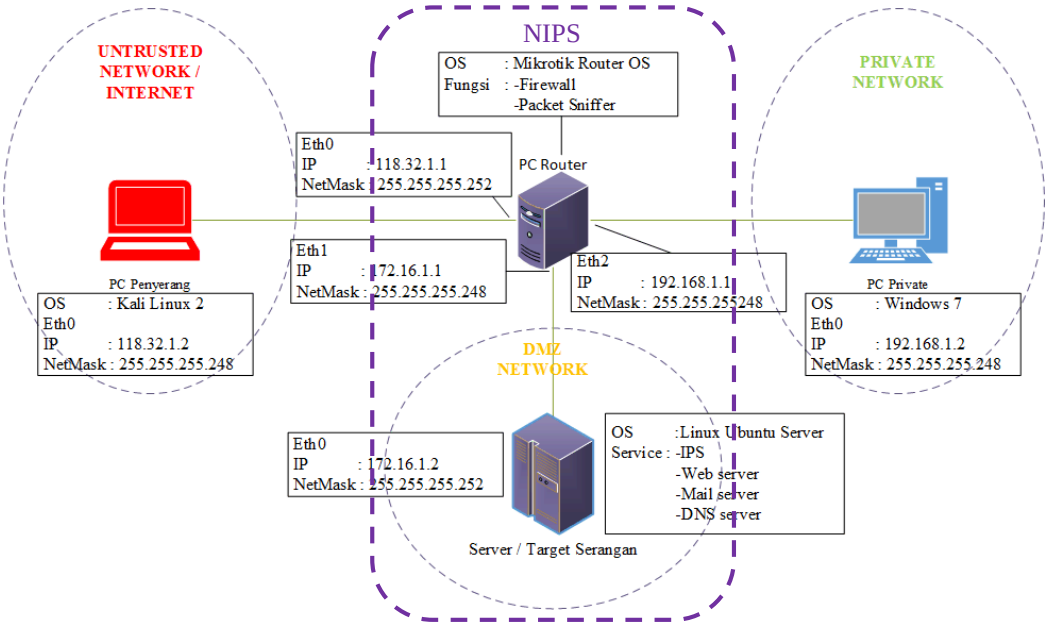
BAB III
PERANCANGAN SISTEM

Pada bab ini akan dibahas tentang bagaimana sistem keamanan jaringan ini dirancang sedemikian rupa meliputi topologi yang digunakan, kebutuhan perangkat yang digunakan, serta konfigurasi yang dilakukan sehingga IPS dan DMZ dapat dipadukan dan berjalan dengan baik.

3.1 Topologi Jaringan

Pada topologi jaringan ini DMZ diterapkan, yakni dengan dibuatnya sebuah jaringan bernama DMZ network yang dikhususkan untuk menampung server sehingga terpisah dengan PC private di private network. Jenis topologi logikal yang diimplementasikan dalam perangcangan ini adalah *shared media topology*. Berikut gambaran dari topologi yang akan dirancang ditunjukan pada Gambar 3.1:



Gambar 3.1 Topologi Jaringan Secara Umum

Berikut penjelasan topologi pada gambar 3.1 :

1 Untrusted Network

Jaringan eksternal yang berada diluar area administratif administrator jaringan (seperti Internet). PC penyerang akan terhubung kesini.

2 Mikrotik PCRouter

Sebuah PC yang bersistem operasi MikroTik 5.20. Memiliki tiga NIC yang masing-masing akan terhubung ke untrusted network, DMZ network, dan private network. Firewall: Salah satu fitur yang disediakan sistem oprasi MikroTik yang berguna untuk memilah paket data yang masuk maupun keluar apakah akan diteruskan atau dibuang, sesuai dengan aturan yang dibuat.

3 Packet sniffer

Sebuah tools yang disediakan MikroTik yang digunakan untuk menangkap paket data yang masuk maupun keluar; pada sistem ini packet sniffer disetting agar informasi yang terkumpul dialirkan ke IPS yang berada di Ubuntu Server secara terusmenerus.

4 DMZ Network

Jaringan tambahan yang dibuat untuk menghubungkan server yang mana dapat bebas diakses oleh publik.

5 Ubuntu Server

Server bersistem oprasi Ubuntu Server 14.04.3 LTS. Menjadi wadah bagi mailserver, webserver juga IPS. Server ini akan menjadi sasaran uji serangan pada tahap pengujian.

