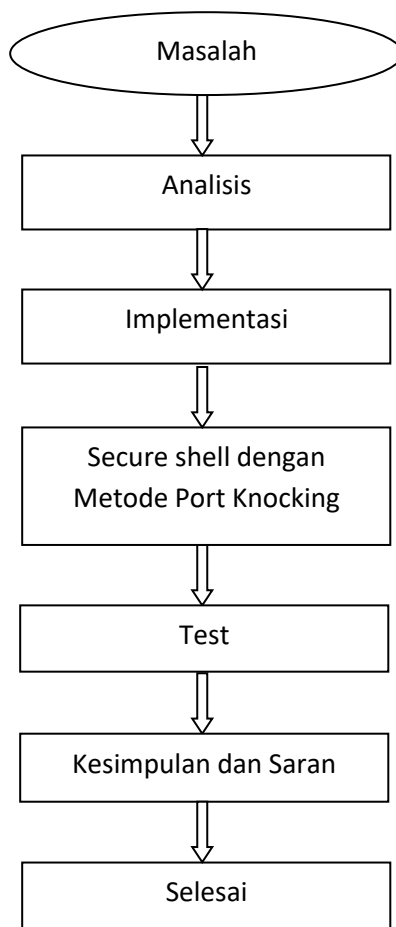


BAB III

METODE PENELITIAN

4.1 Desain Penelitian

Menurut (Sudaryono 2015:3) desain penelitian berisi rumusan tentang langkah-langkah penelitian, dengan pendekatan, metode penelitian, teknik pengumpulan data, dan sumber data tertentu serta alasan-alasan mengapa menggunakan metode tersebut. Sedangkan menurut (Kuncoro 2009) desain penelitian menggambarkan apa yang akan dilakukan oleh peneliti dalam terminologi teknis. (Sudaryono, 2015: 157).



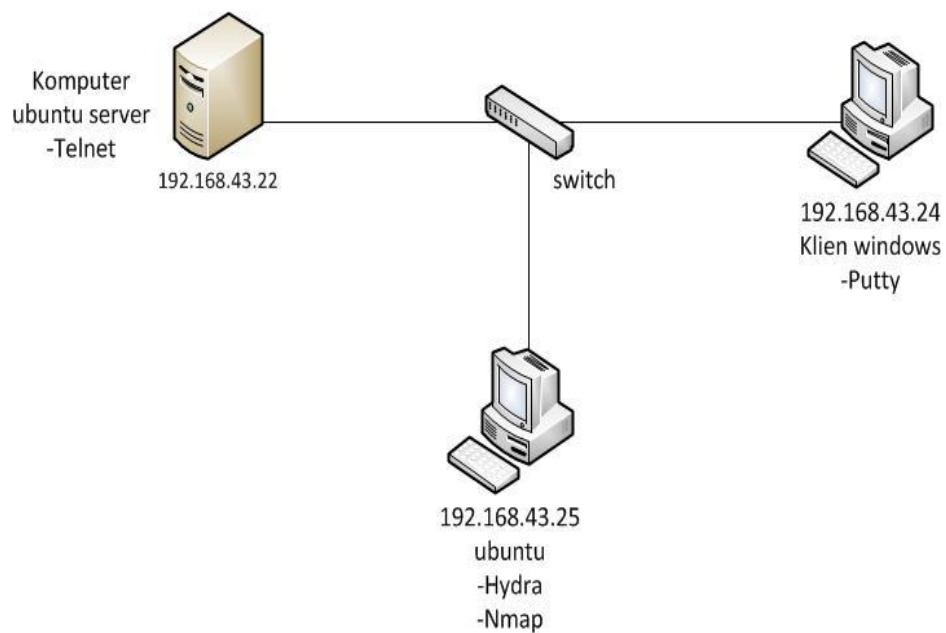
Gambar 3.1 Desain penelitian

4.2 Analisis *Network Security Model Lama*

1. Topologi Jaringan

Topologi jaringan yang dipakai menggunakan satu komputer sebagai klien, satu komputer sebagai *server*, dan satu komputer untuk mengetes proses keamanan jaringan saat melakukan *remote* akses ke *server*. Koneksi *server* pada klien dengan menggunakan *switch*.

