BAB IV
PENGUJIAN DAN ANALISIS

Bab ini membahas tahapan proses pengujian dari sistem keamanan yang dibangun. Objek penelitian adalah IPS dan DMZ yang diimplementasikan PC router mikrotik dipadukan dengan Ubuntu server. Pengujian dan analisis ini bertujuan untuk mengetahui apakah sistem yang telah dibuat sesuai dengan apa yang direncanakan, dan bekerja secara efektif sesuai apa yang diharapkan. Pengujian

4.1 Persiapan Pengujian

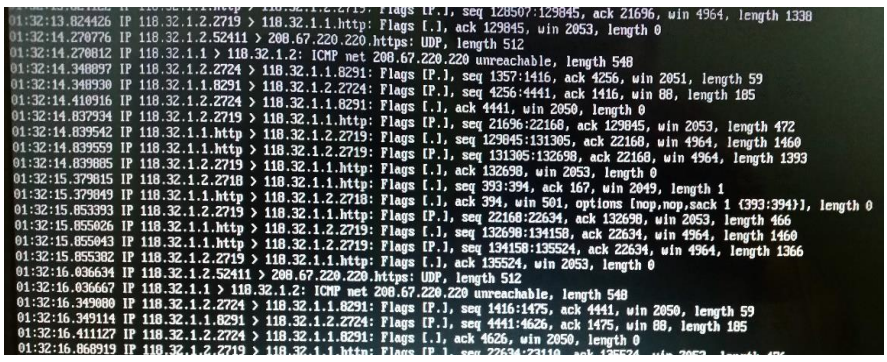
Sebelum pengujian dilakukan ada beberapa tahapan yang harus dilakukan,diantaranya:, memeriksa aliran data packet sniffer, inisialisasi sistem keamanan.

4.1.1 Pemeriksaan Aliran Data Trafr dari packet sniffer mikrotik

Aliran Data dari packet sniffer mikrotik ke IPS snort di ubuntu server dijembatani oleh *trafr*. Oleh karena itu pada tahap ini aliran data dari packet sniffer akan diperiksa terlebih dahulu menggunakan *tcpdump.* Berikut syntax yang digunakan untuk melakukan pemeriksaan kali ini.

```
./trafr –s | tcpdump –r - .s
```

yntax ini memerintahkan tcpdump untuk menampilkan seluruh paket data yang di sadap oleh packet sniffer. Berikut hasil pemeriksaan tcpdump, diperlihatkan pada gambar 4.1.



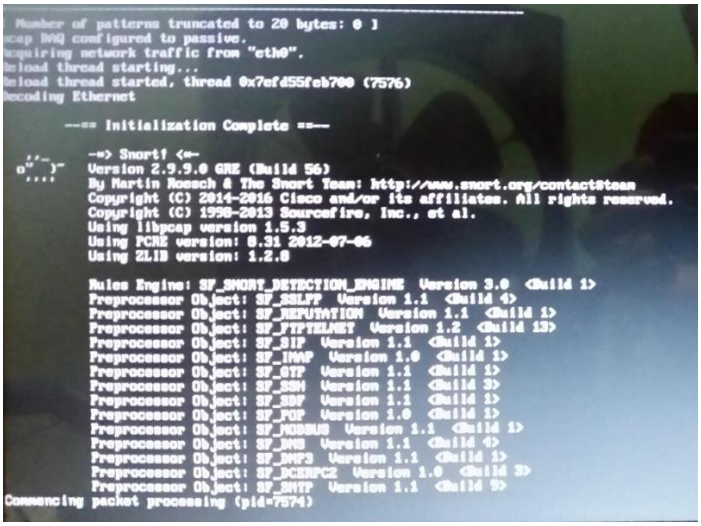
Gambar 4.1 Tcpdump Menampilkan Output Packet Sniffer

4.1.2 Inisialisasi Sistem NIPS

Pada tahap ini IPS snort pada server diberikan perintah untuk mulai melakukan analisis terhatap paket paket yang dikirimkan Mikrotik melalui *trafr*. Dan perintah untuk *swatch* agar mulai menganalisis output snort pada syslog. Berikut syntax yang deberikan pada server.

```
Swatch –c /root/.swatchrc –t /var/log/syslog –t–
args follow=name --daemon
./trafr –s | snort –c /etc/snort/snort.conf –l
/var/log/snort/ -K ASCII
```

Setelah diinisialisasi IPS telah siap diuji. Berikut tampilan server setelah proses inisialisasi selesai diperlihatkan pada gambar 4.2.

