



POLITEKNIK NEGERI MANADO JURUSAN TEKNIK ELEKTRO

MODUL PRAKTIKUM KEAMANAN JARINGAN



**JURUSAN TEKNIK ELEKTRO
PROGRAM STUDI TEKNIK KOMPUTER
POLITEKNIK NEGERI MANADO**

LEMBAR PENGESAHAN

PRAKTIKUM KEMAMAN JARINGAN

Oleh :
ROBY STEVI LUMBU, SST., MT

Manado, November 2019

Menyetujui,

Ketua Jurusan Teknik Elektro

Koordinator Program Studi,



Fanny J Doringin,
ST.,MT

NIP. 96704301992031003



Marson James Budiman,
SST.,MT

NIP.

197503052003121002

Mengetahui,

Wakil Direktur Bidang Akademik,



Dra. Maryke Alelo, MBA

NIP. 19641213 199103 2 001

DAFTAR ISI

LEMBAR PENGESAHAN.....	i
KATA PENGANTAR.....	ii
DAFTAR ISI.....	iii

MODUL 1 NETWORK SCANNING DAN PROBING

1.1.Tujuan.....	1
1.2.Dasar Teori.....	1
1.3.Tipe-Tipe Scanning	
1.3.1. Connect Scan (-St).....	3
1.3.2. -Ss (Tcp Syn Scan).....	3
1.3.3. Cp Fin Scan (-Sf).....	3
1.3.4. Tcp Xmas Tree Scan (-Sx).....	3
1.3.5. Tcp Null Scan (-Sn).....	3
1.3.6. Tcp Ack Scan (-Sa).....	4
1.3.7. Tcp Windows Scan.....	4
1.3.8. Tcp Rpc Scan.....	4
1.3.9. Udp Scan (-Su).....	4
1.4.Kegiatan Praktikum.....	4
1.4.1.Peralatan.....	4
1.4.2.Topologi Jaringan.....	5
1.4.3.Langkah Kerja.....	5
1.5.Penjelasan.....	15
MODUL 2.....	16
Tujuan.....	16
Dasar Teori.....	16
Kegiatan Praktikum.....	19
2.3.1.Peralatan.....	19
2.3.2.Topologi Jaringan.....	19

2.3.3.Langkah Kerja.....	19
Penjelasan.....	26
MODUL 3.....	27
3.1. Tujuan.....	27
3.2. Teori Dasar.....	27
3.3. Kegiatan Praktikum.....	29
3.3.1.Peralatan.....	29
3.3.2.Topologi.....	29
3.3.3.Langkah Kerja.....	30
3.4. Penjelasan.....	33
MODUL 4.....	34
4.1.Tujuan.....	34
4.2.Teori Dasar.....	34
4.3.Kegiatan Praktikum.....	37
4.3.1.Peralatan.....	37
4.3.2.Topologi.....	37
4.3.3.Langkah Kerja.....	37
4.4.Kesimpulan.....	40
 MODUL 5	
5.1.Tujuan.....	41
5.2.Dasar Teori.....	41
5.2.1.Portsentry.....	41
5.2.2.Honeypot.....	42
5.2.2.1. High Interaction Honeypot.....	43
5.2.2.2. Low Interaction Honeypot.....	43
5.3.KEGIATAN PRAKTIKUM.....	43
5.3.1.Peralatan.....	43
5.3.2.Topologi Jaringan.....	44
5.3.3.Langkah Kerja.....	44

5.4.KESIMPULAN.....	52
MODUL 6 INTRUSION DETECTION SYSTEM [TRIPWIRE].....	53
6.1.Tujuan.....	53
6.2.Teori Dasar.....	53
6.2.1.Tripwire.....	53
6.3.Kegiatan Praktikum.....	54
6.3.1.Peralatan.....	54
6.3.2.Topologi Jaringan.....	54
6.3.3.Langkah Kerja.....	55
6.4.Kesimpulan.....	59
MODUL 7 SYMMETRIC CRYPTOGRAPHY.....	60
7.1.Tujuan.....	60
7.2.Teori Dasar.....	60
7.3.Kegiatan Rangkuman.....	66
7.3.1.Peralatan.....	66
7.3.2.Topologi Jaringan.....	66
7.3.3.Langkah Kerja.....	67
7.4.Kesimpulan.....	78
MODUL 8 ASYMMETRIC CRYPTOGRAPHY.....	79
8.1.Tujuan.....	79
8.2.Teori Dasar.....	79
8.2.1.PGP Secara Umum.....	79
8.2.2.GnuPG.....	80
8.3.Kegiatan Rangkuman.....	82
8.3.1.Peralatan.....	82
8.3.2.Topologi Jaringan.....	82
8.3.3.Langkah Kerja.....	83
8.4.Kesimpulan.....	92

MODUL 1

NETWORK SCANNING DAN PROBING

1.1. Tujuan

- Mengenalkan pada mahasiswa tentang konsep Scanner dan Probing
- Mahasiswa memahami konsep layanan jaringan dan port numbering
- Mahasiswa mampu menganalisa kelemahan jaringan menggunakan software scanning yang ada

1.2. Dasar Teori

Server tugasnya adalah melayani client dengan menyediakan service yang dibutuhkan. Server menyediakan service dengan bermacam-macam kemampuan, baik untuk lokal maupun remote. Server listening pada suatu port dan menunggu incoming connection ke port. Koneksi bisa berupa lokal maupun remote.

Port sebenarnya suatu alamat pada stack jaringan kernel, sebagai cara dimana transport layer mengelola koneksi dan melakukan pertukaran data antar komputer. Port yang terbuka mempunyai resiko terkait dengan exploit. Perlu dikelola port mana yang perlu dibuka dan yang ditutup untuk mengurangi resiko terhadap exploit.

Ada beberapa utility yang bisa dipakai untuk melakukan diagnosa terhadap sistem service dan port kita. Utility ini melakukan scanning terhadap sistem untuk mencari port mana saja yang terbuka, ada juga sekaligus memberikan laporan kelemahan sistem jika port ini terbuka.

Port Scanner merupakan program yang didesain untuk menemukan layanan (service) apa saja yang dijalankan pada host jaringan. Untuk mendapatkan akses ke host, cracker harus mengetahui titik-titik kelemahan yang ada. Sebagai contoh, apabila cracker sudah mengetahui bahwa host menjalankan proses ftp server, ia dapat menggunakan kelemahan-kelemahan yang ada pada ftp server untuk mendapatkan akses. Dari bagian ini kita dapat mengambil kesimpulan bahwa layanan yang tidak benar-benar diperlukan sebaiknya dihilangkan untuk memperkecil resiko keamanan yang mungkin terjadi.

▫ VirtualBox

VirtualBox adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi "tambahan" di dalam sistem operasi "utama". atau bias dikatakan sebagai tempat untuk simulasi sebuah sistem operasi. Virtual box dapat digunakan jika kita ingin menginstal atau mencoba sebuah sistem operasi di computer kita.

▫ Penjelasan Wireshark

Wireshark merupakan Network Protocol Analyzer, juga termasuk salah satu network analysis tool atau packet sniffer. Wireshark memungkinkan pengguna mengamati data dari jaringan yang sedang beroperasi atau dari data yang ada di disk, dan langsung melihat dan mensortir data yang tertangkap, mulai dari informasi singkat dan detail bagi masing masing paket termasuk full header dan porsi data, dapat diperoleh. Dan dalam hal penggunaannya, mudah untuk dipelajari dan dimengerti.

▫ Penjelasan Openvas

OpenVAS (Open Vulnerability Assessment System) merupakan Tools yang banyak digunakan untuk mencari celah keamanan dan menguji keamanan sebuah sistem. OpenVAS hampir sama dengan Nessus (Tools yang banyak digunakan untuk melakukan scanning pada web) bedanya OpenVAS ini Open Source (Terbuka)

▫ Kelebihan OpenVAS:

- Powerful Vulnerability Scanning Solution Management
- Intelligent Custom scan
- Detailed Reporting Risk Assessment Remediation

▫ Kurangnya OpenVAS:

- Biasanya sulit digunakan untuk menemukan Issue tertentu. biasanya organisasi atau administrator di perusahaan besar lebih senang menggunakan Versi berbayar seperti

▫ Penjelasan Nmap

Nmap ("Network Mapper") merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw

dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya.

Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan.

1.3. Tipe-Tipe Scanning

1.3.1. Connect Scan (-St)

Jenis scan ini konek ke port sasaran dan menyelesaikan three-way handshake (SYN, SYN/ACK, dan ACK). Scan jenis ini mudah terdeteksi oleh sistem sasaran.

1.3.2. -Ss (TCP SYN Scan)

Paling populer dan merupakan scan default nmap. SYN scan juga sukar terdeteksi, karena tidak menggunakan 3 way handshake secara lengkap, yang disebut sebagai teknik half open scanning. SYN scan juga efektif karena dapat membedakan 3 state port, yaitu open, filtered ataupun close. Teknik ini dikenal sebagai half-opening scanning karena suatu koneksi penuh TCP tidak sampai terbentuk. Sebaliknya, suatu paket SYN dikirimkan ke port sasaran. Bila SYN/ACK diterima dari port sasaran, kita dapat mengambil kesimpulan bahwa port itu berada dalam status LISTENING. Suatu RST/ACT akan dikirim oleh mesin yang melakukan scanning sehingga koneksi penuh tidak akan terbentuk. Teknik ini bersifat siluman dibandingkan TCP connect penuh, dan tidak akan tercatat pada log sistem sasaran.

1.3.3. TCP FIN Scan (-Sf)

Teknik ini mengirim suatu paket FIN ke port sasaran. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk setiap port yang tertutup. Teknik ini hanya dapat dipakai pada stack TCP/IP berbasis UNIX.

1.3.4. CP Xmas Tree Scan (-Sx)

Teknik ini mengirimkan suatu paket FIN, URG, dan PUSH ke port sasaran. Berdasarkan RFC 793, sistem sasaran akan mengembalikan suatu RST untuk semua port yang tertutup.

1.3.5. TCP Null Scan (-Sn)

Teknik ini membuat off semua flag. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk semua port yang tertutup.

1.3.6.CP ACK Scan (-Sa)

Teknik ini digunakan untuk memetakan set aturan firewall. Dapat membantu menentukan apakah firewall itu merupakan suatu simple packet filter yang membolehkan hanya koneksi-koneksi tertentu (koneksi dengan bit set ACK) atau suatu firewall yang menjalankan advance packet filtering.

1.3.7.CP Windows Scan

Teknik ini dapat mendeteksi port-port terbuka maupun terfilter/tidak terfilter pada sistem sistem tertentu (sebagai contoh, AIX dan FreeBSD) sehubungan dengan anomali dari ukuran windows TCP yang dilaporkan.

1.3.8.TCP RPC Scan

Teknik ini spesifik hanya pada system UNIX dan digunakan untuk mendeteksi dan mengidentifikasi port RPC (Remote Procedure Call) dan program serta normor versi yang berhubungan dengannya.

1.3.9.UDP Scan (-Su)

Teknik ini mengirimkan suatu paket UDP ke port sasaran. Bila port sasaran memberikan respon berupa pesan (ICMP port unreachable) artinya port ini tertutup. Sebaliknya bila tidak menerima pesan di atas, kita dapat menyimpulkan bahwa port itu terbuka. Karena UDP dikenal sebagai connectionless protocol, akurasi teknik ini sangat bergantung pada banyak hal sehubungan dengan penggunaan jaringan dan system resource. Sebagai tambahan, UDP scanning merupakan proses yang amat lambat apabila anda mencoba men-scan suatu perangkat yang menjalankan packet filtering berbeban tinggi.

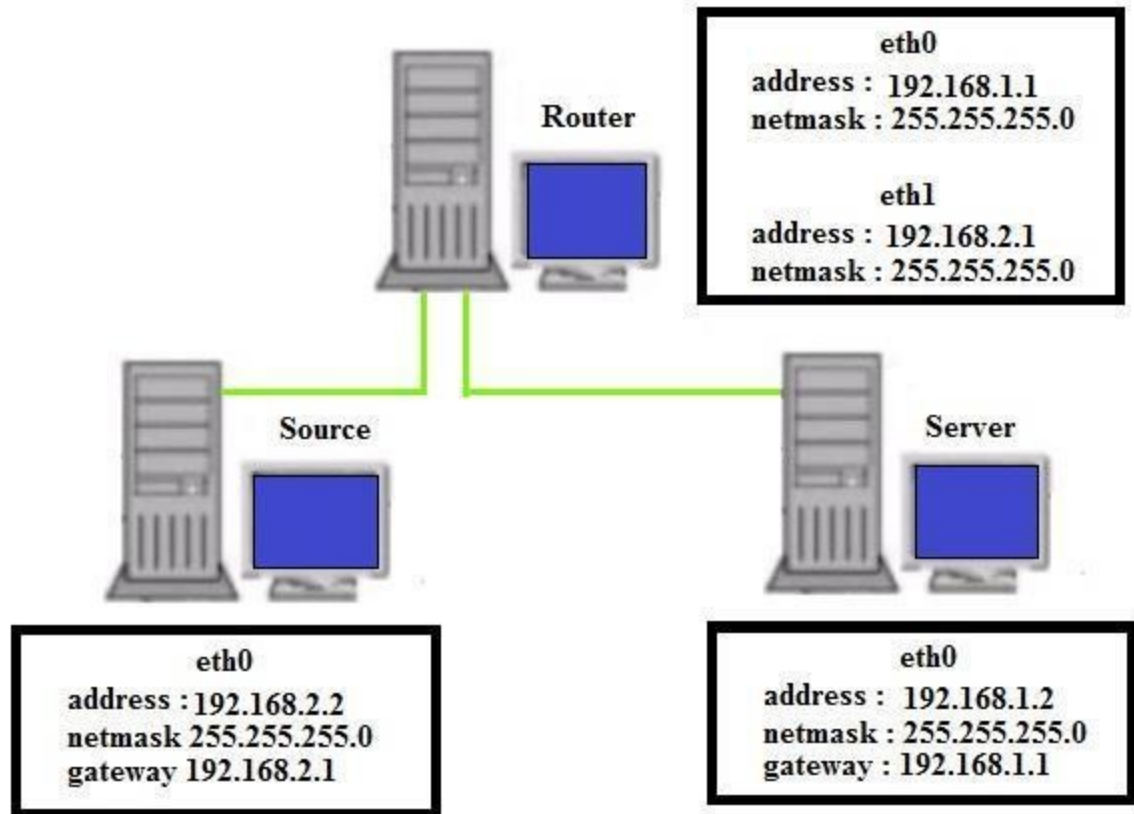
1.4.KEGIATAN PRAKTIKUM

1.4.1.Peralatan

Alat dan bahan

- ▣ 1 buah laptop
- ▣ Virtual Machine(VirtualBox/VMware)
- ▣ ISO : Debian6

1.4.2. Topologi Jaringan



1.4.3. Langkah Kerja

- 1) Instal Virtualbox
- 2) Setelah Virtualbox terinstall lanjutkan dengan menginstal Sistem Operasi (Debian) buat 3 sistem operasi diClone hingga menjadi 2 Sistem Operasi untuk server dan router.
- 3) Lakukan konfigurasi IP Server, IP Router, dan IP Client dengan perintah “nano /etc/network/interfaces”.

```
File Edit View Terminal Help
GNU nano 2.2.4 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
#NetworkManager
auto eth0
iface eth0 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    gateway 192.168.1.1

[ Read 15 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^L UnCut Text ^T To Spell
```

Gambar 1.1 Settingan IP Server

```
File Edit View Terminal Help
GNU nano 2.2.4 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#allow-hotplug eth0
#NetworkManager
auto eth0
iface eth0 inet static
    address 192.168.1.1
    netmask 255.255.255.0

auto eth1
iface eth1 inet static
    address 192.168.2.1
    netmask 255.255.255.0

[ Read 19 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^L UnCut Text ^T To Spell
```

Gambar 1.2 Settingan IP Router

```

File Edit View Terminal Help
GNU nano 2.2.4 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#allow-hotplug eth0
#NetworkManager
auto eth0
iface eth0 inet static
    address 192.168.2.2
    netmask 255.255.255.0
    gateway 192.168.2.1

[ Read 16 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^L UnCut Text ^T To Spell

```

Gambar 1.3 Settingan IP Client

- 4) Setelah selesai mengkonfigurasi IP, masukkan perintah “Ctrl+x+y enter” perintah tersebut untuk menyimpan dan keluar dari interfaces tersebut. Selanjutnya hubungkan ke 3 Sistem Operasi dan diuji PING IP.

```

File Edit View Terminal Help
root@susan:/home/susan# ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_req=1 ttl=64 time=0.023 ms
64 bytes from 192.168.2.2: icmp_req=2 ttl=64 time=0.039 ms
64 bytes from 192.168.2.2: icmp_req=3 ttl=64 time=0.020 ms
64 bytes from 192.168.2.2: icmp_req=4 ttl=64 time=0.021 ms
^C
--- 192.168.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.020/0.025/0.039/0.009 ms
root@susan:/home/susan# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_req=1 ttl=64 time=3.57 ms
64 bytes from 192.168.1.1: icmp_req=2 ttl=64 time=0.416 ms
64 bytes from 192.168.1.1: icmp_req=3 ttl=64 time=0.674 ms
64 bytes from 192.168.1.1: icmp_req=4 ttl=64 time=0.722 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.416/1.346/3.574/1.291 ms
root@susan:/home/susan# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=64 time=3.94 ms
64 bytes from 192.168.1.2: icmp_req=1 ttl=63 time=3.95 ms (DUP!)

```

Gambar 1.4 ping

5) Pada server install wireshark ,apache,proftpd,telnetd,dan

```
ssh #apt-get install wireshark
```

```
#apt-get install apache2
```

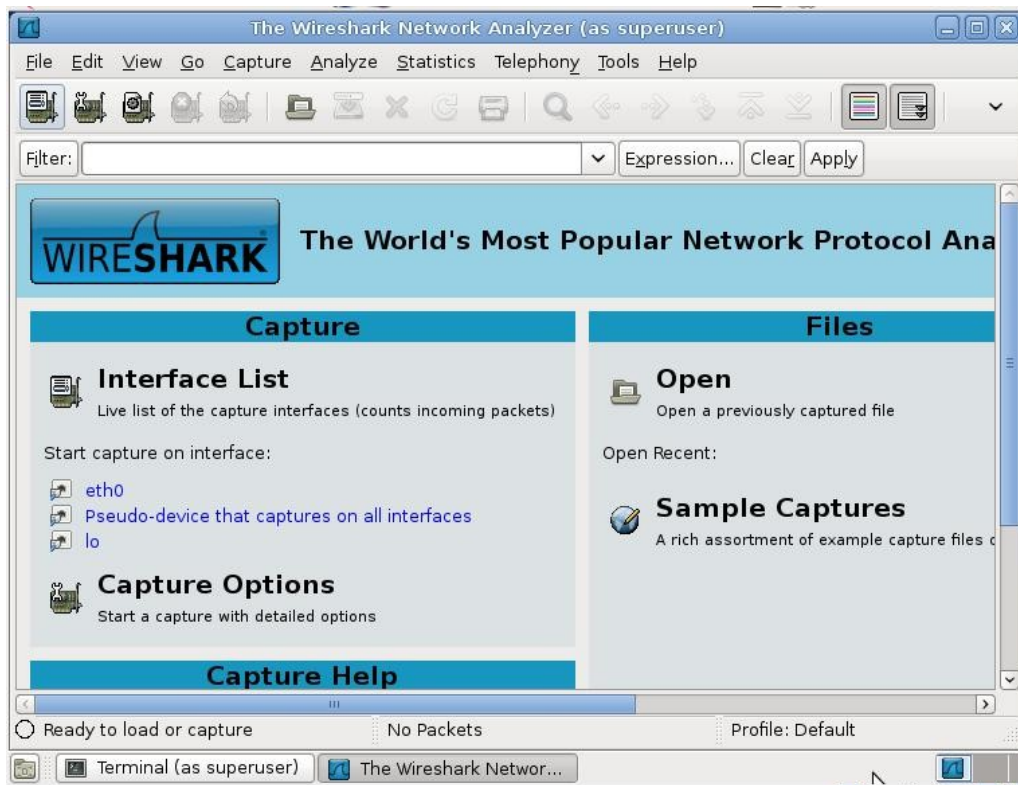
```
#apt-get install proftpd
```

```
#apt-get install telnetd
```

```
#apt-get install ssh
```

Setelah wireshark terpasang, buka wireshark pilih eth0

```
#wireshark
```



Gambar 1.5 Wireshark

6) Di client install nmap

```
#apt-get install nmap
```

Kemudian

```
#nmap -sT -v 192.168.1.2 (IP server)
```

```
#nmap -sS -v 192.168.1.2 (IP server)
```

```
#nmap -O -v 192.168.1.2 (IP server)
```

```
#nmap -sF -v 192.168.1.2 (IP server)
```

```
File Edit View Terminal Help
Scanning 192.168.1.2 [4 ports]
Completed Ping Scan at 07:15, 0.01s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
  Try using --system-dns or specify valid servers with --dns-servers
Initiating Connect Scan at 07:15
Scanning 192.168.1.2 [1000 ports]
Discovered open port 21/tcp on 192.168.1.2
Discovered open port 111/tcp on 192.168.1.2
Discovered open port 53/tcp on 192.168.1.2
Discovered open port 80/tcp on 192.168.1.2
Discovered open port 22/tcp on 192.168.1.2
Completed Connect Scan at 07:15, 0.47s elapsed (1000 total ports)
Host 192.168.1.2 is up (0.0037s latency).
Interesting ports on 192.168.1.2:
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

Gambar 2.1 nmap -sT -v 192.168.1.2

```
File Edit View Terminal Help
root@susan:/home/susan# nmap -sS -v 192.168.1.2

Starting Nmap 5.00 ( http://nmap.org ) at 2017-02-15 07:17 PST
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 07:17
Scanning 192.168.1.2 [4 ports]
Completed Ping Scan at 07:17, 0.00s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
  Try using --system-dns or specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 07:17
Scanning 192.168.1.2 [1000 ports]
Discovered open port 21/tcp on 192.168.1.2
Discovered open port 22/tcp on 192.168.1.2
Discovered open port 111/tcp on 192.168.1.2
Discovered open port 53/tcp on 192.168.1.2
Completed SYN Stealth Scan at 07:17, 0.44s elapsed (1000 total ports)
Host 192.168.1.2 is up (0.0019s latency).
Interesting ports on 192.168.1.2:
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
111/tcp   open  rpcbind
```

Gambar 2.2 nmap -sS -v 192.168.1.2

```
File Edit View Terminal Help
root@susan:/home/susan# nmap -sF -v 192.168.1.2

Starting Nmap 5.00 ( http://nmap.org ) at 2017-02-15 07:19 PST
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 07:19
Scanning 192.168.1.2 [4 ports]
Completed Ping Scan at 07:19, 0.01s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Initiating FIN Scan at 07:19
Scanning 192.168.1.2 [1000 ports]
Completed FIN Scan at 07:19, 1.57s elapsed (1000 total ports)
Host 192.168.1.2 is up (0.0017s latency).
Interesting ports on 192.168.1.2:
Not shown: 995 closed ports
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
```

Gambar 2.3 nmap -sF -v 192.168.1.2

