Jurnal KomtekInfo (Komputer Teknologi Informasi)
e-ISSN 2502-8758 || p-ISSN 2356-0010
Vol : 6 || No : 1 || 2019 Hal 29-39
http://lppm.upiyptk.ac.id/ojsupi/index.php/KOMTEKINFO

ANALISIS FIREWALL DEMILITARIZED ZONE DAN SWITCH PORT SECURITY PADA JARINGAN UNIVERSITAS PUTRA INDONESIA YPTK

Syafri Arlis [1], Sahari [2]
[1,2] Universitas Putra Indonesia YPTK Padang, Indonesia
E-mail: syafri_arlis@upiyptk.ac.id [1], sahari@upiyptk.ac.id [2]

ABSTRAK

Perkembangan teknologi informasi semakin pesat, hal ini dapat membantu semua aspek pekerjaan manusia dalam mengolah dan mendapatkan suatu informasi. Pada sisi positif memudahakan pekerjaan manusia, tetapi pada sisi lain dari aspek keamanan sangat mengancam privasi manusia dalam mengolah dan mendapatkan suatu informasi. Teknik-teknik sistem keamanan jaringan dan pencegahan terhadap serangan pada sistem informasi perlu dikembangkan sehingga integrity, availability dan confidentiality. Salah satunya adalah dengan cara membangun sistem keamanan jaringan dan sistem pencegahan serangan. Pada penelitian ini melakukan analisa sistem keamanan jaringan komputer menggunakan firewall Demiliteralized Zone (DMZ) dengan menggunakan IPtables yang merupakan standar dari system Linux dan Switch Port Security (SPS). Pemanfaatan dengan memadukan kedua teknologi ini untuk mencapai tingkat keamanan yang maksimum dan mampu mem-block usaha penyerangan intruder dengan berbagai serangan yang terindentifikasi.

Kata Kunci : firewall, demiliteralized zone (dmz), iptables, integrity

ABSTRACT

The development of information technology so rapidly, greatly helped the works of man. On the one hand man to be very helpful, but on the other side of the system's security level to rise sharply so that in essence the sides of human life is in a threatened position.The techniques of network security systems and precautions against attacks on information systems continue to be developed so that the integrity, availability and confidentiality in an information system becomes more secure. One way is by building a network security system and attack prevention system. In this paper, the authors construct a computer network security systems using a firewall Demiliteralized Zone (DMZ) by using IPtables which is the standard of Linux systems and and Switch Port Security (SPS). Utilization by combining these two technologies to achieve maximum levels of security and is able to block the intruder will attempt an attack with a variety of attacks identified.

Keyword : firewall, demiliteralized zone (dmz), iptables, integrity

1. Pendahuluan

Perkembangan *Internet* menjadi fenomenal, hal ini ditandai dengan penambahan jumlah koneksi yang lebih cepat dari jaringan yang pernah diciptakan sebelumnya seperti jaringan telepon. Jutaan user yang terhubung ke dunia melalui *internet*, secara kasar separuhnya telah menjadikan internet sebagai bisnis yang baru [1]. Dengan dijadikannya *internet* sebagai sarana dalam pengolahan data dan informasi, masalah keamanan data menjadi hal penting untuk diperhatikan. Salah satu ancaman yang paling umum mengancam keamanan suatu jaringan komputer selain virus adalah *intruder*, yang biasanya dilakukan oleh *hacker* dan *cracker* [2].

Berbagai macam kemampuan meng-hack web server dan database server. Membuktikkan bahwa keamanan web merupakan hal terpenting dalam sebuah bisnis yang bergerak dengan menggunakan website beserta sistem operasinya. Web server merupakan salah satu target public

Diajukan pada : 28 Maret 2019 || Diterima pada : 27 Mei 2019 || Diterbitkan Pada : 01 Juni 2019

yang menyangkut sebuah organisasi. Keamanan web server sama pentingnya dengan keamanan website atau aplikasi web tersebut dan jaringan disekitarnya. Dengan adanya kemungkinan akses ilegal tersebut, maka dikembangkan suatu mekanisme yang dapat mengamankan web server dan database server dari akses yang dilakukan pihak ilegal. Untuk itu perlu adanya jaringan komputer yang memerlukan sistem firewall yang berfungsi sebagai sistem keamanan jaringan dan menjaga semua perangkat yang ada didalamnya. Dengan fasilitas yang dimiliki pada firewall, maka komunikasi melalui suatu jaringan komputer dapat berfungsi dengan baik.