6 NIPS

Pada sistem keamanan ini aplikasi yang digunakan untuk IPS adalah SNORTpada ubuntu server berfungsi sebagai penganalisis paket data. Data yang dianalisis dialirkan dari packet sniffer pada mikrotik. Jika terdeteksi adanya pola penyusupan sistem ini akan menambahkan IP Address pengirim ke Blacklist pada firewall di Mikrotik

7 Web Server

Perangkat lunak yang berfungsi untuk melayani permintaan halaman web melalui protokol HTTP. Perangkat lunak yang digunakan adalah apache2., berjalan diatas sistem operasi linux Ubuntu. Pada sistem ini webserber digunakan sebagai antarmuka untuk mailserver.

8 Mail Server

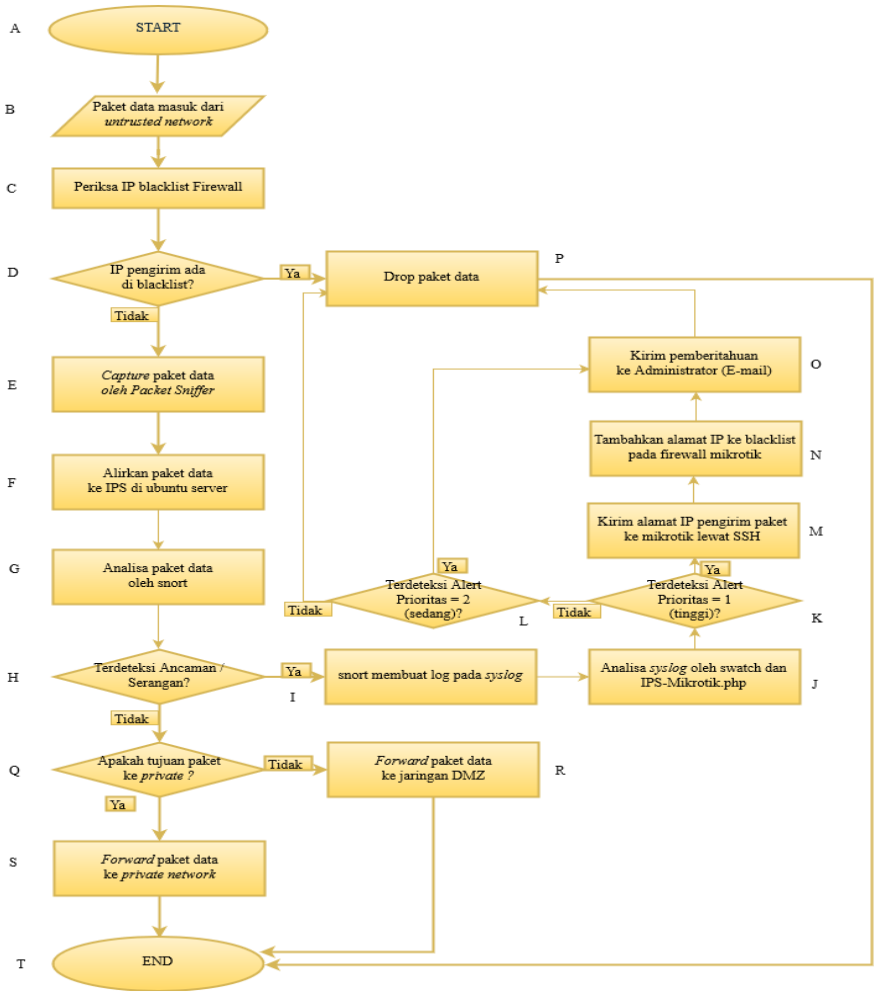
Perangkat lunak yang digunakan untuk mail server adalah Squirrel Mail 1.4.22. Protokol yang digunakan adalah SMTP dan POP3. Mail server ini berjalan diatas sistem operasi Ubuntu server.

9 Private Network

Adalah jaringan yang dibuat khusus untuk perangkat perangkat jaringan internal.yang tidak bebas diakses oleh publik,.

3.2 Diagram Alir Sistem

Sistem keamanan yang dirancang memiliki alur kerja yang sudah ditentukan. Berikut gambaran dari alur kerja sistem keamanan ini diperlihatkan pada Gambar 3.2.



Gambar 3.2 Diagram Alir Sistem

Berikut merupakan keterangan dari diagram alir sistem pada Gambar 3.2, dijelaskan pada tabel 3.1 dan 3.2.

