PRAKTIKUM
KEAMANAN JARINGAN
(FIREWALL)

DAFTAR ISI

KATA PENGANTAR .....
DAFTAR ISI .....
PETUNJUK PRAKTIKUM .....
MODUL 1 NETWORK SCANNING DAN PROBING .....
MODUL 2 PASWORD MANAGEMENT .....
MODUL 3 FIREWALL (IPTABLES) .....
MODUL 4 FIREWALL (TCPWRAPPER) .....
MODUL 5 INTRUSION DETECTION SYSTEM (SNORT) .....
MODUL 6 INTRUSION DETECTION SYSTEM (TRIPWIRE) .....
MODUL 7 INTRUSION DETECTION SYSTEM (PORTSENTRY) .....
MODUL 8 SNIFFING DAN SESSION HIJACKING .....
MODUL 9 EMAIL SECURITY .....
MODUL 10 EMAIL SECURITY .....
MODUL 11 WEB SECURITY .....
MODUL 12 FINAL PROJECT .....
DAFTAR PUSTAKA .....

MODUL 1
NETWORK SCANNING DAN PROBING

TUJUAN PEMBELAJARAN:

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

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 incomming connection ke port. Koneksi bisa berupa lokal maupuan 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.

Netstat

Nenstat merupakan utility yang powerfull untuk menngamati current state pada server, service apa yang listening untuk incomming connection, interface mana yang listening, siapa saja yang terhubung.

Nmap

Merupakan software scanner yang paling tua yang masih dipakai sampai sekarang.

Nessus

Nessus merupakan suatu tools yang powerfull untuk melihat kelemahan port yang ada pada komputer kita dan komputer lain. Nessus akan memberikan report secara lengkap apa kelemahan komputer kita dan bagaimana cara mengatasinya.

TUGAS PENDAHULUAN

1. Sebutkan langkah dasar yang biasa dipakai untuk melakukan proses hacking !
2. Sebutkan cara penggunaan netstat dan option-option yang dipakai serta arti option tersebut ?
3. Sebutkan cara pemakaian software nmap dengan menggunakan tipe scanning:
   - TCP Connect scan
   - TCP SYN Scan
   - TCP FIN scan
   - TCP Xmas Tree scan
   - TCP null scan
   - TCP ACK scan
   - TCP Windows scan
   - TCP RPC scan
   - UDP scan
   - OS fingerprinting
4. Apa kegunaan dari utility chkconfig ?
5. Bagaimana cara mematikan dan menghidupkan service yang ada
6. Sebutkan cara pemakaian software nessus untuk melihat kelemahan sistem jaringan kita !

PERCOBAAN

1. Pastikan nmap terinstal pada komputer anda,jika belum ambil source code pada server yang telah disediakan dan lakukan installasi.
2. Pastikan nessus terinstal pada komputer anda,jika belum ambil source code pada server yang telah disediakan dan lakukan installasi.
3. Jalankan :
   a. ”netstat –tpane | grep tcp | wc –l”
   b. nmap –sS –P0 ip_lokal_komputer_anda | grep open | wc -l
4. Apa hasil yang anda dapat ? bandingkan apakah sama? Bagaimana supaya mendapat hasil yang sama ?
5. Jalankan :
   a. ”netstat –tupane | grep 0.0 | wc –l”
   b. nmap –sSU –P0 ip_lokal_komputer_anda | grep open | wc –l
      Agak membutuhkan waktu yang lama kira-kira 25 menit. Lanjutkan dengan yang lain.
6. Port mana saja yang terbuka ?
7. Jalankan nmap dengan beberapa option yang anda buat pada tugas pendahuluan yaitu : TCP Connect scan, TCP SYN Scan, TCP FIN scan, TCP Xmas Tree scan, TCP null scan, TCP ACK scan, TCP Windows scan, TCP RPC scan, UDP scan, OS fingerprinting
8. Jalankan nessus ke komputer lokal dan analisa hasilnya.

9. Jalankan chkconfig –list | grep $(runlevel | cut –d” ” –f2) :on
10. Matikan beberapa service yang tidak ingin dijalankan dan restart komputer anda jalankan lagi mulai percobaan 3 - 10, dan bandingkan hasilnya sebelum direstart !
11. Bekerjalah dengan teman anda, dan lakukan port scanning ke teman anda secara bergantian.

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Network Scanner dan Probing

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Sebutkan option atau bentuk-bentuk scanning yang bisa dilakukan nmap
3. Cari di internet beberap tools scanning yang ada dan bagaimana cara pemakaian dan hasilnya?

MODUL 2
PASSWORD MANAGEMENT

TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep dasar autentikasi password di linux
2. Memahami konsep shadow password
3. Mampu menganalisa kelemahan password dengan program password cracker yang ada.