Pada *server* memiliki *ip address* 192.168.43.22 dan klien *windows* memiliki *ip address* 192.168.43.24, dan klien *ubuntu* 192.168.43.25. Berikut contoh gambar topologi jaringan lama:



Gambar 3.2 Topologi jaringan

2. *Software yang sedang dipakai*

Server memakai sistem operasi *ubuntu* 16.04.1 LTS. Pada *server ubuntu* diterapkan *telnet server* dengan aplikasi *telnetd* untuk *remote* akses ke *server*. Klien memakai sistem operasi *windows* dengan aplikasi *putty* untuk melakukan proses *remote* ke *server*, dan juga memakai aplikasi *Hydra* dan *Nmap* untuk menguji sistem keamanan pada proses terjadinya *remote* akses ke *server*.

4.3 Implementasi *Network Security Model* Baru

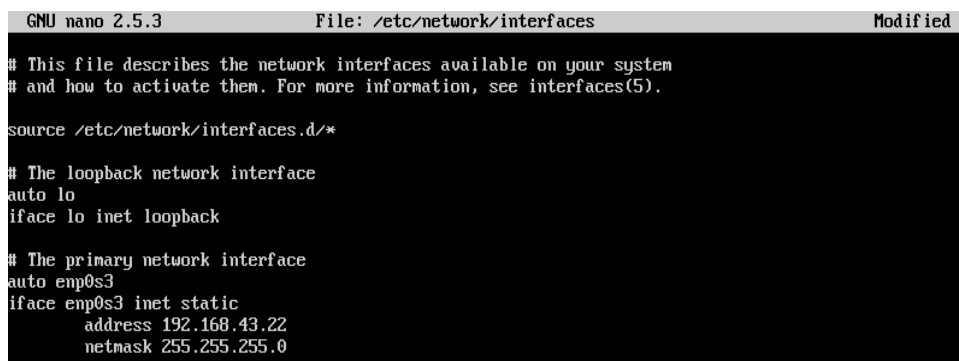
4.3.1 *Software Yang Dipakai*

Pada sistem operasi masih menggunakan *ubuntu* 16.04.1 LTS. *Server* tersebut menerapkan *SSH server* dengan aplikasi *openssh*. Dan metode *port knocking* dengan aplikasi *knockd*. Untuk menguji sistem keamanan saat *remote* ke *server* dengan aplikasi *hydra*, dan untuk *remote* akses masih menggunakan aplikasi *putty*.

4.3.2 Tahapan Rencana Implementasi

Peneliti menyiapkan tiga komputer, satu komputer sebagai *server*, satu komputer sebagai klien, dan satu komputer untuk menguji keamanan *remote* akses. Komputer *server* di *install* dengan sistem operasi *Ubuntu* 16.04.1 LTS. Pada *server* diimplementasikan *secure shell* dan *port knocking* sebagai berikut:

1. Konfigurasi *interfaces* memberi *ip address* 192.168.43.22 *netmask* 255.255.255.0 dan *save* ctrl x pilih *yes* lalu ketik *service networking restart*.



```
GNU nano 2.5.3      File: /etc/network/interfaces      Modified
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
    address 192.168.43.22
    netmask 255.255.255.0
```

Gambar 3.3 *Nano /etc/network/interfaces*

2. *Install openssh.*

```
root@ubuntu:~# apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  openssh-client openssh-sftp-server
Suggested packages:
  ssh-askpass libpam-ssh keychain monkeysphere rssh molly-guard
The following packages will be upgraded:
  openssh-client openssh-server openssh-sftp-server
3 upgraded, 0 newly installed, 0 to remove and 107 not upgraded.
Need to get 1,075 kB of archives.
After this operation, 4,096 B of additional disk space will be used.
Do you want to continue? [Y/n] y_
```

Gambar 3.4 Apt-get install openssh-server

3. Konfigurasi ssh ganti *port* menjadi 3322 dan *permitrootlogin* ganti yes lalu ctrl x pilih yes.

```
GNU nano 2.5.3      File: /etc/ssh/sshd_config      Modified
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 3322
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify     ^C Cur Pos     ^Y Prev Page
^X Exit          ^R Read File    ^_ Replace      ^U Uncut Text  ^T To Spell    ^_ Go To Line   ^U Next Page
```