```
root@susan:/home/susan# nmap -O -v 192.168.1.2

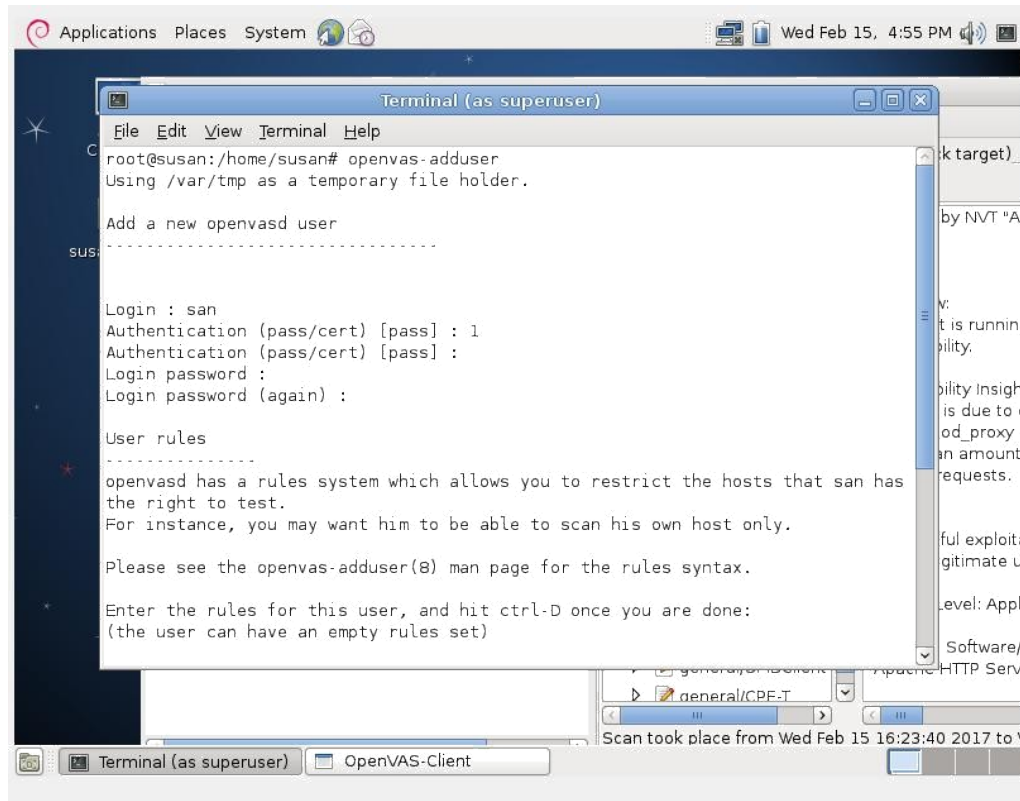
Starting Nmap 5.00 ( http://nmap.org ) at 2017-02-15 19:09 PST
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 19:09
Scanning 192.168.1.2 [4 ports]
Completed Ping Scan at 19:09, 3.01s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Read data files from: /usr/share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -PN
Nmap done: 1 IP address (0 hosts up) scanned in 3.63 seconds
Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
root@susan:/home/susan# █
```

Gambar 2.4 nmap -O -v 192.168.1.2

- 7) Pastikan pada client openvas sudah terinstall
- 8) Konfigurasi openvas di client

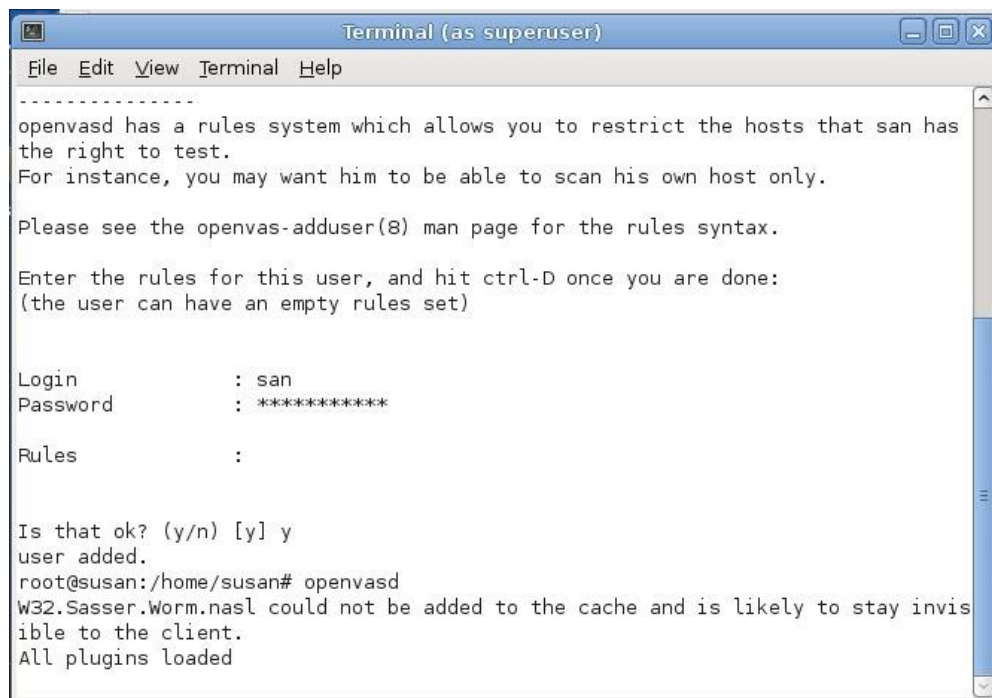
Lakukan perintah

➤ # openvas-adduser



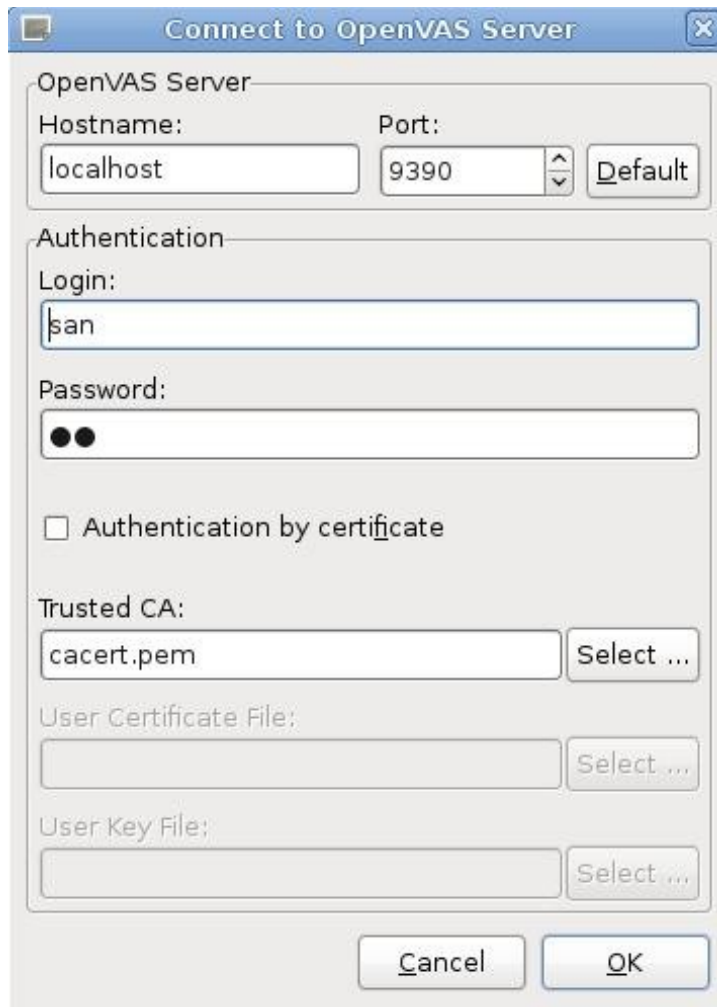
Gambar 2.5

openvasd



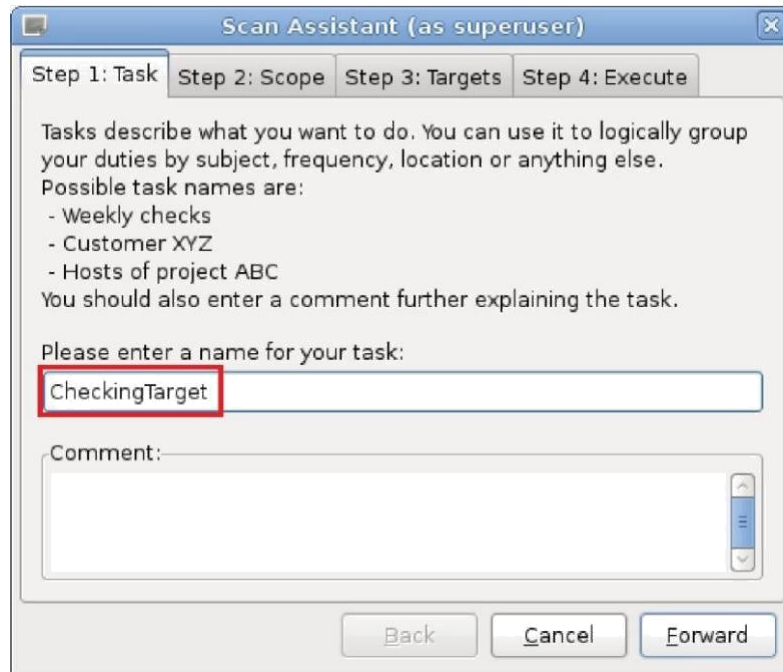
9) Selanjutnya pada client pilih applications > accessories > openvas-client

10) Setelah terbuka openvas pilih > file > connect



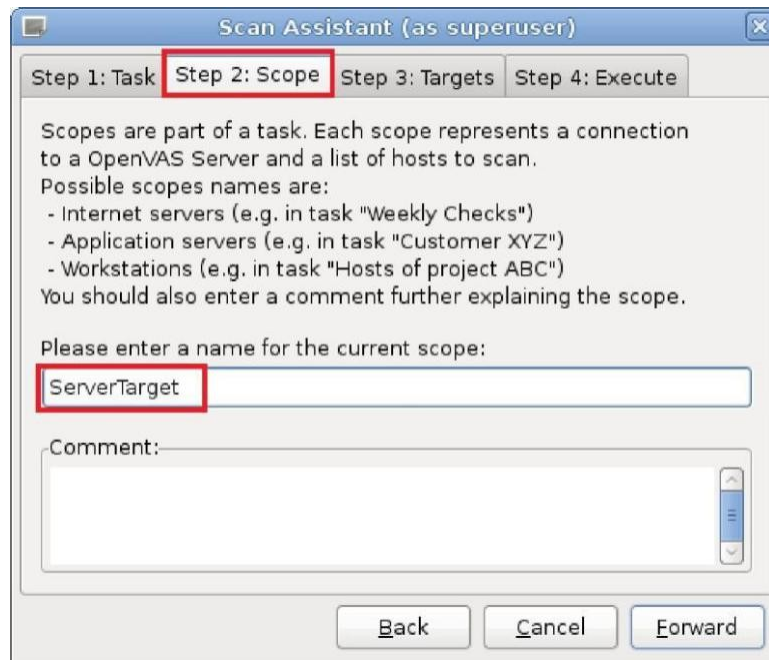
Gambar 3.2

11) Setelah itu buka openvas pilih > file > scan assistant-Untuk Task, beri nama misal :
CheckingTarget



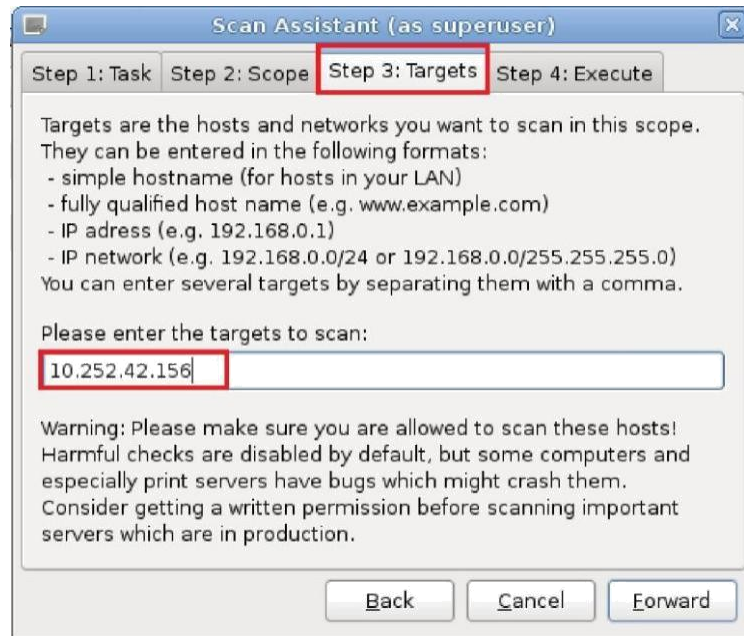
Gambar 3.3

- Pada tab Scope, beri nama : ServerTarget



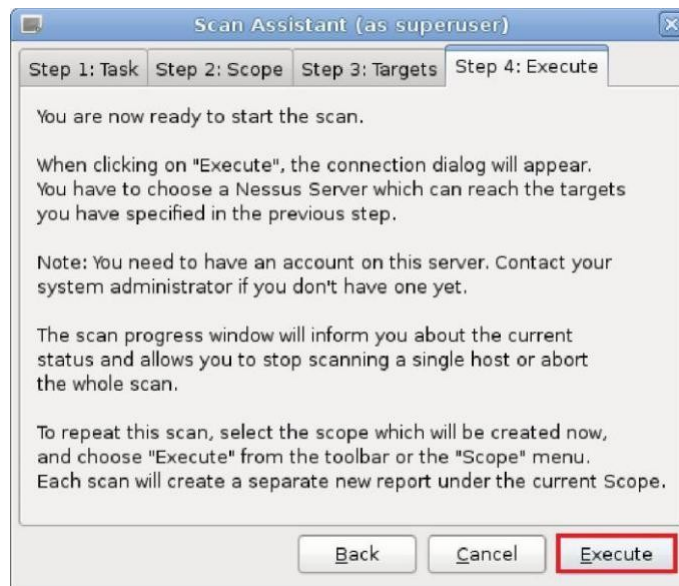
Gambar 3.4

- Pilih Target dan masukkan IP yang akan discan.



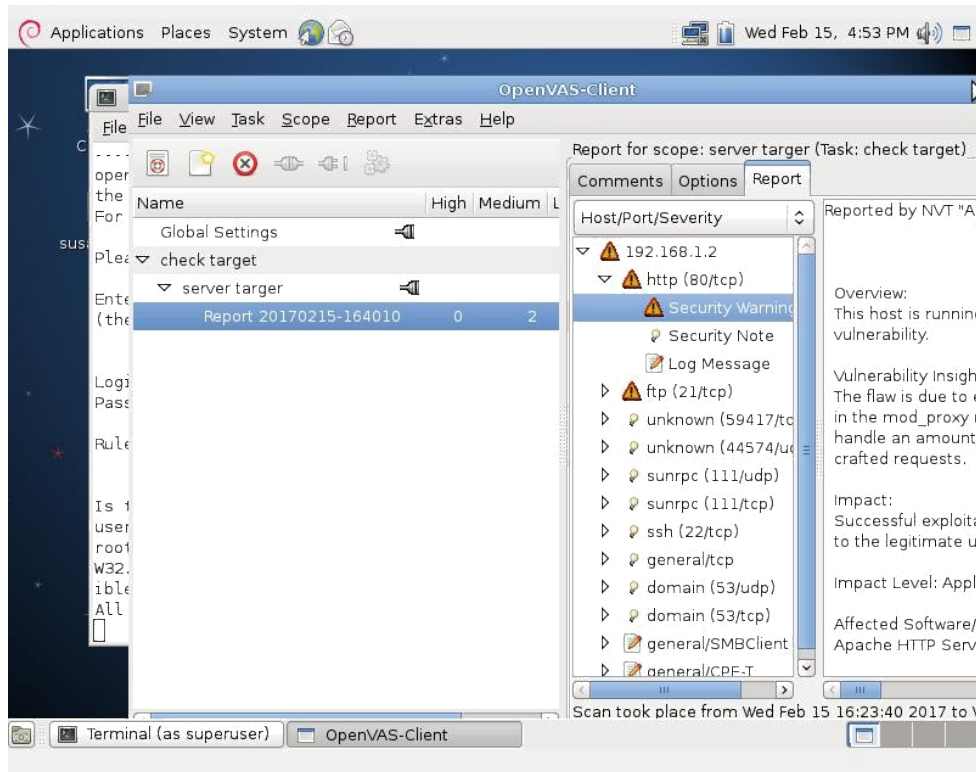
Gambar 3.5

- Sebelum pilih Execut, jalankan server dan router terlebih dulu



Gambar 4.1

12) Hasil scanning sebagai berikut



Gambar 4.2 tampilan pada openvas-client.

1.5. Penjelasan

-Seperti pada gambar di atas pada server target > Report20170215-164010, terdapat informasi tentang keamanan pada port dan port 21.

MODUL 2
Network Security
Enumeration & Password Management

2.1 Tujuan

1. Mengenalkan pada mahasiswa tentang konsep Scanner dan Probing.
2. Mahasiswa memahami konsep layanan jaringan dan port numbering.
3. Mahasiswa mampu menganalisa kelemahan jaringan menggunakan software scanning yang ada.

2.2 Dasar Teori

Untuk dapat mengakses sistem operasi Linux digunakan mekanisme password. Pada distribusi-distribusi Linux yang lama, password tersebut disimpan dalam suatu file teks yang

terletak di `/etc/passwd`. File ini harus dapat dibaca oleh setiap orang (world readable) agar dapat digunakan oleh program-program lain yang menggunakan mekanisme password tersebut.

Contoh isi file `/etc/passwd` :

```
root:..CETo68esYsA:0:0:root:/root:/bin/bash
bin:jvXHHBGCK7nkg:1:1:bin:/bin:
daemon:i1YD6CckS:2:2:daemon:/sbin:
adm:bj2NcvrnubUqU:3:4:adm:/var/adm:
rms:x9kxv932ckadsf:100:100:Richard M Stallman:/home/rms:/bin/bash
dmr:ZeoW7CaIcQmjhl:101:101:Dennis M
Ritchie:/home/dmr:/bin/bash
linus:IK40Bb5NnkAHk:102:102:Linus
Torvalds:/home/linus:/bin/bash
```

Field pertama : nama login

Field kedua : password yang terenkripsi

Field ketiga : User ID

Field keempat : Group ID

Field kelima : Nama sebenarnya

Field keenam : Home directory user

Field ketujuh : User Shell

Password login yang terdapat pada file `/etc/passwd` dienkripsi dengan menggunakan algoritma DES yang telah dimodifikasi. Meskipun demikian hal tersebut tidak mengurangi kemungkinan password tersebut dibongkar (crack). Karena penyerang (attacker) dapat melakukan dictionary-based attack dengan cara :

- a. menyalin file `/etc/passwd` tersebut
- b. menjalankan program-program yang berguna untuk membongkar password, contohnya adalah John the Ripper (www.openwall.com/john/).

Untuk mengatasi permasalahan ini pada distribusi-distribusi Linux yang baru digunakan program utility shadow password yang menjadikan file `/etc/passwd` tidak lagi berisikan informasi password yang telah dienkripsi, informasi tersebut kini disimpan pada file `/etc/shadow` yang hanya dapat dibaca oleh root.

Berikut ini adalah contoh file `/etc/passwd` yang telah di-shadow :

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
rms:x:100:100:Richard M Stallman:/home/rms:/bin/bash
dmr:x:101:101:Dennis M Ritchie:/home/dmr:/bin/bash
linus:x:102:102:Linus Torvalds:/home/linus:/bin/bash
```

Dengan demikian, penggunaan shadow password akan mempersulit attacker untuk melakukan dictionary-based attack terhadap file password.

Selain menggunakan shadow password beberapa distribusi Linux juga menyertakan program hashing MD5 yang menjadikan password yang dimasukkan pemakai dapat berukuran panjang dan relatif mudah diingat karena berupa suatu passphrase.

Mekanisme yang telah disediakan sistem operasi tersebut di atas tidaklah bermanfaat bila pemakai tidak menggunakan password yang "baik". Berikut ini adalah beberapa kriteria yang dapat digunakan untuk membuat password yang "baik" :

1. Jangan menggunakan nama login anda dengan segala variasinya.
2. Jangan menggunakan nama pertama atau akhir anda dengan segala variasinya.
3. Jangan menggunakan nama pasangan atau anak anda.

4. Jangan menggunakan informasi lain yang mudah didapat tentang anda, seperti nomor telpon, tanggal lahir.
5. Jangan menggunakan password yang terdiri dari seluruhnya angka ataupun huruf yang lama.
6. Jangan menggunakan kata-kata yang ada di dalam kamus, atau daftar kata lainnya.
7. Jangan menggunakan password yang berukuran kurang dari enam karakter.
8. Gunakan password yang merupakan campuran antara huruf kapital dan huruf kecil.
9. Gunakan password dengan karakter-karakter non-alfabet.
10. Gunakan password yang mudah diingat, sehingga tidak perlu ditulis.
11. Gunakan password yang mudah diketikkan, tanpa perlu melihat pada keyboard.

Beberapa tool yang bisa dipakai untuk melihat strong tidaknya password adalah john the ripper. Kita bisa memakai utility ini untuk melihat strong tidaknya suatu password yang ada pada komputer.

▫ Wireshark

Wireshark merupakan Network Protocol Analyzer, juga termasuk salah satu network analysis tool atau packet sniffer. Wireshark memungkinkan pengguna mengamati data dari jaringan yang sedang beroperasi atau dari data yang ada di disk, dan langsung melihat dan mensortir data yang tertangkap, mulai dari informasi singkat dan detail bagi masing-masing paket termasuk full header dan porsi data, dapat diperoleh. Dan dalam hal penggunaannya, mudah untuk dipelajari dan dimengerti.

▫ FTP

Protokol pengiriman berkas (bahasa Inggris: File Transfer Protocol) adalah sebuah protokol Internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pengiriman berkas (file) komputer antar mesin-mesin dalam sebuah Antarmuka Jaringan. FTP merupakan salah satu protokol Internet yang paling awal dikembangkan, dan masih digunakan hingga saat ini untuk melakukan pengunduhan (download) dan pengunggahan (upload) berkas-berkas komputer antara klien FTP dan server FTP.

▫ SSH

Secure Shell (SSH) adalah sebuah protokol jaringan kriptografi untuk komunikasi data yang aman, login antarmuka baris perintah, perintah eksekusi jarak jauh, dan layanan jaringan lainnya antara dua jaringan komputer. Ini terkoneksi, melalui saluran aman atau

melalui jaringan tidak aman, server dan klien menjalankan server SSH dan SSH program klien secara masing-masing. Protokol spesifikasi membedakan antara dua versi utama yang disebut sebagai SSH-1 dan SSH-2.