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
```

Keterangan :
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 :
menyalin file /etc/passwd tersebut
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 sama.
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 pasword yang ada pada komputer.

TUGAS PENDAHULUAN

1. Bagaimana cara installasi john the ripper password ?
2. Jelaskan cara penggunaan john the ripper ?
3. Bagaimana kriteria password dikatakan strong atau tidak ?
4. Apa kegunaan shadow password pada linux ?

PERCOBAAN

Manajemen Password menggunakan sudo

1. Buat 3 user, userbaru, userkanan dan userkiri.
2. Login sebagai root, ketik :

   # visudo

   Pada dasarnya visudo ini membuka file /etc/sudoers. File ini hanya bisa dibuka lewat visudo saja dan tidak bisa dibuka lewat vi atau gedit, yang merupakan editor linux.
4. Coba baca isi file /etc/sudoers dg vi. Perhatikan isinya. Coba hapus baris paling bawah. Bisakah? Mengapa?
5. Coba login sebagai salah satu user dan nyalakan daemon httpd dengan perintah :
   # /etc/init.d/httpd start
3. Berhasilkah anda menyalakan daemon httpd ? Mengapa?
6. Coba login sebagai root dan nyalakan daemon httpd dengan perintah :
   # /etc/init.d/httpd start
4. Berhasilkah anda menyalakan daemon httpd ? Mengapa ?
7. Agar user biasa mampu menjalankan daemon httpd, anda harus mengedit file /etc/sudoers untuk memberikan hak tambahan user. Caranya dengan menambahkan baris dibawah pada visudo, lalu ketik I, yang berarti visudo berada dalam mode insert.

   userbaru localhost=NOPASSWD: /etc/init.d/httpd

   Arti baris ini adalah user userbaru dapat mengakses komputer yang bernama localhost untuk menjalankan daemon httpd tanpa password.
8. Setelah itu coba login sebagai userbaru lalu ketikkan :

   # sudo /etc/init.d/httpd start
5. Berhasilkah anda mengaktifkan daemon httpd sebagai userbaru? Apakah anda diprompt password?
9. Sekarang coba anda logi sebagai userkanan dengan perintah su

   # su userkanan
6. Ketik passwordnya.
10. Kemudian jalankan perintah ini :

    # sudo /etc/init.d/httpd restart
11. Berhasilkah anda mengaktifkan daemon httpd sebagai userbaru? Apakah anda diprompt password? Setelah anda beri password, apakah anda bisa menjalankan httpd ? Apa peringatan yg diberikan ?
12. Sekarang coba anda tambahkan hak untuk melakukan mount cdrom pada userkiri.
    Dalam keadaan normal, apakah anda dapat melakukan mount sebagai userkiri ? Siapakah user yang berhak melakukan mount ?
13. Untuk menambahkan hak mount pada userkiri, tambahkan baris berikut dibawah baris ini

    #%sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

    dengan baris :

    userkiri localhost = STORAGE

Artinya bahwa userkiri pada komputer lokalhost memiliki kemampuan manajemen Storage yang ditunjukkan oleh baris Cmd_Alias berikut :

Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount

14. Kemudian sebagai userkiri, jalankan perintah sudo :
    # sudo mount /dev/cdrom /mnt/cdrom
15. Apakah userkiri berhasil melakukan mount cdrom? Apakah anda diprompt password ketika melakukan sudo ? Mengapa ?
16. Selain fdisk, userkiri mampu melakukan perintah fdisk, sfdisk, parted, partprobe dan mount
17. Coba lakukan perintah sudo dengan fdisk, sfdisk, parted, partprobr dan umount.
18. Untuk melakukan umount, cukup kerjakan ;
    # sudo umount /mnt/cdrom
19. Coba anda login sebagai userkanan dan lakukan sudo. Apakah berhasil ? Apa peringatan yang dituliskan?
20. Coba masuk sebagai root dan lakukan perintah ini :
    # tail /var/log/secure
7. Dapatkah anda melihat bahwa pelanggaran yg dilakukan userkanan tercatat di file /var/log/secure ? Jika iya, copy paste pelanggaran tersebut.
21. Dari percobaan diatas, jawab pertanyaan ini :
    1. Terangkan apa fungsi SUDO ?
    2. Terangkan pula format log /var/log/secure ?
    3. Apa guna var/log/secure ? (selain merekan pelanggaran dari sudo)

Melihat Password dengan John The Ripper

1. Login sebagai root dan buatlah beberapa 4 user baru, selanjutnya untuk 3 nama user, beri password user sama dengan nama user . Nama user terserah anda.

Contoh : Userkiri, passwd: userkiri; userkanan, passwd : userkanan; userbaru, passwd: userbaru. Satu user dengan password yang unik, contoh : niken, passwd :kenis34. Sedangkan root, passwdnya : 123456.

2. Login sebagai root dan install john the ripper dari source.

3. Cara instalasi source :
    # tar -xvzf john-1.7.2.tar.gz --dir=/usr/local

Akan terbentuk direktori john-1.7.2 di usr/local

4. Setelah itu masuklah ke direktori john-1.7.2
    # cd john-1.7.2
    # cd src
    # make
    #make clean generic
8. Tunggu sampai proses kompilasi selesai karena cukup memakan waktu, kemudian masuklah ke direktori run
    #cd ../run
    # ./john --test

5. Bila benar, anda akan melihat baris ini pada baris terbawah :
    Benchmarking: NT LM DES [32/32 BS]... DONE
    Raw: 2727K c/s real, 2777K c/s virtual

6. Setelah itu mari mengcrack password dengan john the ripper. Lakukan langkah-langkah berikut :

umask 077

Apa guna perintah umask ? Apa arti umask 077 ?

Masuk ke direktori run dari john-1.7-2

Jika password anda sudah ter-shadow, anda perlu melakukan unshadow

./unshadow /etc/passwd /etc/shadow > mypasswd

Coba lihat isi mypasswd. Apakah benar sekarang semua password telah ter-unshadowed ? Copy paste baris yang mengandung 4 user dan account root. Untuk membuka, berikan perintah ini.

vi mypasswd

Untuk melihat password yang dicrack oleh john the ripper, lihat dengan peintah ini

john --show mypasswd

Lihatlah, apakah semua user yang anda buat dapat dicrack oleh john? Jika tidak, usermana yang tidak dapat dicrack ?

Dari apa yang anda lakukan, apa fungsi perintah unshadow?

Lanjutkan langkah-langkah berikut :

Copy file berikut dan pastekan ke direktori berikut :

#cd john-1.7.2/run

Lihatlah apakah file password.lst dan all.chr ada ? File password.lst berisi listing password yang biasa dipakai oleh unix.

Buatlah direktori /usr/share/john/password.lst dan kopikan file password.lst

#cp password.lst /usr/share/john/password.lst

#cp all.chr /usr/share/john/all.chr

Jalankan lagi john untuk mengcrack semua password user. Ini mungkin makan waktu lama.

./john mypasswd

Tunggulah sampai 10 menit, bila masih belum selesai, keluarkan perintah Ctrl C untuk menghentikan john bekerja. Capture hasilnya.

Password yang dicrack ditempatkan di folder /john-1.7.2/run/john.pot. Tapi file ini tidak dapat dibuka.

Untuk melihat hasil crack, jalankan perintah ini.

john --show mypasswd

Capture-lah output perintah diatas.

Untuk mengcrack user tertentu, anda dapat menggunakan opsi ini :

john –show --users=userbaru mypasswd

Jika ingin mengetahui variasi perintah untuk john, lihat dokumentasi tambahan ttg john the ripper atau carilah di internet.

Cracking paling baik dilakukan dengan menggunakan opsi incremental :

john -i mypasswd

Bila terlalu lama hentikan proses.

Capture hasilnya.

Jika ada peringatan ini, Crash recovery file is locked: /root/.john/john.rec, artinya anda harus mengcopy file /root/.john/john.rec, lalu hapus file lama, dan ubah dari john(copy).rec menjadi john.rec

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Password Management

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Jelaskan cara kerja john the ripper dalam melihat password
3. Jelaskan cara kerja program yang anda buat dan bagaimana password bisa disebut strong dan bad ?

MODUL 3
KONFIGURASI FIREWALL [IPTABLES]

TUJUAN PEMBELAJARAN:

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

DASAR TEORI

Firewall adalah sistem atau sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan. Secara prinsip, firewall dapat dianggap sebagai sepasang mekanisme : yang pertama memblok lalu lintas, yang kedua mengijinkan 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 protokol
  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

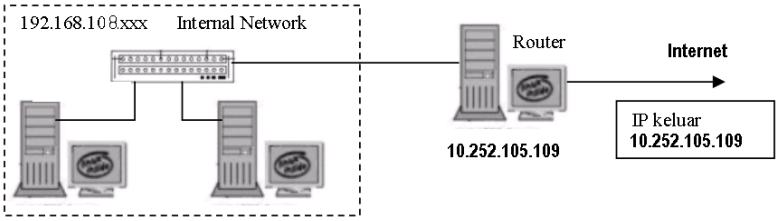
network level firewall. Firewall ini bisa dikatakan sebagai jembatan. Application-Proxy Firewall biasanya berupa program khusus, misal squid

TUGAS PENDAHULUAN

1. Sebutkan dan jelaskan dengan singkat apa yang disebut dengan konsep logging ?
2. Sebutkan fasilitas logging yang ada di linux !
3. Sebutkan beberapa software yang biasa dipakai untuk melakukan monitoring log di linux.

PERCOBAAN

1. Bangun desain jaringan sebagai berikut :



2. Setting komputer sebagai router (PC1) sbb :
   - Setting Ip_forward
     - #echo 1> /proc/sys/net/ipv4/ip_forward
   - Setting menggunakan NAT
     - # iptables –t nat –A POSTROUTING –o eth0 –s I *IP number* -d 0/0 –j MASQUERADE
   - Setting IP
     - Eth0 → 192.168.105.109 Bcast:192.168.105.255 Mask:255.255.255.0
     - Eth0:1 → 192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
   - Setting Routing
     - # route add default gw 192.168.105.1

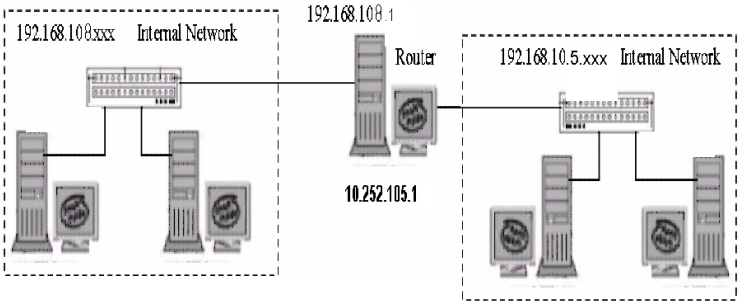
3. Setting komputer client sbb :
   - PC2
     - Setting IP
       - inet addr:192.168.108.10 Bcast:192.168.108.255 Mask:255.255.255.0
   - PC3
     - Setting IP
       - inet addr:192.168.108.5 Bcast:192.168.108.255 Mask:255.255.255.0
   - PC4
     - Setting IP
       - inet addr:192.168.108.20 Bcast:192.168.108.255 Mask:255.255.255.0
   - Setting Gateway untuk PC2, PC3 & PC4
     - route add default gw 192.168.1.1

4. Lakukan test konektifitas
   - Router PC 1
     - ping 192.168.108.10, ping 192.168.108.5, ping 192.168.108.20, ping 192.168.105.1, ping 202.154.187.4
   - PC 2
     - ping 192.168.105.109, ping 192.168.108.5, ping 192.168.108.20, ping 192.168.105.1, ping 202.154.187.4
   - PC 3
     - ping 192.168.105.109, ping 192.168.108.10, ping 192.168.108.20, ping 192.168.105.1, ping 202.154.187.4
   - PC 4
     - ping 192.168.105.109, ping 192.168.108.10, ping 192.168.108.5, ping 192.168.105.1, ping 202.154.187.4

5. Jalankan rule firewall sebagai berikut :

- Setting memblok PC2 dan PC3 supaya tidak bisa mengakses web dan FTP
  - #iptables –A FORWARD –m state –state NEW –m multiport –s 192.168.108.5/24 –d 0/0 –p tcp –dport www, -j REJECT
  - #iptables –A FORWARD –m state –state NEW –m multiport –s 192.168.108.5/24 –d 0/0 –p tcp –dport ftp, -j REJECT
  - #iptables –restore, iptables save

6. Praktikum 2 :
   a. Buat desain jaringan sbb :



   b. Bangun Jaringan sendiri
   c. Install web server, FTP Server, dan Telnet pda jaringan 192.168.105.xxx
   d. Buat jaringan 192.168.108.xxx ada yang bisa akses web, ftp dan telnet dan ada yang tidak
   e. Buat jaringan 192.168.105.xxx tidak boleh melakukan perintah ping ke 192.168.108.xxx

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Konfigurasi Firewall [iptables]

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Apa command iptables untuk melakukan blocking terhadap http ?
3. Apa command iptables untuk melakukan blocking terhadap MAC address tertentu ?
4. Apa saja command iptables yang dibuat jika kita hanya memperbolehkan ssh yang jalan di jaringan ?
5. Bagaimana jika yang diperbolehkan adalah ssh, web dan email ?
6. Bagaimana untuk blocking command ping ?

MODUL 4
KONFIGURASI FIREWALL
[TCP WRAPPER]

TUJUAN PEMBELAJARAN:

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

DASAR TEORI

Pada sistem operasi pada umumnya mempunyai program aplikasi yang jalan pada sistem operasi tersebut. Pada sistem operasi linux, dikenal istilah service untuk menggantikan nama aplikasi secara global. Ada beberapa service yang dimanage di linux :

- Beberapa Aplikasi ditimbulkan melalui init
  Service ini menyediakan dumb terminal (virtual terminal), dalam satu mesin bisa menjalankan beberapa terminal biasanya dengan menekan tombol ctrl+alt+Fx. Dikonfigurasi pada /etc/inittab. Perubahan inittab bisa diaktifkan menggunakan command init q
- Beberapa Service dimanage pada :
  - System V Scripts
    Merupakan metode yang paling umum digunakan untuk menaging service, Biasanya membutuhkan file konfigurasi. Service distart dengan script di /etc/init.d/. Misal untuk network :
    /etc/init.d/network restart atau Service network restart
  - xinetd
    Hanya beberapa service yang ada pada xinetd, service ini tidak memerlukan start/stop terhadap service. Dan file Konfigurasi yang biasa dipakai adalah :
    /etc/xinetd.conf → Top level configuration file
    /etc/xinetd.d/service → service specification configuration

TCP Wrapper

Merupakan salah satu pengelolaan service yang diatur pada /etc/xinetd.d dan system v scripts. Penglolaan service ini bisa melakukan blocking service tertentu kepada client atau nomor IP tertentu.

Ada dua file yang dipakai untuk melakukan blocking dan unblocking yaitu /etc/hosts.allow (diperbolehkan access) dan hosts.deny (dilarang akses)

Dengan Basic Syntax sbb :

daemon_list: client_list [:option]

Contoh syntax yang dipakai adalah sbb :

/etc/hosts.allow

vsftd:192.168.0.

in.telned, portmap: 192.168.0.8

/etc/host.deny

sshd: ALL EXCEPT .cracker.org EXCEPT trusted.cracker.org

sshd: 192.168.0. EXCEPT 192.168.0.4

Selain menggunakan Tcp wrapper, dimungkinkan juga membatasi hak akses xinetd pada Pada file di /etc/xinetd.d dengan menambahkan Syntax

only_from no_ip
no_access no_ip
acces_times = 08.00-18.00
per_source = 2

TUGAS PENDAHULUAN

1. Sebutkan dan jelaskan dengan singkat apa yang disebut dengan konsep logging ?
2. Sebutkan fasilitas logging yang ada di linux !
3. Sebutkan beberapa software yang biasa dipakai untuk melakukan monitoring log di linux.

PERCOBAAN

1. Bangun jaringan menjadi 2 subnet
   192.168.0.0/24 dan 192.168.1.0/24
   Bangun salah satu menjadi router
2. Pada salash satu jaringan 192.168.0.0/24 :
   Install telnet-server
   Install openssh
3. Beri rule sebagai berikut amati yang terjadi
   - Pada /etc/hosts.allow
     ALL: localhost
   - Pada /etc/hosts.deny
     sshd: ALL EXCEPTS 192.168.0.
   - Pada /etc/sinetd.d/telnet
     only_from = 192.168.0.w 192.168.0.y 192.168.0.z
   - Pada /etc/xinetd.conf
     no_access = 192.168.1.0/24
4. Lakukan pengaksesan telnet dan openssh pada setiap komputer yang ada
5. Amati yang terjadi mana yang bisa masuk ke server telnet dan ssh dan mana yang tidak
6. Berikan kesimpulan praktikum anda .

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Konfigurasi Firewall [tcp wrapper]

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Apa perbedaan firewall yang ada pada iptables dan tcp wrapper, jelaskan secara singkat
3. Berdasarkan praktikum service apa saja yang bisa diblok atau tida diblok oleh tcp wrapper?

MODUL 5
INTRUSION DETECTION SYSTEM [SNORT]

TUJUAN PEMBELAJARAN:

4. Mengenalkan pada mahasiswa tentang konsep Manajemen Log di linux
5. Mahasiswa memahami berbagai macam file log yang ada di linux
6. Mahasiswa mampu melakukan analisa terhadap file log yang ada di linux

DASAR TEORI

Deteksi Penyusupan (Intrusion Detection)

Deteksi penyusupan adalah aktivitas untuk mendeteksi penyusupan secara cepat dengan menggunakan program khusus yang otomatis. Program yang dipergunakan biasanya disebut sebagai Intrusion Detection System (IDS).

Tipe dasar dari IDS adalah:

- Rule-based systems - berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mencatat lalulintas yang sesuai dengan database yang ada, maka langsung dikategorikan sebagai penyusupan.
- Adaptive systems - mempergunakan metode yang lebih canggih. Tidak hanya berdasarkan database yang ada, tapi juga membuka kemungkinan untuk mendeteksi terhadap bentuk bentuk penyusupan yang baru.

Bentuk yang sering dipergunakan untuk komputer secara umum adalah rule-based systems.

Pendekatan yang dipergunakan dalam rule-based systems ada dua, yakni pendekatan pencegahan (preemptory) dan pendekatan reaksi (reactionary). Perbedaannya hanya masalah waktu saja. Pendekatan pencegahan, program pendeteksi penyusupan akan memperhatikan semua lalu lintas jaringan. Jika ditemukan paket yang mencurigakan, maka program akan melakukan tindakan yang perlu. Pendekatan reaksi, program pendeteksi penyusupan hanya mengamati file log. Jika ditemukan paket yang mencurigakan, program juga akan melakukan tindakan yang perlu.

Snort

Mengoperasikan Snort

Tiga (3) buah mode, yaitu

1. **Sniffer mode**, untuk melihat paket yang lewat di jaringan.
2. **Packet logger mode**, untuk mencatat semua paket yang lewat di jaringan untuk di analisa di kemudian hari.
3. **Intrusion Detection mode**, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan setup dari berbagai rules / aturan yang

akan membedakan sebuah paket normal dengan paket yang membawa serangan.

Sniffer Mode

Untuk menjalankan snort pada sniffer mode tidaklah sukar, beberapa contoh perintah-nya terdapat di bawah ini,