Tabel 3.1 Keterangan Diagram Alir Sistem

No.	Keterangan
A.	Sistem keamanan telah dimulai
B.	Data yang berasal dari *untrusted network* masuk ke pc router mikrotik
C.	Firewall mikrotik memeriksa apakah IP pengirim ada pada blacklist
D.	Firewall menentukan apakah IP pengirim termasuk blacklist atau tidak
E.	Mikrotik menyadap paket data yang masuk
F.	Protokol Melakukan enkapsulasi data yang disadap kemudian dikirimkan ke ubuntu server
G.	Melakukan dekapsulasi data dari mikrotik kemudian snort melakukan analisis terhadap kemungkinan adanya pola ancaman/serangan
H.	Snort menentukan apakah paket data yang dikirim memiliki pola ancman
I.	Snort menulis alert yang berisi prioritas, kategori serangan, dan IP pengirim pada file yang bernama *syslog*
J.	*log monitoring program* menganalisa *syslog* dari ada atau tidaknya alert yang dibuat oleh snort. Ada dua *log monitoring program* yang digunakan. Swatch dan IPS-Mikrotik.php
K.	*Log monitoring program* menentukan apakah prioritas dari alert yang ditulis snort adalah prioritas tinggi
L.	*Log monitoring program* menentukan apakah prioritas dari alert yang ditulis snort adalah prioritas sedang
M.	Ketika prioritas alert snort terdeteksi tinggi, IPS-Mikrotik.php akan mengirimkan alamat IP dan perintah tambah blacklist ke mikrotik melewati menggunakan SSH
N.	Mikrotik menerima alamat IP yang dikirimkan IPS-Mikrotik.php akan mengeksekusi script untuk menambahkan alamat IP ke blacklist firewall
O.	Ketika alert snort yang terdeteksi memiliki prioritas >= 2, Swatch akan mengirim email peringatan kepada Administrator

Tabel 3.2 Lanjutan Tabel Keterangan Diagram Alir

No.	Keterangan
P.	Paket data di drop
Q.	PC router mikrotik menentukan tujuan paket data yang akan dikirim
R.	Paket data diteruskan ke jaringan DMZ
S.	Paket data diteruskan ke jaringan
T	Siklus pengiriman paket data selesai

3.3 Komponen Sistem

Pada perancangan sistem ini diperlukan beberapa komponen, baik perangkat keras maupun perngkat lunak.

3.3.1 Perangkat Keras

Perancangan sistem ini memerlukan beberapa perangkat keras, diantaranya dijelaskan pada Tabel 3.3.

Tabel 3.3 Kebutuhan Perangkat Keras

No.	Perangkat Keras	Jumlah	Spesifikasi
1	PC ROUTER	1 unit	1. Intel x86 compatible processor 2. RAM 128 MB 3. HDD 8GB 4. Ethernet Card (x3)
2	Server	1 unit	1. Intel 1386 compatible processor 2. RAM 1GB 3. HDD 16 GB 4. Ethernet Card
3	PC Penyerang	1 unit	1. Intel 1386 compatible processor 2. RAM 1GB 3. HDD 16 GB 4. Ethernet Card
4	PC Private	1 unit	1. Intel 1386 compatible 2. RAM 1GB 3. HDD 16 GB 4. Ethernet Card
5	Kabel UTP	3x2 meter	Standar, Crimped

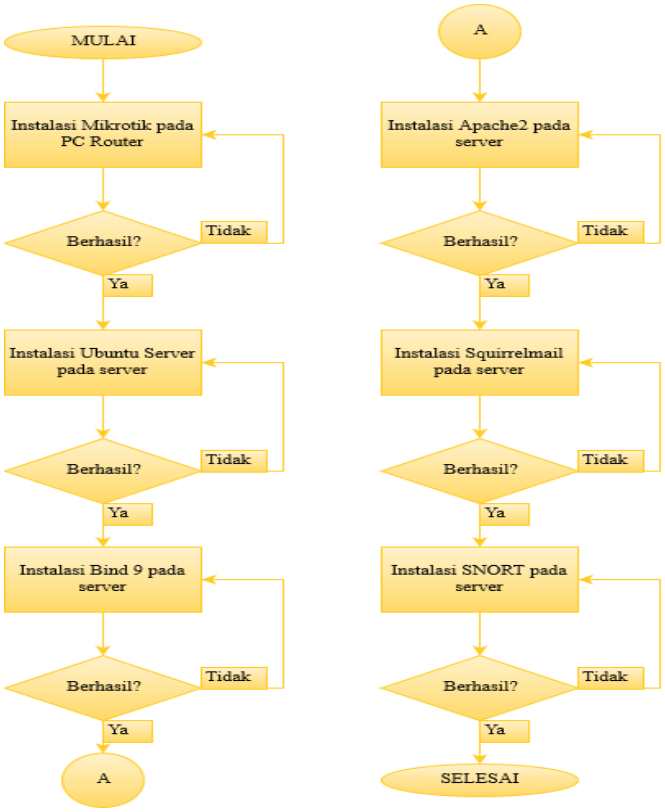
3.3.2 Perangkat Lunak

Perancangan sistem ini memerlukan beberapa perangkat lunak baik sistem operasi maupun aplikasi pendukung, diantaranya:

1. LINUX Ubuntu Server 14.04.3 LTS sebagai Sistem operasi server
2. Mikrotik Router OS 5.20 sebagai sistem operasi PC router.
3. SNORT sebagai badan utama IPS yang berjalan pada Ubuntu server.
4. Apache 2 sebagai Webserver yang berjalan pada Ubuntu server.
5. Squirrelmail 1.4.22 sebagai Mailserver yang berjalan pada Ubuntu server.
6. Bind 9 sebagai DNS server yang berjalan pada Ubuntu server.