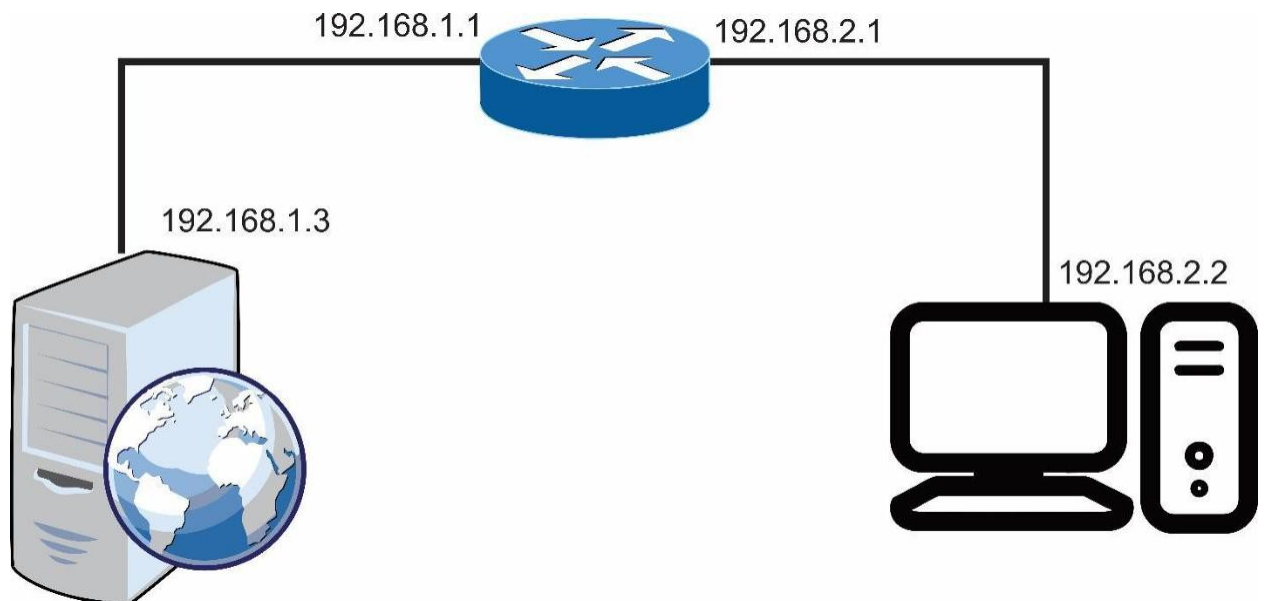
2.3 KEGIATAN PRAKTIKUM

2.3.1 Peralatan

Alat dan bahan

- 1 buah laptop
- Virtual Machine(VirtualBox/VMware)
- ISO : Debian6

2.3.2 Topologi Jaringan



2.3.3 Langkah Kerja

Melakukan Sniffing pada Jaringan

- 1) Pada router install wireshark dengan perintah
`#apt-get install wireshark`
- 2) Selanjutnya pada server install proftpd dan ssh dengan perintah
`#apt-get install proftpd ssh`
Pada saat install proftpd akan muncul tampilan proftpd konfigurasi kemudian pilih standalone.

```
Terminal (as superuser)
File Edit View Terminal Help
root@susan:/home/susan# apt-get install proftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'proftpd-basic' instead of 'proftpd'
proftpd-basic is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

3) Buat beberapa user account di server untuk mengakses aplikasi tersebut Dengan perintah :

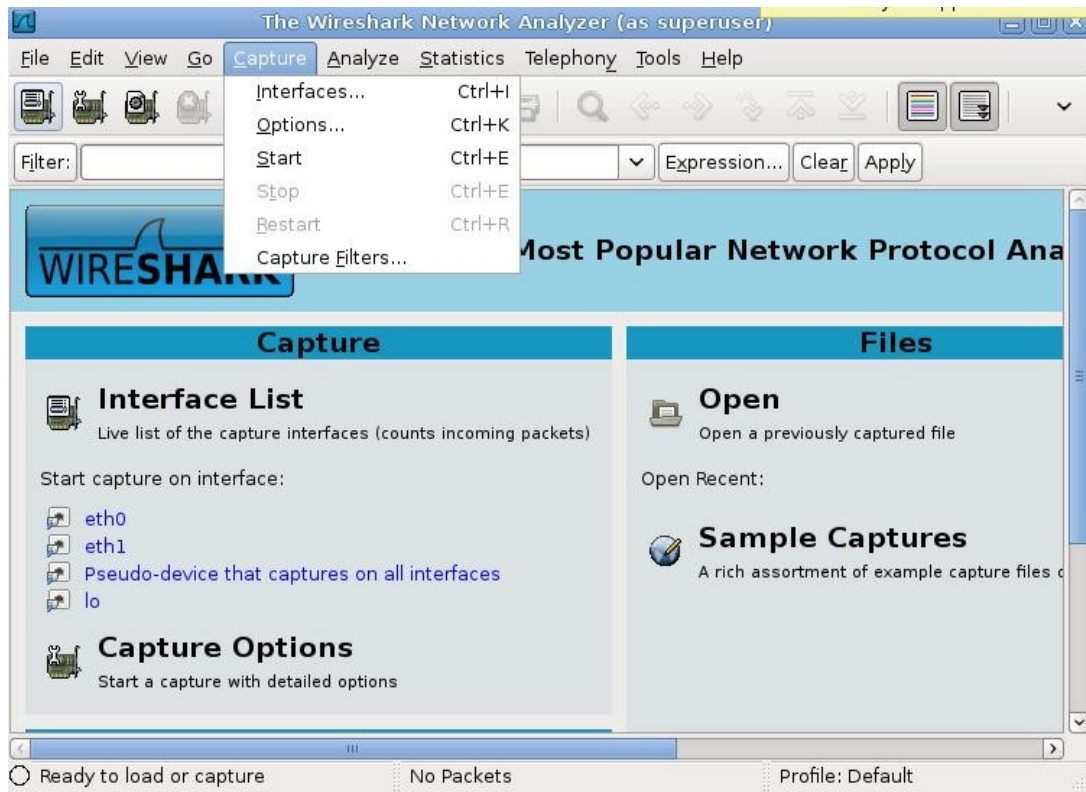
```
# adduser ...
```

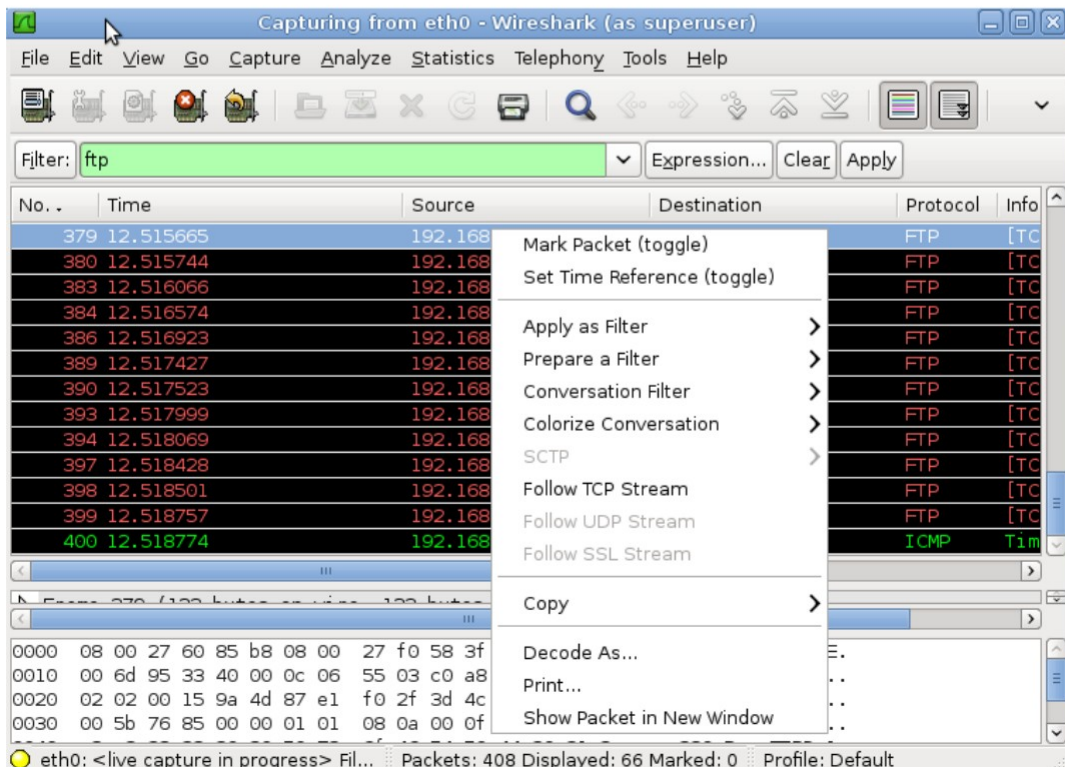
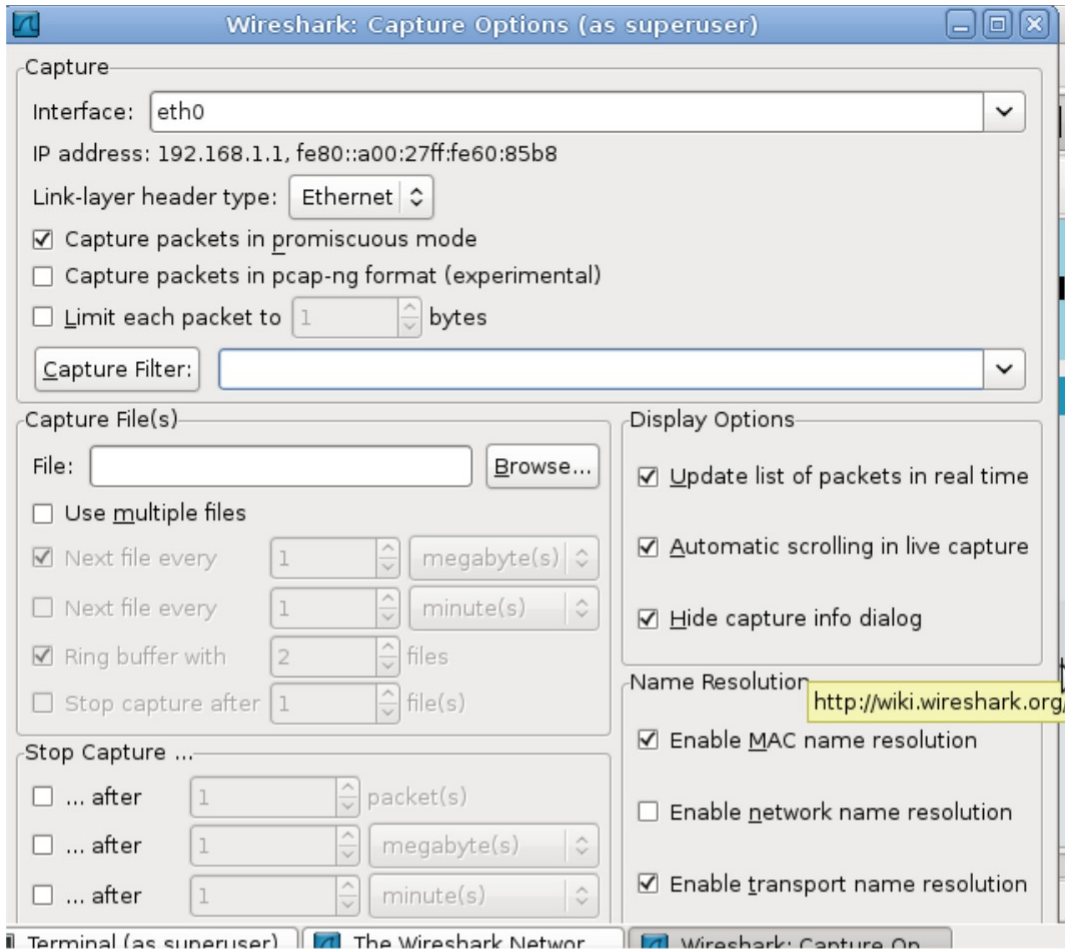
4) Setelah itu, di client ketik perintah

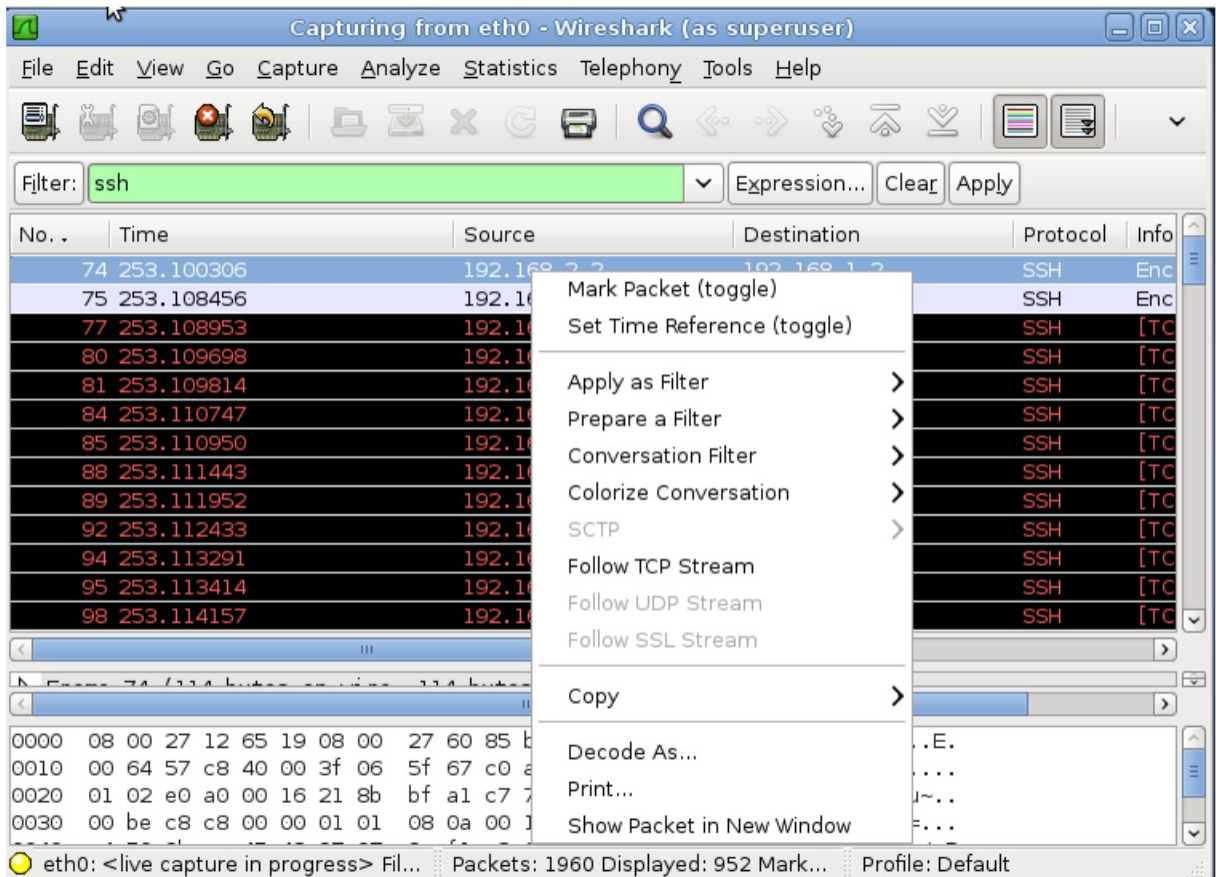
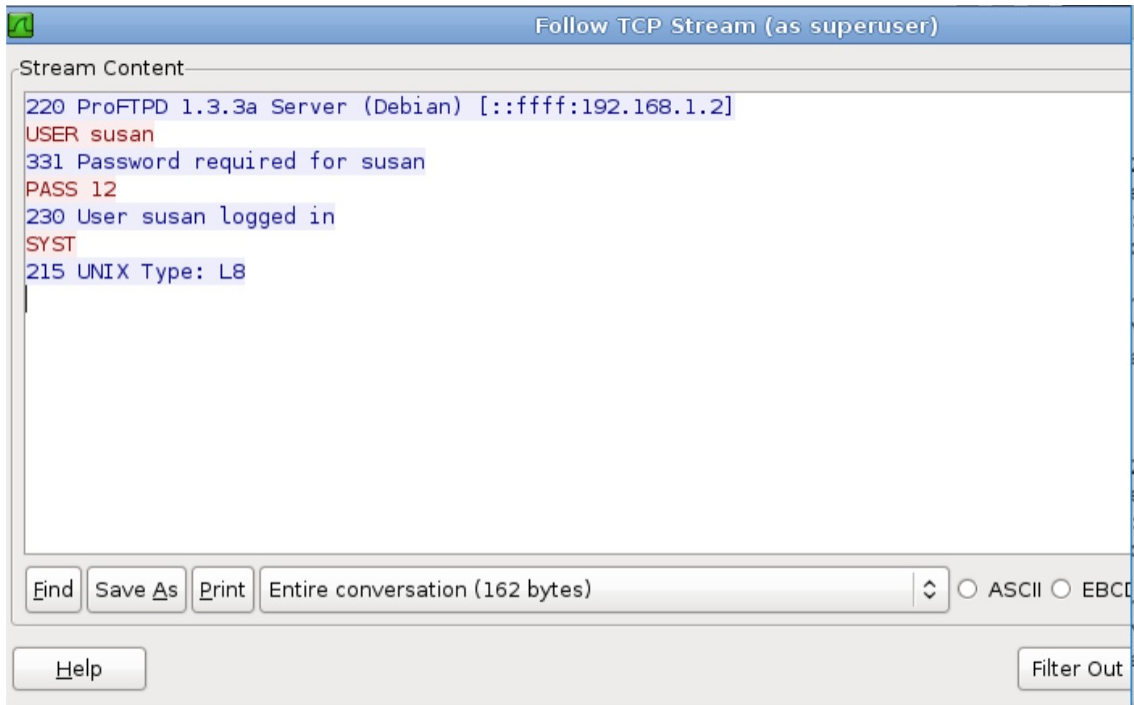
```
#ftp 192.168.1.2 ---- IP SERVER
```

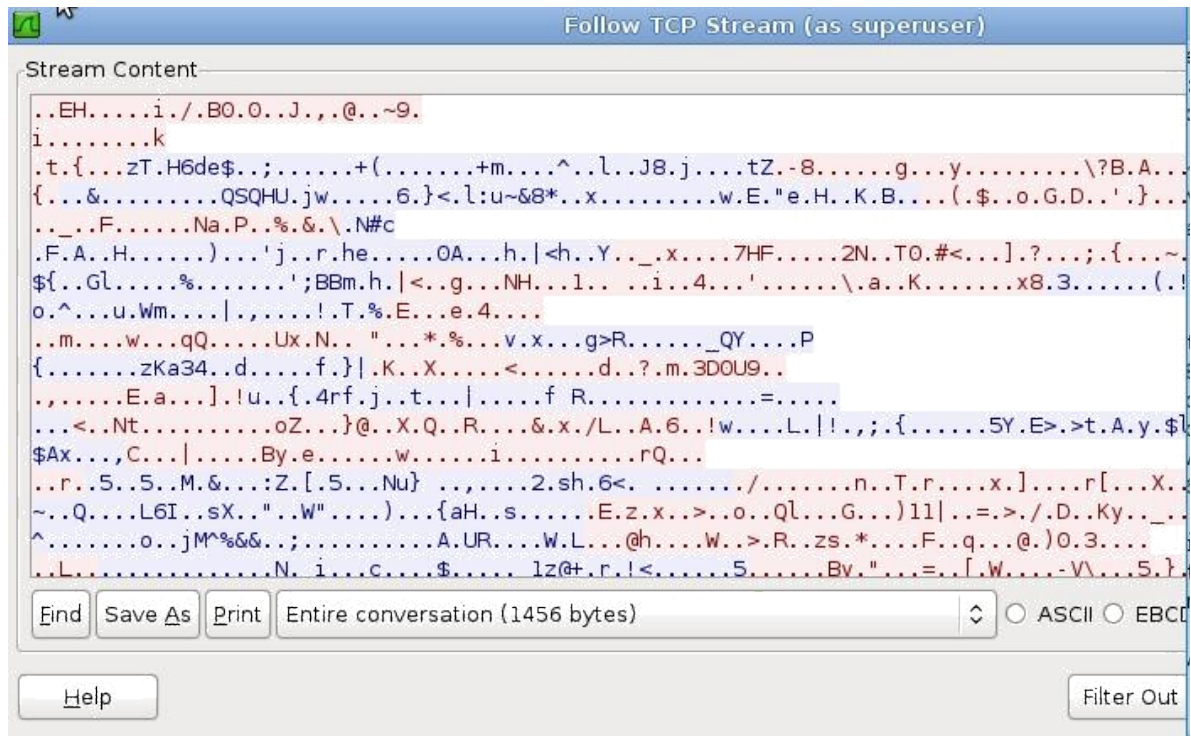
```
#ssh 192.168.1.2 ---- IP SERVER
```

5) Jalankan wireshark pada Router, pada tampilan wireshark pilih “capture > options,selanjutnya hilangkan tanda centang seperti pada gambar dibawah selanjutnya tekan “enter”









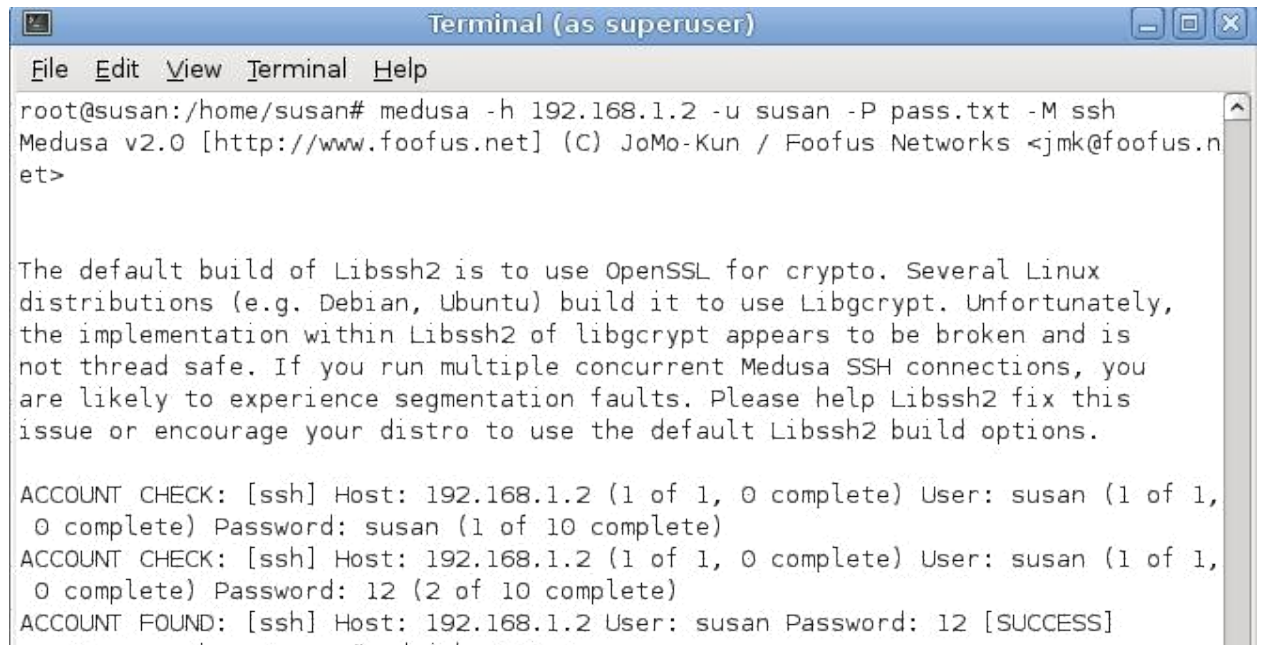
Enumeration

- 1) Install Medusa . Untuk mendapatkan username dan password dari suatu aplikasi jaringan bisa digunakan tool medusa dari linux. Dalam percobaan ini akan digunakan tool medusa. Instalasi medusa pada Client.

apt-get install medusa



- 2) Pastikan di client sudah terinstall nmap. Setelah itu ketik perintah #nmap 192.168.1.2 ---- IP SERVER
Untuk melihat port mana saja yang terbuka
- 3) Lakukan penetrasi ke PC Server dengan perintah berikut: # medusa -h 192.168.1.2 -u susan -P pass.txt -M ssh



```
Terminal (as superuser)
File Edit View Terminal Help
root@susan:/home/susan# medusa -h 192.168.1.2 -u susan -P pass.txt -M ssh
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

The default build of Libssh2 is to use OpenSSL for crypto. Several Linux
distributions (e.g. Debian, Ubuntu) build it to use Libgcrypt. Unfortunately,
the implementation within Libssh2 of libgcrypt appears to be broken and is
not thread safe. If you run multiple concurrent Medusa SSH connections, you
are likely to experience segmentation faults. Please help Libssh2 fix this
issue or encourage your distro to use the default Libssh2 build options.

ACCOUNT CHECK: [ssh] Host: 192.168.1.2 (1 of 1, 0 complete) User: susan (1 of 1,
0 complete) Password: susan (1 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.2 (1 of 1, 0 complete) User: susan (1 of 1,
0 complete) Password: 12 (2 of 10 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.1.2 User: susan Password: 12 [SUCCESS]
```

NB: -h : koneksi ke suatu host

-u : username yang sudah diketahui

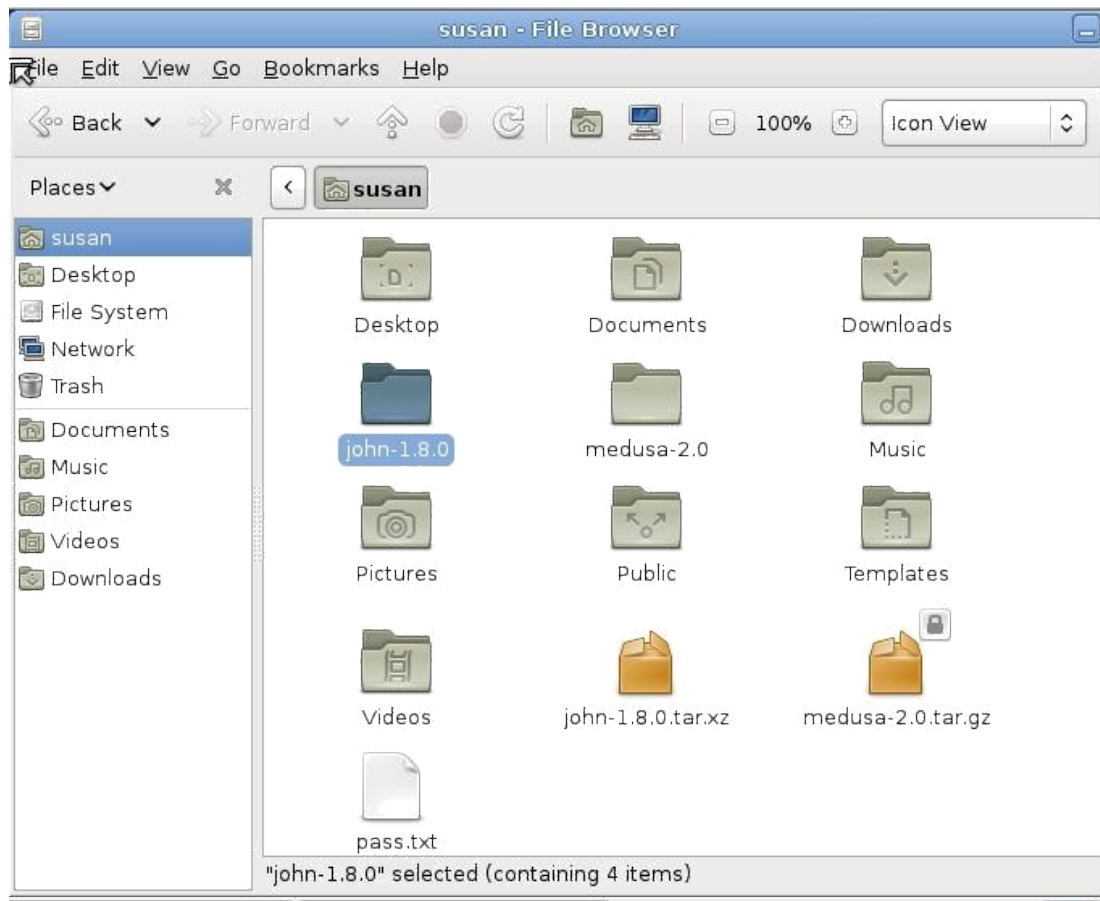
-U : pencarian username dari wordlist

-P : pencarian password dari wordlist (bisa download dari internet)

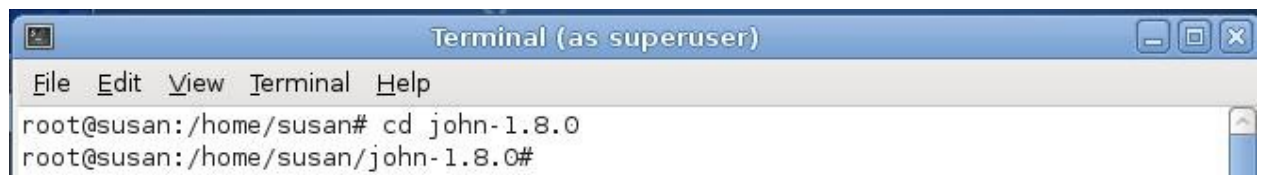
-M : service / aplikasi yang berjalan pada suatu sistem jaringan (bisa juga dipilih ftp, ssh, telnet, snmp,smb,vnc, dll)

Konfigurasi John The Ripper

1. Setelah konfigurasi pada medusa konfigurasi pada John The Ripper pada debian client.
2. Download package John The Ripper pada situs resmi debian client.
3. Masukkan package tersebut di user yang sedang login. Lihat pada gambar dibawah ini.



- 4) Setelah itu, masuk src pada folder John caranya pada gambar dibawah ini



- 5) Sesudah itu, ketikkan perintah make, Sesudah itu clean pada make, ketikkan perintah pada gambar dibawah ini.

```
root@susan:/home/susan/john-1.8.0# make clean linux-x86-sse2
```

- 6) Masuk ker folder run pada folder John.
- 7) Hasilnya akan terlihat sebagai berikut, tergantung seberapa rumit kombinasi passwordnya dan akan berpengaruh terhadap lama proses crackingsnya.

```
Terminal (as superuser)
File Edit View Terminal Help
0g 0:02:35:47 3/3 0g/s 23.32p/s 46.46c/s 46.46C/s bryors..busko1
0g 0:02:36:27 3/3 0g/s 23.31p/s 46.45c/s 46.45C/s mamad..mosay
0g 0:02:36:29 3/3 0g/s 23.31p/s 46.45c/s 46.45C/s mamad..mosay
0g 0:02:36:35 3/3 0g/s 23.31p/s 46.45c/s 46.45C/s mhley..alfel
0g 0:02:36:38 3/3 0g/s 23.31p/s 46.45c/s 46.45C/s mhley..alfel
0g 0:02:36:40 3/3 0g/s 23.31p/s 46.45c/s 46.45C/s alfos..arlay
0g 0:02:52:19 3/3 0g/s 23.29p/s 46.44c/s 46.44C/s sinka..siere
0g 0:02:52:21 3/3 0g/s 23.30p/s 46.44c/s 46.44C/s siena..jjjkk
0g 0:02:52:23 3/3 0g/s 23.29p/s 46.44c/s 46.44C/s siena..jjjkk
0g 0:02:53:01 3/3 0g/s 23.29p/s 46.43c/s 46.43C/s cenne..llone
0g 0:02:53:03 3/3 0g/s 23.29p/s 46.43c/s 46.43C/s llona..lllls
0g 0:02:53:05 3/3 0g/s 23.29p/s 46.43c/s 46.43C/s llona..lllls
0g 0:02:53:07 3/3 0g/s 23.29p/s 46.43c/s 46.43C/s lllll..llidi
0g 0:02:53:09 3/3 0g/s 23.29p/s 46.43c/s 46.43C/s lllll..llidi
0g 0:02:53:11 3/3 0g/s 23.29p/s 46.43c/s 46.43C/s llido..mac
0g 0:02:53:13 3/3 0g/s 23.29p/s 46.43c/s 46.43C/s llido..mac
0g 0:02:53:15 3/3 0g/s 23.30p/s 46.43c/s 46.43C/s moi..michior
0g 0:02:53:17 3/3 0g/s 23.29p/s 46.44c/s 46.44C/s moi..michior
12          (susan)
12          (root)
2g 0:02:54:44 3/3 0.000190g/s 23.29p/s 46.43c/s 46.43C/s criasom..11240
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@susan:~/home/susan/ohn-1 8 0/run# █
```

2.4 PENJELASAN

Pada percobaan kali ini kita melakukan pencarian password yang cocok dengan username dengan menggunakan Medusa dan John The Ripper, Dan juga melakukan sniffing pada jaringan dengan menggunakan ftp dan ssh yang akan ditampilkan di wireshark

MODUL 3
NETWORK SECURITY
KONFIGURASI FIREWALL

3.1.TUJUAN

1. Mengenalkan pada mahasiswa tentang konsep dasar firewall
2. Mahasiswa mampu melakukan proses filtering menggunakan iptables

3.2.TEORI DASAR

Firewall adalah sebuah perangkat lunak (software) atau sistem keamanan jaringan berbasis hardware, yang mengontrol lalu lintas jaringan yang masuk dan keluar dengan cara menganalisis paket data, dan menentukan apakah mereka bisa diizinkan untuk diakses atau tidak, berdasarkan aturan setting yang telah ditetapkan sebelumnya.

Firewall biasanya sudah ada di dalam berbagai perangkat komputer, terutama di dalam sistem operasionalnya. Sehingga memungkinkan komputer pribadi untuk menolak segala akses internet publik yang mengandung ancaman seperti virus, spam, dan lain sebagainya. Firewall adalah sistem atau sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan. Secara prinsip, firewall dapat dianggap sebagai sepasang mekanisme : yang pertama memblokir lalu lintas, yang kedua mengizinkan lalu lintas jaringan. Firewall dapat digunakan untuk melindungi jaringan anda dari serangan jaringan oleh pihak luar, namun firewall tidak dapat melindungi dari serangan yang tidak melalui firewall dan serangan dari seseorang yang berada di dalam jaringan anda, serta firewall tidak dapat melindungi anda dari program-program aplikasi yang ditulis dengan buruk. Secara umum, firewall biasanya menjalankan fungsi:

Analisa dan filter paket

Data yang dikomunikasikan lewat protokol di internet, dibagi atas paket-paket. Firewall dapat menganalisa paket ini, kemudian memperlakukannya sesuai kondisi tertentu. Misal, jika ada paket a maka akan dilakukan b. Untuk filter paket, dapat dilakukan di Linux tanpa program tambahan.

Bloking isi dan protocol

Firewall dapat melakukan bloking terhadap isi paket, misalnya berisi applet Jave, ActiveX, VBScript, Cookie.

Autentikasi koneksi dan enkripsi

Firewall umumnya memiliki kemampuan untuk menjalankan enkripsi dalam autentikasi identitas user, integritas dari satu session, dan melapisi transfer data dari intipan pihak lain. Enkripsi yang dimaksud termasuk DES, Triple DES, SSL, IPSEC, SHA, MD5, BlowFish,IDEA dan sebagainya

Secara konseptual, terdapat dua macam firewall yaitu :

Network level

Firewall network level mendasarkan keputusan mereka pada alamat sumber, alamat tujuan dan port yang terdapat dalam setiap paket IP. Network level firewall sangat cepat dan sangat transparan bagi pemakai. Application level firewall biasanya adalah host yang berjalan sebagai proxy server, yang tidak mengizinkan lalu lintas antar jaringan, dan melakukan logging dan auditing lalu lintas yang melaluinya Application level.

Application level firewall menyediakan laporan audit yang lebih rinci dan cenderung lebih memaksakan model keamanan yang lebih konservatif daripada network level firewall. Firewall ini bisa dikatakan sebagai jembatan. Application-Proxy Firewall biasanya berupa program khusus, misal squid.

Firewall IPTables packet filtering memiliki tiga aturan (policy), yaitu:

a. INPUT

Mengatur paket data yang memasuki firewall dari arah intranet maupun internet. Kita bias mengelola komputer mana saja yang bisa mengakses firewall. misal: hanya komputer IP 192.168.1.100 yang bisa SSH ke firewall dan yang lain tidak boleh.

b. OUTPUT

Mengatur paket data yang keluar dari firewall ke arah intranet maupun internet. Biasanya output tidak diset, karena bisa membatasi kemampuan firewall itu sendiri.

c. FORWARD

Mengatur paket data yang melintasi firewall dari arah internet ke intranet maupun sebaliknya. Policy forward paling banyak dipakai saat ini untuk mengatur koneksi internet berdasarkan port, mac address dan alamat IP.

Selain aturan (policy) firewall iptables juga mempunyai parameter yang disebut dengan TARGET, yaitu status yang menentukan koneksi di iptables diizinkan lewat atau tidak.

TARGET ada tiga macam yaitu:

a. ACCEPT

Akses diterima dan diizinkan melewati

firewall b.REJECT

Akses ditolak, koneksi dari komputer klien yang melewati firewall langsung terputus, biasanya terdapat pesan "Connection Refused". Target Reject tidak menghabiskan bandwidth internet karena akses langsung ditolak, hal ini berbeda dengan DROP.

c. DROP

Akses diterima tetapi paket data langsung dibuang oleh kernel, sehingga pengguna tidak mengetahui kalau koneksinya dibatasi oleh firewall, pengguna melihat seakan – akan server yang dihubungi mengalami permasalahan teknis. Pada koneksi internet yang sibuk dengan trafik tinggi Target Drop sebaiknya jangan digunakan.

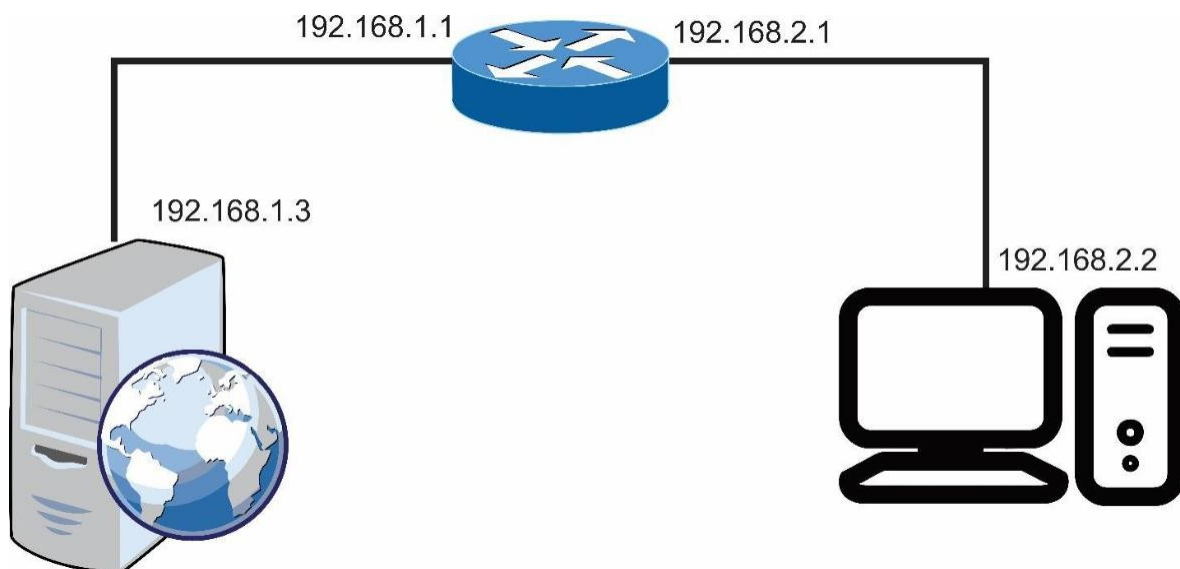
3.3.KEGIATAN PRAKTIKUM

3.3.1. Peralatan

Alat dan bahan

- 1 buah laptop
- Virtual Machine(VirtualBox/VMware)
- ISO : Debian6

3.3.2.Topologi



3.3.3.Langkah Kerja

- a. Install ftp dan ssh server pada sisi PC Server (firewall)
apt-get install proftpd
- b. Buatlah rule firewall sebagai berikut, dan ujilah rule anda tsb :
- c. Reject akses dari client ke ssh server

Accept akses dari client ke ftp server

Tolak semua akses ke Firewall.

Perintah:

```
# iptables -A INPUT -s 192.168.2.2 -p tcp --dport 22 -j REJECT
```

```
# iptables -A INPUT -s 192.168.2.2 -p tcp --dport 21 -j ACCEPT
```

```
# iptables -A INPUT -j REJECT
```

```
#iptables -nL untuk melihat hasilnya
```

Untuk menghapus rule sebelumnya masukan perintah : # iptables -F