```
#snort –v
#snort –vd
#snort –vde
#snort –v –d –e
```

dengan menambahkan beberapa switch –v, -d, -e akan menghasilkan beberapa keluaran yang berbeda, yaitu

-v, untuk melihat header TCP/IP paket yang lewat.
-d, untuk melihat isi paket.
-e, untuk melihat header link layer paket seperti ethernet header.

Packet Logger Mode

Tentunya cukup melelahkan untuk melihat paket yang lewat sedemikian cepat di layar terutama jika kita menggunakan ethernet berkecepatan 100Mbps, layar anda akan scrolling dengan cepat sekali susah untuk melihat paket yang di inginkan. Cara paling sederhana untuk mengatasi hal ini adalah menyimpan dulu semua paket yang lewat ke sebuah file untuk di lihat kemudian, sambil santai … Beberapa perintah yang mungkin dapat digunakan untuk mencatat paket yang ada adalah

```
./snort –dev –l ./log
./snort –dev –l ./log –h 192.168.0.0/24
./snort –dev –l ./log –b
```

perintah yang paling penting untuk me-log paket yang lewat adalah

```
-l ./log
```

yang menentukan bahwa paket yang lewat akan di log / di catat ke file ./log. Beberapa perintah tambahan dapat digunakan seperti –h 192.168.0.0/24 yang menunjukan bahwa yang di catat hanya packet dari host mana saja, dan –b yang memberitahukan agar file yang di log dalam format binary, bukan ASCII.

Untuk membaca file log dapat dilakukan dengan menjalankan snort dengan di tambahkan perintah –r nama file log-nya, seperti,

```
./snort –dv –r packet.log
./snort –dvr packet.log icmp
```

Intrusion Detection Mode

Mode operasi snort yang paling rumit adalah sebagai pendeteksi penyusup (intrusion detection) di jaringan yang kita gunakan. Ciri khas mode operasi untuk pendeteksi penyusup adaah dengan menambahkan perintah ke snort untuk membaca file konfigurasi –c nama-file-konfigurasi.conf. Isi file konfigurasi ini lumayan banyak, tapi sebagian besar telah di set secara baik dalam contoh snort.conf yang dibawa oleh source snort.

Beberapa contoh perintah untuk mengaktifkan snort untuk melakukan pendeteksian penyusup, seperti

```
./snort –dev –l ./log –h 192.168.0.0/24 –c snort.conf
```

./snort –d –h 192.168.0.0/24 –l ./log –c snort.conf

Untuk melakukan deteksi penyusup secara prinsip snort harus melakukan logging paket yang lewat dapat menggunakan perintah –l nama-file-logging, atau membiarkan snort menggunakan default file logging-nya di directory /var/log/snort. Kemudian menganalisa catatan / logging paket yang ada sesuai dengan isi perintah snort.conf.

Ada beberapa tambahan perintah yang akan membuat proses deteksi menjadi lebih effisien, mekanisme pemberitahuan alert di Linux dapat di set dengan perintah –A sebagai berikut,

-A fast, mode alert yang cepat berisi waktu, berita, IP & port tujuan.
-A full, mode alert dengan informasi lengkap.
-A unsock, mode alert ke unix socket.
-A none, mematikan mode alert.

Untuk mengirimkan alert ke syslog UNIX kita bisa menambahkan switch –s, seperti tampak pada beberapa contoh di bawah ini.

./snort –c snort.conf –l ./log –s –h 192.168.0.0/24
./snort –c snort.conf –s –h 192.168.0.0/24

Untuk mengirimkan alert binary ke workstation windows, dapat digunakan perintah di bawah ini,

./snort –c snort.conf –b –M WORKSTATIONS

Agar snort beroperasi secara langsung setiap kali workstation / server di boot, kita dapat menambahkan ke file /etc/rc.d/rc.local perintah di bawah ini

/usr/local/bin/snort –d –h 192.168.0.0/24 –c /root/snort/snort.conf –A full –s –D

atau

/usr/local/bin/snort –d –c /root/snort/snort.conf –A full –s –D

dimana –D adalah switch yang menset agar snort bekerja sebagai Daemon (bekerja dibelakang layar).

TUGAS PENDAHULUAN

1. Sebutkan dan jelaskan dengan singkat apa yang disebut dengan konsep logging ?
2. Sebutkan fasilitas logging yang ada di linux !
3. Sebutkan beberapa software yang biasa dipakai untuk melakukan monitoring log di linux.

PERCOBAAN

1. Siapkan 3 file source
   - Libpcap-0.8.3.tar.gz
   - Pcre-5.0.tar.gz
   - Snort-2.3.2.tar.gz
2. Buat Direktori Snort Pada Root
   #Mkdir /Snort
3. Copikan Semua File Tadi Ke /Snort
4. Lakukan Langkah Installasi Sbb :
   - Langkah 1 Installasi Libpcap

```
# cd /Snort
# gzip -Dc Libpcap-0.8.3.Tar.Gz | Tar -Xf -
# Cd Libpcap-0.8.3
# ./Configure ; Make
 # Make Install
```

- Langkah 2 Installasi Libpcre

```
# Cd /Snort
# Gzip -Dc Pcre-5.0.Tar.Gz | Tar -Xf -
# Cd Pcre-5.0
# ./Configure ; Make
# Make Install
```

- Langkah 3 Insallasi Snort

```
# Cd /Snort
# Gzip -Dc Snort-2.3.2.Tar.Gz | Tar -Xf -
# Cd Snort-2.3.2
# ./Configure ; Make
```

5. Manjalankan snort
   a. Bekerjalah dengan teman anda, salah satu menjalankan snort yang satunya menjalankan aplikasi yang lain.
   b. Jalankan perintah ping dari komputer lain ke komputer snort, buka terminal yang lain dan jalankan nmap.
   c. Jalankan snort dengan menggunakan mode sniffer
      - snort –v
      - #snort –vd
      - #snort –vde
      - #snort –v –d –e

      Jelaskan perbedaan hasil dari option di atas.
   d. Untuk mempermudah pembacaan masukkan hasil snort ke dalam file, jalankan perintah berikut :
      - snort –dev –l ./log
   e. Untuk membaca file snort berikan option –r pada snort
   f. Jalankan perintah ping dari komputer lain ke komputer snort, buka terminal yang lain dan jalankan nmap.
   g. Menggunakan mode paket sniffer, analisa hasilnya.
      - snort [-i interface] [-P snap-length] [filter-expression]
   h. Menjalankan snort dengan rule
      - snort -c /usr/local/share/rules/snort.conf -b -s
   i. Mengaktifkan snort untuk mendeteksi penyusup
      - snort –dev –l ./log –c snort.conf
   j. Untuk menjadi daemon berikan option –D pada snort ” snort –D”

6. Menjalankan snort dengan mode NIDS (Network Intrusion Detection System)
   a. Opsi e, dihilangkan karena kita tidak perlu mengetahui link layer MAC. Opsi v dihilangkan juga

      snort -d -h 192.168.1.0/24 -l /var/log/snort -c /etc/snort/snort.conf

b. Bekerjasamalah dengan rekan anda. Sekarang coba jalankan scanning dari komputer lain dengan nmap menuju komputer yang anda pasangi snort. Terlebih dulu jalankan snort dengan mode NIDS, kemudia lakukan scanning dengan perintah :

   # snort -d -h 192.168.1.0/24 host <no_ip_snort> -l /var/log/snort –c /etc/snort/snort.conf

   #nmap -sS -v <no_ip_snort>

c. Lihatlah apakah scan anda terekam oleh snort. Jika iya, copy paste hasil snort pada bagian scanning SYN. Untuk melihat, gunakan perintah :

   # snort –dev –r <nama-log-file> | more

   Apakah scanning ini ditandai sebagai alert ? Coba lihat di /var/log/snort

d. Jalankan snort. Buka halaman web. Apakah ini terdeteksi sebagai alert?

e. Sekarang coba ubah rule snort. Buat rule baru yaitu alltcp.rules.

   alert tcp any any -> any any (msg:"TCP Traffic";sid:9000000;rev:0;)

   Apa artinya ?

f. Coba lihat snort.conf. Beri tanda # pada semua rule lain kecuali rule anda yaitu : alltcp.rules.

g. Bukalah halaman web, lihatlah apakah ada tanda sebagai alert atau tidak

h. Coba lakukan scanning seperti perintah b. Lihatlah apakah ada tanda sebagai alert atau tidak

i. Apa yang dapat anda simpulkan dari langkah diatas ?

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Intrusion Detection System [Snort]

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Download rule terbaru di snort dan bandingkan dengan rule yang lama, apa saja perubahan yang ada !
3. Jelaskan rule apa saja yang bisa didekteksi oleh snort !
4. Untuk mempermudah pembacaan data snort dimungkinkan dimasukkan dalam database, carilah artikel tentang konfigurasi snort menggunakan database
5. Jelaskan juga aplikasi yang bisa dipakai untukmembaca database snort!

MODUL 6
INTRUSION DETECTION SYSTEM [PORTSENTRY]

TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep Manajemen Log di linux
2. Mahasiswa memahami berbagai macam file log yang ada di linux
3. Mahasiswa mampu melakukan analisa terhadap file log yang ada di linux

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.

PortSentry dapat di download secara pada http://www.psionic.com.

Beberapa fitur utama dari PortSentry:

- 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 privilige 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/always_ignore 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/portsentry/portsentry.ignore isikan IP address yang perlu di abaikan sama dengan isi file /etc/portsentry/always_ignore.
- Pada file /etc/portsentry.modes 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.

TUGAS PENDAHULUAN

1. Sebutkan dan jelaskan dengan singkat apa yang disebut dengan konsep logging ?
2. Sebutkan fasilitas logging yang ada di linux !
3. Sebutkan beberapa software yang biasa dipakai untuk melakukan monitoring log di linux.

PERCOBAAN

1. Siapkan file portsentry portsentry-1*.rpm , taruh ditempat yang anda inginkan (cara menjalankan portsentry menyesuaikan nantui extract file kita)
2. Jalankan Perintah berikut untuk installasi
   [root@localhost portsentry-1.1]# rpm -ivh portsentry-1*.rpm

3. Edit file konfigurasi :
   vi /etc/portsentry/portsentry.conf (waktu extraxt sourec di taruh di /usr/src, selanjutnya setelah diextract timbul direktori bari portsentry-1.1 dan ketika diinstal timbul lagi subdirektori baru yaitu portsentry dimana semua file running dan konfigurasi berada.
   Edit bagian berikut

```
# Edit bagian HISTORY_FILE dan BLOCKED_FILE menjadi:
#
HISTORY_FILE="/var/log/portsentry/portsentry.history"
BLOCKED_FILE="/var/log/portsentry/portsentry.blocked"
#
```

```
#
################################
#                Misc.                Configuration                Options                #
################################
RESOLV_HOST="0"
######################
#                Scan                trigger                value                #
######################
SCAN_TRIGGER="0"
#EOF
```

4. Edit File /etc/portsentry/portsentry.ignore, isi dengan IP yang tidak terblokir, misal :

```
# Format : <Ip Address>/<Netmask>
#  Misalnya:  Konfigurasi  Ip  di  Router  initrd@vmlinuz.unixminix.com
#                    eth0                :                202.212.77.99/30
#                    eth1                :                192.168.1.1/24
#
#            Maka            Daftar            Hosts-nya            menjadi            :
#
#                Exclude                all                local                interface
202.212.77.99
192.168.1.1
127.0.0.1
#                    Exclude                    default                    Gateway
202.212.77.98
#
#                                Exclude                                nameserver
202.212.77.1
#
#  Catatan:  jika  kita  tidak  mencantumkan  nilai  mask_length-nya
#            maka            diasumsikan            bernilai            32            bits.
# Jadi 192.168.1.1 sama dengan 192.168.1.1/32
```

5. File /etc/portsentry/portsentry.modes