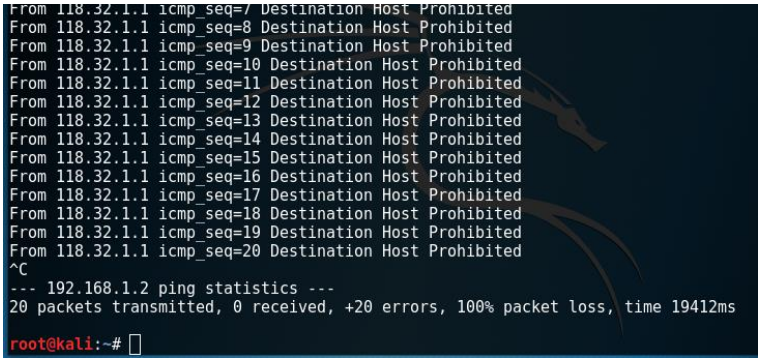


Gambar 4.2 IPS snort standby

4.2 Pengujian DMZ

Pada tahap ini akan dilakukang pengujian terhadap implementasi DMZ pada sistem. DMZ berfungsi untuk memisahkan jaringan untuk server dan private computer.kemudian menggunakan firewall untuk membatasi hak akses untrusted network ke privat network. Pengujian dilakukan menggunakan paket ICMP ping dari untrusted network.

Berikut merupakan tampilan uji ping dari pc penyerang ke pc private, diperlihatkan pada gambar 4.3.



Gambar 4.3 Hasil Uji Ping ke PC Private

Berikut merupakan data hasil uji ping dari pc penyerang, diperlihatkan pada Tabel 4.1.

Tabel 4.1 Hasil Pengujian DMZ

Pengujian	**Respon yang diharapkan**	**Pengamatan**	**Kesimpulan**
Ping 192.168.1.2	Firewall menolak koneksi dari *untrusted network* ke *private network*	Menampilkan pesan reject “Destination Host Probihited”	Diterima
Ping 172.16.1.2	Firewall mengijinkan koneksi dari *untrusted network* ke *DMZ network*	ping reply dari 172.16.1.2”	Diterima

4.3 Pengujian IPS

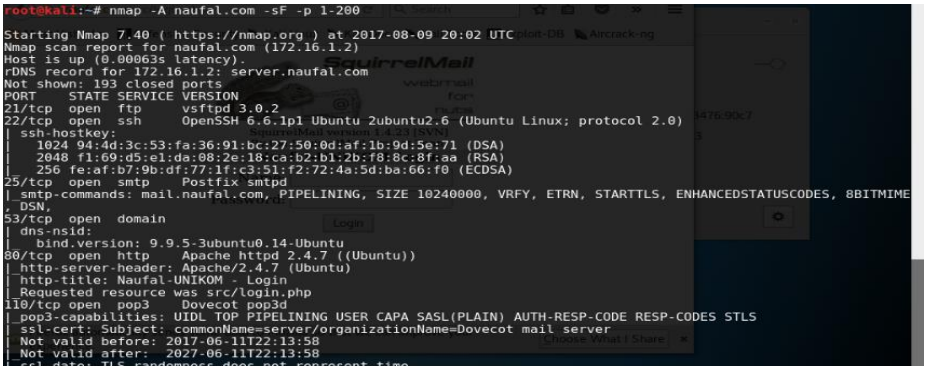
Pada tahap ini dilakukan pengujian terhadap sistem yang telah diinisialisasi. Pengujian dilakukan dengan memberikan ancaman terhadap server berupa port scanning, Ping of Death attack (dengan dan tanpa teknik *ip spoofing*). Proses ini dilakukan dari PC Penyerang yang terhubung dari *untrusted network*.