```
root@susan:/home/susan# iptables -A INPUT -s 192.168.2.2 -p tcp --dport 22 -j REJECT
root@susan:/home/susan# iptables -A INPUT -s 192.168.2.2 -p tcp --dport 21 -j ACCEPT
root@susan:/home/susan# iptables -A INPUT -j REJECT
root@susan:/home/susan# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           tcp dpt:22 reject-with icmp-port-unreachable
ACCEPT    tcp  --  192.168.2.2           0.0.0.0/0             tcp dpt:21
REJECT    all  --  0.0.0.0/0             0.0.0.0/0             reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@susan:/home/susan# iptables -F
root@susan:/home/susan#
```

Hasil testing ssh, ftp, ping di client

```
Terminal (as superuser)
File Edit View Terminal Help
root@susan:/home/susan# ftp 192.168.1.2
Connected to 192.168.1.2.
220 ProFTPD 1.3.3a Server (Debian) [::ffff:192.168.1.2]
Name (192.168.1.2:root): susan
331 Password required for susan
Password:
230 User susan logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bye
221 Goodbye.
root@susan:/home/susan# ssh 192.168.1.2
ssh: connect to host 192.168.1.2 port 22: Connection refused

root@susan:/home/susan# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
From 192.168.2.2 icmp_seq=2 Destination Host Unreachable
From 192.168.2.2 icmp_seq=3 Destination Host Unreachable
From 192.168.2.2 icmp_seq=4 Destination Host Unreachable
```

Bloking dengan menggunakan MAC address

- a. Catat MAC address di sisi client, dengan perintah #ifconfig pada client, dan selanjutnya lakukan perintah berikut di PC Server

```
# iptables -A INPUT -m mac --mac-source 08:00:27:60:85:b8 -d 0/0 -j REJECT
```

```
Terminal (as superuser)
File Edit View Terminal Help
root@susan:/home/susan# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:60:85:b8
          inet addr:192.168.2.2  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe60:85b8/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:35280 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10741 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4304350 (4.1 MiB)  TX bytes:1006265 (982.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:718 (718.0 B)  TX bytes:718 (718.0 B)

root@susan:/home/susan# iptables -A INPUT -m mac --mac-source 08:00:27:60:85:b8
-d 0/0 -j REJECT
```

Buka di client ping IP SERVER

```
root@susan:/home/susan# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
From 192.168.2.2 icmp_seq=2 Destination Host Unreachable
From 192.168.2.2 icmp_seq=3 Destination Host Unreachable
From 192.168.2.2 icmp_seq=4 Destination Host Unreachable
```

Project selanjutnya :

Buatlah rule sebagai berikut:

- Akses HTTP diperbolehkan dari INTERNET
- Akses SSH ditolak dari INTERNET
- Paket ping ditolak baik dari LAN maupun dari INTERNET

Masukan perintah di bawah pada pc Router

a. Akses HTTP diperbolehkan dari INTERNET

```
# iptables -A FORWARD -i eth1 -p tcp --dport 80 -j ACCEPT
```

b. Akses SSH ditolak dari INTERNET

```
# iptables -A FORWARD -i eth1 -p tcp --dport 22 -j REJECT
```

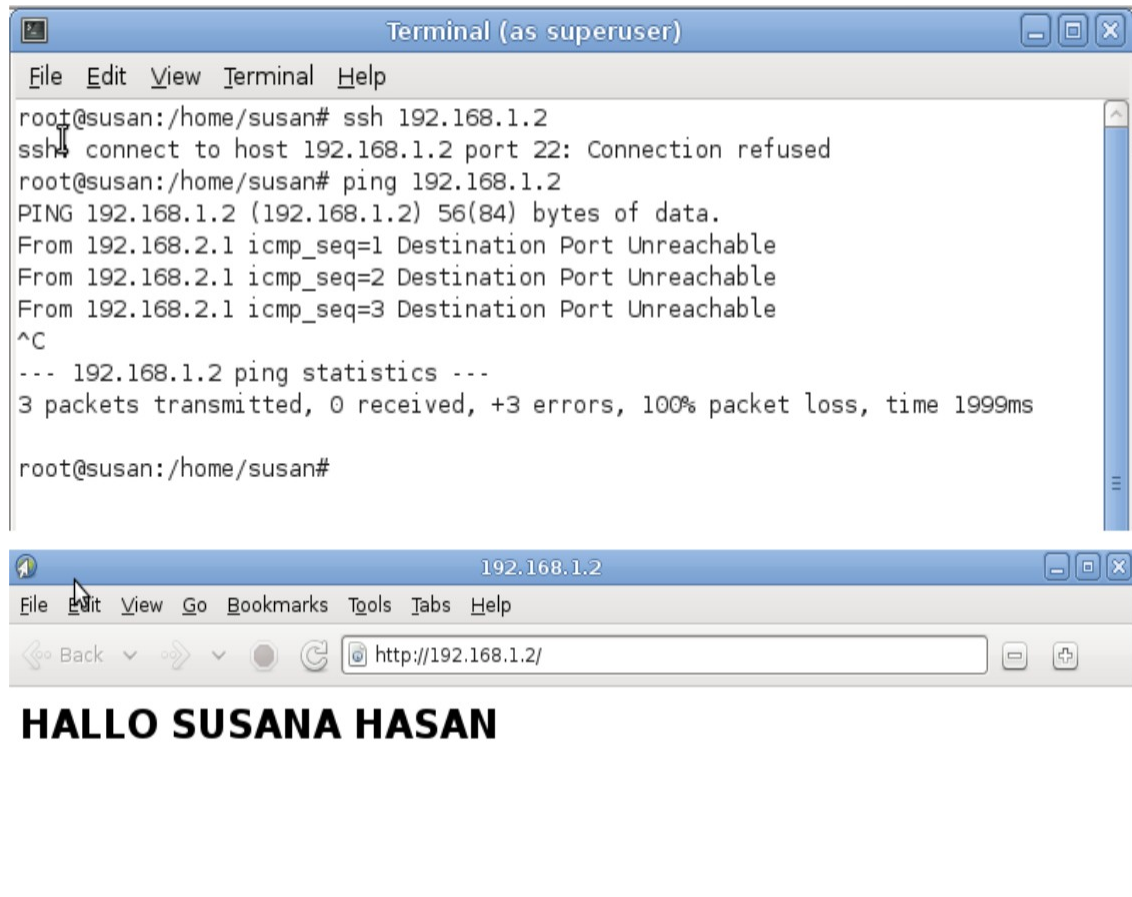
c. Paket ping ditolak baik dari LAN maupun dari INTERNET

```
# iptables -A FORWARD -i eth1 -p icmp -j REJECT# iptables -A FORWARD -
i eth0 -p icmp -j DROP
```

d. Lihat rule di iptables dan catat hasilnya dengan perintah # iptables -nL

```
root@susan:/home/susan# iptables -A FORWARD -i eth1 -p tcp --dport 80 -j ACCEPT
root@susan:/home/susan# iptables -A FORWARD -i eth1 -p tcp --dport 22 -j REJECT
root@susan:/home/susan# iptables -A FORWARD -i eth1 -p icmp -j REJECT
root@susan:/home/susan# iptables -A FORWARD -i eth0 -p icmp -j DROP
root@susan:/home/susan#
```

Hasil testing ssh, ping, internet di client



3.4.PENJELASAN

Firewall digunakan untuk mengatur jaringan masuk dan keluar komputer/server. Dengan melarang suatu aplikasi atau service dari jangkauan jaringan.

MODUL 4
NETWORK SECURITY
KONFIGURASI FIREWALL(TCP WRAPPER)

4.1.TUJUAN

1. Memperkenalkan konsep dasar firewall yang lain pada linux, yaitu tcp wrapper
2. Memahami perbedaan konsep firewall iptables dan tcp wrapper
3. Mampu mengaplikasikan tcp wrapper

4.2.TEORI DASAR

Firewall adalah sebuah perangkat lunak (software) atau sistem keamanan jaringan berbasis hardware, yang mengontrol lalu lintas jaringan yang masuk dan keluar dengan cara menganalisis paket data, dan menentukan apakah mereka bisa diizinkan untuk diakses atau tidak, berdasarkan aturan setting yang telah ditetapkan sebelumnya.

Firewall biasanya sudah ada di dalam berbagai perangkat komputer, terutama di dalam sistem operasionalnya. Sehingga memungkinkan komputer pribadi untuk menolak segala akses internet publik yang mengandung ancaman seperti virus, spam, dan lain sebagainya. Firewall adalah sistem atau sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan. Secara prinsip, firewall dapat dianggap sebagai sepasang mekanisme : yang pertama memblokir lalu lintas, yang kedua mengizinkan lalu lintas jaringan. Firewall dapat digunakan untuk melindungi jaringan anda dari serangan jaringan oleh pihak luar, namun firewall tidak dapat melindungi dari serangan yang tidak melalui firewall dan serangan dari seseorang yang berada di dalam jaringan anda, serta firewall tidak dapat melindungi anda dari program-program aplikasi yang ditulis dengan buruk. Secara umum, firewall biasanya menjalankan fungsi:

Analisa dan filter paket

Data yang dikomunikasikan lewat protokol di internet, dibagi atas paket-paket. Firewall dapat menganalisa paket ini, kemudian memperlakukannya sesuai kondisi tertentu. Misal, jika ada paket a maka akan dilakukan b. Untuk filter paket, dapat dilakukan di Linux tanpa program tambahan.

Bloking isi dan protocol

Firewall dapat melakukan bloking terhadap isi paket, misalnya berisi applet Jave, ActiveX, VBScript, Cookie.

Autentikasi koneksi dan enkripsi

Firewall umumnya memiliki kemampuan untuk menjalankan enkripsi dalam autentikasi identitas user, integritas dari satu session, dan melapisi transfer data dari intipan pihak lain. Enkripsi yang dimaksud termasuk DES, Triple DES, SSL, IPSEC, SHA, MD5, BlowFish,IDEA dan sebagainya

Secara konseptual, terdapat dua macam firewall yaitu :

Network level

Firewall network level mendasarkan keputusan mereka pada alamat sumber, alamat tujuan dan port yang terdapat dalam setiap paket IP. Network level firewall sangat cepat dan sangat transparan bagi pemakai. Application level firewall biasanya adalah host yang berjalan sebagai proxy server, yang tidak mengijinkan lalu lintas antar jaringan, dan melakukan logging dan auditing lalu lintas yang melaluinya Application level.

Application level firewall menyediakan laporan audit yang lebih rinci dan cenderung lebih memaksakan model keamanan yang lebih konservatif daripada network level firewall Firewall ini bisa dikatakan sebagai jembatan. Application-Proxy Firewall biasanya berupa program khusus, misal squid.

Firewall IPTables packet filtering memiliki tiga aturan (policy), yaitu:

d.INPUT

Mengatur paket data yang memasuki firewall dari arah intranet maupun internet. kita bias mengelola komputer mana saja yang bisa mengakses firewall. misal: hanya komputer IP 192.168.1.100 yang bisa SSH ke firewall dan yang lain tidak boleh.

e. OUTPUT

Mengatur paket data yang keluar dari firewall ke arah intranet maupun internet. Biasanya output tidak diset, karena bisa membatasi kemampuan firewall itu sendiri.

f. FORWARD

Mengatur paket data yang melintasi firewall dari arah internet ke intranet maupun sebaliknya. Policy forward paling banyak dipakai saat ini untuk mengatur koneksi internet berdasarkan port, mac address dan alamat IP.

Selain aturan (policy) firewall iptables juga mempunyai parameter yang disebut dengan TARGET, yaitu status yang menentukan koneksi di iptables diizinkan lewat atau tidak.

TARGET ada tiga macam yaitu:

d. ACCEPT

Akses diterima dan diizinkan melewati

firewall e. REJECT

Akses ditolak, koneksi dari komputer klien yang melewati firewall langsung terputus, biasanya terdapat pesan "Connection Refused". Target Reject tidak menghabiskan bandwidth internet karena akses langsung ditolak, hal ini berbeda dengan DROP.

f. DROP

Akses diterima tetapi paket data langsung dibuang oleh kernel, sehingga pengguna tidak mengetahui kalau koneksinya dibatasi oleh firewall, pengguna melihat seakan – akan server yang dihubungi mengalami permasalahan teknis. Pada koneksi internet yang sibuk dengan trafik tinggi Target Drop sebaiknya jangan digunakan.

TCP Wrappers

Secara default redhat akan mengizinkan servis-servis tertentu (misal : telnet) dengan tanpa pembatasan. Untuk itu diperlukan pembatasan-pembatasan (proteksi) tertentu sehingga dapat mengurangi kerawanan keamanan jaringan.

Salah satu aplikasi pada sistem UNIX yang digunakan untuk melakukan packet filtering adalah TCP Wrappers. TCP Wrappers merupakan salah satu metode filter (access control list) di sistem operasi Unix Like untuk membatasi suatu host yang ingin menggunakan service yang ada di server. Biasanya TCP Wrappers sudah terinstal secara default waktu penginstalan Linux.

Program ini bekerja dengan cara membungkus inetd (internet daemon : aplikasi yang menjalankan servis-servis internet) agar lebih aman. Sebagai contoh ada permintaan koneksi telnet dari internet, jika sistem kita tidak mempunyai tcp wrappers maka inetd akan memanggil telnetd dan session telnet akan terbentuk tanpa melakukan pembatasan apapun. Hal ini berbeda dengan TCP Wrappers yang telah terinstal, sebelum memanggil telnetd, TCP Wrapper akan memeriksa dulu berdasarkan pembatasan-pembatasan yang telah disetting kemudian memutuskan apakah koneksi tersebut akan diizinkan atau tidak. Lapisan network yang digunakan TCP Wrappers untuk memonitor dan mengontrol trafik

TCP di server adalah pada level aplikasi. Sistem yang menyediakan fasilitas seperti firewall. Sebuah host (dengan beberapa service) diisolasi dari jaringan luar. Fungsi yang disediakan seperti log dari request dan access control.

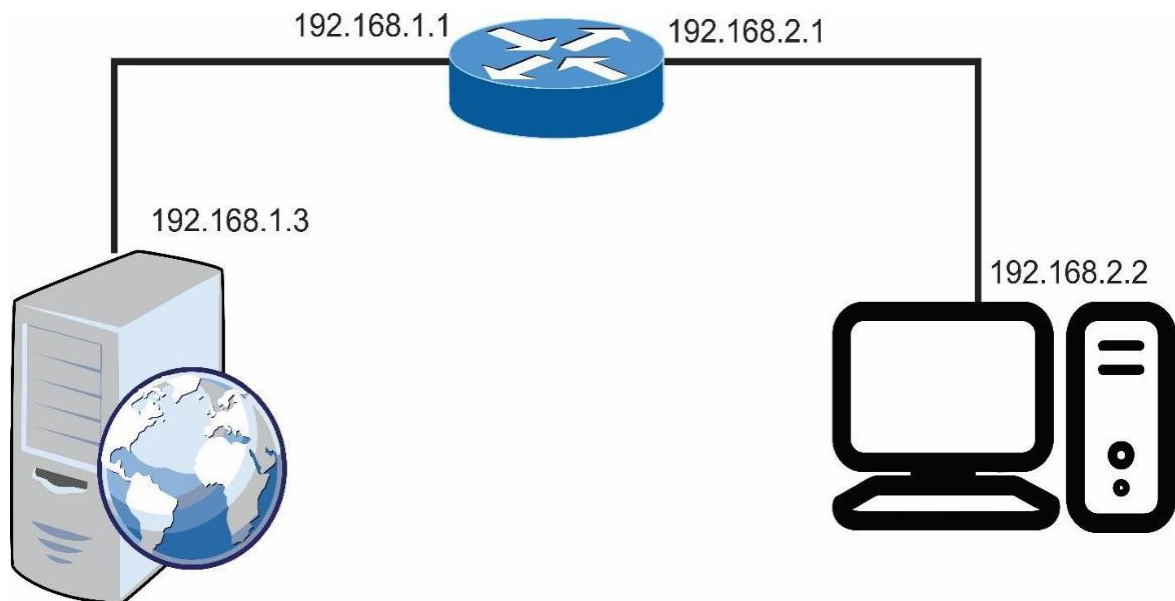
4.3.KEGIATAN PRAKTIKUM

4.3.1.Peralatan

Alat dan bahan

- ▣ 1 buah laptop
- ▣ Virtual Machine(VirtualBox/VMware)
- ▣ ISO : Debian 6.0.6 DVD 2

4.3.2.Topologi



4.3.3.Langkah Kerja

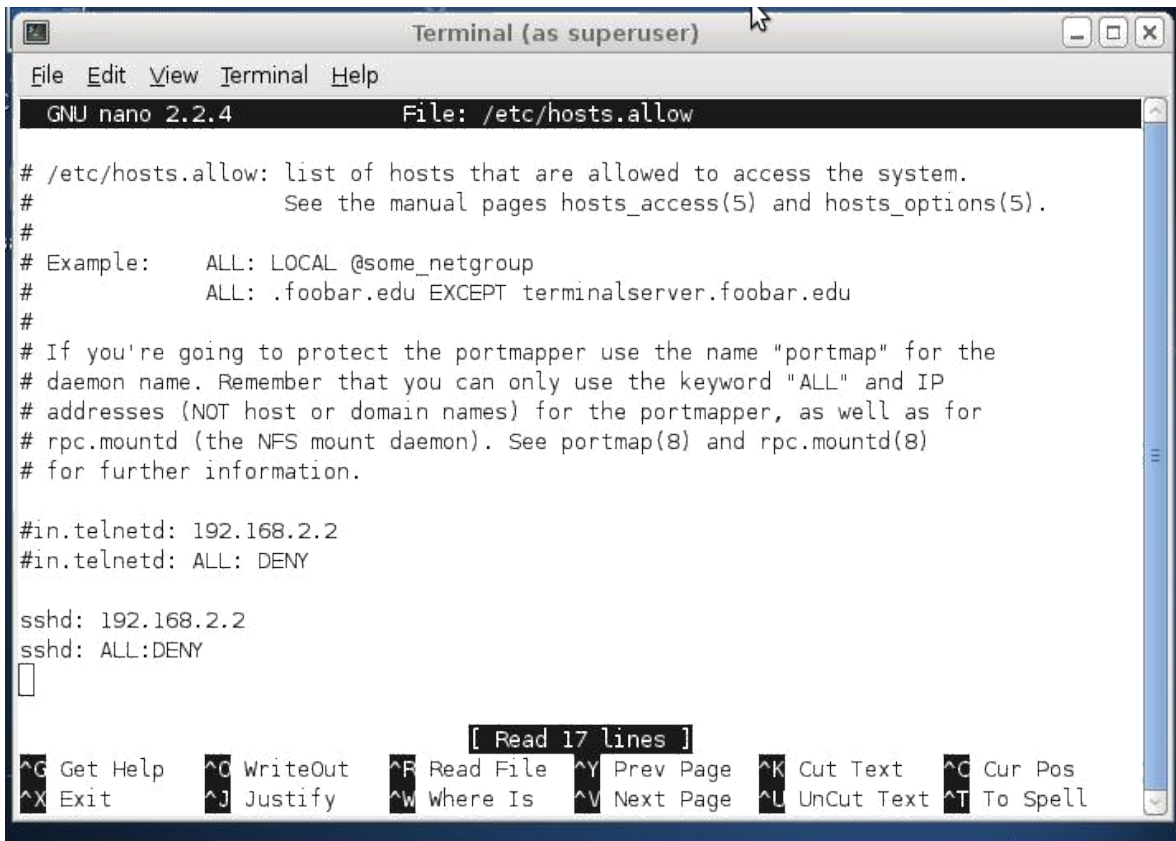
Konfigurasi pada Pc server

- 1) Pada server telah terinstall telnet dan ssh
- 2) Beri rule pada server sebagai berikut dan amati yang terjadi dengan melakukan akses dari client

Masukan perintah “nano /etc/hosts.allow”

```
root@susan:/home/susan# nano /etc/hosts.allow
root@susan:/home/susan#
```

Untuk mengakses telnetd tanda “#” nya dihilangkan,namun jika hanya ingin ssh yang di akses maka tanda pagar yang pada ssh dihilangkan agar dapat diakses.



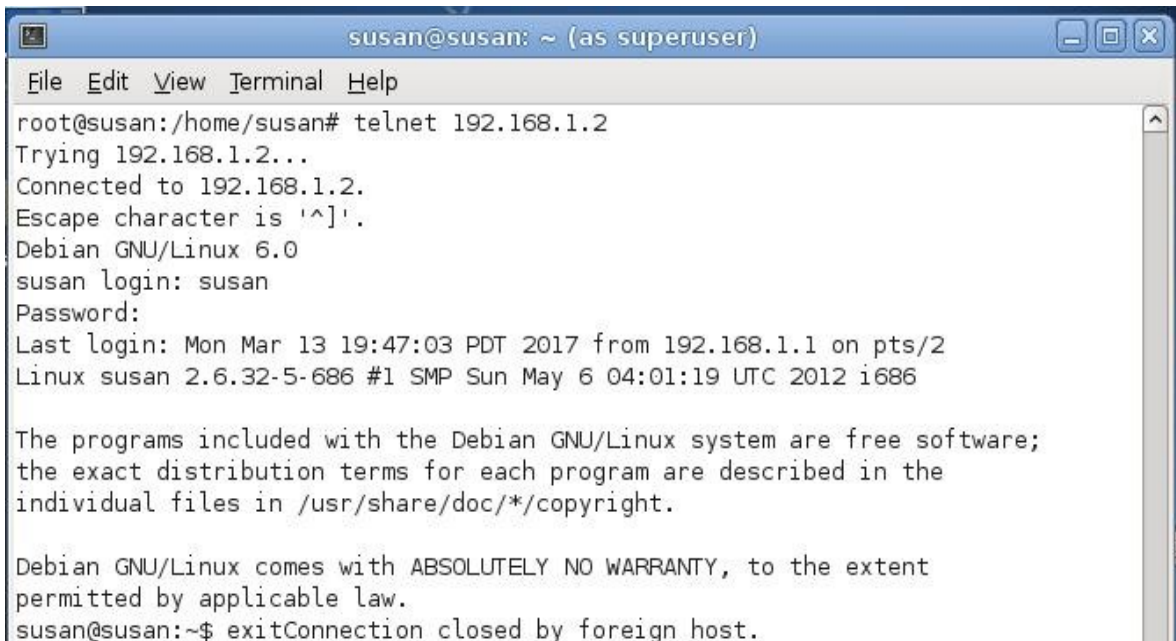
```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /etc/hosts.allow

# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:  ALL: LOCAL @some_netgroup
#          ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.

#in.telnetd: 192.168.2.2
#in.telnetd: ALL: DENY

sshd: 192.168.2.2
sshd: ALL: DENY
[ Read 17 lines ]
^G Get Help  ^C WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^L UnCut Text ^T To Spell
```

Lakukan tes pada pc client untuk dapat mengetahui bahwa ssh dan telnet dapat di akses atau Tidak



```
susan@susan: ~ (as superuser)
File Edit View Terminal Help
root@susan:/home/susan# telnet 192.168.1.2
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
Debian GNU/Linux 6.0
susan login: susan
Password:
Last login: Mon Mar 13 19:47:03 PDT 2017 from 192.168.1.1 on pts/2
Linux susan 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
susan@susan:~$ exitConnection closed by foreign host.
```

Pada gambar di bawah, pc router tidak dapat mengakses telnet karena hanya ip client yang dapat diakses untuk telnet



```
susan@susan: ~ (as superuser)
File Edit View Terminal Help
root@susan:/home/susan# telnet 192.168.1.2
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
Connection closed by foreign host.
root@susan:/home/susan#
```

i) Selanjutnya masukan perintah pada nano /etc/hosts.deny, tapi sebelumnya matikan pada nano /etc/hosts.allow dengan cara memberi tanda pagar (, # □).

a. Rule yang dibuat : Telnet server bisa diakses oleh 192.168.2.2 b. Perintah untuk rule diatas:

in.telnetd: 192.168.2.2

ii) Untuk memberi keterangan pada client, jika tidak dapat melakukan koneksi, bisa diberi keterangan dengan menggunakan twist, lakukan pada nano /etc/hosts.deny.

Seperti gambar di bawah ini :



```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /etc/hosts.deny
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

in.telnetd: 192.168.2.2 : twist /bin/echo "Anda tidak dapat memasuki area "
#sshd: ALL:EXCEPT 192.168.2.2

[ Read 22 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Untuk melakukan test masuk pada pc client dan masukan perintah “telnet 192.168.2.2”

```
root@susan:/home/susan# telnet 192.168.1.2
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
Anda tidak dapat memasuki area
Connection closed by foreign host.
root@susan:/home/susan# █
```

4.4.KESIMPULAN

Kesimpulan dari praktek ini, saya dapat menjadikan allow akses dan deny akses yang telah di tentukan di firewall.

MODUL 5
NETWORK SECURITY
INTRUSION DETECTION SYSTEM
[PORTSENTRY & HONEYPOT]

5.1.TUJUAN

1. Mengenalkan pada mahasiswa tentang konsep portsentry dan honeypot di linux
2. Mahasiswa memahami sistem blocking portsentry di linux
3. Mahasiswa memahami sistem pendeteksian serangan dengan honeypot
4. Mahasiswa mampu melakukan analisa terhadap portsentry yang ada di linux

5.2.DASAR TEORI

Dari sekian banyak hal yang paling banyak di takuti orang pada saat mengkaitkan diri ke Internet adalah serangan virus & hacker. Penggunaan Software Firewall akan membantu menahan serangan dari luar. Pada kenyataan di lapangan, menahan serangan saja tidak cukup, kita harus dapat mendeteksi adanya serangan bahkan jika mungkin secara otomatis menangkal serangan tersebut sedini mungkin. Proses ini biasa disebut dengan istilah Intrusion Detection. PortSentry adalah sebuah perangkat lunak yang di rancang untuk mendeteksi adanya port scanning & meresponds secara aktif jika ada port scanning. Port scan adalah proses scanning berbagai aplikasi servis yang dijalankan di server Internet. Port scan adalah langkah paling awal sebelum sebuah serangan di lakukan. Cara kerja port sentry dengan melakukan melihat komputer yang melakukan scan dan secara aktif akan memblokir mesin penyerang agar tidak dapat masuk & melakukan transaksi dengan Server kita.

- Berjalan di atas soket TCP & UDP untuk mendeteksi scan port ke sistem kita.
- Mendeteksi stealth scan, seperti SYN/half-open, FIN, NULL, X-MAS.
- PortSentry akan bereaksi secara real-time (langsung) dengan cara memblokir IP address si penyerang. Hal ini dilakukan dengan menggunakan ipchains/ipfwadm dan memasukan ke file /etc/host.deny secara otomatis oleh TCP Wrapper.
- PortSentry mempunyai mekanisme untuk mengingat mesin / host mana yang pernah connect ke dia. Dengan cara itu, hanya mesin / host yang terlalu sering melakukan sambungan (karena melakukan scanning) yang akan di blokir.
- PortSentry akan melaporkan semua pelanggaran melalui syslog dan mengindikasikan nama system, waktu serangan, IP mesin penyerang, TCP / UDP port tempat serangan

dilakukan. Jika hal ini di integrasikan dengan Logcheck maka administrator system akan memperoleh laporan melalui e-mail.

Dengan adanya berbagai fitur di atas maka system yang kita gunakan tampaknya seperti hilang dari pandangan penyerang. Hal ini biasanya cukup membuat kecut nyali penyerang.

Penggunaan PortSentry sendiri sangat mudah sekali, bahkan untuk penggunaan biasa saja praktis semua instalasi default tidak perlu di ubah apa-apa dapat langsung digunakan. Yang mungkin perlu di tune-up sedikit adalah file konfigurasi portsentry yang semuanya berlokasi di `/etc/portsentry` secara default. Untuk mengedit file konfigurasi tersebut anda membutuhkan privilege sebagai root. Beberapa hal yang mungkin perlu di set adalah:

- file `/etc/portsentry/portsentry.conf` merupakan konfigurasi utama portsentry. Disini secara bertahap diset port mana saja yang perlu di monitor, responds apa yang harus di lakukan ke mesin yang melakukan portscan, mekanisme menghilangkan mesin dari routing table, masukan ke `host.deny`. Proses setting sangat mudah hanya dengan membuka / menutup tanda pagar (#) saja.
- pada file `/etc/portsentry/portsentry.ignore.static` masukan semua IP address di LAN yang harus selalu di abaikan oleh portsentry. Artinya memasukan IP address ke sini, agar tidak terblokir secara tidak sengaja.
- Pada file `/etc/default/portsentry` kita dapat menset mode deteksi yang dilakukan portsentry. Semakin baik mode deteksi yang dipilih (`advanced stealth TCP/UP scanning`), biasanya PortSentry akan semakin sensitif & semakin rewel karena sedikit-sedikit akan memblokir mesin.