3.4 Instalasi Sistem

Setelah seluruh komponen yang diperlukan sistem ini telah disiapkan, langkah selanjutnya adalah instalasi sistem operasi dan aplikasi pendukung untuk sistem ini. Gambaran mengenai langkah langkah instalasi sistem diperlihatkan pada Gambar3.3.



Gambar 3.3 Diagram Alir Instalasi Sistem

Berikut penjelasan dari tahapan-tahapan instalasi sistem yang diperlihatkan pada Gambar 3.3:

1. Tahap pertama, instalasi sistem operasi pada PC router menggunakan Mikrotik Router OS. Terus ulangi tahap ini bila tidak berhasil melakukan instalasi Mikrotik Router OS.
2. Setelah instalasi sistem operasi pada PC router berhasil dilakukan, lakukan instalasi sistem operasi LINUX Ubuntu Server 14.04.3 LTS pada PC server. Jika tidak berhasil melakukan instalasi sistem operasi pada server ulangi kembali tahap ini.
3. Selanjutnya lakukan instalasi Bind 9 pada server ubuntu sebagai DNSserver yang berguna untuk menerjemahkan alamat domain menjadi IP address bagi DNS client. Jika instalasi DNS server tidak berhasil ulangi kembali tahap ini. DNS server Bind9 dapat diinstall menggunakan syntax `sudo apt-get install bind9`
4. Setelah melakukan instalasi sistem operasi pada server tahap selanjutnya adalah instalasi Apache2 pada server ubuntu sebagai aplikasi webserver yang diperlukan sebagai antarmuka web mailserver. Jika tidak berhasil ulangi kembali tahap ini. Web server Apache 2 dapat diinstall menggunakan syntax `sudo apt-get install apache2`
5. Kemudian setelah instalasi webserver berhasil dilanjutkan dengan instalasi Squirrelmail 1.4.22 sebagai mailserver pada server ubuntu. Jika tidak berhasil ulangi kembali tahap ini.
6. Selanjutnya, tahap terahir adalah instalasi SNORT pada server sebagai bagian utama dari sistem NIPS yang beguna sebagai penganalisis paket yang berhasil *sniff* oleh *packer sniffer* pada PC router Mikrotik. Jika tahap instalasi SNORT tidak berhasil, ulangi tahap ini..

3.5 Konfigurasi Ubuntu Server

Setelah tahapan-tahapan instalasi dilakukan, tahap selanjutnya adalah mengatur konfigurasi pada server. Pada tahap ini dilakukan konfigurasi untuk membuat sebuah mail server dengan domain “naufal.com”.

3.5.1 Konfigurasi DNS server

Setelah instalasi DNS server Bind9 berhasil, akan muncul file konfigurasi yang berada didalam direktori `/etc/bind/`. Kemudian edit file default zone menggunakan syntax `nano /etc/bind/named.conf.default-zones`. Tambahkan script berikut ini pada file tersebut.

```
zone "naufal.com" IN {
type master;
file "/etc/bind/db.naufal.com";
allow-update { none; };
};
zone "16.172.in-addr.arpa" {
type master;
file "/etc/bind/db.172";
};
```

Kemudian buat file db.naufal.com dengan syntax `nano /etc/bind/db.naufal.com`. Tambahkan script berikut ini pada file tersebut.

```
;
$TTL 1D
$ORIGIN naufal.com.
@    IN   SOA  ubuntu.naufal.com.root.naufal.com.(
1         ; serial
1D        ; refresh
1H        ; retry
1W        ; expire
3H )      ; minimum

@         IN   NS        ubuntu.naufal.com.
IN   A         172.16.1.2
ubuntu    IN   A         172.16.1.2
          IN   mx10      mail.naufal.com.
www       IN   CNAME     ubuntu
mail      IN   CNAME     ubuntu
```

```
ftp        IN    CNAME      ubuntu
```

Kemudian buat juga file db.172 dengan syntax `nano /etc/bind/db.172`. Tambahkan script berikut ini pada file tersebut.

```
;
$TTL 1D
@     IN    SOA  ubuntu.naufal.com.root.naufal.com.(
1           ; serial
1D          ; refresh
1H          ; retry
1W          ; expire
3H )        ; minimum

@           IN    NS         ubuntu.naufal.com.
2.1         IN    PTR        ubuntu.naufal.com.
2.1         IN    PTR        www.naufal.com.
2.1         IN    PTR        mail.naufal.com.
2.1         IN    PTR        ftp.naufal.com.
```

Selanjutnya edit file resolv.conf dengan syntax `nano /etc/resolv.conf`. Tambahkan script berikut ini pada file tersebut.

```
nameserver 172.16.1.2
search naufal.com
domain www.naufal.com
```

Setelah seluruh konfigurasi DNS server dilakukan, restart service bind9 dengan syntax `etc/init.d/bind9 restart`.