```
######
atcp
audp
####
```

6. Bukalah port sebanyak mungkin untuk persiapan portsentry.
7. Insialisasi Daemon

   #/etc/init.d/portsentry start
8. Jika sudah jalan, jalankan # tail -f /var/log/messages, akan keluar hasil spt berikut :
   Nov 20 08:35:27 localhost portsentry[2192]: adminalert: PortSentry is now active and listening.
9. Pada komputer lain jalankan nmap pada komputer yang diinstal portsentry apa yang terjadi.

10. Jika sudah jalan, jalankan # tail -f /var/log/messages, amati hasilnya, . Apa korelasinya dengan step sebelumnya.?
11. Selanjutnya tutup/matikan service portsentry dan jalankan nmap lagi, apa yang terjadi
12. Jalankan netstat –taup, amati hasilnya, lihat pada baris portsentry, apa maksud output di atas ?

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Intrusion Detection System [Portsentry]

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Dengan bekerja hanya mendeteksi port dimana sebaiknya portsentry ditempatkan ?
3. Jelaskan arsitektur portsentry sehingga bisa melakukan blok menggunakan firewall jika ada yang dicurigai!

MODUL 7
INTRUSION DETECTION SYSTEM [TRIPWIRE]

TUJUAN PEMBELAJARAN:

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

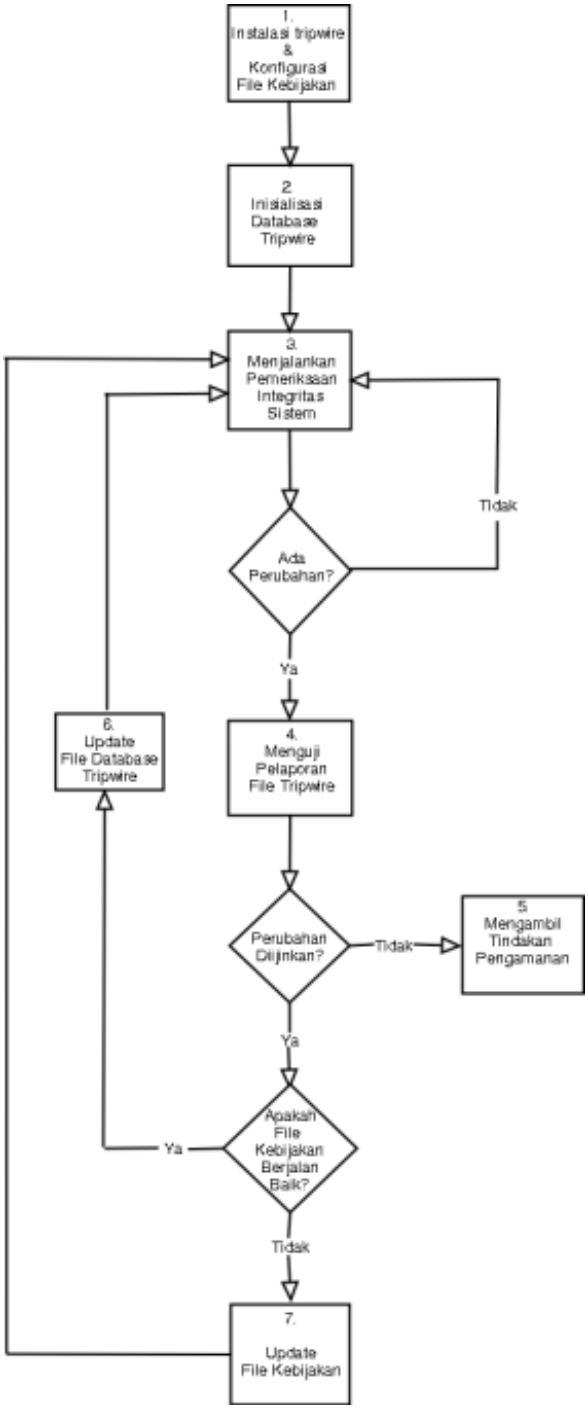
DASAR TEORI

Pemasangan program intrusi deteksi sebenarnya ditujukan untuk mendeteksi penyusup ataupun hacker ke suatu jaringan atau network dan bisa memantau seluruh ulah sang hacker yang sedang dilakukan olehnya.

Type IDS sendiri secara garis besar dibagi 2 yaitu hostbase dan network base IDS. Snort termasuk dalam Network base. Salah satu model host-based IDS adalah tripwire

Program tripwire berfungsi untuk menjaga integritas file system dan direktori, dengan mencatat setiap perubahan yang terjadi pada file dan direktori. Konfigurasi tripwire meliputi pelaporan melalui email, bila menemukan perubahan file yang tidak semestinya dan secara otomatis melakukan pemeriksaan file melalui cron. Penggunaan tripwire biasanya digunakan untuk mempermudah pekerjaan yang dilakukan oleh System Administrator dalam mengamankan System. Tripwire merupakan salah satu

Cara kerja tripwire adalah melakukan perbandingan file dan direktori yang ada dengan database sistem. Perbandingan tersebut meliputi perubahan tanggal, ukuran file, penghapusan dan lain-lainnya. Setelah tripwire dijalankan, secara otomatis akan melakukan pembuatan database sistem. Kemudian secara periodik akan selalu melaporkan setiap perubahan pada file dan direktori.



Berikut ini merupakan penjelasan dari skema di atas:

1. Anda melakukan instalasi tripwire dan melakukan pengaturan *policy file* serta inisialisasi database,
2. Selanjutnya Anda bisa menjalankan pemeriksaan integritas sistem.
3. Bila ditemukan perubahan ukuran, tanggal maupun kepemilikan pada file tersebut, maka tripwire akan melakukan laporan pada sistem tentang adanya perubahan pada file terkait.

4. Jika perubahan tidak diijinkan, maka Anda bisa mengambil tindakan yang diperlukan.
5. Sebaliknya, jika perubahan pada file tersebut diijinkan, maka tripwire akan memeriksa *Policy File*, apakah policy file berjalan dengan baik?
6. Jika *policy file* tidak berjalan dengan benar, maka policy file harus di-update sesegera mungkin.
7. Jika *policy file* sudah berjalan dengan benar, maka tripwire akan melakukan update database file database.
8. Dan demikian seterusnya proses ini berlangsung.

TUGAS PENDAHULUAN

1.

PERCOBAAN

1. Siapkan file source tripwire, ambil pada komputer yang sudah disediakan.
2. Lakukan installasi file tripwire yang ada

   ```
   rpm -Uvh tripwire-2.3.1-18.3.1.i386.rpm
   Preparing...                ########################################### [100%]
   1:tripwire                  ########################################### [100%]
   ```

3. Lakukan pre-konfigurasi Jalankan file twinstall.sh di direktori /etc/tripwire/

   ```
   /etc/tripwire/twinstall.sh
   ```

4. Membuat kunci:

   ```
   Enter the site keyfile passphrase:
   Verify the site keyfile passphrase:
   Generating key (this may take several minutes)...Key generation complete.
   Enter the local keyfile passphrase:
   Verify the local keyfile passphrase:
   Generating key (this may take several minutes)...Key generation complete.
   ```

5. Menandai file konfigurasi dan aturan (policy) dengan kunci yang dibuat pada poin diatas.

   ```
   ---------------------------------------------
   Signing configuration file...
   Please enter your site passphrase:
   Wrote configuration file: /etc/tripwire/tw.cfg
   A clear-text version of the Tripwire configuration file
   /etc/tripwire/twcfg.txt

    ---------------------------------------------
   Signing policy file...
   Please enter your site passphrase:
   Incorrect site passphrase.
   Please enter your site passphrase:
   Wrote policy file: /etc/tripwire/tw.pol
   A clear-text version of the Tripwire policy file
   /etc/tripwire/twpol.txt
   ```

6. Inisialisasi tripwire:

   ```
   /usr/sbin/tripwire --init
   ```

7. Menjalankan tripwire

   ```
   /usr/sbin/tripwire --check
   ```

8. Update policy

   Jika terjadi perubahan policy tripwire, edit file policy sesuai dengan kebutuhan (defaultnya adalah twpol.txt). Misal, menginginkan setiap kali ada perubahan pada file crontab, server

langsung mengirimkan pemberitahuan ke email anda.

- copy file twpol.txt menjadi twpol.txt.new, kemudian edit file twpol.txt.new

```
(
  rulename = "Critical configuration files",
  severity = $(SIG_HI),
emailto = isbat@eepis-its.edu )
{
    #/etc/crontab              -> $(SEC_BIN) ;
}
```

- Perbaharui data tripwire:

```
/usr/sbin/twadmin --create-polfile -S /etc/tripwire/site.key
/etc/tripwire/twpol.txt.new
```

- Inisialisasi ulang

```
/usr/sbin/tripwire --init
```

- Jalankan kembali tripwire

```
/usr/sbin/tripwire --check
```

9. Sebelum policy email kita jalankan, mungkin kita bisa mengecek terlebih dahulu apakah tripwire bisa mengirim email apa tidak secara langsung dari command :

```
/usr/sbin/tripwire --test --email isbat@eepis-its.edu
```

10. Untuk mencetak hasil tripwire, jalankan perintah berikut :

```
# twprint -m r --twrfile /var/lib/tripwire/report/<name>.twr
```

11. Supaya tripwire bisa disetting sesuai keperluan, misal akan melakukan cek setiap hari, tambahan file tripwire-check dan edit isinya 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 "/etc/tripwire/twinstall.sh" and/or "tripwire --init""
else
  test -f /etc/tripwire/tw.cfg && /usr/sbin/tripwire --check
fi
```

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Network Address Translator Dasar

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Berdasarkan percobaan yang anda lakukan jelaskan cara kerja tripwire dalam melakukan integriry checker?
3. Carilahr di internet Rule apa saja yang bisa dideteksi oleh tripwire

MODUL 8
SNIFFING DAN
SESSION HIJACKING

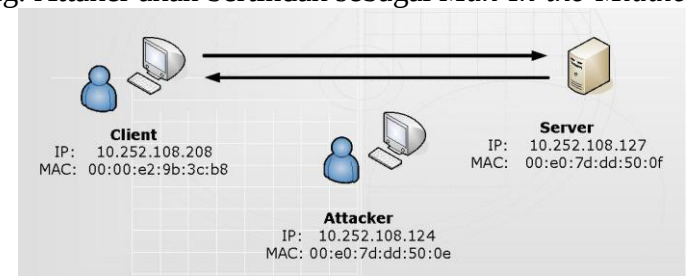
TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep sniffing dan session hijacking
2. Mahasiswa mampu menangani masalah sniffing dan session hijacking

DASAR TEORI

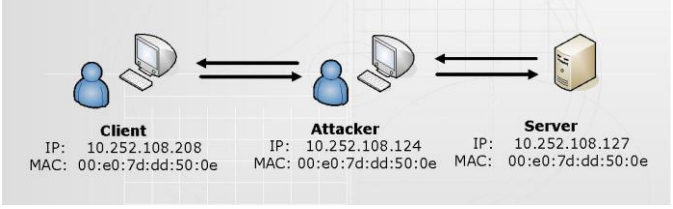
Sniffer adalah program yang membaca dan menganalisa setiap protokol yang melewati mesin di mana program tersebut diinstal. Secara default, sebuah komputer dalam jaringan (workstation) hanya mendengarkan dan merespon paket-paket yang dikirimkan kepada mereka. Namun demikian, kartu jaringan (network card) dapat diset oleh beberapa program tertentu, sehingga dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket tersebut dikirimkan. Aktifitasnya biasa disebut dengan sniffing.

Untuk dapat membaca dan menganalisa setiap protokol yang melewati mesin, diperlukan program yang bisa membelokkan paket ke komputer attaker. Biasa disebut serangan spoofing. Attaker akan bertindak sebagai *Man-In-the-Middle* (*MIM*).



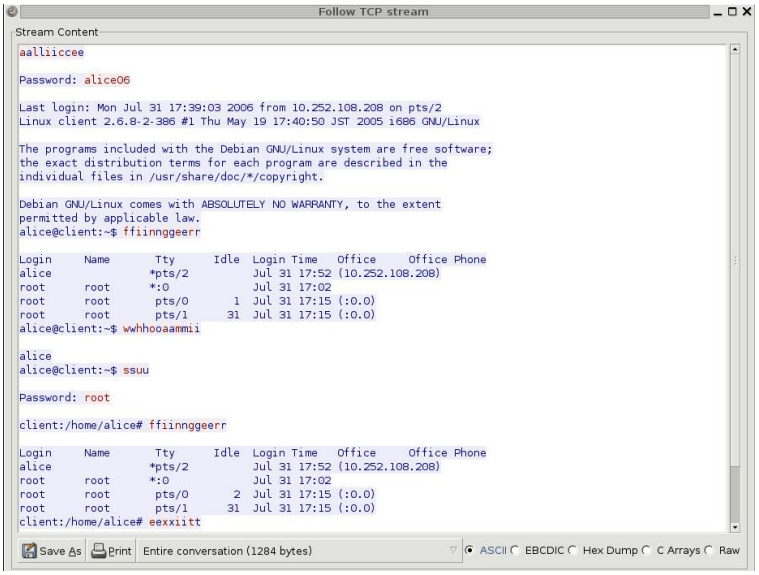
Koneksi TCP sebelum Spoofing

Gambar di atas mengilustrasikan koneksi TCP yang sebenarnya, tanpa ada sebuah host yang bertindak sebagai *MIM*. Kemudian host *attacker* menjalankan program *Spoofing*, berarti host *attacker* akan bertindak sebagai host yang dilewati data antara host client dan host server.