Gambar 3.5 Nano /etc/ssh/sshd_config

4. *Restart ssh*

```
root@ubuntu:~# service ssh restart
root@ubuntu:~#
```

Gambar 3.6 *Service ssh restart*

5. *Install knockd*

```
root@ubuntu:~# apt-get install knockd
Reading package lists... Done
Building dependency tree
Reading state information... Done
knockd is already the newest version (0.5-3ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 110 not upgraded.
root@ubuntu:~#
```

Gambar 3.7 *Apt-get install knockd*

6. *Install iptables*

```
root@ubuntu:~# apt-get install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables is already the newest version (1.6.0-2ubuntu3).
0 upgraded, 0 newly installed, 0 to remove and 110 not upgraded.
```

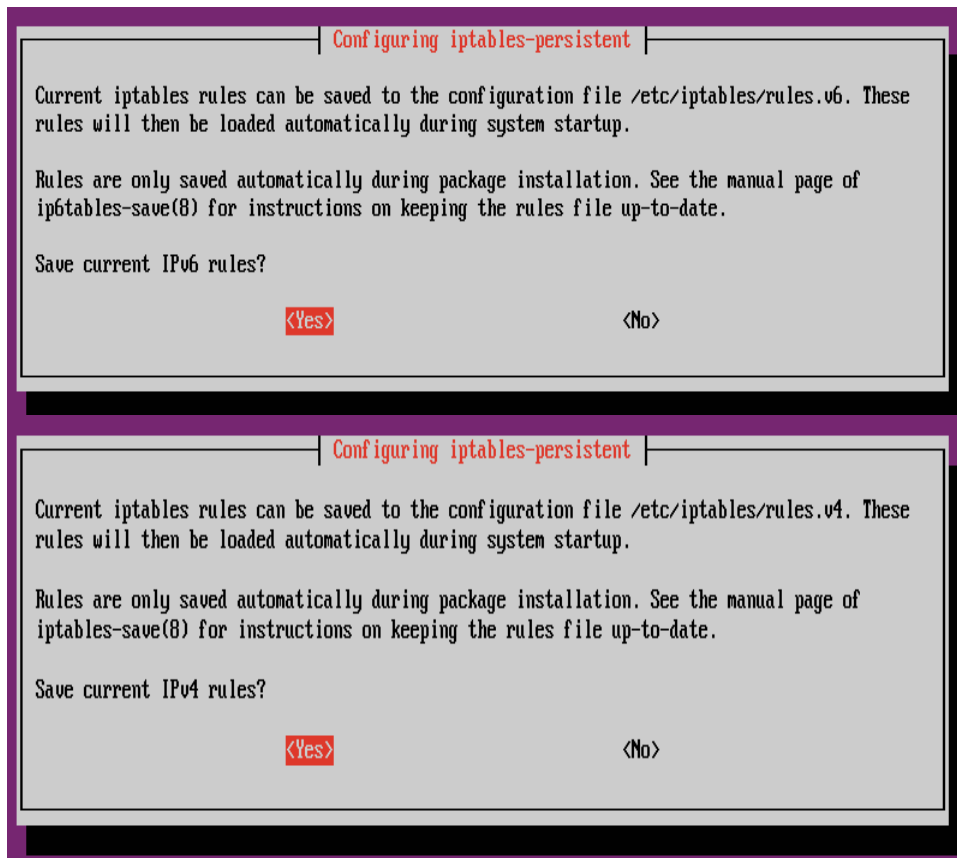
Gambar 3.8 *Apt-get install iptables*

7. *Menambah aturan iptables*

```
root@ubuntu:~# iptables --flush
root@ubuntu:~# iptables -t nat --flush
root@ubuntu:~# iptables -t mangle --flush
root@ubuntu:~# iptables --policy OUTPUT ACCEPT
root@ubuntu:~# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@ubuntu:~# iptables -A INPUT -p tcp --destination-port 3322 -j DROP
```