3.5.2 Konfigurasi Web Server

Setelah instalasi webserver berhasil, akan muncul file konfigurasi yang berada didalam direktori `/etc/pache2/apache2.conf` juga tempat penyimpanan khusus untuk file web yang akan ditampilkan pada browser. Tempat penyimpanan tersebut biasanya disimpan di direktori`/var/www/` atau `/home/user/public_html`.

3.5.3 Konfigurasi Mail Server

Setelah web server berhasil diinstall, install beberapa software pendukung untuk mail server, diantaranya: Postfix, Dovecot, Squirrelmail.

Pertama, install Postfix sebagai *mail transfer agent* menggunakan syntax.`sudo apt-get install postfix` buka file konfigurasi menggunakan file editor dengan syntax `nano /etc/postfix/main.cf` kemudian edit file tersebut menjadi:

```
myhostname = mail.naufal.com
mydomain = naufal.com
myorigin = $myhostname
inet_interfaces = all
mydestination = =$myhostname,$mydomain
mynetworks_style = subnet
mynetworks = 172.16.0.0/16, 127.0.0.0/8
```

Kemudian install Dovecot sebagai *mail delivery agent* menggunakan syntax `apt-get install dovecot` dan `apt-get install dovecot-common`. Lalu edit file konfigurasi dovecot menggunakan editor dengan `syntax nano /etc/dovecot/dovecot.conf`. Kemudian edit beberapa bagian file tersebut menjadi:

```
protocols = pop3 imap
disable_plaintext_auth = no
pop3_uidl_format = %08Xu%08Xv
```

Kemudian, instalasi Squirrelmail sebagai *web mail* menggunakan syntax `apt-get install squirrelmail`. Kemudian edit file konfigurasi apache2 menggunakan syntax `nano /etc/apache2/apache.conf`. agar squirrelmail bisa diakses, buat konfigurasi virtual host menggunakan pada file tersebut dengan menambahkan script berikut:

```
NameVirtualHost 172.16.1.2:80
<VirtualHost 172.16.1.2:80>
 ServerAdmin admin@naufal.com
 DocumentRoot /usr/local/squirrelmail
```

```
 ServerName mail.naufal.com
</VirtualHost>
```

Setelah seluruh konfigurasi mail server dilakukan, restart seluruh service yang berhubungan menggunakan syntax berikut:

```
etc/init.d/apache2 restart
etc/init.d/postfix restart
etc/init.d/dovecot restart
etc/init.d/squirrelmail restart
```

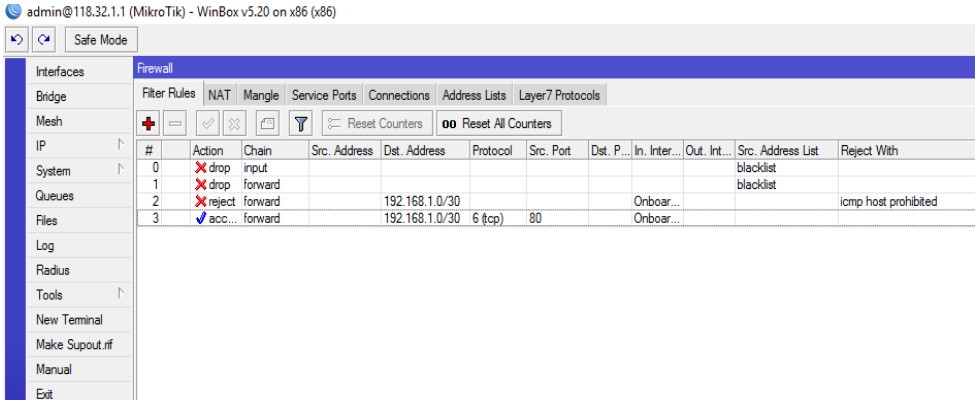
Mail server kini bisa diakses melalui web browser. Berikut tampilan *home page* dari mail server diperlihatkan pada Gambar 3.5



Gambar3.4 Home Page Mail Server.