5.2.2. Honeypot

Honeypot merupakan sumber sistem informasi yang bersifat terbuka (`opensif`) yang memfokuskan pada proses pengumpulan informasi tentang aktifitas ilegal si Attacker yang mencoba menyusup dan mengeksplorasi authorisasi system komputer (server). Dengan Honeypot kita bisa mengetahui tingkah laku si Attacker diantaranya : port yang diserang, perintah-perintah yang dipergunakan, dan jenis aktifitas lainnya yang bisa direkam. Honeypot akan melindungi server asli yang kita miliki karena kita mendirikan server palsu yang tanpa disadari sebenarnya si Attacker sedang

menyerang sistem yang bukan sebenarnya sehingga terperangkap. Macam-Macam Honeypot

Honeypot sendiri dibagi menjadi dua kategori yaitu :

5.2.1.1. High Interaction Honeypot

adalah sistem yang mengoperasikan Sistem Operasi penuh sehingga penyerang akan melihatnya sebagai sebuah sistem operasi/host yang siap untuk dieksploitasi (dan memang seperti itu lah keadaannya). Inti dari High Interaction adalah sistem ini nantinya akan diserang oleh penyerang. Yang perlu dipahami dari High Interaction Honeypot adalah sistem ini bukan sebuah software ataupun daemon yang siap diinstall pada komputer Host namun lebih kepada sebuah paradigma, sebuah arsitektur jaringan, dengan kata lain High Interaction Honeypot adalah sekumpulan komputer yang dirancang sedemikian rupa dalam sebuah jaringan agar terlihat dari sisi penyerang dan tentunya sekumpulan computer ini akan terus dimonitor dengan berbagai tools networking. Komputer-komputer ini bisa dikatakan adalah komputer secara fisik (komputer yang benar-benar ada) atau komputer secara virtual (Virtual Operating System seperti VMware dan XEN).

5.2.1.2. Low Interaction Honeypot

mensimulasikan sebuah sistem operasi dengan service-service tertentu (misalnya SSH, HTTP, FTP) atau dengan kata lain sistem yang bukan merupakan sistem operasi secara keseluruhan, service yang berjalan tidak bisa dieksploitasi untuk mendapatkan akses penuh terhadap honeypot. Low interaction akan melakukan analisa terhadap jaringan dan aktifitas worm. Sayangnya perkembangan dari Honeypot (Honeyd Low Interaction Honeypot) sendiri tidak terlalu cepat bahkan update terbaru terjadi pada tahun 2007.

5.3. KEGIATAN PRAKTIKUM

5.3.1. Peralatan

Alat dan bahan

- 1 buah laptop
- Virtual Machine (VirtualBox/VMware)
- ISO : Debian6

5.3.2. Topologi Jaringan



Client	Router 1	Router 2	Serv
Netmask : 255.255.255.0	Address : 192.168.2.1	Address : 172.25.1.2	Netmask : 255.0.0.0
	Eth1 Address : 172.25.1.1 Netmask : 255.255.0.0 Gateway : 172.25.1.2	Eth1 : Address : 10.0.0.1 Netmask : 255.0.0.0	

5.3.3.Langkah Kerja

Konfigurasi pada server

- Langkah pertama yang harus di lakukan adalah menginstall portsentry pada pc server
- Setelah terinstal portsentry masukan perintah “Edit nano etc/portsentry/portsentry.conf”

```
root@susan:/home/susan# nano /etc/portsentry/portsentry.conf
root@susan:/home/susan#
```

- Ubah perintah pada

BLOCK_UDP="1" di ubah menjadi 1 Seperti di gambar

BLOCK_TCP="1" di ubah menjadi 1 Seperti di gambar

```
susan@susan: ~
File Edit View Terminal Help
GNU nano 2.2.4 File: /etc/portentry/portentry.conf

# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="1"
BLOCK_TCP="1"

#####
# Dropping Routes:#
#####
# This command is used to drop the route or add the host into
# a local filter table.
#
# The gateway (333.444.555.666) should ideally be a dead host on
# the *local* subnet. On some hosts you can also point this at
# localhost (127.0.0.1) and get the same effect. NOTE THAT
# 333.444.555.66 WILL *NOT* WORK. YOU NEED TO CHANGE IT!!
#
# ALL KILL ROUTE OPTIONS ARE COMMENTED OUT INITIALLY. Make sure you

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^L UnCut Text ^T To Spell
```

□ Masukan ip address yang akan kita berikan akses

```
susan@susan: ~
File Edit View Terminal Help
GNU nano 2.2.4 File: /etc/port Sentry/port Sentry.ignore.static
#
# PortSentry can support full netmasks for networks as well. Format is:
#
# <IP Address>/<Netmask>
#
# Example:
#
#192.168.2.2
10.0.0.1
172.25.1.1
# Etc.
#
# If you don't supply a netmask it is assumed to be 32 bits.
#
#
127.0.0.1/32
10.0.0.1
[ Read 29 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^L UnCut Text ^T To Spell
```

□ Setelah itu restart portsentry untuk mengaktifkan konfigurasi yang kita buat

□ Langkah selanjutnya lakukan scanning port melalui nmap dari client ke server

```
root@susan:/home/susan# nmap -sT 10.0.0.2
Starting Nmap 5.00 ( http://nmap.org ) at 2017-03-15 23:16 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -PN
Nmap done: 1 IP address (0 hosts up) scanned in 0.07 seconds
```

□ Langkah selanjutnya lakukan scanning port melalui nmap dari router1 ke server

```
root@susan:/home/susan# nmap -sT 10.0.0.2
Starting Nmap 5.00 ( http://nmap.org ) at 2017-03-15 23:16 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -PN
Nmap done: 1 IP address (0 hosts up) scanned in 0.07 seconds
```

□ Lakukan scanning port pada router 2 dengan ip yang kita masukan pada list untuk tidak di blokir

```
susan@susan: ~
File Edit View Terminal Help

root@susan:/home/susan# nmap -sT 10.0.0.2

Starting Nmap 5.00 ( http://nmap.org ) at 2017-03-15 23:15 PDT
Interesting ports on 10.0.0.2:
Not shown: 976 filtered ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
110/tcp   closed pop3
111/tcp   open  rpcbind
113/tcp   closed auth
135/tcp   closed msrpc
139/tcp   closed netbios-ssn
143/tcp   open  imap
199/tcp   closed smux
256/tcp   closed fw1-secureremote
443/tcp   closed https
445/tcp   closed microsoft-ds
554/tcp   closed rtsp
587/tcp   closed submission
993/tcp   closed imaps
995/tcp   closed pop3s
1025/tcp  closed NFS-or-IIS
```

Pada /etc/hosts.deny akan di tambahkan langsung seperti berikut

```
susan@susan: ~
File Edit View Terminal Help

GNU nano 2.2.4 File: /etc/hosts.deny

# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

#in.telnetd: 192.168.2.2 : twist /bin/echo "Anda tidak dapat memasuki area "
#sshd: ALL:EXCEPT 192.168.2.2

#ALL: 192.168.2.2
ALL: 192.168.2.2
ALL: 192.168.2.2
█

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Maka porstentry telah selesai dijalankan

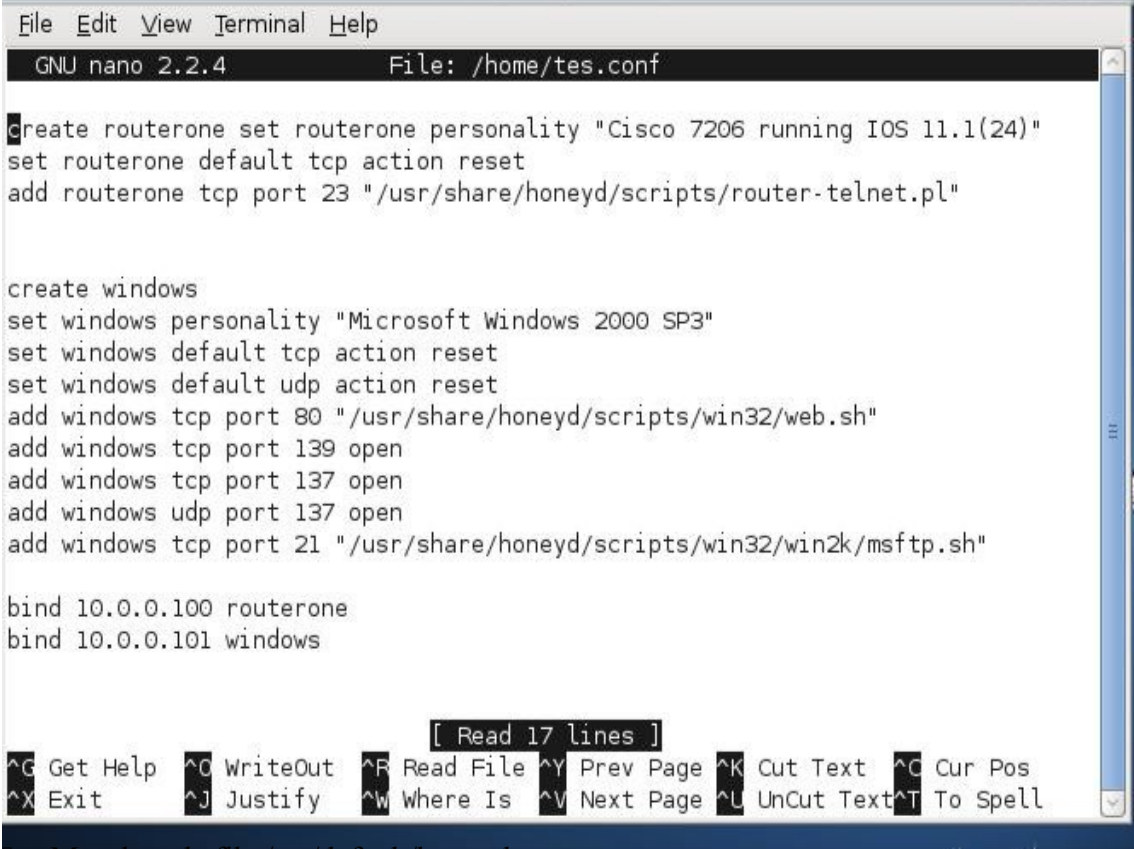
Konfigurasi honeyd pada server

□ Langkah pertama hapus konfigurasi portsenry pada server

□ Langkah selanjutnya menginstal honeyd #apt-get install honeyd

□ Masukkan script berikut dengan perintah “nano /etc/home/tes.conf”

```
Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer
```



```
File Edit View Terminal Help
GNU nano 2.2.4 File: /home/tes.conf

create routerone set routerone personality "Cisco 7206 running IOS 11.1(24)"
set routerone default tcp action reset
add routerone tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"

create windows
set windows personality "Microsoft Windows 2000 SP3"
set windows default tcp action reset
set windows default udp action reset
add windows tcp port 80 "/usr/share/honeyd/scripts/win32/web.sh"
add windows tcp port 139 open
add windows tcp port 137 open
add windows udp port 137 open
add windows tcp port 21 "/usr/share/honeyd/scripts/win32/win2k/msftp.sh"

bind 10.0.0.100 routerone
bind 10.0.0.101 windows

[ Read 17 lines ]
^G Get Help ^C WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^O Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

□ Masuk pada file /etc/default/honeyd

```
File Edit View Terminal Help
GNU nano 2.2.4 File: /etc/default/honeyd

# Defaults for honeyd initscript

# Master system-wide honeyd switch. The initscript
# will not run if it is not set to yes.
RUN="yes"

# Default options.
# Interface to listen on (if unset honeyd will select
# an interface himself)
# Note: Use only one! if you wish to use
# more than one use multiple -i in OPTIONS
INTERFACE="eth0"

# Network Honeyd will listen for. IF this is not set
# Honeyd will claim _all_ IP addresses set on the configured
# interface (which is probably _not_ what you want)
# This "sane" default will prevent you from doing it.
NETWORK=10.0.0.2

[ Read 39 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Lakukan arp poisoning dari server

```
0 Aktifkan honeyd seperti pada gambar berikut

root@susan:/home/susan# farpd -i eth0 10.0.0.100
arpd[2950]: listening on eth0: arp and (dst 10.0.0.100) and not ether src 08:00:
27:12:65:19
root@susan:/home/susan# farpd -i eth0 10.0.0.101
arpd[2953]: listening on eth0: arp and (dst 10.0.0.101) and not ether src 08:00:
27:12:65:19
root@susan:/home/susan#
```

```
Terminal (as superuser)
File Edit View Terminal Help
)
honeyd[1922]: Killing unknown connection: tcp (192.168.2.2:33266 - 10.0.0.100:23
)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Expiring OS fingerprint for 172.25.1.1
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Expiring OS fingerprint for 192.168.2.2
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
honeyd[1922]: Connection to closed port: udp (10.0.0.1:5353 - 224.0.0.251:5353)
^Choneyd[1922]: exiting on signal 2
root@susan:/home/susan# nano /home/tes.conf
root@susan:/home/susan#
```

Lakukan scanning port pada ip fake 10.0.0.100 dan 10.0.0.101

```
root@susan:/home/susan# nmap -sT -PO 10.0.0.101

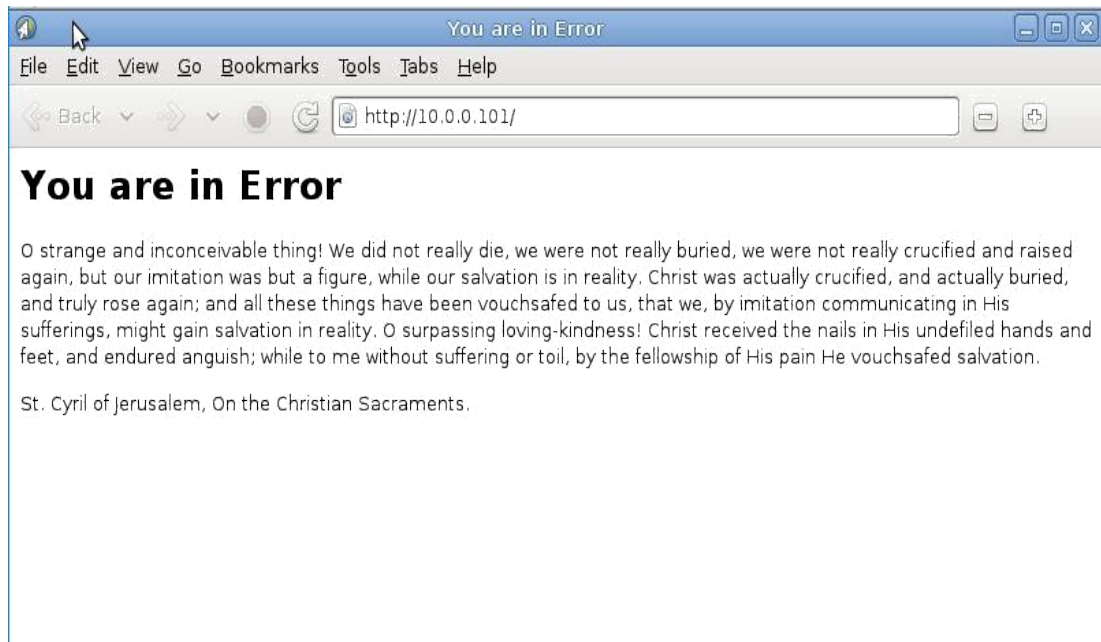
Starting Nmap 5.00 ( http://nmap.org ) at 2017-03-16 02:58 PDT
All 1000 scanned ports on 10.0.0.101 are filtered

Nmap done: 1 IP address (1 host up) scanned in 23.93 seconds
root@susan:/home/susan# nmap -sT -PO 10.0.0.100

Starting Nmap 5.00 ( http://nmap.org ) at 2017-03-16 03:00 PDT
All 1000 scanned ports on 10.0.0.100 are filtered

Nmap done: 1 IP address (1 host up) scanned in 135.40 seconds
root@susan:/home/susan#
```

□ Lakukan scanning port untuk mengecek kalau internet jadi



5.4.KESIMPULAN

Portsentry dapat mencegah port scanning, dan Honeypot data meredirect attacker ke server palsu selagi melindungi server asli.\

MODUL 6
INTRUSION DETECTION SYSTEM
[TRIPWIRE]

6.1. Tujuan

1. Mengenalkan pada mahasiswa tentang konsep integrator cek pada IDS
2. Mampu membedakan konsep IDS host base dan network base
3. Mampu melakukan instalasi, konfigurasi dan memakaai Tripwire sebagai program hostbase IDS dengan sistem integrator Checking

6.2. Teori Dasar

6.2.1. Tripwire

Tripwire merupakan salah satu program IDS yang masuk ke dalam jenis host base. Untuk memonitoring semua sistem yang ada di server cukuplah sulit untuk dilakukan. Hal itu disebabkan banyaknya file yang dikelola dan tidak mungkin dilakukan pengecekan satu-per-satu. Oleh karena itu diperlukannya tripwire untuk melakukan auditing file di server. Logika yang dilakukan suatu program tripwire adalah dengan membuat suatu baseline database yang ada pada sistem. Dimana apabila suatu file berubah maka tripwire akan mencatat dan memberitahukan perubahan tersebut kepada admin. Program tripwire berfungsi untuk menjaga integritas file sistem dan direktori, dengan mencatat setiap perubahan yang terjadi pada file atau direktori. Konfigurasi tripwire meliputi pelaporan melalui email apabila menemukan perubahan file yang tidak semestinya dan secara otomatis melakukan pemeriksaan file. Tripwire mampu mempermudah pekerjaan yang dilakukan oleh admin dalam mengamankan suatu sistem yang begitu banyak.

Beberapa hal yang mapu dilakukan oleh tripwire antara lain file integrity cheking, tripwire mampu mendeteksi perubahan file, serta tripwire melakukan perbandingan antara database file sebelum pengecekan dengan database file setelah pengecekan.

Hal yang tidak dapat dilakukan oleh tripwire antara lain, tripwire tidak dapat menghalangi perubahan file/sistem; tripwire bukan merupakan suatu antivirus; program tripware mampu dimanipulasi; serta false positif karena salah setting pada file policy, file konfigurasi, atau tidak update database. Secara garis besar cara kerja dari tripwire adalah melakukan perbnadingan file dan direktori yang ada dengan database sistem. Perbandingan tersebut meliputi perubahan tanggal, ukuran file, penghapusan, perubahan isi file serta lain

sebagainya. Setelah tripwire dijalankan, secara otomatis akan melakukan pembuatan database sistem. Setelah itu secara periodic akan melaporkan setiap perubahan pada file dan direktori kepada admin.

Percobaan dengan menggunakan program tripwire diperlukan suatu web server sederhana guna untuk melakukan monitoring dan mencatat semua kegiatan yang terjadi pada suatu web server tersebut. Dalam direktori tripwire itu sendiri terdapat dua file yang perlu dikonfigurasi, konfigurasi file yang terdapat pada “/etc/tripwire/twcfg.txt” konfigurasi file policy “/etc/tripwire/twpol.txt” untuk menjalankan hasil yang telah dikonfigurasi terdapat pada file “/etc/tripwire/twinstall.sh”. Langkah selanjutnya inialisasi tripwire dengan meng-generate database, menjalankan tripwire guna untuk melakukan pengecekan integrity, melakukan pengecekan pada tripwire yang terdapat pada print report, melakukan update policy file. Setelah penyetingan selesai tripwire akan melakukan pengecekan terhadap integrity file, dan kejanggalan dari file tersebut dapat dilaporkan dengan mengirimkan laporan/pesan ke email.

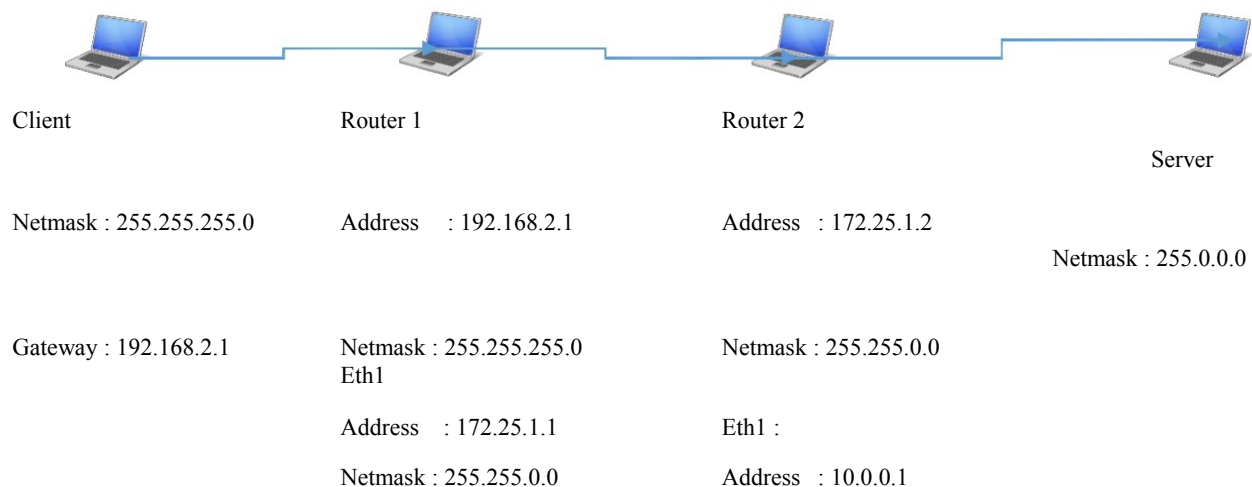
6.3. Kegiatan Rangkuman

6.3.1. Peralatan

Alat dan bahan

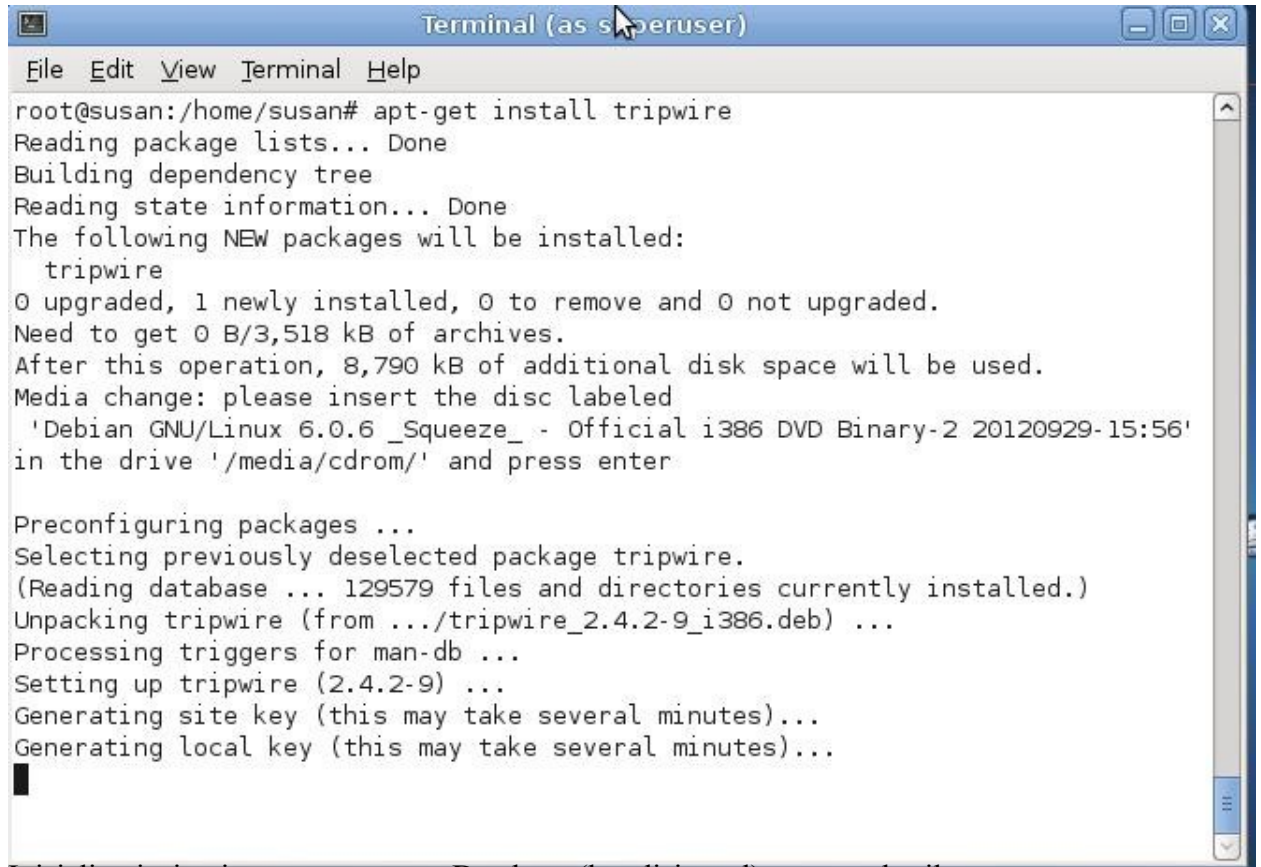
- ▣ 1 buah laptop
- ▣ Virtual Machine(VirtualBox/VMware)
- ▣ ISO : Debian6

6.3.2. Topologi Jaringan



6.3.3. Langkah Kerja

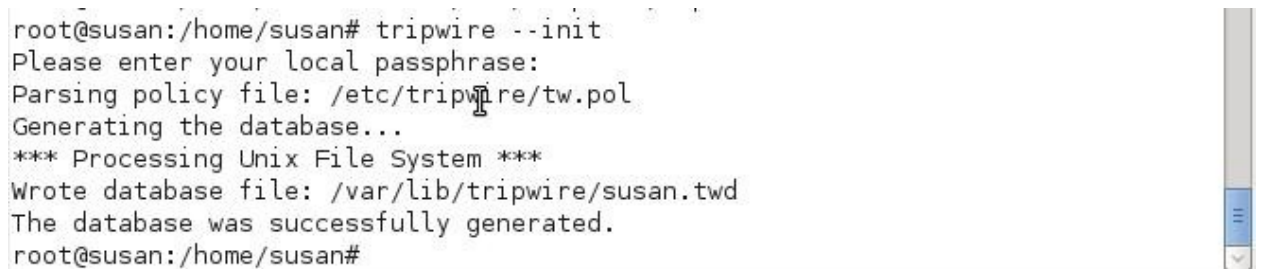
- Langkah pertama yang harus di lakukan adalah menginstall tripwire



```
Terminal (as susan)
File Edit View Terminal Help
root@susan:/home/susan# apt-get install tripwire
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  tripwire
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/3,518 kB of archives.
After this operation, 8,790 kB of additional disk space will be used.
Media change: please insert the disc labeled
'Debian GNU/Linux 6.0.6 _Squeeze_ - Official i386 DVD Binary-2 20120929-15:56'
in the drive '/media/cdrom/' and press enter


Preconfiguring packages ...
Selecting previously deselected package tripwire.
(Reading database ... 129579 files and directories currently installed.)
Unpacking tripwire (from .../tripwire_2.4.2-9_i386.deb) ...
Processing triggers for man-db ...
Setting up tripwire (2.4.2-9) ...
Generating site key (this may take several minutes)...
Generating local key (this may take several minutes)...
█
```

- Inisialisasi tripwire, men-generate Database (kondisi awal) => catat hasilnya



```
root@susan:/home/susan# tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
Wrote database file: /var/lib/tripwire/susan.twd
The database was successfully generated.
root@susan:/home/susan#
```

- Menjalankan tripwire, melakukan integrity check (pengecekan terhadap intruder)



```
root@susan:/home/susan# tripwire --check | more
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
█
```

```
Terminal (as Superuser)
File Edit View Terminal Help
Note: Report is not encrypted.
Open Source Tripwire(R) 2.4.1 Integrity Check Report

Report generated by:      root
Report created on:       Thu Mar 16 09:16:42 2017
Database last updated on: Never

=====
Report Summary:
=====

Host name:                susan
Host IP address:         127.0.1.1
Host ID:                 None
Policy file used:        /etc/tripwire/tw.pol
Configuration file used: /etc/tripwire/tw.cfg
Database file used:      /var/lib/tripwire/susan.twd
Command line used:       tripwire --check

=====
Rule Summary:
=====

--More--
```

□ Cek hasil tripwire, dengan menggunakan default policy, amati dan catat output yang dihasilkan . Default policy dapat dilihat di :

```
nano /etc/tripwire/twpol.txt.new
```

```
# Lakukan beberapa percobaan untuk menguji policy diatas.
```

a. Lakukan telnet dari PC Client dan tambahkan file pada folder /home di PC Server

```
# telnet <no_ip_server>
```

```
# touch /home/data.txt
```

b. Copylah file mkdir pada folder /bin

```
# cp /bin/mkdir /home
```

c. Copylah file data.txt pada folder /home

```
# cp /home/data.txt /bin
```

```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /etc/tripwire/twpol.txt.new
SEC_CRIT = $(IgnoreNone)-SHA;
SEC_BIN = $(ReadOnly);
SEC_CONFIG = $(Dynamic);
SIG_HI = 100;
SIG_MED = 66;
SIG_LOW = 33;
(
    rulename = "Deteksi intruder",
    severity = $(SIG_MED)
)
{
    /bin -> $(SEC_BIN);
    /home -> $(SEC_BIN);
}
(
    rulename = "keamana user",
    severity = $(SIG_MED)
)
{
    [ Read 23 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^L UnCut Text ^T To Spell
```

Cek kondisi berikut :

- telnet dari client ip server 10.0.0.2 dan buatlah sebuah file difolder :
touch /root/data.txt
- cek kembali hasilnya di PC server