Gambar 3.9 *Aturan iptables*

8. *Install iptables persistent pilih yes*



Gambar 3.10 Apt-get install iptables-persistent

9. *Iptables-save menyimpan rule iptables yang telah diinput.*

```
root@ubuntu:~# iptables-save
# Generated by iptables-save v1.6.0 on Thu Jan  5 19:16:43 2017
*nat
:PREROUTING ACCEPT [4:864]
:INPUT ACCEPT [4:864]
:OUTPUT ACCEPT [11:813]
:POSTROUTING ACCEPT [11:813]
COMMIT
# Completed on Thu Jan  5 19:16:43 2017
# Generated by iptables-save v1.6.0 on Thu Jan  5 19:16:43 2017
*filter
:INPUT ACCEPT [1:229]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [18:1403]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 3322 -j DROP
COMMIT
# Completed on Thu Jan  5 19:16:43 2017
```

Gambar 3.11 Iptables-save

10. Atur ketukkan *port knocking* pada *sequence* 100 200 300 dan *seq_timeout* 5.

```
GNU nano 2.5.3      File: /etc/knockd.conf

[options]
    UseSyslog
    logfile = /var/log/knockd_log.log
[openSSH]
    sequence      = 100,200,300
    seq_timeout   = 5
    command       = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 3322 -j ACCEPT
    tcpflags      = syn
[closeSSH]
    sequence      = 400,500,600
    seq_timeout   = 5
    command       = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 3322 -j ACCEPT
    tcpflags      = syn
```

Gambar 3.12 Nano /etc/knockd.conf

11. Konfigurasi *default knockd* pada *start_knockd* diganti 1 dan *knockd_opts* diganti *enp0s3*.

```
GNU nano 2.5.3      File: /etc/default/knockd

#####
#
# knockd's default file, for generic sys config
#
#####

# control if we start knockd at init or not
# 1 = start
# anything else = don't start
#
# PLEASE EDIT /etc/knockd.conf BEFORE ENABLING
START_KNOCKD=1

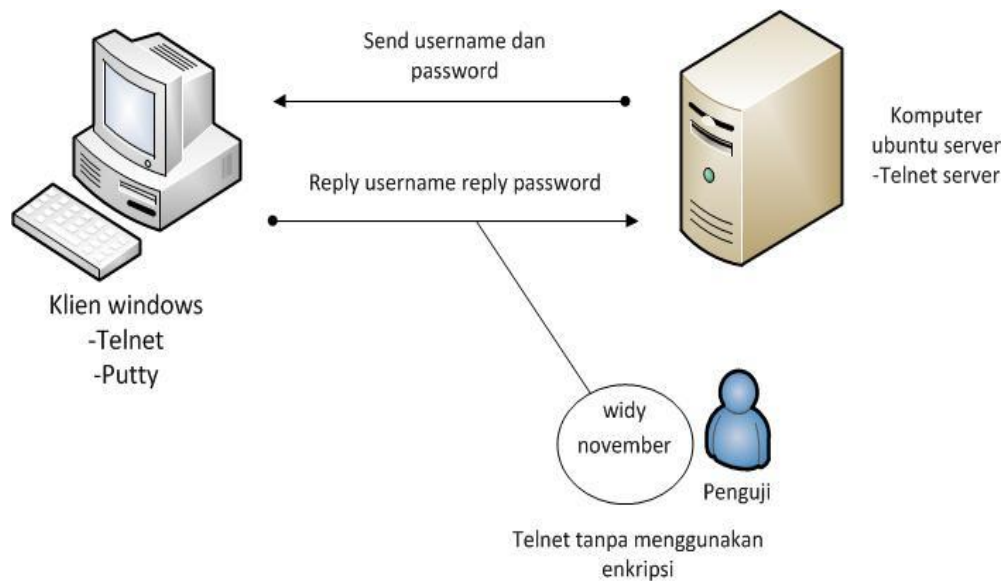
# command line options
KNOCKD_OPTS="-i enp0s3"
```

Gambar 3.13 Nano /etc/default/knockd

Sesudah konfigurasi *knockd* maka ketik *service knockd restart*, untuk menjalankan *knockd* ketik *service knockd start*. Pada komputer *ubuntu* untuk menguji keamanan *remote* akses ke *server* di install aplikasi *hydra* dan *nmap* dengan perintah *apt-get install hydra*, *apt-get install nmap*.