3.6 Konfigurasi DMZ

Setelah topologi berhasil diterapkan, jaringan DMZ berhasil ditambahkan. Kemudian dilakukan konfigurasi firewall pada pc router mikrotik untuk membatasi akses dari untrusted network ke private network. Berikut merupakan konfigurasi dari filter firewall yang digunakan pada mikrotik pc router, diperlihatkan pada Gambar 3.5.



Gambar 3.5 Konfigurasi Firewall DMZ

3.7 Konfigurasi NIPS

Pada penelitian ini metode IPS yang digunakan adalah NIPS. Jaringan yang dilindungi oleh NIPS ini adalah DMZ network. NIPS digunakan untuk mendeteksi pola serangan yang ditujukan pada DMZ network. NIPS ini akan buat untuk menangani beberapa kejadian menggunakan respon sistem yang diperlihatkan pada tabel 3.4

Tabel 3.4 List Event yang Ditangani NIPS

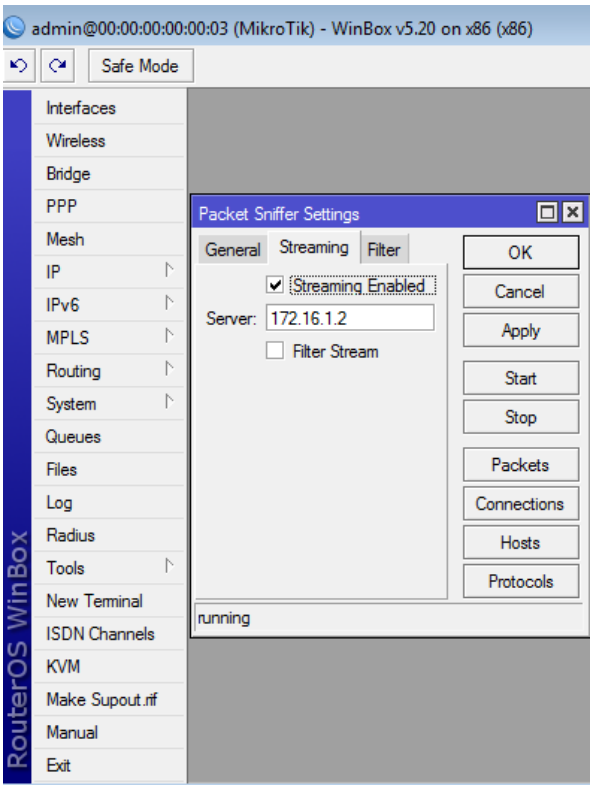
No.	Event	Prioritas	Respon			
			Blacklist IP Address	E-mail alert ke kepala administrator	E-mail alert ke staff administrator	Buat log di Syslog
1	Scan FIN	2	TIDAK	TIDAK	YA	YA
2	Ping of Death	1	YA	YA	YA	YA
3	Apache Killer	1	YA	YA	YA	YA

Adapun beberapa hal yang perlu dikonfigurasi pada sistem ini, diantaranya: packet sniffer, snort, log monitoring program, dan blacklist firewall.

3.7.1 Konfigurasi Packet Sniffer

Pertamatama konfigururasi packet sniffer pada mikrotik pc router agar menyadap seluruh data yang masuk dari *untrusted network.*

Berikut merupakan gambaran dari konfigurasi packet sniffer mikrotik, diperlihatkan pada gambar 3.6.



Gambar3.6 Konfigurasi Packet Sniffer Mikrotik

Pada gambar 3.6 diperlihatkan opsi streaming di-enable, hal ini memungkinkan packet data yang telah disadap bisa dialirkan ke IDS yang ada pada ubuntu server. Data yang tersadap dienkapsulasi dan dialirkan oleh *tazmen sniffer protocol* yang dimiliki mikrotik router os.

3.7.2 Konfigurasi snort

Program utama yang digunakan untuk sistem ini adalah *snort*. Sebelum instalasi snort ada beberapa perangkat lunak pendukung yang diperlukan. Diantaranya bisa dipersiapka menggnakan syntax berikut:

```
sudo apt-get install flex bison buildessential
checkinstall systemback libpcap-dev libnet1-dev
libpcre3-dev libmysqlclient15-dev libnet-filter-
queue-dev iptables-dev libssh2-php libc6:i386
libdumbnet-dev swatch
```

Selain itu agar paket data yang dikirimkan oleh packet sniffer pada mikrotik bisa dibaca oleh IPS snort pada server ubuntu, paket tersebut perlu di dekapsulasi menggunakan sebuah perangkat lunak yang bernama *trafr*. Program ini harus didownload terlebih dahulu menggunakan syntax "`wget www.mikrotik.org /download/trafr.tgz`" kemudian lakukan unpacking pada file tersebut sehingga muncul file bernama *trafr*. Masukan perintah "`./trafr -s | tcpdump -r - -n`" untuk mengecek apakah trafr berhasil melakukan dekapsulasi paket dari packet sniffer mikrotik.