```

Terminal (as superuser)
File Edit View Terminal Help
Command line used:          tripwire --check

=====
Rule Summary:
=====

-----
Section: Unix File System
-----

Rule Name                      Severity Level   Added   Removed   Modified
-----
* Deteksi intruder             66               0       0          1
  keamana user                  66               0       0          0

Total objects scanned:  425
Total violations found:  1

=====
Object Summary:
=====

--More--

```

□ **Tambahkan user baru dari client**

```

root@susan:/home/susan# adduser ssl
Adding user `ssl' ...
Adding new group `ssl' (1005) ...
Adding new user `ssl' (1005) with group `ssl' ...
Creating home directory `/home/ssl' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for ssl
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
root@susan:/home/susan#

```

□ Supaya tripwire bisa disetting sesuai keperluan, misal akan melakukan cek setiap hari, tambahkan file tripwire-check sebagai berikut :

```

# /bin/sh
HOST_NAME=`uname -n`
if [ ! -e /var/lib/tripwire/${HOST_NAME}.twd ]; then
    echo "Error: Tripwire database for ${HOST_NAME} not found"
    echo "Run "/usr/sbin/tripwire --init""
else
    test -f /etc/tripwire/tw.cfg && /usr/sbin/tripwire --check
fi

```

- Jalankan kembali tripwire dan ceklah hasilnya (amati dan catat hasilnya) :

```
# tripwire --check
```

```

Host name:                susan
Host IP address:         127.0.1.1
Host ID:                 None
Policy file used:       /etc/tripwire/tw.pol
Configuration file used: /etc/tripwire/tw.cfg
Database file used:    /var/lib/tripwire/susan.twd
Command line used:     tripwire --check

=====
Rule Summary:
=====

-----
Section: Unix File System
-----

Rule Name                Severity Level    Added    Removed    Modified
-----
* Deteksi intruder      66                8        0          8
* keamana user          66                0        0          2

Total objects scanned: 433
Total violations found: 18

```

6.4. Kesimpulan

Tripwire membuat suatu baseline database dengan melakukan auditing file. Berfungsi untuk menjaga integritas file sistem.

MODUL 7
SYMMETRIC CRYPTOGRAPHY

7.1. Tujuan

1. Mengenalkan pada mahasiswa tentang konsep cryptography
2. Mahasiswa mampu membuat program enkripsi Caesar dan RC4
3. Mahasiswa mampu membuat program dekripsi Caesar dan RC4

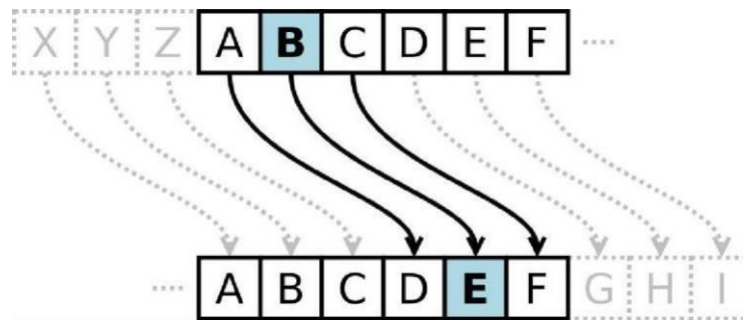
7.2. Teori Dasar

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Terdapat 2 jenis kriptografi dipandang dari masanya :

1. Kriptografi klasik : Caesar cipher, Affine cipher, Vigenere cipher dll.
2. Kriptografi modern, terbagi 2 yaitu :
 - a. Kriptografi simetrik : RC4, DES, AES, IDEA
 - b. Kriptografi asimetrik : RSA, DSA, El gama

Kriptografi Klasik (Caesar)

Pada Caesar cipher, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu 3). Susunan alphabet setelah digeser sejauh 3 huruf membentuk sebuah table substitusi sebagai berikut :



Gambar 1. Kriptografi Caesar

Kriptografi Simetrik

Kriptografi simetrik atau dikenal pula sebagai kriptografi kunci rahasia, merupakan kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi. Secara matematis dapat dinyatakan bahwa :

$$E_k(m) = c \quad (4)$$

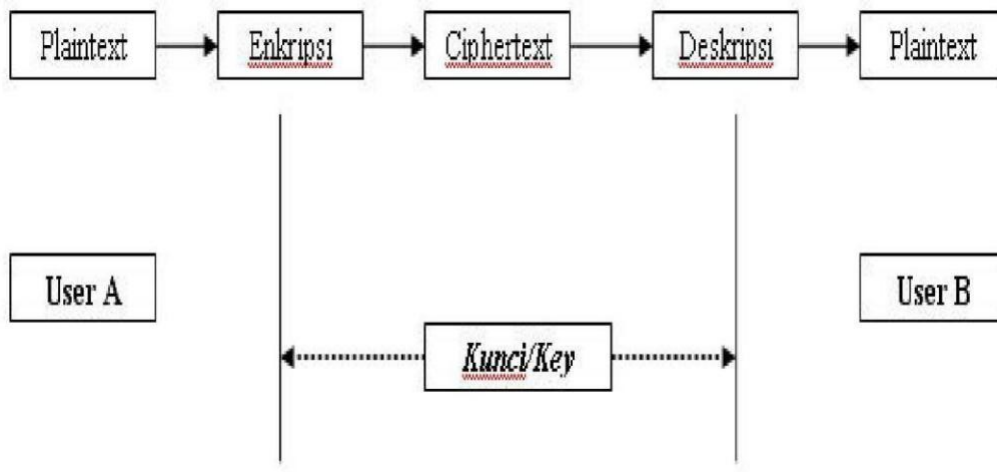
$$D_k(c) = m \quad (5)$$

$$D_k(D_k(c)) = c \quad (6)$$

Dalam algoritma simetri, kunci yang digunakan dalam proses enkripsi dan dekripsi adalah sama atau pada prinsipnya identik. Kunci ini pun bisa diturunkan dari kunci lainnya. Oleh karena itu sistem ini sering disebut secret-key ciphersystem.

Agar komunikasi tetap aman, kunci yang menggunakan teknik enkripsi ini harus betul-betul dirahasiakan.

Kriptografi simetrik sangat menekankan pada kerahasiaan kunci yang digunakan untuk proses enkripsi dan dekripsi. Oleh karena itulah kriptografi ini dinamakan pula sebagai kriptografi kunci rahasia. Gambaran proses sederhana enkripsi dengan algoritma simetri:



Gambar 2. Blok Diagram algoritma Simetri

Algoritma RC4

RC4 merupakan merupakan salah satu jenis stream cipher, yaitu memproses unit atau input data pada satu saat. Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip. Metode enkripsi RC4 sangat cepat kurang lebih 10 kali lebih cepat dari DES.

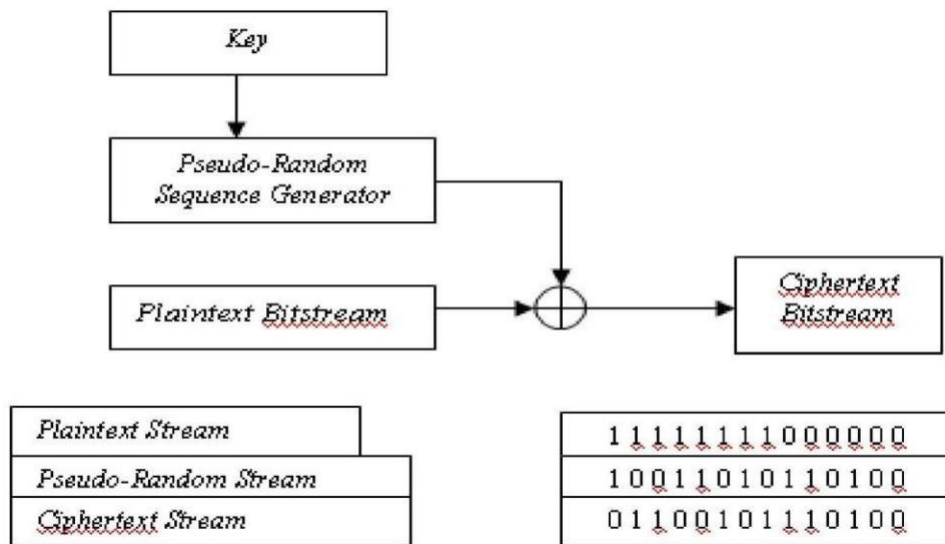
RC4 merupakan stream cipher yang didesain oleh Rivest untuk RSA Data Security (sekarang RSA Security) pada 1987. RC4 menggunakan panjang variabel kunci dari 1 s.d 256 byte untuk menginisialisasi state tabel. State table digunakan untuk pengurutan menghasilkan byte pseudo-random yang kemudian menjadi stream pseudo-random. Setelah di-XOR dengan plaintext sehingga didapatkan ciphertext. Tiap elemen pada state table di swap sedikitnya sekali. Kunci RC4 sering dibatasi sampai 40 bit, tetapi dimungkinkan untuk menggunakan kunci 128 bit. RC4 memiliki kemampuan penggunaan kunci antara 1 sampai 2048 bit.

Panjang kunci merupakan faktor utama dalam sekuritas data. RC4 dapat memiliki kunci sampai dengan 128 bit. Protokol keamanan SSL (Secure Socket Layer) pada Netscape Navigator menggunakan algoritma RC4 40-bit untuk enkripsi simetrisnya.

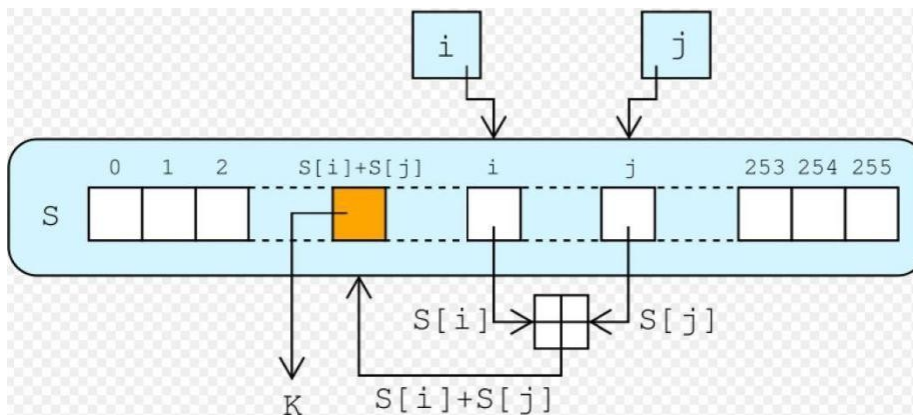
Algoritma RC4 memiliki dua fase, setup kunci dan pengenkripsian. Setup untuk kunci adalah fase pertama dan yang paling sulit dalam algoritma ini. Dalam setup Sbit kunci (S merupakan panjang dari kunci), kunci enkripsi digunakan untuk menghasilkan variabel enkripsi yang menggunakan dua buah array, state dan kunci, dan sejumlah-S hasil dari operasi penggabungan. Operasi penggabungan ini terdiri dari pemindahan (swapping) byte, operasi modulo, dan rumus lain. Operasi modulo merupakan proses yang menghasilkan nilai sisa dari satu pembagian. Sebagai contoh, 11 dibagi 4 adalah 2 dengan sisa pembagian 3, begitu juga jika tujuh modulo empat maka akan dihasilkan nilai tiga.

Variabel enkripsi dihasilkan dari setup kunci dimana kunci akan di XOR-kan dengan plain text untuk menghasilkan teks yang sudah terenkripsi. XOR merupakan operasi logik yang membandingkan dua bit biner. Jika bernilai beda maka akan dihasilkan nilai 1. Jika kedua bit sama maka hasilnya adalah 0. Kemudian penerima pesan akan mendekripsinya dngan meng XOR-kan kembali dengan kunci yang sama agar dihasilkan pesan dari plain text tersebut.

Untuk menunjukkan cara kerja dari algoritma RC4, berikut dapat dilihat pada blok di bawah :



Gambar 3. Blok Diagram algoritma RC 4 secara umum



Gambar 4. Proses pembangkitan acak untuk kunci RC4

RC4 menggunakan dua buah kotak substitusi (S-Box) array 256 byte yang berisi permutasi

dari bilangan 0 sampai 255 dan S-Box kedua yang berisi permutasi fungsi dari kunci dengan panjang yang variabel.

Cara kerja algoritma RC4 yaitu inisialisasi Sbox pertama, $S[0], S[1], \dots, S[255]$, dengan bilangan 0 sampai 255. Pertama isi secara berurutan $S[0] = 0, S[1] = 1, \dots, S[255] = 255$. Kemudian inisialisasi array lain (S-Box lain), misal array K dengan panjang 256. Isi array K dengan kunci yang diulangi sampai seluruh array $K[0], K[1], \dots, K[255]$ terisi seluruhnya.

Langkah-langkah algoritma RC4:

1. Proses inisialisasi S-Box (Array

S) For $i = 0$ to 255

$S[i] = i$

2. Proses inisialisasi S-Box (Array K) untuk kunci.

Lakukan padding jika panjang kunci < 256 .

Array Kunci // panjang kunci "length". for $i = 0$ to 255

$K[i] = \text{Kunci}[i \bmod \text{length}]$

3. Kemudian lakukan langkah pengacakan S-Box dengan langkah sebagai berikut : $j = 0$

For $i = 0$ to 255 $j = (j + S[i] + K[i]) \bmod 256$ isi

$S[i]$ dan isi $S[j]$ ditukar

Endfor

4. Dengan demikian berakhirilah proses persiapan kunci RC4. Untuk membangkitkan kunci enkripsi, dilakukan proses sebagai berikut: $i = 0, j = 0$

for $\text{idx} = 0$ to $\text{plainteks}-1$ do $i = (i + 1) \bmod 256$
 $j = (j + S[i]) \bmod 256$

```

isi S[i] dan S[j] ditukar      t = (S[i] + S[j]) mod
256 k = S [t]
c = P[idx]      k
endfor

```

Perhatikan bahwa k kecil merupakan kunci yang langsung beroperasi terhadap plainteks, sedangkan K besar adalah kunci utama atau kunci induk. Bila terdapat plainteks P, maka operasi enkripsi berupa :

$$C = P \oplus k$$

Sedangkan operasi dekripsi
berupa : $P = k \oplus C$

□
Pada chmod 777 maka keterangannya akan tertulis

rw-rw-rw- yang apabila kita terjemahkan dengan angka biner adalah sebagai berikut

<i>rw-</i>	<i>rw-</i>	<i>rw-</i>
<i>111</i>	<i>111</i>	<i>111</i>
<i>4+2+1</i>	<i>4+2+1</i>	<i>4+2+1</i>
<i>7</i>	<i>7</i>	<i>7</i>

sedangkan jika kita mengetikkan syntag chmod 755 maka pada keterangan akan tertulis

rw-r-xr-x

yang bila dibinerkan adalah

<i>r</i>	<i>r-</i>	<i>r</i>
<i>1</i>	<i>x</i>	<i>1</i>
	<i>10</i>	

<i>4+</i>	<i>4+</i>	<i>4</i>
<i>7</i>	<i>5</i>	<i>+</i>
		<i>5</i>

Teman-teman sudah mengerti atau belum apa sih arti dari

rwx?

*r=read=4 -> permission untuk hak read /
baca w=write=2 -> permission untuk hak
write / tulis x=execute=1 -> permission untuk
hak execute /*

menjalankan file executable

jadi jika kita menetikkan `chmod 777=rwxrwxrwx` dan jika kita menetikkan `chmod 755=rwxr-xr-x`

-tiga kolom `rwx` pertama menyatakan permission yg dimiliki owner file/direktori.

-tiga kolom `rwx` kedua menyatakan permission yg dimiliki group dari ownernya.

-tiga kolom `rwx` ketiga menyatakan permission yg dimiliki oleh other berarti disini selain owner dan grup.

7.3. Kegiatan Rangkuman

7.3.1. Peralatan

Alat dan bahan

- 1 buah laptop
- Virtual Machine(VirtualBox/VMware)
- ISO : Debian6



7.3.2. Topologi Jaringan

Server

Netmask : 255.255.255.0

Address : 192.168.7.1

Client

Address : 192.168.7.2

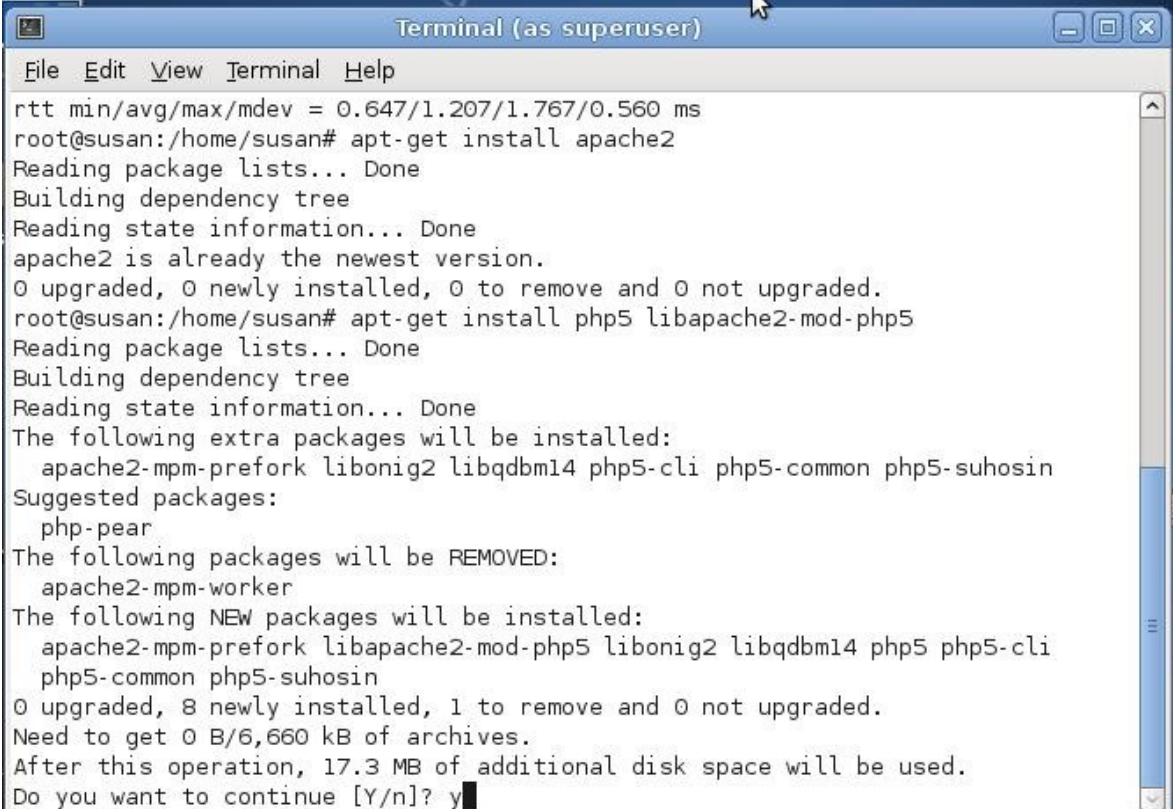
Netmask : 255.255.255.0

7.3.3. Langkah Kerja

7.3.3.1. Lakukan instalasi apache2 php5 pada PC Server :

```
# apt-get install apache2
```

```
# apt-get install php5 libapache2-mod-php5
```



```
Terminal (as superuser)
File Edit View Terminal Help
rtt min/avg/max/mdev = 0.647/1.207/1.767/0.560 ms
root@susan:/home/susan# apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@susan:/home/susan# apt-get install php5 libapache2-mod-php5
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-mpm-prefork libonig2 libqdbm14 php5-cli php5-common php5-suhosin
Suggested packages:
  php-pear
The following packages will be REMOVED:
  apache2-mpm-worker
The following NEW packages will be installed:
  apache2-mpm-prefork libapache2-mod-php5 libonig2 libqdbm14 php5 php5-cli
  php5-common php5-suhosin
0 upgraded, 8 newly installed, 1 to remove and 0 not upgraded.
Need to get 0 B/6,660 kB of archives.
After this operation, 17.3 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

7.3.3.2. Selanjutnya Restart apache :

```
# /etc/init.d/apache2 restart
```

7.3.3.3. Buat file php sebagai berikut: nano /var/www/info.php



```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/info.php
<?php
phpinfo();
?>
```

7.3.3.4. Tes konfigurasi dengan mengakses dari PC Client, buka web browser di PC

Client dan masukkan alamat :

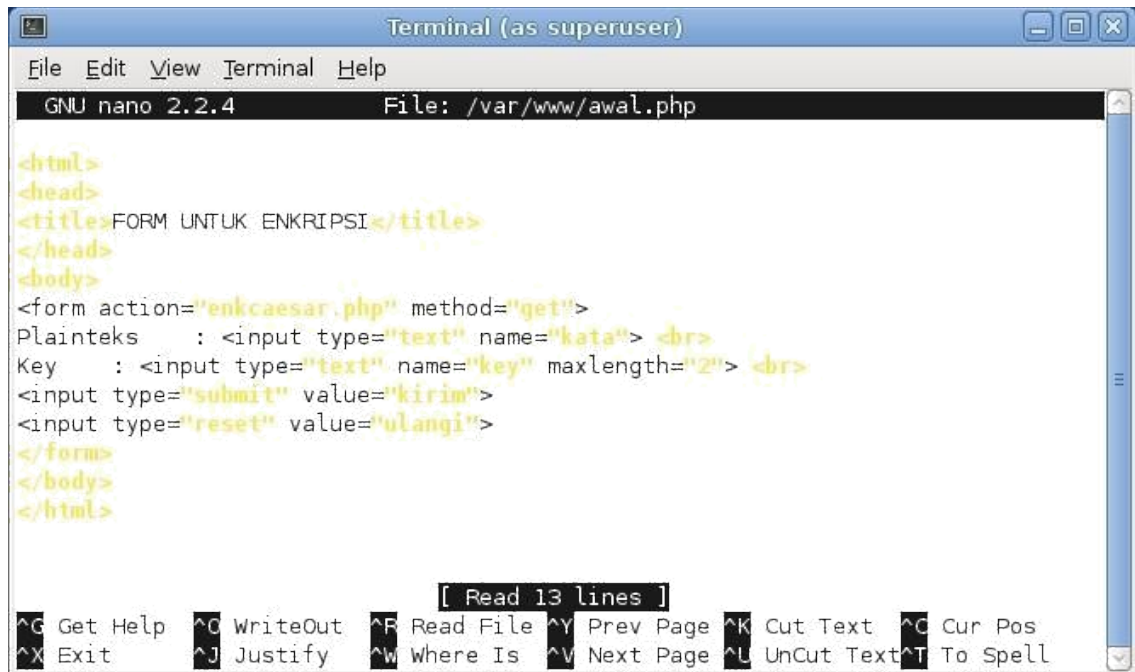
http://<no_ip_pc_server>/info.php

System	Linux susan 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686
Build Date	Feb 10 2012 14:09:56
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2/
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/suhosin.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS
PHP Extension Build	API20090626,NTS
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled

7.3.3.5.Kriptografi klasik (Caesar cipher)

Pembuatan Form Masukkan PHP

1. Buat file untuk masukan plainteks dan key (berupa bilangan), beri nama file: awal.php di PC Server



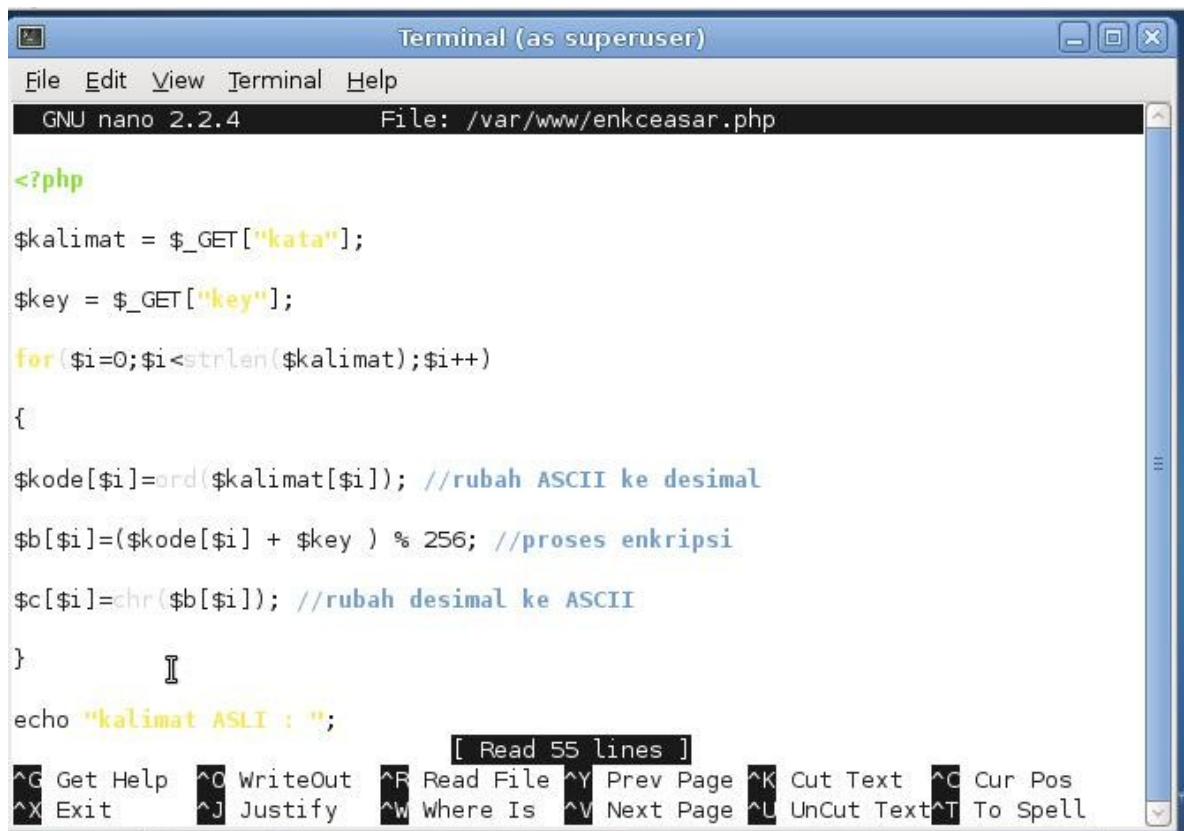
```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/awal.php

<html>
<head>
<title>FORM UNTUK ENKRIPSI</title>
</head>
<body>
<form action="enkcaesar.php" method="get">
Plainteks : <input type="text" name="kata"> <br>
Key : <input type="text" name="key" maxlength="2"> <br>
<input type="submit" value="kirim">
<input type="reset" value="ulangi">
</form>
</body>
</html>

[ Read 13 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^L UnCut Text ^T To Spell
```

Proses Enkripsi dengan Caesar Algorithm

2. Buat file untuk melakukan proses enkripsi, beri nama file: enkcaesar.php di PC Server



```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/enkcaesar.php

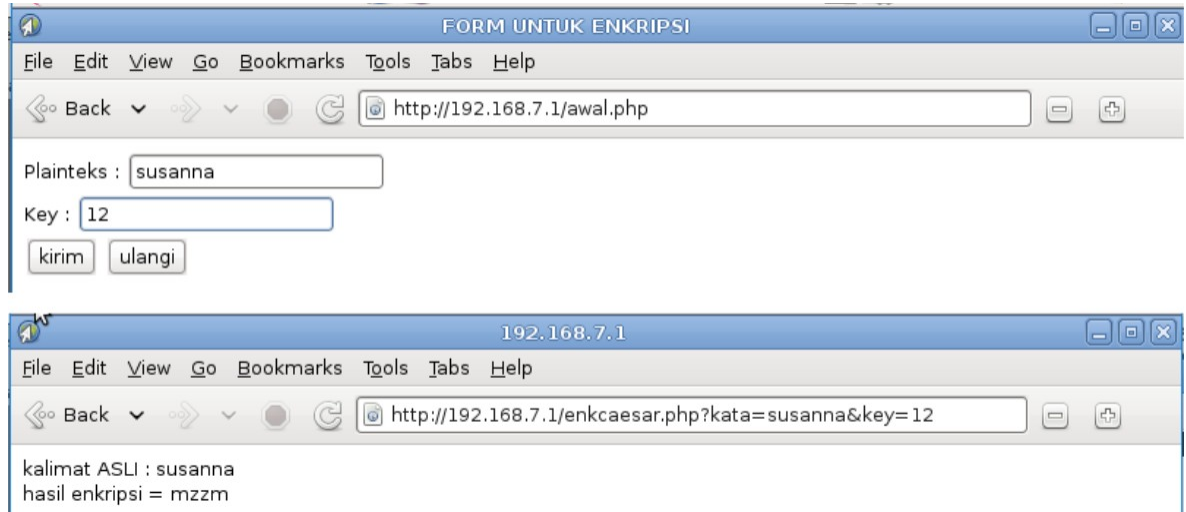
<?php
$kalimat = $_GET["kata"];
$key = $_GET["key"];
for($i=0;$i<strlen($kalimat);$i++)
{
$kode[$i]=ord($kalimat[$i]); //rubah ASCII ke desimal
$b[$i]=($kode[$i] + $key ) % 256; //proses enkripsi
$c[$i]=chr($b[$i]); //rubah desimal ke ASCII
}
echo "kalimat ASLI : ";

[ Read 55 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^L UnCut Text ^T To Spell
```