4.3.3 Perbedaan *Network Security Model* Lama dengan Model Baru

1. *Network security model* lama saat terjadi *remote* akses antara klien dan server menggunakan *telnet* tidak terenkripsi berikut contoh gambar:

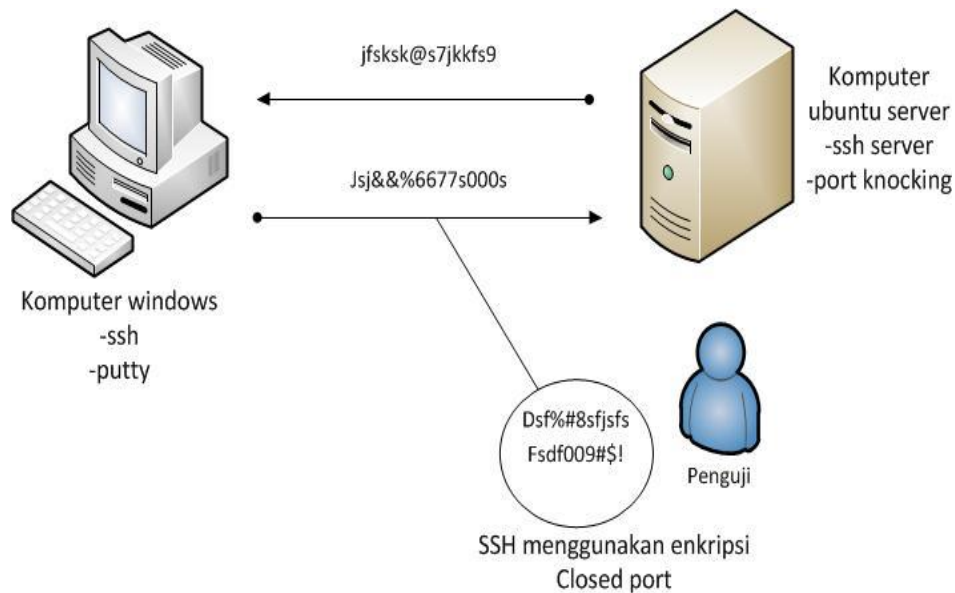


Gambar 3.14 *Telnet*

(Sumber: Burande, *et al.*, 2014: 4)

Pada gambar diatas dalam melakukan *telnet*, klien *windows* memakai aplikasi *putty* untuk melakukan *remote* akses ke server dengan port 23. Dalam aplikasi klien *windows* akan mengirimkan permintaan ke server *telnet*. Server tersebut akan membalas meminta nama pengguna dan kata sandi, jika di terima sama server maka *telnet* klien akan tersambung ke *telnet server*. Dalam proses *remote* akses ke server menggunakan *telnet* tidak menggunakan enkripsi.

2. *Network security model baru pada proses remote akses antara klien dan server terenkripsi dan juga harus melalui port knocking yang telah di atur berikut contoh gambar:*



Gambar 3.15 Ssh dengan metode *port knocking*

(Sumber: Burande, *et al.*, 2014: 4)

Pada gambar diatas dalam melakukan proses *remote* akses ke *server*, komputer *windows* memakai aplikasi *putty* dan melalui *port* 3322. *Port* tersebut di tutup dengan metode *port knocking* dan diatur berapa ketukan sesuai *port* berapa yang diinginkan. Ssh memiliki kunci *public* dan *private* dalam identitasnya. Klien *windows* melakukan otentikasi ke *server* dengan kunci *public* dan *private* yang sama dengan *server*, juga menggunakan *username* dan *password*.

4.4 Lokasi dan Jadwal Penelitian

4.4.1 Lokasi Penelitian

Lokasi penelitian dilakukan pada komplek Batam Executive Centre Blok E
No.15.

4.4.2 Jadwal Penelitian

Penelitian akan dilakukan selama 5 bulan dimulai dari September 2016 sampai dengan Januari 2017 dapat dilihat pada tabel berikut ini:

Tabel 3.1 Jadwal Penelitian

No	Kegiatan	Sep 2016				Okt 2016				Nov 2016				Des 2016				Jan 2017			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Pengajuan judul																				
2	Pengajuan surat ijin penelitian																				
3	Analisis Masalah																				
4	Implementasi SSH dan Port knocking																				
5	Pengujian																				
6	Laporan																				