Sistem keamanan yang kurang baik yang ada sekarang ini membuat kekhawatiran instansi karena *firewall* yang ada sekarang tidak berfungsi lagi. Instansi mengkhawatirkan akan terjadi kehilangan dan pengrusakan sistem database dari pihak luar yang tidak berwenang dalam mengakses data, oleh karena itu diperlukan aplikasi yang dapat menjaga sistem keamanan jaringan yang memblok *port* mana yang diizinkan dan tidak diizinkan dalam mengakses oleh user yaitu dengan memakai sistem keamanan *firewall* yang menggunakan konsep *Demilitarized Zone* (DMZ) dan *switch port security*.

2. Tinjauan Literatur

Keamanan suatu sistem memberikan jalur akses yang *secure* antara pengguna yang saling mengirim dan menerima informasi dalam menyediakan perlindungan terhadap data. Dimana keamanan sistem merupakan suatu aktivitas yang berkaitan dengan jaringan komputer dan aktivitas tersebut memberikan implikasi terhadap keamanan. Hacker ataupun intruder biasanya memiliki keahlian dapat melihat kelemahan perangkat lunak pada komputer dalam suatu jaringan, kemudian mempublikasikan secara terbuka di internet atau media lain untuk memancing agar sistem diperbaiki menjadi lebih baik. Namun teknologi informasi tidak saja membawa pengaruh baik, informasi tersebut menjadi sebuah tindak kejahatan biasanya disebut cracker.

Tahap-tahap pembangunan dan pengembangan sistem keamanan jaringan komputer adalah sebagai berikut:

1. Studi pustaka / *internet*
2. Identifikasi ancaman
3. Analisis dan merumuskan tindakan
4. Analisa dan merumuskan proses/ *rule* untuk menghindari ancaman
5. Membangun proses dan menerapkan *rule* untuk menghindari ancaman
6. Implementasi dan pengujian terhadap proses yg dibangun atau aturan yang telah diterapkan pada *firewall*.

2.1. Metode Pengamanan

Metode pengamanan yang dapat dilakukan adalah pengaturan terhadap:

2.1.1 Authentication

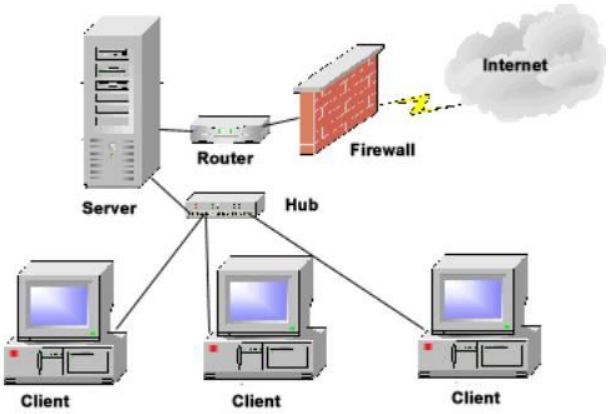
Merupakan jenis perangkat atau pemahaman individu yang dipergunakan untuk mengakses sistem. Hal yang menjadi perhatian utama dalam proses *authentication* .

2.1.2 Authorization

Meruapakan pemahaman tentang *resource* apa yang tersedia untuk pengguna dan perangkat yang telah lulus dari proses validasi.