Koneksi TCP setelah Spoofing

Setelah host *attacker* menjadi host yang berada di tengah-tengah dari dua host yang saling berkomunikasi, kemudian *attacker* melakukan analisa traffic dengan menjalankan program ethereal. Dengan menganalisa traffic TCP yang sudah tercapture, *attacker* dapat mengetahui apa saja yang dilakukan oleh host client terhadap host server.



Follow TCP Stream yang dijalankan attacker

Ada dua macam serangan spoofing yang terjadi :

1. ARP Spoofing, yang bekerja dalam satu jaringan

   ARP Spoofing berusaha menggantikan MAC address yang sebenarnya dengan MAC address penyerang sehingga ketika si target berkomunikasi dengan orang lain, maka harus melewati penyerang, selanjutnya data bisa disadap.

   ARP Spoofing merupakan awal serangan selanjutnya, biasanya serangan ini diteruskan dengan melakukan pengambilalihan session atau yang biasa disebut session hijacking.

   Session Hijacking

   Session Hijacking adalah mengambil alih sebuah session pada satu koneksi jaringan.Secara garis besar dibagi menjadi dua tipe, yaitu *active session hijacking* dan *passive session hijacking*.

   Active Session Hijacking

   Pada serangan ini, *attacker* mengambil alih sebuah session yang terjadi dengan cara memutuskan sebuah komunikasi yang terjadi. *Attacker* bertindak sebagai *man-in-the-middle* dan aktif dalam komunikasi antara client dengan server. Serangan ini membutuhkan keahlian untuk menebak nomer *sequence* (SEQ) dari server, sebelum client dapat merespon server. Pada saat ini, nomer *sequence* yang dibuat oleh setiap sistem operasi berbeda-beda. Cara yang lama adalah dengan menambahkan nilai konstan untuk nomer *sequence* selanjutnya. Sedangkan mekanisme yang baru adalah dengan membuat nilai acak untuk membuat nilai awal dari nomer *sequence* ini.

Ketika sebuah komputer *client* melakukan koneksi terhadap komputer *server*, *attacker* menyisipkan komputernya di antara dua koneksi tersebut. Ada empat proses untuk melakukan *active session hijacking*, antara lain:

- Tracking the connection (mencari koneksi yang sedang terjadi)

  Attacker akan mencari target, yaitu client dan server yang akan melakukan komunikasi. *Attacker* menggunakan *sniffer* untuk mencari target atau dengan mengidentifikasi host yang diinginkan dengan menggunakan *scanning tool* seperti nmap. Sebelum mengetahui siapa yang akan melakukan komunikasi dan pada port berapa komunikasi tersebut berjalan, *attacker* harus melakukan *ARP Spoofing* terhadap dua host yang saling berkomunikasi.

  Cara ini dilakukan agar *attacker* dapat melihat komunikasi yang terjadi, kemudian dapat mengetahui nomer *sequence* (SEQ) dan *acknowledgement* (ACK) yang diperlukan. Nomer ini digunakan oleh *attacker* untuk memasukkan paket diantara dua komunikasi.
- Desynchronizing the connection (Melakukan pembelokan koneksi)

  Langkah ini dilakukan ketika sebuah koneksi sudah terjadi antara client dan server yang tidak sedang mengirimkan data. Dalam keadaan ini, nomer *sequence* (SEQ) dari server tidak sama dengan nomer *sequence* (SEQ) dari client yang melakukan komunikasi. Begitu juga sebaliknya, nomer nomer *sequence* (SEQ) dari client tidak sama dengan nomer *sequence* (SEQ) dari server.

  Untuk melakukan desynchronisasi koneksi antara client dan server, nomer *SEQ* atau *ACK* dari server harus dirubah. Hal ini dapat dilakukan, jika dikirimkan data kosong (*null data*) ke server. Sehingga nomer *SEQ* atau *ACK* dari server akan berubah, sedangkan nomer *SEQ* atau *ACK* dari client yang melakukan komunikasi dengan server tidak berubah atau terjadi penambahan.
- Resetting Connection (Membuat koneksi baru)

  Setelah melakukan desynchronisasi, *attacker* mengirimkan sebuah *reset flag* ke server. Hal ini dilakukan untuk membuat koneksi baru dengan nomer *sequence* yang berbeda. Komunikasi antara client dengan server yang terjadi sebelumnya akan terputus.
- Injecting Packet (Memasukkan paket)

  Pada langkah ini, *attacker* dapat melakukan interupsi terhadap komunikasi antara client dan server, sehingga *attacker* dapat memasukkan paket lain pada koneksi tersebut.

Passive Session Hijacking

Serangan pembajakan session yang dilakukan secara pasif dapat dilakukan menggunakan *sniffer*. Alat ini dapat memberikan seorang *attacker* informasi berupa id user dan password dari client yang sedang melakukan login ke server. ID user dan password ini dapat digunakan oleh *attacker* untuk melakukan login pada lain waktu.

Sniffing password merupakan contoh serangan yang dapat dilakukan ketika *attacker* memperoleh akses pada suatu jaringan

Beberapa hal yang bisa dipakai untuk menanggulangi arp spoofing adalah : gunakan arp tabel secara permanen dan gunakan enkripsi

2. IP Spoofing yang bekerja antar jaringan
   IP spoofing adalah membuat paket IP menggunakan *source IP address* orang lain. Orang yang melakukan serangan DoS (Deniel Of Service) biasanya mengelabuhi target dengan menyamar/IP Headernya diganti dengan IP Header orang lain. Beberapa serangan yang biasa digunakan Ping Of Death, Syn Flood, Land Attack, Teradrop.

TUGAS PENDAHULUAN

1. Jelaskan apa yang disebut dengan DoS ?
2. Jelaskan apa yang disebut dengan Ping Of Death, Syn Flood, Land Attack, Teradrop!
3. Jelaskan pula apa yang disebut dengan Serangan Buffer Over Flow ?
4. Dalam arp spoofing ada istilah yang disebut dengan arp cache poisoning, jelaskan dengan singkat apa itu arp cache poisoning !
5. Carilah command untuk melakukan bloking terhadap ip spoofing menggunakan iptables.

PERCOBAAN

1. Percobaan arp spoofing
   a. Bekerjalah dengan teman sebelah untuk melakukan percobaan ini, setiap kelompok minimal 3 orang. Satu berfungsi sebagai penyerang, satu berfungsi sebagai target, satu komputer adalah yang dihubungi oleh target menjalankan aplikasi tertentu
   b. Pastikan telnet dan ssh diinstall pada komputer yang dihubungi oleh target
   c. Pastikan ethereal diinstall pada komputer penyerang/attacker
   d. Pada komputer attacker lakukan langkah berikut :
      - Install arposion
      - Jalankan arpoison

        arpoison -i eth0 -d ip_yg _dihubungi_target -s ip_target
        -t mac_yg_dihubungi_target -r mac_target
      - Jalankan ethereal pada attacker, start dan tunggu data masuk
   e. Pada komputer target jalankan perintah berikut :
      - Dari komputer target ke jalankan telnet ke komputer ip_yg _dihubungi_target
      - Jalankan beberapa perintah linux dari telnet tersebut.
      - Keluar dari telnet
   f. Pada komputer attacker tutup ethereal, selanjutnya lihat hasil capture. Seharusnya ada paket yang ke dan dari komputer target ke komputer tujuan. Analisa paket tcp khusus telnet dan lihat pada telnet data dan klik kanan pilih follow tcp string, seharusnya anda akan dapat password dan user serta apa saja yang pernah dilakukan oleh target.
   g. Kembali lakukan langkah 1.d sampai 1.f. tapi jangan memakai telnet tapi ssh dan bandingkan memakai ethereal apda 1.f apa perbedaannya. Berikan kesimpulan anda.

h. Pada komputer target tambahan arp komputer teman yang akan dihubungi secara permanen. Selanjutnya lakukan percobaan 1.d-1.f. Apakah pada ethereal terlihat data telnet ? Berikan kesimpulan anda.

2. Percobaan ip spoofing
   a. Bekerjalah dengan teman sebelah untuk melakukan percobaan ini, setiap kelompok minimal 2 orang. Satu berfungsi sebagai penyerang, satu berfungsi sebagai target.
   b. Siapkan beberapa utility ip spoofing, mintalah source pada dosen/asisten praktikum
   c. Kompilasi dan jalankan beberapa tools yang sudah disiapkan dan komputer target jalankan ethereal. Analisa paket yang muncul dan berikan kesimpulan anda.
      - Jalankan IDS snort pada setiap komputer target, analisa hasil paket yang ada.
      - Jalankan ethereal pada target
      - Jalankan langkah ini pada attacker
        a. gcc pod_spoofing.c –o pod_spoofing
        b. ./pod_spoofing ip_palsu ip_target
      - Setelah beberapa saat stop ethereal dan analisa paket di ethereal berikan kesimpulan anda.

      - Jalankan ethereal pada target
      - Jalankan langkah ini pada attacker
        a. gcc syn_flood.c –o syn_flood
        b. ./syn_flood ip_palsu ip_target port_awal port_akhir
      - Setelah beberapa saat stop ethereal dan analisa paket di ethereal berikan kesimpulan anda

      - Jalankan ethereal pada target
      - Jalankan langkah ini pada attacker
        a. gcc land_attack.c –o land_attack
        b. ./land_attack –t ip_palsu –p no_port –c jumlah_paket
      - Setelah beberapa saat stop ethereal dan analisa paket di ethereal berikan kesimpulan anda

      - Jalankan ethereal pada target
      - Jalankan langkah ini pada attacker
        a. gcc teardrop+spoofing.c –o teardrop+spoofing
        b. ./teardrop+spoofing ip_target ip_palsu –n jumlah_pengulangan
      - Setelah beberapa saat stop ethereal dan analisa paket di ethereal berikan kesimpulan anda

3. Blok ip spoofing menggunakan iptables yang sudah anda dapatkan pada tugas pendahuluan dan jalankan percobaan 2 lagi tangkap data memakai ethereal apakah kelihat seperti pada percobaan 2 ? Berikan kesimpulannya.

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Sniffing dan Session Hijacking

Dasar

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Simpulkan perbedaan setiap metode yang ada pada percobaan ip spoofing
3. Apa type transport layer yang dipakai ip spoofing, mengapa demikian, beri penjelasan.
4. Sebutkan metode yang dipakai untuk menangkal arp spoofing dan ip spoofing

MODUL 9
EMAIL SECURITY (INSTALL EMAIL DAN ANTI SPAM)

TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang Email Secrity di linux
2. Mahasiswa mampu melakukan installasi dan konfigurasi anti email dan penambahan spam di email server

DASAR TEORI

Layanan paling populer di Internet adalah *Electronic Mail* atau orang sering menyingkatnya menjadi e-mail. Jika kita mempunyai program client e-mail misalnya Eudora dan memiliki akses kelayanan e-mail, maka dapat mengirim e-mail ke setiap orang yang alamat e-mailnya kita ketahui.

Untuk melihat keamanan sistem Internet perlu diketahui cara kerja system Internet. Antara lain, yang perlu diperhatikan adalah hubungan antara komputer di Internet, dan protokol yang digunakan. Internet merupakan jalan raya yang dapat digunakan oleh semua orang (*public*). Untuk mencapai server tujuan, paket informasi harus melalui beberapa system (router, gateway, hosts, atau perangkat-perangkat komunikasi lainnya) yang kemungkinan besar berada di luar kontrol dari kita. Setiap titik yang dilalui memiliki potensi untuk dibobol, disadap, dipalsukan.