Tes Proses Enkripsi

3. Buka web browser dari PC Client dan akseslah file php dari PC Server

http://<no_ip_pc_server>/awal.php



Pembuatan Form untuk proses dekripsi

4. Buat file untuk masukan key (berupa bilangan), agar bisa menghasilkan kembali plainteks maka key harus sama dengan proses enkripsi, beri nama file: akhir.php di PC Server

```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/akhir.php

<html>
<head>
  <title>Form untuk Deskripsi</title>
</head>
<body>
  <form action="dekCaesar.php" method="get">
    Key : <input type="text" name="key" maxlength="2"> <br>
    <input type="submit" value="kirim">
    <input type="reset" value="ulangi">
  </form>
</body>
</html>
```

Proses Dekripsi dengan Caesar Algorithm

5. Buat file untuk melakukan proses dekripsi, beri nama file : dekCaesar.php di PC Server

```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/dekCaesar.php

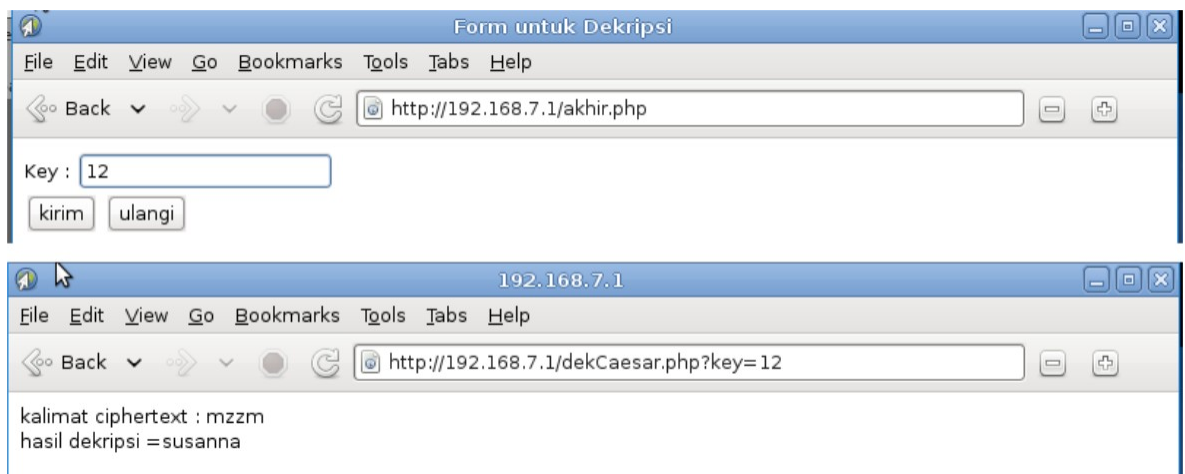
<?php
$key = $_GET["key"];
$nmfile = "enkripsi.txt";
$fp = fopen($nmfile,"r");
$isi = fread($fp,filesize($nmfile));

for ($i=0;$i<strlen($isi);$i++)
{
    $kode[$i]=ord($isi[$i]);
    $b[$i]=($kode[$i] - $key ) % 256;
    $c[$i]=chr($b[$i]);
}
echo "kalimat ciphertext : ";
for ($i=0;$i<strlen($isi);$i++)
{
    echo $isi[$i];
}
echo "<br>";
echo "hasil dekripsi =";
for ($i=0;$i<strlen($isi);$i++)
{
    echo $c[$i];
}
echo "<br>";
?>
```

Tes Proses Dekripsi

Buka web browser dari PC Client dan akseslah file php dari PC

Server http://<no_ip_pc_server>/akhir.php



Kriptografi Modern (Simetrik RC4)

Pembuatan Form Masukan PHP

- Gunakan kembali file di poin 3.a, beri nama yang berbeda : awalrc4.php . Buat di PC Server, dan rubah hanya baris berikut :



```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/awalrc4.php

<html>
<head>
  <title>FORM UNTUK ENKRIPSI</title>
</head>
<body><form action="penkripsi.php" method="get">
Plainteks  : <input type="text" name="kata"> <br>
Key       : <input type="text" name="kcenkripsi" maxlength="16"> <br>
<input type="submit" value="kirim">
<input type="reset" value="ulangi">
</form>
</body>
</html>
```

NB : untuk kunci, dimasukkan kata tanpa spasi sebanyak 16 karakter
Proses Pembentukan Kunci Enkripsi dengan RC4 Algorithm

- Buat file untuk memproses setupkey dan enkripsi RC4, beri nama file penkripsi.php Buat program untuk setupkey:

```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/penkripsi.php

<?php
function setupkey() //proses pengacakan kunci di SBox
{
echo "<br>";
$kce = $_GET["kce"];
echo "Kunci enkripsi = $kce";
echo "<br>";
    for ($i=0;$i<strlen($kce);$i++)
    {
        $key[$i]=ord($kce[$i]); //rubah ASCII ke desimal
    }
    global $m;
    $m=array();
    // inisialisasi Sbox
    for ($i=0;$i<256;$i++){
        $m[$i] = $i;
    }
    //Lakukan permutasi thd nilai2 di dalam larik S
    $j = $k = 0;
    for ($i=0;$i<256;$i++)
    {
        $a = $m[$i];
        $j = ($j + $m[$i] + $key[$k]) % 256;
        //pertukarkan nilai S[i] dengan S[j]
        $m[$i] = $m[$j];
    }
}

```

Proses Enkripsi Algoritma RC4

Tambahkan program untuk enkripsi RC4 dibawah fungsi setupkey

```

function crypt2($inp)
{
    global $m;
    $x=0;$y=0;
    $bb='';
    $x = ($x+1) % 256;
    $a = $m[$x];
    $y = ($y+$a) % 256;
    //pertukarkan nilai S[i] dan S[j]
    $m[$x] = $b = $m[$y];
    $m[$y] = $a;
    //proses XOR antara plaintext dengan kunci
    //dengan $inp sebagai plaintext
    //dan $m sebagai kunci
    $bb= ($inp^$m[($a+$b) % 256]) % 256;
    return $bb;
}

$kalimat = $_GET["kata"];

^G Get Help    ^O WriteOut    ^R Read File    ^Y Prev Page    ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where Is    ^V Next Page    ^L UnCut Text  ^T To Spell

```

Tampilkan kalimat asli dan hasil enkripsi RC4

```

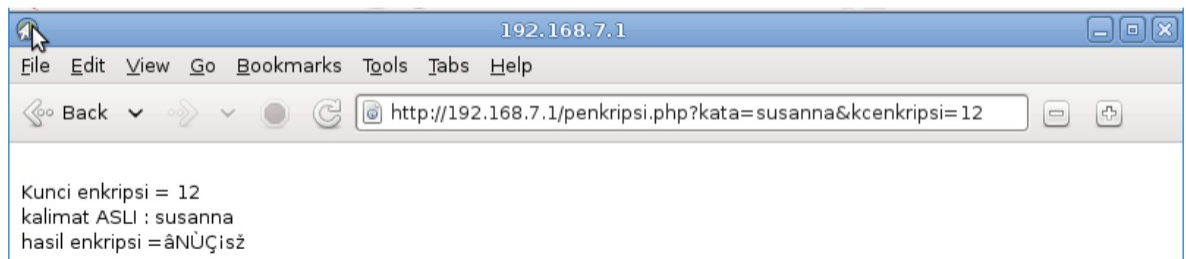
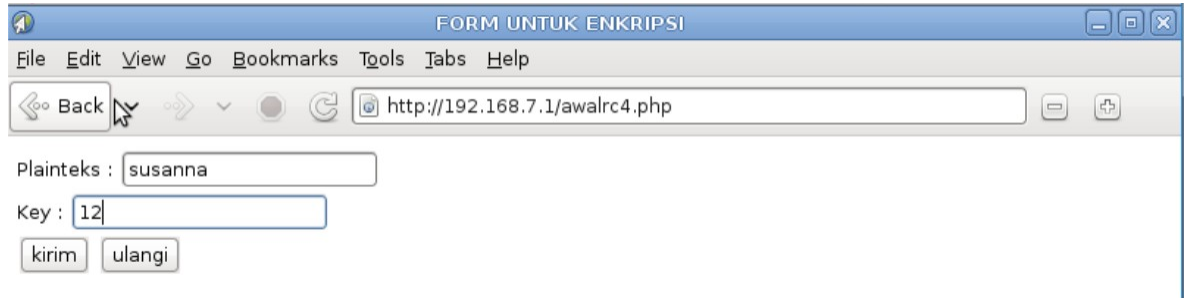
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/penkripsi.php

$kalimat = $_GET["kata"];
setupkey();
for ($i=0;$i<strlen($kalimat);$i++)
{
    $kode[$i]=ord($kalimat[$i]); //rubah ASCII ke desimal
    $b[$i]=crypt2($kode[$i]); //proses enkripsi RC4
    $c[$i]=chr($b[$i]); //rubah desimal ke ASCII
}
echo "kalimat ASLI : ";
for ($i=0;$i<strlen($kalimat);$i++)
{
    echo $kalimat[$i];
}
echo "<br>";
echo "hasil enkripsi =";
$hsl = '';
for ($i=0;$i<strlen($kalimat);$i++)
{
    echo $c[$i];
    $hsl = $hsl . $c[$i];
}
echo "<br>";
//simpan data di file
^G Get Help    ^O WriteOut    ^R Read File    ^Y Prev Page    ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where Is    ^V Next Page    ^L UnCut Text  ^T To Spell

```

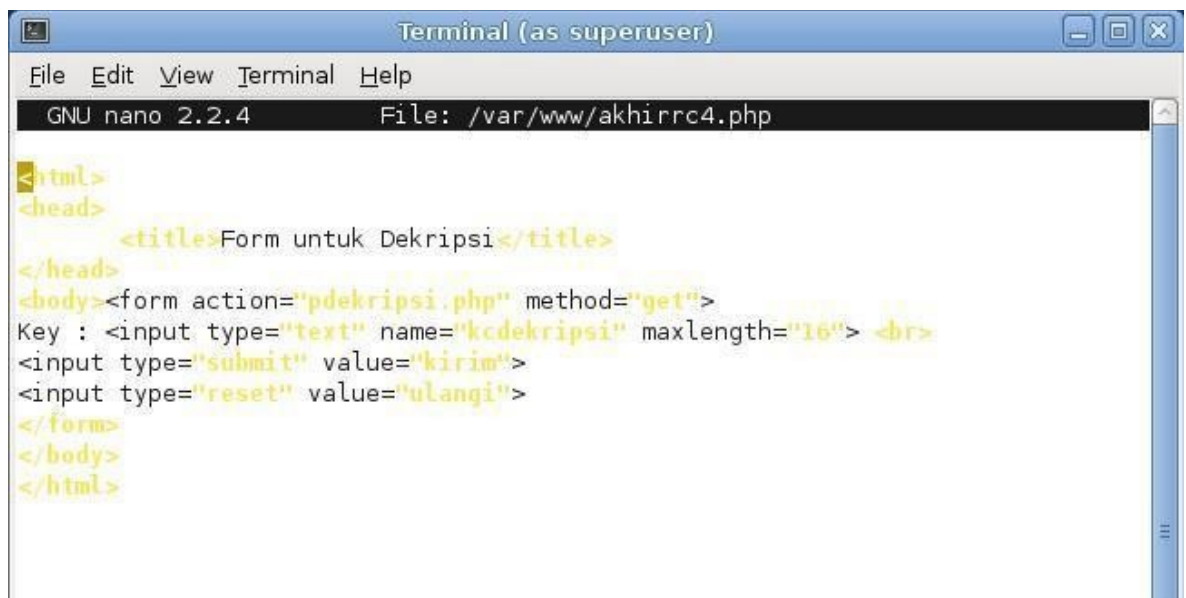

Tes Proses Enkripsi

Buka web browser dari PC Client dan akseslah file php dari PC Server
`http://<no_ip_pc_server>/awalrc4.php`



Pembuatan Form untuk proses dekripsi

Gunakan kembali file di 3.e. dan rubah beberapa baris berikut : Buat file untuk
Masukan key (berupa bilangan), agar bisa menghasilkan kembali plainteks maka
key harus sama dengan proses enkripsi, beri nama file: akhirrc4.php di PC
Server

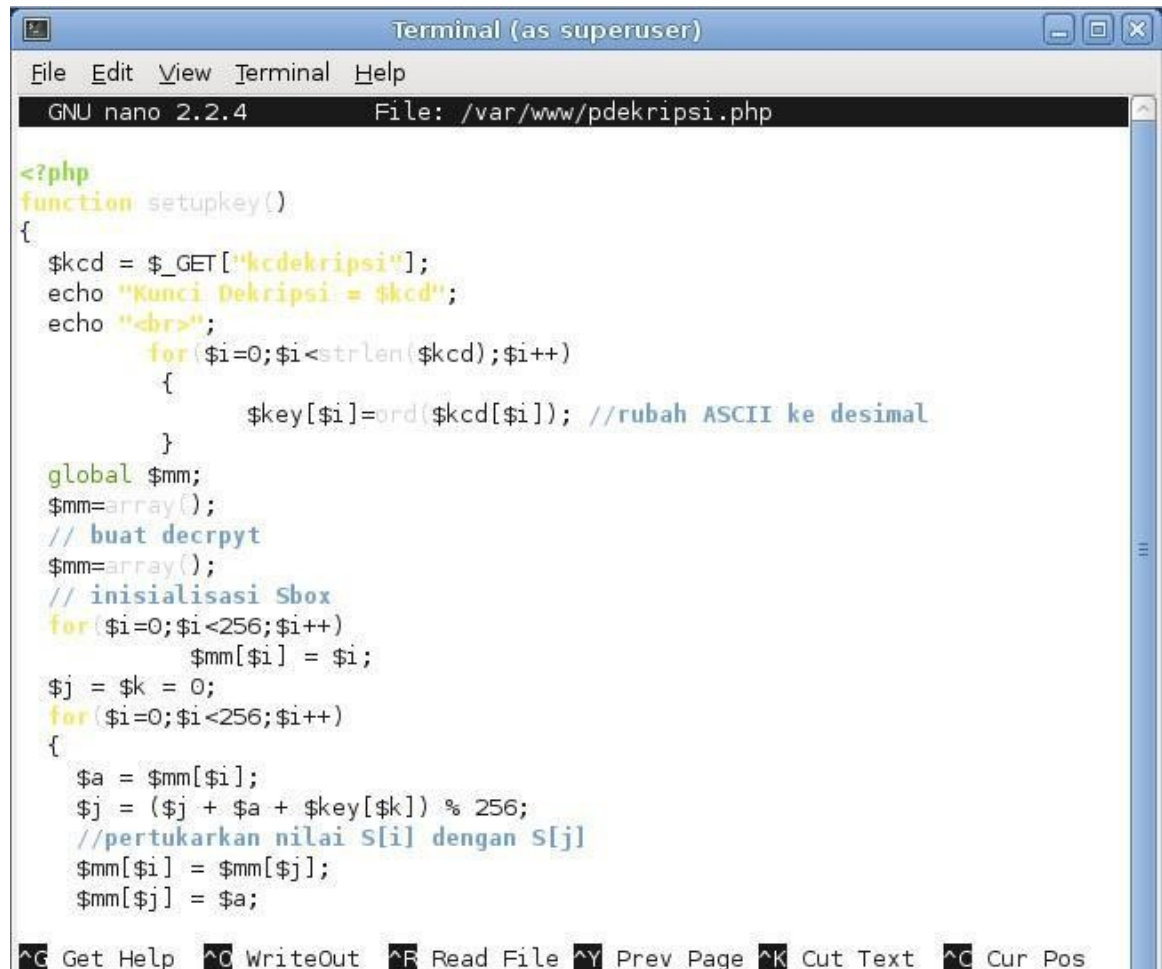


NB : agar bisa menghasilkan kembali plainteks maka key harus sama dengan proses enkripsi

Proses Pembentukan Kunci Dekripsi dengan RC4 Algorithm

Buat file untuk memproses setupkey dan enkripsi RC4, beri nama file pdekripsi.php

Buat program untuk setupkey (proses ini sama dengan proses pembentukan kunci untuk enkripsi):



```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/pdekripsi.php

<?php
function setupkey()
{
    $kcd = $_GET["kcdekripsi"];
    echo "Kunci Dekripsi = $kcd";
    echo "<br>";
    for($i=0;$i<strlen($kcd);$i++)
    {
        $key[$i]=ord($kcd[$i]); //rubah ASCII ke desimal
    }

    global $mm;
    $mm=array();
    // buat decrypt
    $mm=array();
    // inialisasi Sbox
    for($i=0;$i<256;$i++)
        $mm[$i] = $i;
    $j = $k = 0;
    for($i=0;$i<256;$i++)
    {
        $a = $mm[$i];
        $j = ($j + $a + $key[$k]) % 256;
        //pertukarkan nilai S[i] dengan S[j]
        $mm[$i] = $mm[$j];
        $mm[$j] = $a;
    }
}
```

Proses Dekripsi Algoritma RC4

Tambahkan program untuk dekripsi RC4 dibawah fungsi setupkey:

```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/pdekripsi.php

function decrypt2($inp)
{
    global $mm;
    $xx=0;$yy=0;
    $bb='';
    $xx = ($xx+1) % 256;
    $a = $mm[$xx];
    $yy = ($yy+$a) % 256;
    $mm[$xx] = $b = $mm[$yy];
    $mm[$yy] = $a;
    //proses XOR antara ciphertext dengan kunci
    //dengan $inp sebagai ciphertext
    //dan $m sebagai kunci
    $bb = ($inp^$mm[(($a+$b) % 256)] % 256) % 256;
    return $bb;
}
```

Tampilkan hasil dekripsi RC4

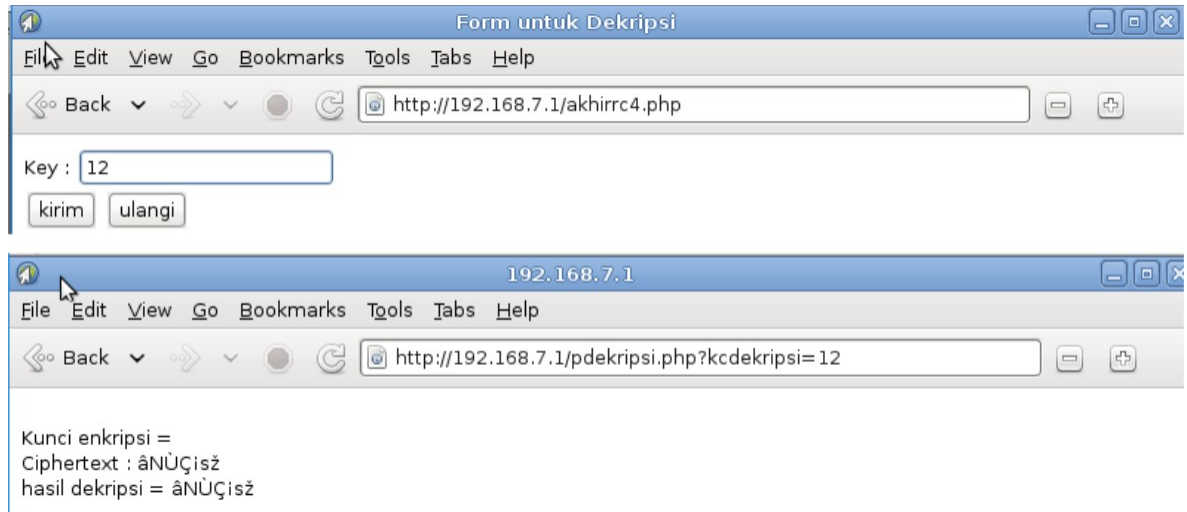
```
Terminal (as superuser)
File Edit View Terminal Help
GNU nano 2.2.4 File: /var/www/pdekripsi.php

setuptkey();
$nmfile = "enkripsirc4.txt";
//ambil data dari file enkripsirc4.txt
$fp = fopen($nmfile,"r");
$isi = fread($fp,filesize($nmfile));
echo "Ciphertext : $isi."<br>";
for ($i=0;$i<strlen($isi);$i++)
{
    $b[$i]=ord($isi[$i]); // rubah ASCII ke desimal
    $d[$i]=decrypt2($b[$i]); // proses dekripsi RC4
    $s[$i]=chr($d[$i]); // rubah desimal ke ASCII
}
echo "hasil dekripsi = ";
for ($i=0;$i<strlen($isi);$i++)
{
    echo $s[$i];
}
echo "<br>";
?>
```

Tes Proses Dekripsi

Buka web browser dari PC Client dan akseslah file php dari PC Server

http://<no_ip_pc_server>/akhirrc4.php



7.4. Kesimpulan

Kesimpulan dari modul ini, bahwa enkripsi memiliki beberapa tipe yang dapat digunakan dan memiliki kelebihan masing-masing.

MODUL 8

ASYMMETRIC CRYPTOGRAPHY

8.1.TUJUAN

1. Mengenalkan pada mahasiswa tentang konsep cryptography PGP
2. Mahasiswa mampu melakukan konfigurasi PGP
3. Mengenalkan mahasiswa tentang konsep digital signature
4. Mengenalkan mahasiswa tentang konsep hash function

8.2.TEORI DASAR

8.2.1. PGP Secara Umum

PGP adalah suatu metode enkripsi informasi yang bersifat rahasia sehingga jangan sampai diketahui oleh orang lain yang tidak berhak. Informasi ini bisa berupa E-mail yang sifatnya rahasia, nomor kode kartu kredit, atau pengiriman dokumen rahasia perusahaan melalui Internet. PGP menggunakan metode kriptografi yang disebut “public key encryption”: yaitu suatu metode kriptografi yang sangat sophisticated. PGP menggunakan sistem pasangan kunci privat dan kunci publik. Kunci privat merupakan kunci yang dipegang oleh penggunanya dan tidak boleh diketahui orang lain, sedangkan kunci publik ditujukan untuk publik terutama orang yang akan menerima pesan enkripsi dari seseorang. Enkripsi yang digunakan dalam PGP menggunakan algoritma tertentu. Proses sederhananya adalah anda meng-encrypt pesan dengan kunci publik rekan anda dan kemudian rekan anda membuka pesan ter-encrypt dengan kunci privatnya.

Proses enkripsi cukup memakan waktu dan utilitas CPU, dengan PGP dan algoritma enkripsinya proses ini bisa lebih cepat dengan cara PGP men-encrypt pesan dengan menggunakan kunci publik penerima dan meng-encrypt sebuah kunci pendek untuk meng-encrypt seluruh pesan. Pesan ter-encrypt dengan kunci pendek ini dikirim ke penerima. Penerima akan men-decrypt pesan dengan menggunakan kunci privatnya untuk mendapatkan kunci pendek tadi dan digunakan untuk men-decrypt seluruh pesan.

PGP lahir dua versi kunci publik yaitu Rivest-Shamir-Adleman (RSA) yang dikembangkan sejak 1977 dan Diffie-Hellman. Versi pertama menggunakan algoritma IDEA (International Data Encryption Algorithm) yang dikembangkan di Zurich untuk men-generate kunci pendek dan meng-encrypt seluruh pesan kemudian meng-encrypt kunci pendek tersebut dengan algoritma RSA. Sedangkan versi kedua menggunakan algoritma CAST untuk men-generate kunci pendek dari seluruh pesan untuk

mengencryptnya kemudian menggunakan algoritma Diffie-Hellman untuk meng-encrypt kunci pendektersebut.

Selain faktor pasangan kunci dan algoritma di atas PGP mempunyai satu lagi fasilitas untuk menyatakan keabsahan dari kunci dan pesan yang terenkripsi yaitu sebuah digital signature (tanda tangan digital). PGP menggunakan algoritma yang efisien untuk mengenerate kode hash (kode yang menyatakan integritas sebuah data) dari informasi nama dan informasi lainnya. Hash yang dihasilkan kemudian di-encrypt dengan kunci privat.

Penerima kemudian akan menggunakan kunci publik pengirim untuk men-decrypt kode hash. Jika cocok maka kode hash tadi menjadi digital signature untuk pesan tersebut, sehingga penerima yakin bahwa pesan tersebut dikirim oleh pengirim yang diketahui. PGP versi RSA menggunakan algoritma MD5 (Message Digest 5, 128bit) untuk menggenerate kode hash sedangkan versi Diffie-Hellman menggunakan algoritma SHA-1.

Adapun prinsip kerja dari PGP adalah sebagai berikut :

- PGP menggunakan teknik yang disebut public key encryption dengan dua kode. Kode-kode ini berhubungan secara intrinstik, namun tidak mungkin untuk memecahkan satu sama lain,
- Ketika dibuat satu kunci, maka secara otomatis akan dihasilkan sepanjang kunci, yaitu kunci publik dan kunci rahasia.
- PGP menggunakan dua kunci, Pertama, kunci untuk proses enkripsi (kunci publik). Disebut kunci publik karena kunci yang digunakan untuk enkripsi ini akan diberitahukan kepada umum. Orang yang akan mengirimkan e-mail rahasia kepada kita harus mengetahui kunci publik ini. Kedua, kunci untuk proses deskripsi (kunci pribadi). Disebut kunci pribadi karena kunci ini hanya diketahui oleh kita sendiri.

8.2.2. GnuPG

GnuPG adalah software enkripsi email pengganti PGP yang lengkap dan bebas. Bebas karena tidak menggunakan algoritma enkripsi yang telah dipatenkan sehingga bias

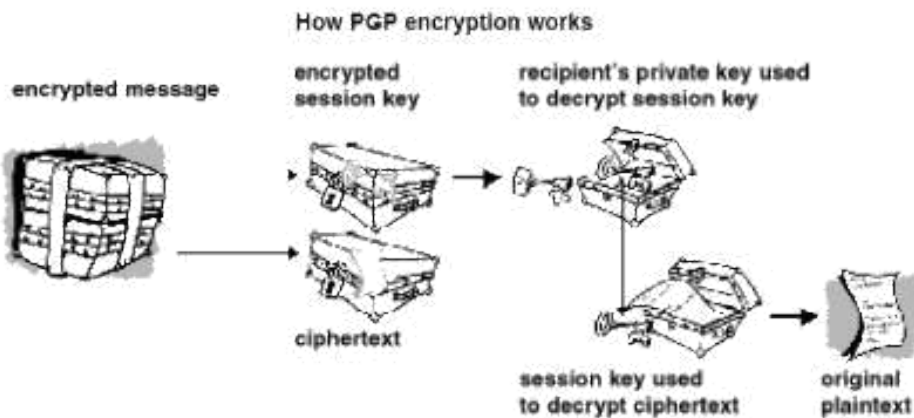
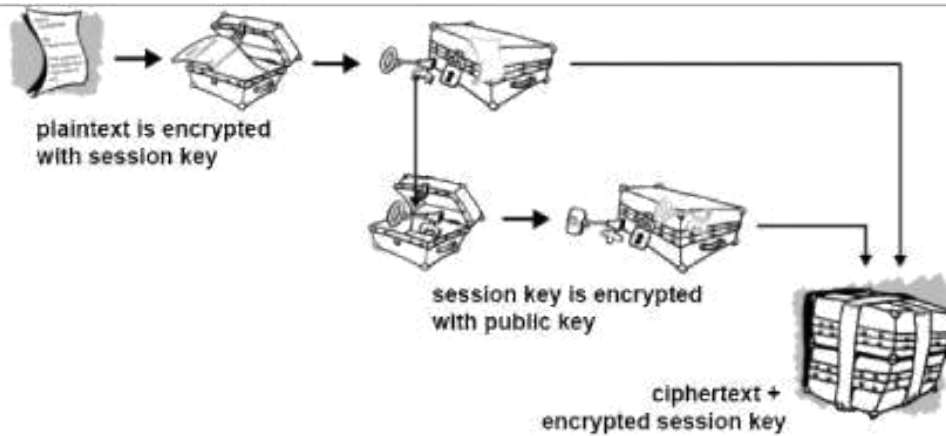
dipakai oleh siapa saja tanpa batasan. GnuPG memenuhi spesifikasi OpenPGP RFC2440.

Beberapa fitur yang ditawarkan GnuPG adalah:

- Penggantian penuh terhadap pemakaian PGP
- Tidak menggunakan algoritma yang telah dipatenkan
- Bebas, berlisensi GNU dan ditulis dari awal (from scratch)
- Fungsi yang lebih baik dibandingkan PGP
- Kompatibel dengan PGP versi 5 dan yang lebih tinggi
- Mendukung algoritma ElGamal (signature dan enkripsi), DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 and TIGER.
- Mudah diimplementasikan jika ada algoritma baru (penggunaan extension modules)
- Easy implementation of new algorithms using extension modules.
- Menggunakan format standar untuk identitas user
- Banyak bahasa yang sudah mentranslasikan
- Terintegrasi dengan HKP keyserver ([wwwkeys.pgp.net](http://www.keys.pgp.net))

GnuPG bekerja sempurna di atas sistem operasi Linux dengan platform x86, mips, alpha, sparc64 ataupun powerpc. Sistem operasi lain dengan platform x86 yang juga bekerja adalah FreeBSD, OpenBSD, NetBSD dan bahkan Windows. Platform lain dengan sistem operasi selain Linux masih dalam pengembangan.