2.2 Firewall

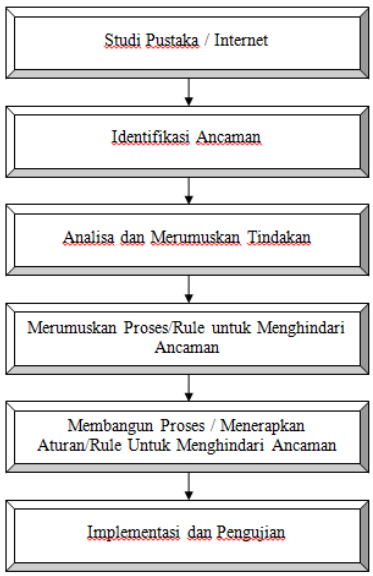
Merupakan sebuah sistem yang memberikan izin lalu lintas jaringan yang dianggap secure dalam melalui dan mencegah lalu lintas jaringan yang tidak aman [4]. Pada umumnya, sebuah firewall diimplementasikan dalam sebuah mesin, yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dengan jaringan lainnya. Pada umumnya *Firewall* digunakan untuk mengawasi akses terhadap akun yang memiliki akses jaringan pribadi dari pihak luar. Saat ini, istilah *firewall* menjadi istilah generik yang merujuk pada suatu sistem dalam mengatur komunikasi antar dua jaringan yang berbeda.



Gambar 1 : Contoh Sebuah Firewall

3. Metodologi Penelitian

Kerangka metodologi penenlitian dapat dilihat pada gambar 3.



Gambar 3: Kerangka Metodologi Penelitian

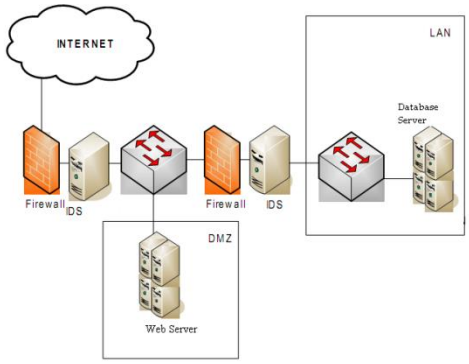
4. Analisa Sistem

4.1 Analisis dan Merumuskan Tindakan

Mengenali ancaman atau serangan yang mungkin terjadi merupakan suatu kebijakan dan strategi pengamanan yang efektif. Kemudian perlu menentukan tingkat keamanan dan

memperkirakan metode atau mekanisme apa yang digunakan untuk mencari solusi. Mekanisme proteksi berbagai jenis serangan yang telah dijelaskan sebelumnya dapat ditanggulangi dengan membangun sebuah sistem keamanan seperti melakukan hal-hal sebagai berikut :

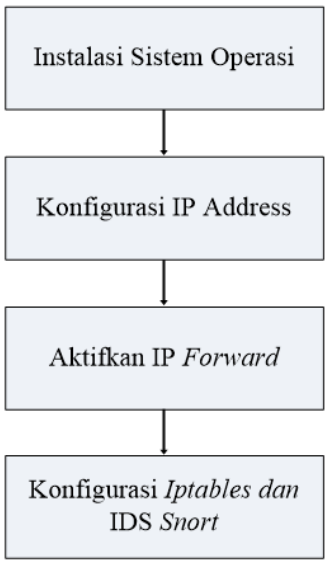
1. Gunakanlah *firewall* yang dapat mengatasi masalah serangan dan mengatur kebijakan dan aturan pada *firewall* terhadap paket data yang akan diteruskan.
2. Menambahkan aplikasi IDS (*Intrusion Detection System*) untuk mendeteksi adanya penyusup dari luar yang dapat menjadi satu dengan *firewall.*



Gambar 4: Arsitektur Firewall DMZ dan Switch Port Security

4.2 Konfigurasi Firewall Demilitarized Zone (DMZ) dan dan Switch Port Security

Sebelum membuat sebuah PC yang akan dikonfigurasi menjadi sebuah *firewall,* ada beberapa hal yang harus dilakukan agar pembuatan *firewall Demilitarized Zone (*DMZ*)* ini berjalan dengan baik. Langkah pertama yang harus dilakukan adalah melakukan konfigurasi terhadap *server* yang akan dijadikan sebagai PC *firewall.* Tahapan konfigurasi *server*, bisa dilihat pada pada gambar 5.



Gambar 5. Tahapan Instalasi dan Konfigurasi Firewall

Aturan dalam konfigurasi *firewall Demiliterated Zone* (DMZ):

1. Akses host luar hanya dapat berhubungan dengan *host-host* yang berada dalam jaringan DMZ. Secara *default* akses dari luar tidak dapat melakukan hubungan dengan *host-host* dalam jaringan DMZ.