Beberapa hal yang bisa dilakukan untuk mengamankan email adalah melakukan installasi anti spam dan anti virus, sehingga email yang kita terima terjamin keamanannya sebab di email kadang disertakan attachment file yang berpotensi Menyebarkan virus, worm dan trojan serta email spam.

TUGAS PENDAHULUAN

1. Jelaskan cara kerja dari Mail Server
2. Sebutkan beberapa software yang dipakai untuk mengamankan email dari spam dan virus

PERCOBAAN

Instalasi Postfix dan mengaktifkan mail service

1. Instalasi Postfix
    - Cek apakah paket2 tersebut sudah terinstall di komputer anda dengan perintah
      # rpm –qa | grep postfix
      Jika ada akan nampak postfix-.....rpm
    - Jika belum install postfix dengan perintah rpm –ivh <postfix..>
    - Cek apakah sendmail juga terinstall, jika iya, hapus dengan perintah:
      # rpm –e <sendmail-...> –nodeps

2.Mengaktifkan service postfix

service potfix start

3. Cek apakah daemon postfix sudah bekerja dengan perintah :

nmap localhost

Capture hasilnya . Jika sudah bekerja, akan nampak port 25 terbuka untuk SMTP.

4. Anda bisa juga mengecek dengan perintah

telnet localhost 25

Ketik quit dan ikuti dengan enter. Capture hasilnya !

5. Konfigurasi Postfix

Untuk mengonfi gurasikan Postfix, Anda tinggal mengedit file konfi gurasi postfix yang berada di /etc/postfix/main.cf . Beberapa parameter penting yang perlu diedit untuk memfungsikan Postfix:

```
myhostname = mail.jerapah.com
mydomain = jerapah.com
myorigin = $myhostname
inet_interfaces = all
```

6. Berikutnya, *reload* service Postfix untukmelihat perubahan dengan mengetikkan perintah berikut:

/etc/init.d/postfix reload

Jika reload gagal, coba restart lagi service postfix. Kemudian ikuti dengan reload.

7. Coba liat perubahan yang anda lakukan dengan perintah :

#postconf –n

Capture hasilnya.

8. Caba cek log mail di /var/log/maillog. Buka dengan perinta vi. Capture hasilnya.
9. Coba restart lagi postfix dengan perintah :

service postfix restart

10. Buat 3 userbaru di servermail anda, yaitu user1, user2 dan user 3

useradd <namauser>

passwd <namauser>

Testing Postfix

11. Kirim mail internal PC :

- Coba telnet dan kirim pesan lewat mail server anda.

  # telnet mail.jerapah.com 25

- Masukkan isi mail anda dengan cara berikut

Jangan lupa, buat user baru user1 dan user2 di PC anda

```
[root@localhost ~]# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.kijang.com ESMTP Postfix
MAIL FROM: user1
250 2.1.0 Ok
RCPT TO: user2
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Test sending email
.
250 2.0.0 Ok: queued as 33C512BD013
quit
221 2.0.0 Bye
```

```
Connection closed by foreign host.
```

Perhatikan bahwa untuk mengakhiri email, ketik <enter> . <enter>

⑩ Coba buka /var/spool/mail/user2 dengan vi. Lihat apakah sama dengan isi mail yang anda kirim. Jika sudah sama, berarti anda berhasil. Copy paste hasil vi-nya.

12. Mengirim mail antar computer. Coba anda lakukan hal yang sama dengan menggunakan mail server yang sudah anda buat.

- Perhatikan konfigurasi jerapah.com.zone.db

```
$TTL 86400
@      IN      SOA        ns.jerapah.com. hostmaster.jerapah.com. (
                                      2001031102 ; serial
                                      10800 ; refresh
                                      3600 ; retry
                                      604800 ; Expire
                                86400 ;
                                                    )


kijang.com.  IN     NS           ns.kijang.com.
ns           IN     A            10.252.105.33
www          IN     CNAME        ns
mail         IN     CNAME        ns
ftp          IN     CNAME        ns
```

- Perhatikan juga file jerapah.com.zone.local

```
$TTL 86400
@    IN    SOA      ns.jerapah.com. hostmaster.jerapah.com. (
                                          42  ; serial (d. adams)
                                          3H  ; refresh
                                          15M ; retry
                                          1W  ; expire
                                          1D  ; minimum
                                          )


@ IN     NS                ns.jerapah.com.
@ IN   A                      10.252.105.33
33       IN                   PTR                  ns.jerapah.com.
```

- Restart dulu DNS server anda. Pastikan hasilnya OK.
- telnet dari computer lain ke computer anda.
  # telnet mail.jerapah.com 25
- kirim ke user yang ada di computer anda.

```
# telnet mail.jerapah.com 25
MAIL FROM: root
RCPT TO: user2
DATA
Test sending mail dari luar
.
```

```
quit
```

- Jika anda gagal mengkoneksi, kemungkinan DNS anda tidak dikenali. Coba ping lagi mail.jerapah.com. Berhasilkah ? Coba hapus firewall dengan iptables -F di sisi server
- Setelah itu cek Security Level Configuration. Coba ubah. System-> Administration -> Firewall and SE Linux. Pada firewall options, Klik Enable Firewall. Klik service telnet dan mail.
- Jika masih gagal, coba gunakan :
  # telnet <no_ip_mailserver> 25
- Coba buka /var/spool/mail/user2 di computer anda dengan vi. Lihat apakah sama dengan isi mail yang anda kirim. Jika sudah sama, berarti anda berhasil. Copy paste hasil vi-nya.

Dovecot (IMAP service)

13. Cek apakah dovecot sudah terintall di PC anda. Bila belom, install rpm dovecot .
14. Cek apakah email client evolution sudah terinstall di PC anda. Jika belum, install rpm-nya
15. Jalankan service dovecot dgn perintah :
    # service dovecot start
16. Cek apakah dovecot sudah terinstall dengan perintah :
    # nmap localhost
    Bila anda melihat service pop3s sudah on, berarti service dovecot sudah berjala
17. Buka email client evolution. Applications->Internet->Email. Perhatikan bahwa bila anda ingin membuka mail untuk user1, maka pilih user1 dan user1@jerapah.com untuk semua setting username dan email address
18. Pada layar welcome, klik forward.
19. Pada layar identity, pada isian full name, masukkan username anda (user1,user2 atau user3). Pada isian email address, masukkan nama email anda (user1@jerapah.com, user2@jerapah.com,user3@jerapah.com). Klik forward
20. Pada layar Receiving mail, masukkan server type adalah IMAP. Server : mail.jerapah.com. Username masukkan user1,2 atau 3. Klik forward
21. Pada layar Receiving Options, klik forward saja.
22. Pada layar Sending email, masukkan server type : SMTP. Server: mail.jerapah.com. Username masukkan user1,2 atau 3. Klik forward
23. Pada layar Account Management, masukkan Name: user1@jerapah.com atau user2@jerapah.com, atau user3@jerapah.com Klik forward
24. Pada layar timezone, pilih Asia/Jakarta, Klik forward
25. Pada layar Done, click Apply. Masukkan password user tersebut.
26. Bila sudah, maka anda akan melihat window Email Client Evolution. Selamat anda sudah membuat account anda di evolution.

Berpasanganlah dengan rekan anda, saling berkirim email. Pada komputer teman anda, buatlah account yang berbeda dari yang tadi anda buat. Misalnya jika yang pertama user1, maka pada komputer teman anda buat account user2. Caranya sama seperti ketika anda membuat account anda yang pertama, mulai dari welcome sampai done.

27. Coba kirim mail dari komputer anda ke teman anda dan sebaliknya. Perhatikan untuk kolom tujuan tidak perlu menyertakan full email address, jadi cukup user1, user2 atau user3.

SpamAssasin untuk menghalau Spam Email pada Postfix

3. Cek versi perl yang digunakan. Modul perl ini digunakan untuk melakukan kompilasi SpamAssassin.

#perl -v
Yang digunakan Perl versi : ...

4. Lakukan instalasi SpamAssasin. Cari file Mail-SpamAssassin-3.1.8.tar.gz. Lakukan unzip dg perintah :
   #tar -xvzf <Mail-Spam....gz> --dir=/usr/local
   #cd <Mail-Spam..>
   #perl Makefile.pl
   # make
   #make test
   #make install
5. Mengkonfigurasi spamassassin. Untuk mengecek dimana letak file binary SpammAssassin, gunakan perintah. File binary adalah file yg digunakan untuk mengeksekusi SpamAssasssin. File konfigurasi adalah file local.cf.
   #which spamassassin
   Letak file binary SpamAssassin adalah : .....
   # locate local.cf.
   Letak file konfigurasi SpamAssassin adalah : .....
6. Backuplah file local.cf pada spamAssassin dan main.cf pada postfix
   #cp /etc/postfix/main.cf /etc/postfix/main.cf.asli
   #cp /etc/mail/spamassassin/local.cf /etc/mail/spamassassin/local.cf.asli
7. Tambahkan baris berikut pada local.cf

```
# How many hits before a message is considered spam.
required_hits 5.0

# Text to prepend to subject if rewrite_subject is used
rewrite_header Subject [*****SPAM*****]

# Encapsulate spam in an attachment
report_safe 1

# Enable the Bayes system
use bayes 1

# Enable Bayes auto-learning
bayes_auto_learn 1
bayes_path /home/spamd/bayes
bayes_file_mode 0666

# Enable or disable network checks
skip_rbl_checks 0
use_razor2 0
use_pyzor 0
```

8. Cek konfigurasi local.cf dg perintah
   # spamassassin --lint
   # spamassassin --lint -D
9. Konfigurasi postfix. Tambahkan baris berikut pada main.cf. Taruh di baris paling bawah.

```
strict_rfc821_envelopes = yes
disable_vrfy_command = yes
smtpd_helo_required = yes
smtpd_client_restrictions =
```

```
smtpd_helo_restrictions =
smtpd_sender_restrictions =

smtpd_recipient_restrictions =
     permit_mynetworks,
     permit_sasl_authenticated,
     reject_unauth_destination,
     reject_invalid_hostname,
    reject_unauth_pipelining,
    reject_non_fqdn_sender,
    reject_unknown_sender_domain,
    reject_non_fqdn_recipient,
    reject_unknown_recipient_domain,
    check_client_access hash:$config_directory/access_client,
    check_sender_access hash:$config_directory/access_sender
    permit
```

10. Konfigurasi daemon spamasassin server dan client (spamd dan spamc). Buat user dan group spamd agar kita dapat menjalankan spamassassin tanpa user root.
    # groupadd -g 601 spamd
    # useradd -u 601 -g 601 -s /sbin/nologin -d /home/spamd spamd
11. Setelah membuat user, jalankan perintah berikut sebagai root:
    # /usr/bin/spamd --daemonize --username spamd --pidfile /home/spamd/spamd.pid
12. Membuat content-filter. Pertama buatlah user dan group bernama filter.
    #groupadd -g 700 filter
    #useradd -u 700 -g 700 -d /home/filer -s /bin/false filter
13. Copylah file spam.chk dari instruktur dan simpanlah di file /usr/local/bin/. Kemudian cek hak permissionnya. Ubahlah menjadi 750
    #chmod 750 spamchk
14. Bukalah file /etc/postfix/master.cf dan tambahkan 2 baris ini :

```
spamchk   unix -      n      n      -      10      pipe

     flags=Rq user=filter argv=/usr/local/bin/spamchk -f ${sender} --
${recipient}

smtp      inet   n      -      n      -      -      smtpd

        -o content_filter=spamchk:dummy
```

15. Lakukan reload postfix. Dan jalankan postfix
    #service postfix reload
    # service postfix restart
16. Testlah dg mengambil file spam dan cobakan dg perintah
    #/usr/bin/spamassassin -D < /root/sample-spam.txt

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Email Security

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Carilah diinternet beberapa anti spam yang bisa digunakan pada email dan bandingkan performance yang ada
3. Carilah diinternet beberapa anti virus yang bisa digunakan pada email dan bandingkan performance yang ada

MODUL 10
EMAIL SECURITY (ANTI VIRUS)

TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang Email Secrity di linux
2. Mahasiswa mampu melakukan installasi dan konfigurasi anti email dan penambahan spam di email server

DASAR TEORI

Layanan paling populer di Internet adalah *Electronic Mail* atau orang sering menyingkatnya menjadi e-mail. Jika kita mempunyai program client e-mail misalnya Eudora dan memiliki akses kelayanan e-mail, maka dapat mengirim e-mail ke setiap orang yang alamat e-mailnya kita ketahui.