4.3.1 Pengujian Port Scan terhadap Server

Pada tahap ini dilakukan *port scanning* terhadap server. Perangkat lunak yang digunakan untuk pengujian ini adalah *nmap*, dan teknik yang digunakan adalah scan FIN.Berikut ini syntax yang dieksekusi pada terminal pc penyerang:

```
nmap -v -sF –A naufal.com
```

Berikut ini merupakan hasil dari port scanning scan FIN yang dilakukan nmap terhadap port dari server ubuntu diperlihatkan pada gambar 4.4 dan Data hasil Uji pada Tabel 4.4



Gambar 4.4 Tampilan Eksekusi nmap

Berikut ini merupakan data hasil uji *PoD Attack* yang ditambahkan opsi *ip spoof*, diperlihatkan pada tabel 4.2

Tabel 4.2 Hasil Uji Scan Fin pada Server

	Respon IPS			
	Tambah IP Address ke Blacklist	E-mail alert ke kepala administrator	E-mail alert ke staff administrator	Buat log di Syslog
Harapan	TIDAK	TIDAK	YA	YA
Pengamatan	TIDAK	TIDAK	YA	YA
Kesimpulan	DITERIMA	DITERIMA	DITERIMA	DITERIMA

Kemudian Berikut ini syntax scan FIN yang ditambahkan opsi *ip spoof* yang dieksekusi pada terminal pc penyerang*:*

```
nmap -v -sF –A --spoof 192.168.1.2 naufal.com
```

Berikut ini merupakan data hasil uji scan FIN yang ditambahkan opsi *ip spoof*, diperlihatkan pada tabel 4.3

Tabel 4.3 Hasil Uji Scan Fin dengan IP Spoof pada Server

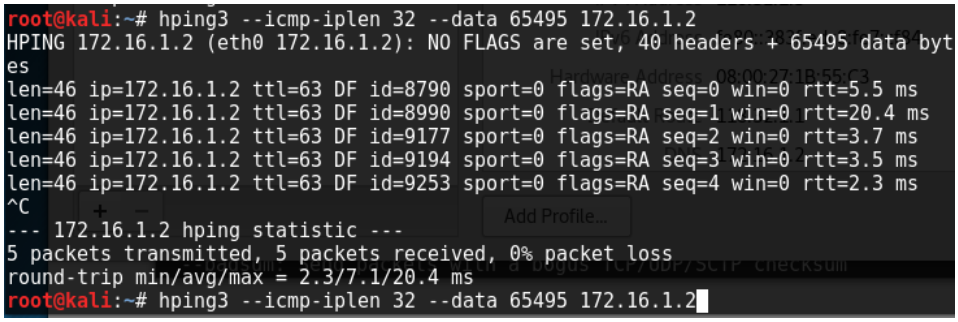
	Respon IPS			
	Tambah IP Address ke Blacklist	E-mail alert ke kepala administrator	E-mail alert ke staff administrator	Buat log di Syslog
Harapan	TIDAK	TIDAK	YA	YA
Pengamatan	TIDAK	TIDAK	YA	YA
Kesimpulan	DITERIMA	DITERIMA	DITERIMA	DITERIMA

4.3.2 Pengujian Ping Of Death Attack terhadap Server

Pada tahap ini dilakukan serangan DoS terhadap server. teknik yang digunakan adalah *PoD Attack*. Berikut ini syntax yang dieksekusi pada terminal pc penyerang*:*

```
Hping3 --icmp --icmp-iplen 32 --data 65495
172.16.1.2
```

Berikut ini merupakan tampilan dari pengujian *PoD Attack* yang dilakukan hping3 terhadap server ubuntu diperlihatkan pada gambar 4.5.



Gambar 4.5 Tampilan Eksekusi hping3

Berikut ini merupakan data hasil ujicoba *PoD Attack* yang dilakukan hping3 terhadap server ubuntu diperlihatkan pada Tabel 4.4

Tabel 4.4 Hasil Uji PoD Attack pada Server

	Respon IPS			
	Tambah IP Address ke Blacklist	E-mail alert ke kepala administrator	E-mail alert ke staff administrator	Buat log di Syslog
Harapan	YA (118.32.1.2)	YA	YA	YA
Pengamatan	YA (118.32.1.2)	YA	YA	YA
Kesimpulan	DITERIMA	DITERIMA	DITERIMA	DITERIMA

Kemudian Berikut ini syntax *PoD Attack* yang ditambahkan opsi *ip spoof* yang dieksekusi hping3 pada terminal pc penyerang*:*

```
Hping3 --icmp --icmp-iplen 32 --data 65495 --spoof
192.168.1.2 172.16.1.2
```

Berikut ini merupakan data hasil uji *PoD Attack* yang ditambahkan opsi *ip spoof*, diperlihatkan pada tabel 4.5