2. Pada jaringan DMZ secara *default* tidak dapat terkoneksi dengan *host-host* jaringan *internal*.
3. *Host* jaringan internal dapat melakukan koneksi secara bebas baik ke jaringan luar maupun ke jaringan DMZ.

4.4 Analisa Mekanisme Kerja Firewall DMZ dan Switch Port Security

Firewall merupakan perangkat yang memberikan izin terhadap lalu lintas jaringan yang dianggap *secure* untuk melaluinya dan mencegah lalu lintas jaringan yang tidak *secure* [5]. Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya. Berdasarkan prinsip kerja Port Security adalah dengan menentukan MAC Address PC yang boleh memasuki atau mengakses suatu Port Interface Switch akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari jaringan luar.

Tabel 1. Kebijakan Firewall

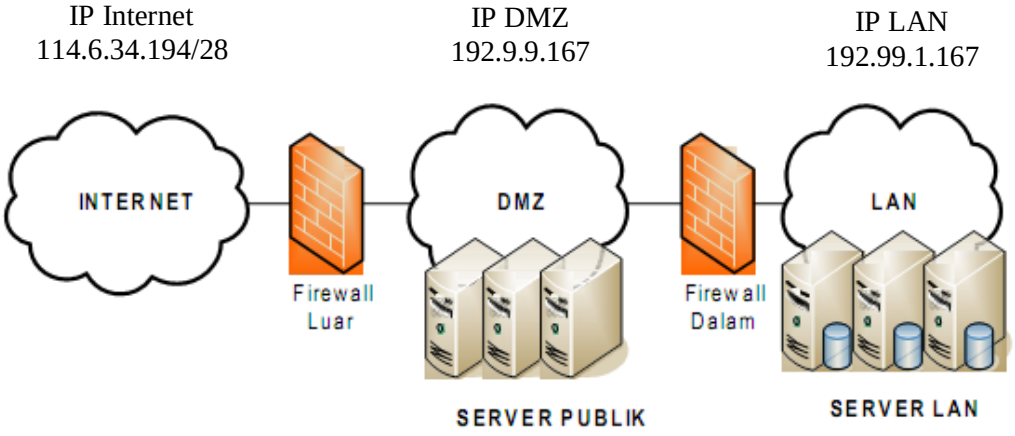
Service	Protocol	Port
DNS	TCP	53
HTTP	TCP	80
Database	TCP	3306

Perintah umum iptables :

```
$iptables [-t table] command [match] [target/jump]
```

4.5 Desain Topologi Demilitarized Zone (DMZ) dan Switch Port Security

Bentuk topologi yang baik terhadapa jaringan yang aman, mengunakan 2 *firewall*. *Firewall* pertama (luar) merupakan *firewall* yang melindungi jaringan luar (internet) dengan *Demiliterized Zone* (DMZ) dan LAN, sedangkan *firewall* kedua (dalam) melindung jaringan LAN dari jaringan *internet* dan DMZ.



Gambar 6: Topologi DMZ

4.5.1 Konfigurasi Firewall

Untuk konfigurasi *firewal*, maka perlu ditentukan service-service yang diperbolehkan untuk diakses, yaitu : HTTP, HTTPS, SSH, DNS. Kemudian buat file yang akan berisi skrip untuk konfigurasi *firewal*.

```
root@Syafri:~# touch /tmp/firewallluar.script
```

Edit file tersebut :

```
root@Syafri:~# vi /tmp/firewallluar.script
```

Tambahkan pada file tersebut dengan option-option berikut :

a. Lokasi IPTables

```
iptables ="/sbin/iptables"
```

b. Nama Interface

```
IF_INT="eth0"
IF_DMZ="eth1"
```

c. Alamat IP Interface

```
IP_INT="114.6.34.195/28"        # IP Ethernet card ke
                                # internet

IP_DMZ="192.9.9.166/30"         # IP Ethernet card ke
                                # DMZ

IP_HTTP="192.9.9.165/30"        # IP Ethernet card HTTP
                                # Server

IP_FWD="114.6.34.194/28"        # IP Ethernet card
                                # Firewall dalam

NET_DMZ="192.9.9.167/240"       # Network DMZ
```