Untuk melihat keamanan sistem Internet perlu diketahui cara kerja system Internet. Antara lain, yang perlu diperhatikan adalah hubungan antara komputer di Internet, dan protokol yang digunakan. Internet merupakan jalan raya yang dapat digunakan oleh semua orang (*public*). Untuk mencapai server tujuan, paket informasi harus melalui beberapa system (router, gateway, hosts, atau perangkat-perangkat komunikasi lainnya) yang kemungkinan besar berada di luar kontrol dari kita. Setiap titik yang dilalui memiliki potensi untuk dibobol, disadap, dipalsukan.

Beberapa hal yang bisa dilakukan untuk mengamankan email adalah melakukan installasi anti spam dan anti virus, sehingga email yang kita terima terjamin keamanannya sebab di email kadang disertakan attachment file yang berpotensi Menyebarkan virus, worm dan trojan serta email spam.

TUGAS PENDAHULUAN

3. Jelaskan cara kerja dari Mail Server
4. Sebutkan beberapa software yang dipakai untuk mengamankan email dari spam dan virus

PERCOBAAN

instalasi clamav

1. Untuk instalasi clamav agar dapat langsung memakai fasilitas built-in zip,gzip,bzip2, periksa apakah library yang dibutuhkan sudah terinstall.

```
root@mizuno root# rpm -qa | grep devel
bzip2-devel-1.0.2-9tr
zlib-devel-1.1.4-5tr
```

2. Selain aplikasi diatas, clamav juga membutuhkan library *gmp* untuk melakukan digital singature pada saat mengupdate database. Beberapa distribusi besar seperti redhat atau mandrake biasanya sudah menyertakan aplikasi gmp yang sudah siap di install dalam bentuk rpm. Bagi yang belum memiliki dapat mendonlot source-nya di http://www.swox.com/gmp/. Lalu lakukan langkah-langkah kompilasi untuk menginstall *libgmp* ini. Kalau sudah selesai baru dilanjutkan dengan instalasi

clamav dibawah

3. Aplikasi lain yang diperlukan adalah **curl**. Pastikan curl yang anda pakai mempunyai versi minimal 7.10.0, lakukan kompilasi sebagai berikut :
   - Siapkan user dengan home di `/var/lib/clamav` dan group yang akan menjalankan clamav daemon, untuk alasan security shell di set ke `/bin/false`

```
root@mizuno clamav-0.80# groupadd clamav
root@mizuno clamav-0.80# useradd  -g clamav -s /bin/false \
-c "Clam AntiVirus" clamav
```

   - ambil/donlot clamav versi terbaru
   - ekstrak dan masuk kedalam direktori clamav dan lakukan konfigurasi awal untuk menyesuaikan OS dan library yang tersedia. Pada tahap ini dapat pula kita lakukan optimasi file binary, misal diset untuk i686

```
root@mizuno root# tar xzpf clamav-0.80.tar.gz
root@mizuno root# cd clamav-0.80

root@mizuno clamav-0.80# CFLAGS="-O3 -march=i686 -mcpu=i686 \
>-funroll-loops -fomit-frame-pointer" \
>./configure \
>--sysconfdir=/etc \
>--bindir=/usr/bin \
>--sbindir=/usr/sbin \
>--libdir=/usr/lib \
>--includedir=/usr/include \
>--mandir=/usr/share/man \
>--with-dbdir=/var/lib/clamav \
>--disable-clamuko
```

   - lanjutkan perintah dberikut :

```
root@mizuno clamav-0.80# make
root@mizuno clamav-0.80# make install
```

   - edit file `/etc/clamd.conf`, ini digunakan untuk mengontrol daemon clamd. Apabila anda merencanakan untuk menggunakan clamscan saja dan tidak menggunakan daemon maka file ini tidak perlu di edit. Edit baris :

```
Example                         menjadi #Example
LocalSocket /tmp/clamd          menjadi #LocalSocket /tmp/clamd
#TCPSocket 3310                 menjadi TCPSocket 3310
#DataDirectory /var/lib/clamav  menjadi DataDirectory
/var/lib/clamav
#User clamav                    menjadi User clamav
#ScanMail                       menjadi ScanMail
```

     atau dengan kata lain matikan example, dan ubah daemon dari local socket menjadi tcp/ip. Tapi ini hanya sementara, hanya untuk mengetes apakah daemon bisa berfungsi.
   - eksekusi daemon dan lakukan periksaan di proses dan tcp/ip port 3310

```
root@mizuno root# /usr/local/sbin/clamd
root@mizuno root# ps aux | grep clamd
root     21327  0.0  4.8  9476 6108 ?        S    20:53   0:00
/usr/local/sbin/clamd
root     21328  0.0  4.8  9476 6108 ?        S    20:53   0:00
/usr/local/sbin/clamd
root     21329  0.0  4.8  9476 6108 ?        S    20:53   0:00
/usr/local/sbin/clamd
root@mizuno root# netstat -tpan
```

```
root@mizuno root# netstat -tpan | grep clamd
tcp        0      0 0.0.0.0:3310            0.0.0.0:*
LISTEN      21327/clamd
```

- test dengan telnet untuk melihat respon daemon

```
root@mizuno root# telnet 127.0.0.1 3310
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
PING <== coba dengan PING (capital)
PONG
Connection closed by foreign host.
```

daemon sukses, ubah kembali menjadi mode local socket.

```
#LocalSocket /tmp/clamd menjadi LocalSocket /var/amavis/clamd
TCPSocket 3310          menjadi #TCPSocket 3310
```

- Ubah hak akses /etc/freshclam.conf dari semula dari 644 menjadi 700
  #chmod 700 /etc/freshclam.conf
- Tambahkan parameter ini pada freshclam.conf
- Lepaskan tanda # dari baris Example
  Example
- Tambahkan baris berikut pada Proxy settings. Lepaskan tanda # dari baris dibawah.
  HTTPProxyServer proxy.eepis-its.edu
  HTTPProxyPort 3128
  HTTPProxyUsername <namaemail>@eepis-its.edu
  HTTPProxyPassword r <passwordmail>
- update database virus clamav dengan tool freshclam, terlebih dahulu buatkan file tujuan log.

```
root@mizuno clamav-0.80# touch /var/log/clam-update.log
root@mizuno clamav-0.80# chmod 600 /var/log/clam-update.log
root@mizuno clamav-0.80# chown clamav /var/log/clam-update.log
```

- bila anda sedang terkoneksi dengan internet, **update sekarang juga !**

update realtime

```
root@mizuno clamav-0.80# /usr/bin/freshclam -l /var/log/clam-
update.log
```

update dapat dijalan secara terjadwal dengan diletakkan di crond atau langsung dari tool freshclam

update dengan daemon freshclam

```
root@mizuno clamav-0.80# freshclam -d -c 2 -l /var/log/clam-
update.log
```

silakan baca petunjuk penggunaan opsi-opsi freshclam pada manual freshclam. atau pada crond cek tiap 30 menit

update dengan crond

```
*/30 * * * * su - clamav -s /bin/bash -c
'/usr/local/bin/freshclam --quiet -l /var/log/clam-update.log'
```

- Pada saat ini aplikasi **clamSMTP** belum perlu dijalankan, masih perlu mengedit konfigurasi postfix dan mencoba **clamSMTP** pada mode debug
- Sekarang edit file main.cf postfix untuk membelok-kan aliran menuju **clamSMTP**.

```
root@opera root# vi /etc/postfix/main.cf
```

pada baris terakhir tambahkan

```
content_filter = scan:127.0.0.1:10025
receive_override_options = no_address_mappings
```

- Edit file master.cf, lalu restart postfix

```
root@opera clamsmtp-1.0# vi /etc/postfix/master.cf
```

Pada baris paling bawah, tambahkan

```
scan      unix  -       -       n       -     16      smtp
        -o smtp_send_xforward_command=yes

127.0.0.1:10026 inet  n -       n       -     16      smtpd
        -o content_filter=
        -o
receive_override_options=no_unknown_recipient_checks,no_header_bo
dy_checks
        -o smtpd_helo_restrictions=
        -o smtpd_client_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o mynetworks_style=host
        -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

Dan reload/restart ulang postfix untuk membaca perubahan

```
root@opera clamsmtp-1.0# service postfix restart
```

- Sebelum aliran dari postfix (file main.cf) dibelokkan menuju clamSMTP, dicoba dahulu dengan debug. Jalankan perintah dari konsole 1.

```
root@opera clamsmtp-1.0# /usr/sbin/clamsmtpd -d 4
clamsmtpd: read config file: /etc/clamsmtpd.conf
clamsmtpd: parsed option: OutAddress: 10026
clamsmtpd: parsed option: ClamAddress: /var/clamav/clamd
clamsmtpd: parsed option: ScanHeader: X-AV-Checked: ClamAV using
ClamSMTP
clamsmtpd: parsed option: TempDirectory: /tmp
clamsmtpd: parsed option: Quarantine: on
clamsmtpd: parsed option: User: clamav
clamsmtpd: starting up...
clamsmtpd: switched to user clamav (uid 503, gid 500)
clamsmtpd: created socket: 10025
clamsmtpd: accepting connections
```

- Buka **konsole baru** dan jalankan netstat dari konsole baru tersebut (konsole 2). Pastikan port 10025 dan 10026 terbuka dan siap menerima request

```
root@opera clamsmtp-1.0# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
State
tcp        0      0 0.0.0.0:10025           0.0.0.0:*
LISTEN
tcp        0      0 127.0.0.1:10026         0.0.0.0:*
LISTEN
tcp        0      0 0.0.0.0:110             0.0.0.0:*
LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*
LISTEN
```

- Dari konsole 2, coba lakukan perintah telnet dan lihat progress-nya di konsole satu.

```
root@opera root# telnet 127.0.0.1 10025
Trying 127.0.0.1...
```

```
Connected to 127.0.0.1.
Escape character is '^]'.
220 smtp.passthru
quit
221 Bye
Connection closed by foreign host.
```

Hasil di konsole 1

```
clamsmtpd: 100000: processing 4 on thread 4002
clamsmtpd: 100000: accepted connection from: 127.0.0.1
clamsmtpd: 100000: SERVER connected to: 127.0.0.1:10026
clamsmtpd: 100000: SERVER < 220 opera.clamsmtp.com ESMTP Postfix
clamsmtpd: 100000: intercepting initial response
clamsmtpd: 100000: CLIENT > 220 smtp.passthru
clamsmtpd: created thread for connection
clamsmtpd: 100000: CLIENT < quit
clamsmtpd: 100000: SERVER > quit
clamsmtpd: 100000: SERVER < 221 Bye
clamsmtpd: 100000: CLIENT > 221 Bye
clamsmtpd: 100000: CLIENT connection closed
clamsmtpd: 100000: SERVER connection closed
```

- Bila percobaan menunjukkan hasil yang sama, bisa diasumsikan bahwa **clamSMTP** berfungsi baik
- Matikan **clamSMTP** mode debug yang ada dikonsole 1 (dengan ^c).

  Agar service **clamSMTP** dapat langsung berfungsi pada saat server boot/restart maka perlu script.

  Cara yang paling mudah dengan menulikan ke dalam file rc.local

```
root@opera clamsmtp-1.0# echo "/usr/sbin/clamsmtpd" >>
/etc/rc.local
```

  Atau, bila ingin service dikenali di sistem init linux (sehingga pada saat booting terlihat progress-nya), silakan ambil file init script di [situs] clamSMTP. Untuk sementara hanya ada untuk versi RedHat/Fedora dan Mandrake. Karena **TSL 2.0** dibangun berdasarkan script RH 7.2 maka yang dipilih init script RedHat/Fedora.