Tabel 4.5 Hasil PoD Attack dengan IP Spoof pada Server

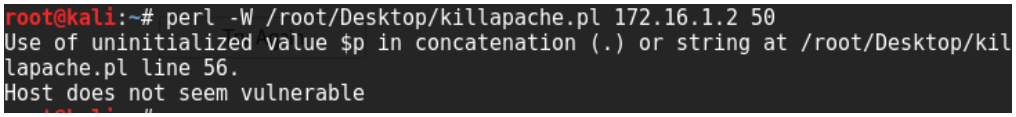
	Respon IPS			
	Tambah IP Address ke Blacklist	E-mail alert ke kepala administrator	E-mail alert ke staff administrator	Buat log di Syslog
Harapan	YA (118.32.1.2)	YA	YA	YA
Pengamatan	YA (192.168.1.2)	YA	YA	YA
Kesimpulan	DITOLAK	DITERIMA	DITERIMA	DITERIMA

4.3.3 Pengujian Apache Range Header Attack terhadap Server

Pada tahap ini dilakukan serangan DoS terhadap server. teknik yang digunakan adalah *Apache Range Header Attack* atau dikenal juga sebagai *Apache Killer*. Pengujian ini dilakukan menggunakan aplikasi perl bernama killapache.pl Berikut ini syntax yang dieksekusi pada terminal pc penyerang*:*

```
Perl –W killapache.pl 172.16.1.2 50
```

Berikut ini merupakan tampilan dari eksekusi killapache.pl terhadap server ubuntu diperlihatkan pada gambar 4.6.



Gambar 4.6 Tampilan Eksekusi killapache.pl

Berikut ini merupakan data hasil ujicoba *Apache Killer* yang dilakukan hping3 terhadap server ubuntu diperlihatkan pada Tabel 4.4

Tabel 4.6 Hasil Uji Apache Killer pada Server

	Respon IPS			
	Tambah IP Address ke Blacklist	E-mail alert ke kepala administrator	E-mail alert ke staff administrator	Buat log di Syslog
Harapan	YA (118.32.1.2)	YA	YA	YA
Pengamatan	YA (118.32.1.2)	YA	YA	YA
Kesimpulan	DITERIMA	DITERIMA	DITERIMA	DITERIMA

4.4 Analisa

Setelah pengujian sistem keamanan jaringan IPS dan DMZ dilakukan, tahap selanjutnya adalah melakukan analisa terhadap data hasil pengujian yang didapatkan

4.4.1 Analisa DMZ

Menurut data yang ditampilkan pada Tabel 4.1 DMZ telah bekerja dengan baik, berjalan sesuai dengan konfigurasi yang telah dipaparkan pada Gambar 3.5. DMZ berhasil dibuat sehingga server bisa dipisahkan dari *private network.* Firewall DMZ dapat membedakan hak akses *untrusted network* ke *private network* dan aksees dari *untrusted network* ke DMZ network.

4.4.2 Analisa IPS

Menurut data yang ditampilkan pada Tabel 4.2, 4.4, 4.6 saat upaya Scan FIN, *PoD Attack*,dan *Apache Killer* dilakukan, IPS dapat mendeteksi, mencatat , memberikan pemberitahuan berupa email kepada administrator, dan melakukan blacklist IP address sesuai jenis serangan dan prioritas dari rule yang telah dibuat.

Begitupun data pada Tabel 4.3 dan 4.5, saat upaya Scan FIN dan *PoD Attack* dengan mode *IP spoofing* dilakukan, IPS dapat mendeteksi, mencatat, memberikan pemberitahuan disertai blacklist ip address sesuai rule yang dibuat. Akan tetapi,

dalam log yang dicatat ip address penyerang tidaklah benar hal ini disebabkan oleh manipulasi dari teknik *IP Spoofing.* Meskipun alamat pengirim pada log yang dibuat adalah salah sistem akan tetap melakukan blacklist terhadap ip address tersebut. Hal ini disebabkan sistem tidak bisa mendeteksi apakah *IP spoofing* atau bukan.

Sehingga pada Tabel 4.5 Penyerang dengan ip address 118.32.1.2 menggunakan ip spoof 192.168.1.2 (alamat IP *Private PC*) untuk melakukan *PoD Attack* ke server. Pada log yang dibuat snort terlihat seperti serangan berasal dari *private PC,* hingga membuat ip address *private PC* ditambahkan kedalam blacklist.