d. Nama Loopback Interface

```
IP_LO="127.0.0.1/32"
IF_LO="127.0.0.1/32"
```

e. Mengaktifkan IP Forwading

```
echo  "1" > /proc/sys/net/ipv4/ip_forward
```

f. Menghapus aturan IPTables yang sudah ada

```
iptables  -F
iptables  -t nat -F
iptables  -t mangle -F
```

g. Memberikan policy awal

```
iptables -P  INPUT  DROP
iptables -P  OUTPUT  DROP
iptables -P  FORWARD  DROP
iptables -T  nat POSTROUTING ACCEPT
iptables -T  nat PREROUTING ACCEPT
iptables -T  mangle INPUT ACCEPT
iptables -T  mangle OUTPUT ACCEPT
iptables -T  mangle FORWARD ACCEPT
iptables -T  mangle PREROUTING ACCEPT
iptables -T  mangle POSTROUTING ACCEPT
```

h. Membatasi akses ke dan dari interface loopback

```
iptables  -A INPUT  -i  $IF_LO  -s  0/0  -j  ACCEPT
iptables  -A OUTPUT  -o  $IF_LO  -s  0/0  -j  ACCEPT
```

i. Menambahkan kolom chain

```
iptables  -N  LAN-INT
iptables  -N  DMZ-INT
iptables  -N  LAN-DMZ
```

j. Memindahkan aturan menurut sumber dan tujuan paket ke kolom (chain)

```
iptables  -A  FORWARD  -i  $IF_DMZ  -o  $IF_INT  -j  DMZ-INT
iptables  -A  FORWARD  -i  $IF_INT  -o  $IF_DMZ  -j  DMZ-INT
iptables  -N  LAN-DMZ
```

k. Akses HTTP dari DMZ ke Internet

```
iptables  -A  DMZ-INT -p  tcp -s $NET_DMZ --sport
1024:65535 -d 0/0 \ --dport 80 -m state -state NEW,
ESTABLISHED  -j ACCEPT

iptables  -A  LAN-INT -p  tcp -s 0/0 --sport 80 -d
$NET_DMZ --dport  \ 1024:65535 -m state --state
ESTABLISHED  -j ACCEPT

iptables  -t nat -A POSTROUTING -o $IF_INT -p tcp -s
$NET_DMZ -sport  1024:65535  -d  0/0  --dport 80 -j
SNAT --to-source $IP_INT
```

l. Akses HTTPS dari DMZ ke Internet

```
iptables  -A  LAN-INT -p  tcp -s $NET_DMZ --sport
1024:65535 -d 0/0  --dport 443 -m state -state NEW,
ESTABLISHED  -j ACCEPT

iptables  -A  LAN-INT -p  tcp -s 0/0 --sport 443 -d
$NET_DMZ --dport   1024:65535 -m state --state
ESTABLISHED  -j ACCEPT

iptables  -t nat -A POSTROUTING -o $IF_INT -p tcp -s
$NET_DMZ -sport  1024:65535  -d  0/0  --dport 443 -j
SNAT --to-source $IP_INT
```

m. Akses Ping dari DMZ ke Internet

```
iptables -A DMZ-INT -p icmp -s $NET_DMZ -d 0/0    -m
state --state NEW,ESTABLISHED -j ACCEPT

iptables -A DMZ-INT -p icmp -s 0/0 -d $NET_DMZ    -m
state --state ESTABLISHED -j ACCEPT
```

n. Akses Ping dari DMZ ke Firewall Luar

```
iptables -A INPUT -i $IF_DMZ -p icmp -s $NET_DMZ    -
d $IP_DMZ -m state --state NEW,ESTABLISHED    -j
ACCEPT

iptables -A OUTPUT -o $IF_DMZ -p icmp -s $IP_DMZ    -
d $NET DMZ -m state --state ESTABLISHED    -j ACCEPT
```