GnuPG dibuat oleh tim GnuPG yang terdiri dari Matthew Skala, Michael Roth, Niklas Hernaes, Rmi Guyomarch and Werner Koch. Gael Queri, Gregory Steuck, Janusz A. Urbanowicz, Marco d'Itri, Thiago Jung Bauermann, Urko Lusa and Walter Koch yang membuat translasi resmi dan Mike Ashley yang mengerjakan GNU Privacy Handbook.



Gambar 1. Cara kerja PGP encryption dan decryption

8.3.KEGIATAN PRAKTIKUM

8.3.1. Peralatan

Alat dan bahan

- 1 buah laptop
- Virtual Machine(VirtualBox/VMware)
- ISO : Debian6

8.3.2. Topologi Jaringan



Gateway : 172.168.2.1

Client Netmask :
255.255.0.0

Address : 172.168.2.2



Router 1

Server

Eth0

Address : 172.168.1.2

Address : 172.168.1.1

Netmask :
255.255.0.0

Netmask : 255.255.0.0

Gateway : 172.168.1.1

Eth1

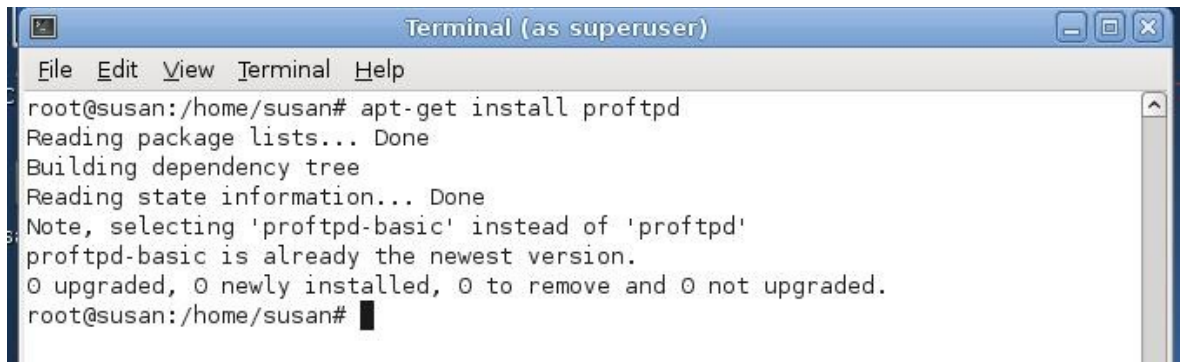
Address : 172.168.2.1

Netmask : 255.255.0.0

8.3.3. Langkah Kerja

- Pembuatan kunci (private dan public key) dengan pgp
- Pada percobaan ini satu berfungsi untuk mengirim pesan yang terenkripsi (PC Client), dan satunya berfungsi untuk menerima pesan terenkripsi dan melakukan dekripsi terhadap pesan tersebut (PC Server). Sebelum PC Client mengirim pesan, maka PC Server akan membuat kunci terlebih dahulu, dan mengirimkan public key-nya ke PC Client.
- Pastikan FTP Server terinstall pada komputer PC Server.

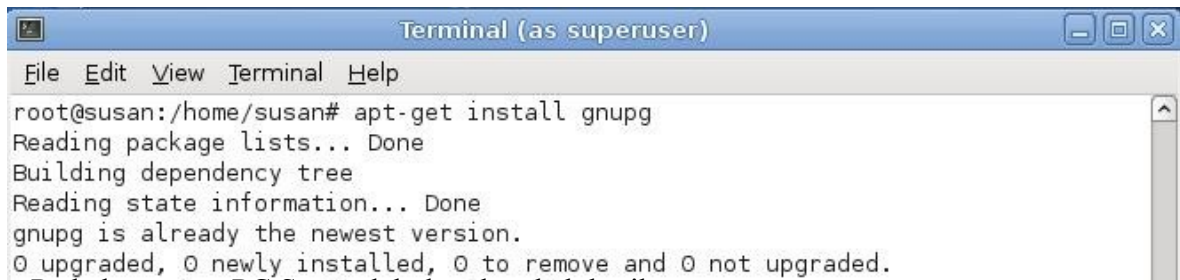
apt-get install proftpd



```
Terminal (as superuser)
File Edit View Terminal Help
root@susan:/home/susan# apt-get install proftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'proftpd-basic' instead of 'proftpd'
proftpd-basic is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@susan:/home/susan#
```

- Pastikan wireshark diinstall pada komputer PC Client #apt-get install wireshark
- Jalankan wireshark pada komputer PC Client
- Pastikan komputer Client dan Server diinstall pgp

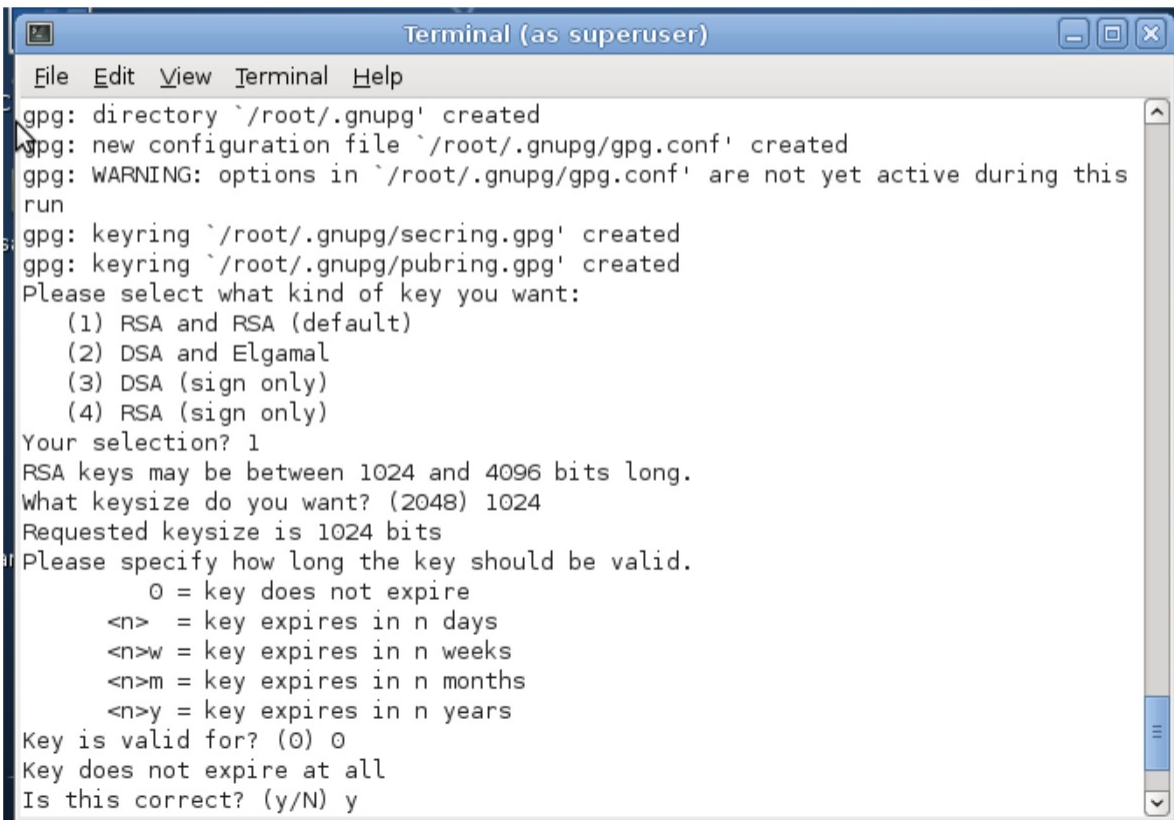
apt-get install gnupg



```
Terminal (as superuser)
File Edit View Terminal Help
root@susan:/home/susan# apt-get install gnupg
Reading package lists... Done
Building dependency tree
Reading state information... Done
gnupg is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

- Pada komputer PC Server lakukan langkah berikut :
- Lakukan pemilihan algoritma yang digunakan untuk membuat keypair #gpg -gen-key

```
root@susan:/home/susan# gpg --gen-key
gpg (GnuPG) 1.4.10; Copyright (C) 2008 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
I
gpg: directory `/root/.gnupg' created
```



```
Terminal (as superuser)
File Edit View Terminal Help
gpg: directory `/root/.gnupg' created
gpg: new configuration file `/root/.gnupg/gpg.conf' created
gpg: WARNING: options in `/root/.gnupg/gpg.conf' are not yet active during this
run
gpg: keyring `/root/.gnupg/secring.gpg' created
gpg: keyring `/root/.gnupg/pubring.gpg' created
Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 1024
Requested keysize is 1024 bits
Please specify how long the key should be valid.
  0 = key does not expire
  <n> = key expires in n days
  <n>w = key expires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y
```

Ket :

Menentukan panjang keypair

Menentukan masa guna keypair

```
Terminal (as superuser)
File Edit View Terminal Help
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Susanna Hasan
Email address: susan@eepis-its.edu
Comment: percobaan dengan gpy
You selected this USER-ID:
    "Susanna Hasan (percobaan dengan gpy) <susan@eepis-its.edu>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.

Not enough random bytes available. Please do some other work to give
the OS a chance to collect more entropy! (Need 284 more bytes)
YSDGBSAJGHDSUJNHSCCJNHDUJCNJSYFDAWHLFYAGSWAHDKAHDKSNCKDSNKJFKSJKFDSMFLMDKFMKDJFK
LDJVNKDSNVKNSKVNKDNVKNVKNFKNKVNFKNVKNFVKFNKVNFKNVKFNKFNKNDFKVNKFNKFNKFNKNDFKVNK
```

Masukan identitas diri

Memasukkan passphrase

```
Terminal (as superuser)
File Edit View Terminal Help
generator a better chance to gain enough entropy.
+++++
.+++++
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 3717649E marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, Oq, On, Om, Of, lu
pub 1024R/3717649E 2017-04-25
    Key fingerprint = 50FE DAE3 1627 DA32 EA6D 8426 4A10 44B2 3717 649E
uid                               Susanna Hasan (percobaan dengan gpy) <susan@eepis-its.edu>
sub 1024R/E803D386 2017-04-25
```

Ket :

Hasil akhir dari pembuatan kunci

- Untuk mengetahui kunci public yang sudah dibuat

```
root@susan:/home/susan# gpg --list-keys
/root/.gnupg/pubring.gpg
-----
pub   1024R/3717649E 2017-04-25
uid           Susanna Hasan (percobaan dengan gpy) <susan@eepis-its.edu>
sub   1024R/E803D386 2017-04-25

root@susan:/home/susan#
```

NB: 1024D (menggunakan DSA), 1024g (dengan elgamal)

3717649E : keyID

Primary key untuk signing, subkey untuk enkripsi.

- Untuk mengetahui kunci privat yang sudah dibuat

```
root@susan:/home/susan# gpg --list-secret-keys
/root/.gnupg/secring.gpg
-----
sec   1024R/3717649E 2017-04-25
uid           Susanna Hasan (percobaan dengan gpy) <susan@eepis-its.edu>
ssb   1024R/E803D386 2017-04-25

root@susan:/home/susan#
```

- Proses ekspor kunci public dengan pgp

Sebelum komputer Client mengirim pesan ke komputer Server, maka komputer Server harus mengekspor terlebih dahulu kuncinya ke komputer Client

#gpg --export --a susan@eepis-its.edu



```
Terminal (as superuser)
File Edit View Terminal Help
ssb 1024R/E803D386 2017-04-25

root@susan:/home/susan# gpg --export --a susan@eepis-its.edu
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.10 (GNU/Linux)

mIOEWP62pwEAPAMDOAtjL54JjbNSBfPEkfj4zazIco5U4uL1RzfQcBExPLOTI4a
0cYCrhcMDHEQFHQX0o70eXeoVVOK7rxRyjn0LtZ4wv5o4hIKwBHIgjiAUqetrNg
b0hhuTPxOpdRrNSI8BKVR1pVqAU6yREsqC9Z6/bPCP/FkFFAm9KqS4bhABEBAAGO
0LN1c2FubmEgSGFzYW4gKHBlcmNvYmFhbiBkZw5nYW4gZ3B5KSA8c3VzYW5AZWVw
aXMtaXRzLmVkdT6IuAQT AQI AIgUCWP62pwIbAwYLCQgHAWI GFQgCCQoLBBY CAwEC
HgECF4AAcGkQShBESjcXZJ56yQP/fCIudTrRdILKJFzZY6ETNY1MrOMy0IjllDFR
U6pkP2rx0bF+jl0tLW4WSAZgh7K03PEE2JT/jBrjFKVpZjifQz8yd3dZd018sKoH
v63UwrIOcf14a90Aw/+QMmLV6o6wf27XORVZN//zBXcg93U3mU3/fkdCQBMorora
OGoaDuW4jQRY/ranAQQA2/nHyV4R9UrI6NJZ1Lj2e3JrLTe7jmy3aKuT AxvkzY45
cN6dZ11cuJvWG3QBS5tofCOBT2+5HfKNdT39qc5ZRk34o4t5cS0T+s+kTFjORffrK
qmoJv/ajgHkU3j8vYKyn901GF+STg5xATcP4dsLgcuV5fId12jIfdoNYfMTI+XkA
EQEAAYifBBgBAGAJBQJY/ranAhsMAAoJEEoQRLI3F2SeozoEAKo/VMWRtJKv0rm2
BivCps2JK7M7sfMG49u7qZJd8NqTB7j7u5Yeq8Ggs2Gz6fn+AVzB5UFXdboAjb/d
nd7R72HwJzJqXLdHf7bDzrdQ7MtxdTLKZxxvm5e8w6juuIKXERovP6CxB4VjleD
Q4AYllNEGF7aKZN6CR7T7P+fwDIy
=+mx7
-----END PGP PUBLIC KEY BLOCK-----
root@susan:/home/susan#
```

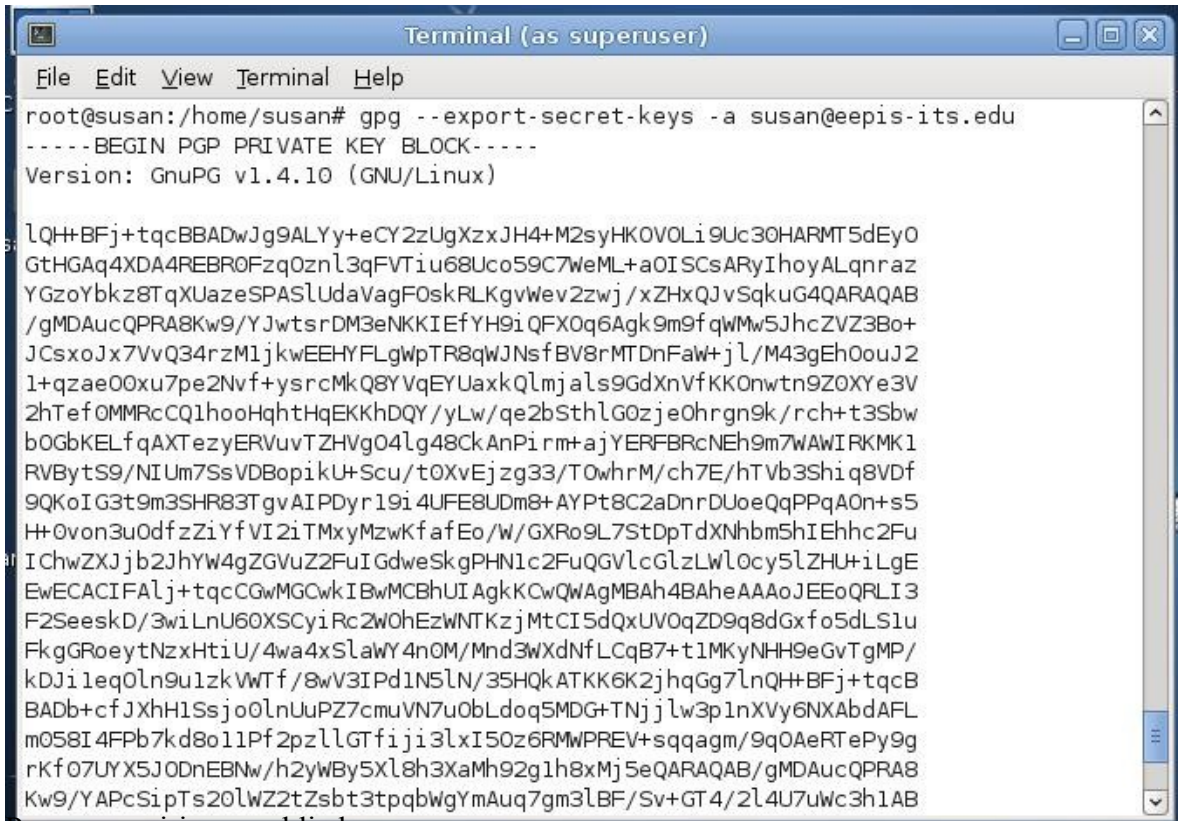
Note : Agar kunci tersebut bisa dikirim ke komputer Client, bisa disimpan dulu public key-nya dalam sebuah file

```
# gpg --export -a susan@eepis-its.edu >
```

susanPub.asc -a : menghasilkan output ASCII

Untuk mengetahui isi kunci private bisa digunakan

```
perintah : #gpg --export-secret-keys -a susan@eepis-its.edu
```



```
Terminal (as superuser)
File Edit View Terminal Help
root@susan:/home/susan# gpg --export-secret-keys -a susan@eepis-its.edu
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v1.4.10 (GNU/Linux)

lQH+BFj+tcqBBADwJg9ALYy+eCY2zUgXzxJH4+M2syHKOV0Li9Uc30HARMT5dEy0
GtHGAq4XDA4REBR0Fzq0zn13qFVTiu68Uco59C7weML+aOI SCsARYIhoyALqnr az
YGzoYbkz8TqXUazeSPASLUdaVagFoskRLKgvWev2zwj/xZHxQJvSqkuG4QARAQAB
/gMDAucQPRA8Kw9/YJwtsrDM3eNKKIEfYH9iQFX0q6Agk9m9fqWMw5JhcZVZ3Bo+
JCsoJx7VvQ34rzM1jkwEEHYFLgwpTR8qWJNsfBV8rMTDnFaw+jl/M43gEh0ouJ2
1+qzae00xu7pe2Nvf+ysrcMkQ8YVqEYUaxkQlmjals9GdXnVfKK0nwt9Z0XYe3V
2hTefOMMRcCQ1hooHqhtHqEKKhDQY/yLw/qe2bSthlG0zjeOhrgn9k/rch+t3Sbw
b0GbKELfqAXTezyERVuvTZHVg04lg48CkAnPirm+ajYERFBRcNEh9m7WAWIRKMK1
RVBytS9/NIUm7SsVDBopikU+Scu/t0XvEjz33/T0whrM/ch7E/hTVb3Shiq8Vdf
9QKoIG3t9m3SHR83TgvAIPDyr19i4UFE8UDm8+AYPt8C2aDnrDUoeQqPPqA0n+s5
H+0von3u0dfzZiYfVI2iTMxymzwKfafEo/W/GXR09L7StDpTdxNhm5hIEhhc2Fu
IChwZXJjb2JhYW4gZGVuZ2FuIGdweSkGPHN1c2FuQGVLcGlzLWl0cy5lZHU+iLgE
EwECACIFAlj+tcqCGwMGCwkIBwMCBhUIAgkKCWQAgMBAh4BAheAAAoJEEoQRLI3
F2SeeskD/3wiLnU60XSCyiRc2W0hEzWNTKzjMtCI5dQxUV0qZD9q8dGxfo5dLS1u
FkgGROeytNzxHtiU/4wa4xSlawY4nOM/Mnd3WXdNfLCqB7+t1MKyNHH9eGvTgMP/
kdJi1eq0ln9u1zkVwTf/8wV3IPd1N5LN/35HQkATKK6K2jhqGg7lnQH+BFj+tcqB
BADb+cfJXhH1Ssjo0lnUuPZ7cmuVN7u0bLdoq5MDG+TNjjlw3p1nXVy6NXAbdAFL
m058I4FPb7kd8o11Pf2pzllGTfji3lxI50z6RMWPREV+sqqagm/9q0AeRtePy9g
rKf07UYX5J0DnEBNw/h2ywBy5Xl8h3XaMh92g1h8xMj5eQARAQAB/gMDAucQPRA8
Kw9/YAPcSipTs20lWZ2tZsbt3tpqbWgYmAuq7gm3lBF/Sv+GT4/2L4U7uwc3h1AB
```

Proses pengiriman public key

Ketika komputer client ingin mengirim pesan ke komputer server, maka server harus

memberikan kunci publiknya terlebih dahulu ke komputer client, bisa dilakukan dengan ftp :

```

root@susan:/home/susan# ftp 172.168.2.2
Connected to 172.168.2.2.
220 ProFTPD 1.3.3a Server (Debian) [::ffff:172.168.2.2]
Name (172.168.2.2:root): susan
331 Password required for susan
Password:
230 User susan logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put susanPub.asc
local: susanPub.asc remote: susanPub.asc
200 PORT command successful
150 Opening BINARY mode data connection for susanPub.asc
226 Transfer complete
1053 bytes sent in 0.00 secs (12854.0 kB/s)
ftp> quit
221 Goodbye.
root@susan:/home/susan#

```

NB: Proses pengiriman juga bisa menggunakan perintah scp yg lebih aman (pastikan di tujuan sudah terinstall ssh) Untuk dari PC Server ke PC Client:

```
# scp susanPub.asc 172.168.2.2: /home/susan
```

Untuk dari PC Client ke PC Server:

```
# scp 172.168.2.2:susanPub.asc /home/susan
```

- Proses enkripsi dengan public key dan pengiriman pesan
- Pada komputer client, lakukan beberapa perintah berikut ini :
- Import kunci yang sudah dikirim oleh Server

```
# gpg --import susanPub.asc
```

```

root@susan:/home/susan# gpg --import susanPub.asc
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 3717649E: public key "Susanna Hasan (percobaan dengan gpy) <susan@eeepis-its.edu>" imported
gpg: Total number processed: 1
gpg:          imported: 1 (RSA: 1)
root@susan:/home/susan#

```

- Cek kunci publik, apakah sudah diterima oleh Client atau belum (pastikan keyID sama dengan di sisi server)

```
# gpg --list-keys
```

- Buat file text berisi pesan yang akan dikirim ke komputer Server.
#nano coba.txt

Di dalam coba.txt masukan kata-kata Praktikum dengan kriptografi asimetrik PGP

- Lakukan proses enkripsi terhadap file coba.txt

```
# gpg --encrypt -r susan@eepis-its.edu -a coba.txt
```

Keterangan :

-a : plain text

-r : recipient

- Hasil enkripsi diatas akan menghasilkan file coba.txt.asc.

```
root@susan:/home/susan# cat coba.txt.asc
-I---BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.10 (GNU/Linux)

hIwDyRI4kugD04YBA/9/xYVYhG+zv60uhYMeGRLRgvwCgarFxlkEiI7hfwmPDr0V
I3YlbwLDxy1j20vH7aPlwv6zUQUWN+iUJlMrTbzE+D4aZkz4oYwu0cUiwaC8UMt
bVZhyPfNi ybDlhhJebn39+Rh0gpTc+TnrKRcTE9EpvQT26bLFuSRHw24wmjcmtJu
Adcj4niYdpYnQe7TsErdTglqtfVSp46fBALYTVjclFhXi7qGdTimL5AtzxI7whNN
X9xs7/eJBKpHJTdsXAhtzjgPye+Xw+c1czb87K14rVE9ImLsMgTE7dkK/Au06fze
B+qBn7lrHTW12fogANI=
=GlAi
-----END PGP MESSAGE-----
root@susan:/home/susan#
```

Kirim file yang telah dienkripsi tersebut ke komputer tujuan (Server), dengan menggunakan ftp/scp seperti langkah sebelumnya.

- Proses dekripsi

- Pastikan di komputer Server telah menerima pesan yang telah dienkripsi dari komputer client. Lakukan proses dekripsi file tersebut dengan menggunakan private key agar bisa membaca pesan aslinya.

```
#gpg --decrypt coba.txt.asc
```

```
root@susan:/home/susan# gpg --decrypt coba.txt.asc

You need a passphrase to unlock the secret key for
user: "Susanna Hasan (percobaan dengan gpy) <susan@eepis-its.edu>"
1024-bit RSA key, ID E803D386, created 2017-04-25 (main key ID 3717649E)

gpg: encrypted with 1024-bit RSA key, ID E803D386, created 2017-04-25
      "Susanna Hasan (percobaan dengan gpy) <susan@eepis-its.edu>"
praktikum dengan kriptografi asimetris PGP
root@susan:/home/susan#
```

- Percobaan dengan hash function untuk data integrity

- Buat file :

```
# nano datahash.txt
```

Selamat datang di kampus Politeknik, Manado

- Lakukan perhitungan hash value untuk data diatas. Amati dan catat nilai hashnya, berapa jumlah karakter hexa hasil md5 tsb:

```
# md5sum datahash.txt
```

- Lakukan perubahan isi file datahash.txt, dengan menghilangkan tanda koma Selamat datang di kampus Politeknik Manado

- Hitung kembali hash value :

```
# md5sum datahash.txt
```

- Rubah kembali isi file datahash.txt, ganti huruf paling depan dgn huruf kecil selamat datang di kampus Politeknik, Manado

- Hitung kembali hash value :

```
# md5sum datahash.txt
```

- Percobaan dengan digital signature untuk authentication dan non-repudiation
- Buat file di sisi PC Server yang akan ditandatangani.

```
# nano data.txt
```

```
selamat datang di Politeknik
```

- Beri signature pada pesan tersebut dgn private key :

```
# gpg -u 3717649E --clearsign
```

```
data.txt Note:
```

```
3717649E sebagai keyID, bisa dilihat dari perintah gpg --list-keys
```

```
Dari perintah diatas akan menghasilkan file : data.txt.asc
```

```
Perlu password untuk private key.
```

- Lihat isi data : data.txt.asc

```
# cat data.txt.asc
```

```

root@susan:/home/susan# cat data.txt.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

selamat datang di Politeknik
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.10 (GNU/Linux)

iJwEAQECAAYFAlj+zrAACgkQShBESjcxZJ7T7ygQAo3Y8hnuVikus0eybJJ1FB6mz
Kna9Dk0m0ksStwUkwMkk+WxE+jmgORN/qqmGfu+SVQLWClXl0aqqT9IgmW6MLbwd
jK/ZKIg+3ECuzW8Uf5vsecky1ODdZM55PMXoxQBlgVy7buXzdvlfHJ5AibFhtoy/
ZOHURe/04JpsiDM8zAQ=
=yAva
-----END PGP SIGNATURE-----
root@susan:/home/susan#

```

Note :

Pada hasil diatas, terdapat digital signature yang dilekatkan pada pesan aslinya.

- Kirim data : data.txt.asc ke sisi PC Client dengan menggunakan scp, kirim juga public key dari PC Server.
- Lakukan import terhadap file public key dari PC Server

```
# gpg --import susanPub.asc
```

```

root@susan:/home/susan# gpg --import susanPub.asc
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 3717649E: public key "Susanna Hasan (percobaan dengan gpy) <susan@eepis-its.edu>" imported
gpg: Total number processed: 1
gpg:         imported: 1 (RSA: 1)
root@susan:/home/susan#

```

- Lakukan dekripsi terhadap file data.txt.asc untuk mengetahui apakah tandatangannya sah dari si pengirim.

```
# gpg --decrypt data.txt.asc
```

```

root@susan:/home/susan# gpg --decrypt data.txt.asc
selamat datang di Politeknik
gpg: Signature made Mon 24 Apr 2017 09:21:04 PM PDT using RSA key ID 3717649E
gpg: Good signature from "Susanna Hasan (percobaan dengan gpy) <susan@eepis-its.edu>"
root@susan:/home/susan#

```

8.4.KESIMPULAN

Asymmetric Cryptography memiliki 2 tipe enkripsi yaitu PGP dan GnuPG.

DAFTAR PUSTAKA

Modul Praktikum Network Security Politeknik Elektronika Negeri Surabaya

Aji, KK. 2007. Keamanan Jaringan. [Online] Tersedia :
"http://kebo.vlsm.org/mediawiki1.9/index.php/Keamanan_Jaringan". [26 Januari 2008]
Ariyus, Dony. 2005. *Computer Security*. Yogyakarta : Andi Offset.

Aan Jiwa P., Agus, 2009, *Penggunaan Firewall Untuk Menjaga Keamanan Sistem Jaringan Komputer*, <http://ilmukomputer.com>

Muammar W. K, 2004, *Firewall*, <http://ilmukomputer.com>