Setelah instalasi perangkat pendukung selesai dilanjutkan dengan instalasi snort menggunakan syntax "`apt-get install snort snort-rules-default`". Kemudian sunting file local.rules menggunakan syntax "`nano /etc/snort/rules/local.rules`", Berikut ini merupakan list dari rule yang akan ditambahkan pada local.rules, diperlihatkan pada tabel 3.5.

Tabel 3.5 Rule Scan Fin

No.	Event	Rule
1	ScanFIN	`Alert tcp $EXTERNAL_NET any -> 172.16.1.2 any (msg:"Scan FIN !"; Classtype: attempted-recon; flow:stateless; Flags:F,12; Priority: 2; Sid:1000002;)`
2	PoD Attack	`Alert tcp $EXTERNAL_NET any -> 172.16.1.2 any (msg:"PoD Attack !"; Classtype: attempted-attack; dsize:>=65507; Priority: 1; Sid:1000003;)`
3	Apache Killer	`Alert tcp $EXTERNAL_NET any -> 172.16.1.2 80 (msg:"Apache Killer !"; Classtype: attempted-attack; flow:to_server, established; content:"Range"; http_header; content:"bytes"; Priority: 2; Sid:1000004;)`

Berikut merupakan rincian deskriptif dari rule yang dibuat untuk mengenali scan FIN diperlihatkan pada tabel 3.6

Tabel 3.6 Rincian Rule untuk Scan Fin

No.	Field	Value	Deskripsi
1	Action	Alert	Keluarkan alert jika rule terpicu
2	Protocol	tcp	Protokol yang akan di filter
3	Src. Address	EXTERNAL_NET	IP pengirim paket data
4	Src. Port	any	Port pengirim paket data
5	Data flow	->	Arah aliran data
6	Dst. Address	172.16.1.2	IP tujuan paket data
7	Dst. Port	any	Port tujuan paket data
8	(option1;	(Msg:”Scan FIN !”;	Pesan yang akan muncul pada alert jika rule ini terpicu
9	Option2;	Classtype: scan-fin;	Klasifikasi event
10	Option3;	flow:stateless;	Rule akan terpicu tanpa dipengaruhi oleh *traffic flow*
11	Option4;	Flags:F,12;	Rule akan terpicu ketika hanya control flag FIN bernilai set,
11	Option4;	Priority: 2;	Tingkat prioritas, 3 (rendah) 2(sedang) 1(tinggi)
12	Option5;)	Sid:1000002;)	Nomor unik identifikasi snort rule

Berikut merupakan rincian deskriptif dari rule yang dibuat untuk mengenali *PoD Attack* diperlihatkan pada tabel 3.7.

Tabel 3.7 Rincian Rule untuk PoD Attack

No.	Field	Value	Deskripsi
1	Action	Alert	Keluarkan alert jika rule terpicu
2	Protocol	icmp	Protokol yang akan di filter
3	Src. Address	EXTERNAL_NET	IP pengirim paket data
4	Src. Port	any	Port pengirim paket data
5	Data flow	->	Arah aliran data
6	Dst. Address	172.16.1.2	IP tujuan paket data
7	Dst. Port	any	Port tujuan paket data
8	(option1;	(Msg:”PoD Attack !”;	Pesan yang akan muncul pada alert jika rule ini terpicu
9	Option2;	Classtype: pod-attack;	Klasifikasi event
10	Option3;	dsize:>=65507	Rule akan terpicu ketika besar paket ICMP lebih dari samadengan 65507 byte
11	Option4;	Priority: 1;	Tingkat prioritas, 3 (rendah) 2(sedang) 1(tinggi)
12	Option5;)	Sid:1000003;)	Nomor unik identifikasi snort rule

Berikut merupakan rincian deskriptif dari rule yang dibuat untuk mengenali *Apache Killer* diperlihatkan pada tabel 3.8.