o. Akses Traceroute dari DMZ ke Internet

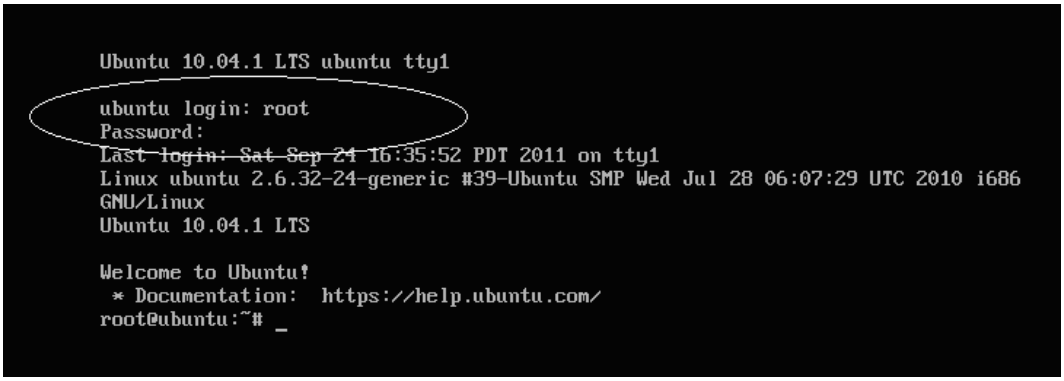
```
iptables -A DMZ-INT -p udp -s $NET_DMZ    --sport
1024:65535 -d 0/0 --dport 33434:33533    -m state --
state NEW,ESTABLISHED -j ACCEPT

iptables -A DMZ-INT -p udp -s 0/0 --sport
33434:33533 -d $NET_DMZ --dport 1024:65535    -m
state --state ESTABLISHED -j ACCEPT

iptables -t nat -A POSTROUTING -o $IF_INT    -p udp -
s $NET_DMZ --sport 1024:65535 -d 0/0    --dport 21-j
SNAT --to-source $IP_INT
```

4.6 Penerapan Rule pada Sistem

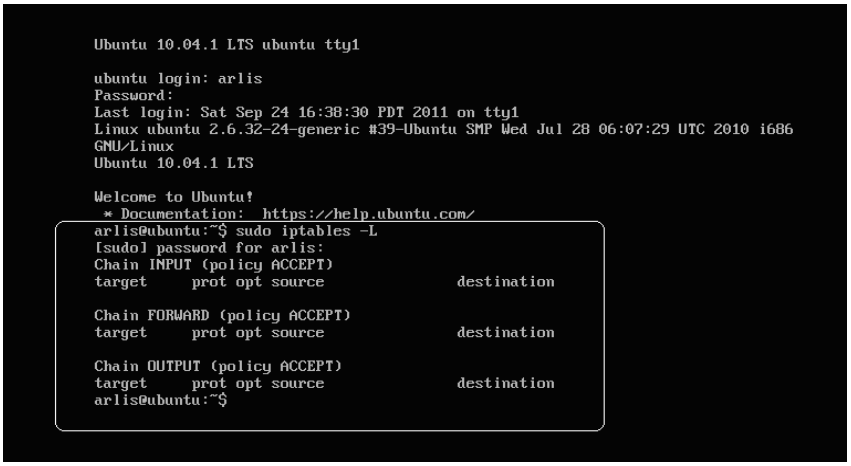
Penerapan rule atau kebijakan keamanan diimplementasikan pada firewall, dimana firewall dibangun pada sistem linux distro ubuntu-16.04.1-server-LTS dengan menggunakan iptables dan dijalankan melalui console atau terminal seperti gambar 7 :



Gambar 7: Login User Root

Setelah login sebagai root, setting Firewall dengan menggunakan iptables :

Iptables [*tipe-perintah*] [*chain*] [*tipe-parameter*] –j [*target*]



Gambar 8: List IPTables

Untuk melihat *rule* yang telah diterapkan pada *firewall*. Pada Gambar 8, chain INPUT, chain FORWARD dan chain OUTPUT masih kosong, karena belum diisi aturan yang baru.

