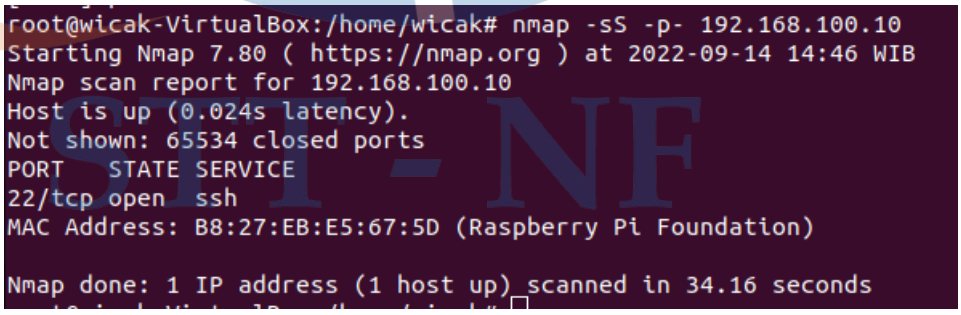
Gambar 29 Nmap Attack F2ban

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



Gambar 30 Alert Nmap F2ban

- # Nmap -sS -p- 192.168.100.10

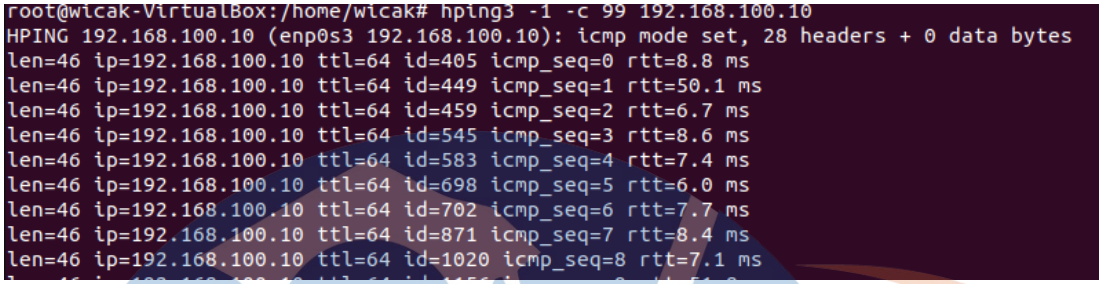


Gambar 31 Nmap Attack f2ban 2

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 -1 -c 99 192.168.1.120

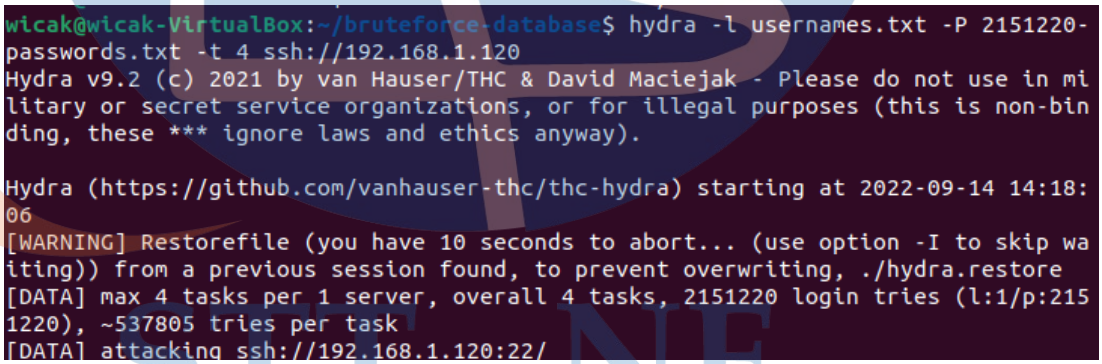


Gambar 32 DDoS Attack Fail2ban

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

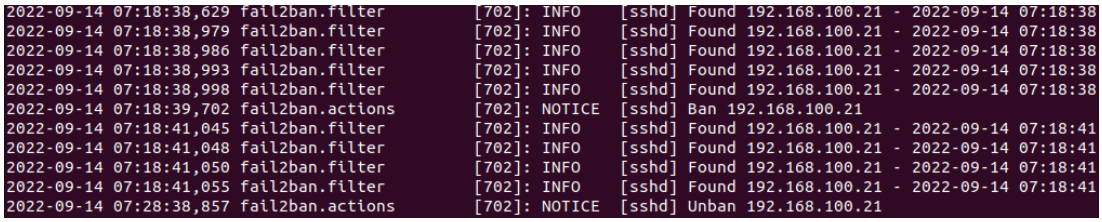
3. Brute Force

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



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.



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.