Tabel 3.8 Rincian Rule Untuk Apache Killer

No.	Field	Value	Deskripsi
1	Action	Alert	Keluarkan alert jika rule terpicu
2	Protocol	tcp	Protokol yang akan di filter
3	Src. Address	EXTERNAL_NET	IP pengirim paket data
4	Src. Port	any	Port pengirim paket data
5	Data flow	->	Arah aliran data
6	Dst. Address	172.16.1.2	IP tujuan paket data
7	Dst. Port	80	Port tujuan paket data
8	(option1;	(Msg:”Apache Killer Attack !”;	Pesan yang akan muncul pada alert jika rule ini terpicu
9	Option2;	Classtype: apache-attack;	Klasifikasi event
10	Option3;	Flow:to_server;	Tujuan Paket data menuju server (berupa request)
11	Option4	Established;	Rule hanya akan terpicu pada koneksi tcp yang telah dibentuk
12	Option5	Content:”Range”;	Mencocokan data yang masuk apakah memiliki pola “Range” didalamnya.
13	Option6	http_header;	Memfokuskan pencocokan pola “Range” pada data http header
	Option7;	Priority: 1;	Tingkat prioritas, 3 (rendah) 2(sedang) 1(tinggi)
	Option8;)	Sid:1000004;)	Nomor unik identifikasi snort rule

Setelah itu edit file konfigurasi snort menggunakan syntax `nano /etc/snort/snort.conf`. Edit beberapa bagian dari file konfigurasi tersebut, diantaranya:

```
#jaringan yang dilindungi (DMZ network)
ipvar HOME_NET 172.16.1.0/30
ipvar EXTERNAL_NET !HOME_NET
#uncomment tagar untuk output snort ke syslog
Output alert_syslog; LOG_AUTH LOG_ALERT
#uncomment tagar untuk include file rule yang
#akan digunakan
Include $RULE_PATH/local.rules
```

Setelah konfigurasi dilakukan, snort telah siap untuk menganalisa paket data yang masuk untuk kemudian mengeluarkan alert pada *syslog* jika terdeteksi ada pola penyerangan.

3.7.3 Log Monitoring Program

Sistem ini menggunakan dua log monitoring program , yaitu *swatch* dan IPS-Mikrotik.php. *Swatch* berfungsi sebagai pengawas syslog yang akan merespon jika snort menulis alert. *Swatch* merespon dengan cara mengirim email peringatan kepada administrator. Untuk mengatur *swatch* dapat dilakukan dengancara mengedit file konfigurasi menggunakan syntax "`nano /root/.swatch.rc`". lalu memasukan script

```
watchfor /Scan FIN/
exec echo "Subject:ALERT: Server mendeteksi upaya
SCAN FIN" | sendmail "staff-it@naufal.com"

watchfor /PoD Attack/
exec echo "Subject:ALERT: Server mendeteksi upaya
PoD Attack pada Server!" | sendmail "staff1-
it@naufal.com; leader-it@naufal.com"
```

```
watchfor /Apache Killer/
exec echo "Subject:ALERT: Server mendeteksi upaya
Apache Range Header Attack pada Server!" |
sendmail "staff1-it@naufal.com; leader-
it@naufal.com"
```

Script ini merupakan dibuat agar swatch mendeteksi adanya kata “Scan FIN” atau “PoD Attack” juga “Apache Killer” pada syslog agar kemudian bisa mengirimkan email peringatan kepada administrator jaringan. Untuk ancanman serangan “Priority: 1”maka sistem akan mengirim email peringatan kepada staff dan kepala administrator jaringan. Sedangkan jika terdeteksi “Priority: 2” maka email peringatan hanya dikirimkan kepada staff saja.

Kemudian IPS-Mikrotik.php adalah sebuah program php yang berfungsi sebagai pengawas syslog. Akan tetapi program ini dibuat hanya merespon alert “Priority:1” yang dikeluarkan snort. Program ini akan merespon dengan cara mengirim alamat IP terdeeteksi ke mikrotik pc router menggunakan SSH. Setelah program ini berhasil dibuat, tambahkan kedalam list scheduler yang bernama *crontab*. Gunakan syntax “`crontab -e`” kemudian tambahkan sebuah script “`* * * * * php /home/naufal/IPS-mikrotik.php`”. dengan demikian program ini akan selalu dieksekusi dalam interval setiap satu menit.

3.7.4 Konfigurasi Blacklist Firewall

Setelah konfigurasi log monitoring program selesai, dilanjutkan dengan konfigurasi pada mikrotik router os agar bisa menerima perintah yang dikirimkan oleh IPS-Mikrotik.php untuk melakukan blacklist pada alamat tertentu. Pertama, buat sebuah akun untuk IPS-Mikrotik,php melakukan login SSH menggunakan syntax `user add name=ips password=ips group=full address=172.16.1.2`.

Kemudian buat sebuah script untuk menambahkan alamat IP yang dikirim IPS-Mikrotik.php ke address list yang bernama blacklist pada firewall.

```
:global ip
/ip firewall address-list add list=blacklist
address=$ip
```

Kemudian, tambah rule pada firewall agar melakukan *drop* untuk setiap paket data yang dikirim dari alamat IP yang berada pada blacklist, menggunakan syntax `ip firewall filter add src-address-list=blacklist action=drop`.