Untuk menerapkan *rule* baru dalam memblok paket protocol ICMP (ping) yang datang dari client yang memiliki alamat IP 192.168.9.165 yang dideteksi sebelumnya oleh snort IDS tanpa ada pesan error :

arlis@ubuntu:~$ sudo iptables –A INPUT –s 192.168.9.165 –p ICMP –j DROP

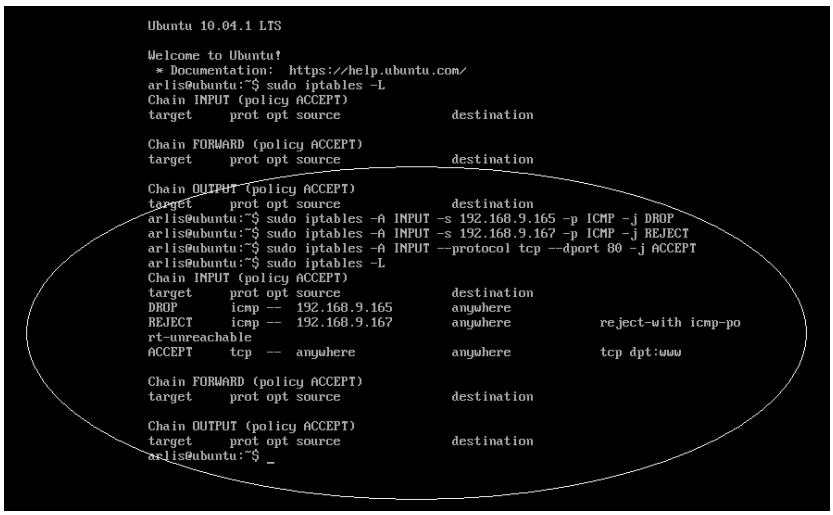
Perintah ini berfungsi untuk memblok paket protocol ICMP (ping) yang datang dari client yang memiliki alamat jaringan 192.168.9.165 dengan disertai pesan error.

arlis@ubuntu:~$ sudo iptables –A INPUT –s 192.168.9.167 –p ICMP –j REJECT

Perintah yang berfungsi untuk memperbolehkan mengakses ke server HTTP (port 80) sebagai berikut :

```
arlis@ubuntu:~$ sudo iptables –A INPUT --protocol tcp --dport 80 –j
                ACCEPT
```

Perintah atau rule diatas dapat dilihat kembali isinya melalui perintah “sudo iptables –L” seperti pada gambar 9.



Gambar 9: List IPTables setelah diberikan Rule

5. Kesimpulan

Dari hasil analisa dan testing dari sistem yang dilakukan maka ada beberapa rekomendasi serta menjadi rujukan dalam sistem ini diantaranya :

1. *Firewall Demiliteralized Zone* (DMZ) dan *switch port security* merupakan sistem jaringan keamanan yang terletak diantara suatu jaringan *private* LAN dan jaringan *public* (*internet*) dengan membuat segmentasi dalam meletakkan *server* Universitas Putra Indonesia YPTK Padang yang bisa diakses *public* dengan aman tanpa harus bisa mengganggu keamanan sistem yang lain.
2. Serangan atau penyusupan dapat dicegah dengan penggunaan *snort* untuk mendeteksi adanya penyusup dari luar yang dapat menjadi satu dengan *firewall.*
3. Untuk mencapai tingkat keamanan yang maksimum dan mampu mem-*block* usaha penyerangan *intruder* dengan berbagai serangan, maka sebaiknya memadukan kedua teknologi keamanan yaitu pemanfaatan *firewall* dengan konsep *Demilitarized Zone* (DMZ) dan *switch port security*.

Referensi

[1] Budi Rahardjo. Security Tools untuk pengamanan, Firewall dan Intrusion Detection System (IDS). IndoCisc.
[2] Haddad Sammir,” Serangan Denial Of Service”, http://www.ilmukomputer.com
[3] Hendrawati, “Desain dan Implementasi Visualisasi Alert Serangan ke Jaringan Komputer”, Tesis Teknik Elektro, 2001

[4] Puji Hartono, *"Sistem Pencegahan Penyusupan pada Jaringan berbasis Snort IDS dan IPTables Firewall",* http://budi.insan.co.id, 2005
[5] Tom Tomas, "*Network Security First Step*", Yogyakarta, 2004
[6] Wack John., Cutler Ken., Pole Jamie., *Guidelines on Firewalls and Firewall Policy*, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology: Gaithersburg, 2002.
[7] Wisnu Baroto, *Memahami Dasar-Dasar Firewall*, PT Elexmedia Komputindo, Jakarta: 2003.
[8] Zwicky ED, Cooper S, Chapman DB. 2000. *Building Internet Firewalls*. Canada : O'Reilly & Associates.