```
root@opera clamsmtp-1.0# wget
http://memberwebs.com/nielsen/software/clamsmtp/contrib/clamsmtpd

root@opera clamsmtp-1.0# mv clamsmtpd /etc/init.d/clamsmtpd
root@opera clamsmtp-1.0# chmod 755 /etc/init.d/clamsmtpd

root@opera clamsmtp-1.0# vi /etc/init.d/clamsmtpd
```

  Edit file init clamSMTP dan pastikan letak direktori dan file-file yang diperlukan sudah sesuai.

  Setelah itu daftarkan kedalam sistem init dan service siap digunakan.

```
root@opera root# chkconfig --add clamsmtpd
root@opera root# chkconfig --list clamsmtpd
clamsmtpd       0:off   1:off   2:off   3:off   4:off   5:off
6:off
root@opera root# chkconfig clamsmtpd on
root@opera root# chkconfig --list clamsmtpd
clamsmtpd       0:off   1:off   2:on    3:on    4:on    5:on
6:off
```

Service clamsmtpd siap dijalankan pada saat sistem booting pada runlevel 2, 3, 4 dan 5.

Dan jalankan sekarang.

```
root@opera root# service clamsmtpd start
Starting ClamSmtpd:                                        [  OK
]
```

- Coba dengan email biasa (tanpa virus), dan lihat output log dari postfix.

```
root@opera root# tail -f /var/log/messages
Oct 27 14:16:09 opera postfix/smtpd[18496]: connect from
adi.clamsmtp.com[192.168.1.250]
Oct 27 14:16:09 opera postfix/smtpd[18496]: 161452FA5:
client=adi.clamsmtp.com[192.168.1.250]
Oct 27 14:16:09 opera postfix/cleanup[18497]: 161452FA5: message-
id=<00a801c4bbec$3d9a87f0$fa01a8c0@redkurawa>
Oct 27 14:16:09 opera postfix/qmgr[18459]: 161452FA5: from=,
size=621, nrcpt=1 (queue active)
Oct 27 14:16:09 opera postfix/smtpd[18496]: disconnect from
adi.clamsmtp.com[192.168.1.250]
Oct 27 14:16:09 opera clamsmtpd: 100004: accepted connection
from: 127.0.0.1
Oct 27 14:16:09 opera postfix/smtpd[18500]: connect from
localhost.localdomain[127.0.0.1]
Oct 27 14:16:09 opera postfix/smtpd[18500]: 3E2942FB3:
client=localhost.localdomain[127.0.0.1]
Oct 27 14:16:09 opera clamd[18501]: /tmp/clamsmtpd.XZt2T0: OK
Oct 27 14:16:09 opera postfix/cleanup[18497]: 3E2942FB3: message-
id=<00a801c4bbec$3d9a87f0$fa01a8c0@redkurawa>
Oct 27 14:16:09 opera postfix/qmgr[18459]: 3E2942FB3:
from=<adi@inixindo.co.id>, size=852, nrcpt=1 (queue active)
Oct 27 14:16:09 opera clamsmtpd: 100004: from=adi@clamsmtp.co.id,
to=anik@clamsmtp.com, status=CLEAN
Oct 27 14:16:09 opera postfix/smtp[18498]: 161452FA5: to=,
relay=127.0.0.1[127.0.0.1], delay=0, status=sent
(250 Ok: queued as 3E2942FB3)
Oct 27 14:16:09 opera postfix/smtpd[18500]: disconnect from
localhost.localdomain[127.0.0.1]
Oct 27 14:16:09 opera postfix/local[18502]: 3E2942FB3: to=,
relay=local, delay=0, status=sent ("|/usr/bin/
procmail")
```

Sedangkan bila e-mail bervirus.

```
....
[root@fitri ~]# tail /var/log/maillog

Nov 30 18:42:25 fitri clamsmtpd: 100008: quarantined virus file
as: /tmp//virus.cllAfF

Nov 30 18:42:25 fitri clamsmtpd: 100008: from=fitri@kijang.com,
to=userbaru@mail.kijang.com, status=VIRUS:ClamAV-Test-File

Nov 30 18:42:25 fitri postfix/smtp[14386]: 364652688E3:
to=<userbaru@mail.kijang.com>, orig_to=<userbaru>,
relay=127.0.0.1[127.0.0.1]:10025, delay=12405,
delays=12405/0.01/0.06/0.02, dsn=2.0.0, status=sent (250 Virus
Detected; Discarded Email)

Nov 30 18:42:25 fitri postfix/qmgr[13387]: 364652688E3: removed
```

```
Nov 30 18:42:25 fitri postfix/smtpd[14388]: disconnect from
localhost.localdomain[127.0.0.1]

Nov 30 18:43:01 fitri dovecot: pop3-login: Login:
user=<userkanan>, method=PLAIN, rip=::ffff:10.252.102.56,
lip=::ffff:10.252.102.56, secured

Nov 30 18:43:01 fitri dovecot: POP3(userkanan): Disconnected:
Logged out top=0/0, retr=0/0, del=0/0, size=0

Nov 30 18:43:01 fitri postfix/smtpd[14400]: connect from
ns.kijang.com[10.252.102.56]

Nov 30 18:43:01 fitri postfix/smtpd[14400]: warning: Illegal
address syntax from ns.kijang.com[10.252.102.56] in RCPT command:
<fitri@>

Nov 30 18:43:01 fitri postfix/smtpd[14400]: disconnect from
ns.kijang.com[10.252.102.56]
```

- **Virus Action**

  Virus action adalah fasilitas baru yang berguna untuk melakukan suatu pekerjaan bila terdeteksi adanya virus dalam email. Fasilitas ini mulai ada dari sejak versi 0.9. Contoh dari script virus action dapat diambil dari situs clamSMTP (file virus_action.sh), donlot file tersebut dan silakan edit beberapa bagian, hasilnya seperti contoh dibawah.

```
#!/bin/sh

# A sample script for virus actions. When testing make sure
# everything can run as the clamav (or relevant) user.

file="/home/users/clamav/virus.log"
dir="/home/users/clamav/quarantine/"

exec 1>>$file
exec 2>>$file

# Add some fun log lines to the log file

echo Sender  $SENDER
echo Recipients  $RECIPIENTS
echo Virus  $VIRUS
echo "-----------------------------------------------------------"

# Move the virus file to another directory
# This only works if Quarantine is enabled
if [ -n "$EMAIL" ]; then
        mv "$EMAIL" "$dir"
fi
```

  Selanjutnya edit file clamsmtp.conf, tambahkan, contoh disini file script diletak-kan di direktori /etc. Ubah akses mode-nya menjadi execute.

```
root@opera root# chown clamav.clamav virus_action.sh
root@opera root# chmod 700 virus_action.sh
```

Tambahkan opsi VirusAction di clamsmtp.conf.

```
VirusAction: /etc/virus_action.sh
```

Jangan lupa restart kembali service clamsmtpd.

```
root@opera root# service clamsmtpd restart
Stopping ClamSmtpd:                                        [  OK
]
Starting ClamSmtpd:                                        [  OK
]
```

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Web Application Security

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.

MODUL 11
WEB SERVER SECURITY

TUJUAN PEMBELAJARAN:

4. Mengenalkan pada mahasiswa tentang konsep Manajemen Log di linux
5. Mahasiswa memahami berbagai macam file log yang ada di linux
6. Mahasiswa mampu melakukan analisa terhadap file log yang ada di linux

DASAR TEORI

Saat ini *web* merupakan salah satu layanan informasi yang banyak diakses oleh pengguna internet di dunia. Sebagai salah satu layanan informasi maka perlu dibangun *web* yang mampu menangani permintaan *(request)* dari banyak pengguna dengan baik *(reliable)* tanpa meninggalkan aspek keamanannya. Masalah keamanan merupakan salah satu aspek yang penting dalam pembangunan *web* karena kelalaian dalam menangani keamanan *web* server dapat berakibat fatal.

Apache merupakan salah satu distribusi *web server* yang populer dengan dukungan *feature* yang sangat banyak. Perhitungan statistik yang ada saat ini menunjukkan bahwa *Apache* menjadi *web server* yang paling banyak digunakan dalam dunia internet, yaitu mencapai nilai 60 % dari seluruh web server yang ada.

Keberhasilan *Apache* mencapai kepopuleran saat ini selain dikarenakan memiliki banyak *feature* yang sering tidak dijumpai pada *web server* yang lain, juga dikarenakan *Apache* merupakan aplikasi gratis yang berjalan dalam berbagai sistem operasi.

Ada beberapa aspek yang perlu diterapkan dalam mengamankan *web server*, antara lain:

1. Layanan *web server* dengan *low previllages*
2. Pengaturan akses terhadap *web server*
3. Meminimalkan layanan publik pada mesin yang menjalankan *web server*
4. Menyediakan *filesystem* khusus untuk layanan web server

Layanan *web server* dengan *low previllages*

Pada sistem operasi berbasis UNIX semacam Linux, FreeBSD, OpenBSD setiap proses memiliki berbagai properti seperti nomor proses, pemilik proses, dan alokasi memori yang digunakan. *Apache web server* merupakan layanan publik, sehingga sangat dianjurkan proses-proses yang dijalankan oleh *Apache* dimiliki oleh user dengan hak akses terhadap sistem yang ada serendah mungkin *(low previllages)*. Idealnya perlu dibuat user yang khusus menjalankan *web server*, misal user dengan nama *www*.

Dari perintah Linux di atas tampak bahwa *home* direktori dari *user* **www** adalah '/' yang secara *default* tidak dimiliki oleh *user* **www** melainkan dimiliki oleh **root** sehingga *user* **www** tidak memiliki akses tulis terhadap *home* direktorinya sendiri dan *shell* yang dimiliki oleh *user* **www** adalah '**/bin/true**' sehingga secara otomatis *user* **www** tidak dapat menggunakan fasilitas-fasilitas semacam **telnet, rlogin, rsh.**

Langkah selanjutnya adalah melakukan setting pada *Apache web server*sehingga *web server* akan dijalankan oleh *user* **www** yang baru saja dibuat. File konfigurasi utama yang digunakan *Apache* adalah file **httpd.conf.** Pada file tersebut ditambahkan line semacam ini :

Pengaturan akses terhadap *web server*

Pengaturan akses pada *Apache web server* dapat dibedakan menjadi 2 macam :

• Pengaturan akses berdasarkan alamat IP dari *client*

• Pengaturan akses dengan proses autentikasi pengguna

Pengaturan akses berdasarkan *IP Address client*

Model pengaturan akses *web server* yang diterapkan disini didasarkan pada informasi *IP address* dari pengguna. Aturan dapat dibuat sehingga untuk file atau direktori tertentu akses dari *IP address* pengguna diterima atau ditolak. Untuk menerapkan aturan ini perlu dilakukan perubahan pada file konfigurasi *Apache* yaitu **httpd.conf.** Ada 3 kata kunci yang berkaitan dengan pengaturan ini yaitu **Order, Deny,** dan **Allow.** Kata kunci **Order** dapat diikuti oleh **deny, allow** atau **allow, deny** yang menunjukkan urutan evaluasi pengaturan berdasarkan aturan **Deny** dan aturan **Allow.** Kata kunci **Allow** maupun **Deny** diikuti oleh kata kunci **from** dan :

• **all** : menunjukkan akses untuk semua *host* diperbolehkan **(Allow)**
atau ditolak **(Deny)**

• *IP address* : yaitu alamat IP yang diperbolehkan atau ditolak semisal :

• **167.205.25.6**

• **167.205.25.** (berarti berlaku untuk alamat IP **167.205.25.0 – 167.205.25.255**) atau **167.205.** atau **167.**

• **167.205.25.0/27** (berlaku untuk **167.205.25.0-167.205.25.31**)

• **167.205.0.0/255.255.0.0** (berlaku untuk **167.205.0.0-167.205.255.255)**

Misalkan anda ingin menolak akses ke direktori **/home/httpd/html** dari pengguna dengan alamat **167.205.*.*** dan *host* dengan domain **.hacker.org** maka pada file **httpd.conf** ditambahkan line semacam ini :

Pengaturan akses *Apache* dapat dilakukan pula dengan membuat aturan-aturan pada file **.htaccess** pada direktori yang bersangkutan baik untuk mengatur akses terhadap file maupun akses terhadap direktori dimana file ini berada.

Pengaturan akses dengan proses autentikasi pengguna

Model pengaturan akses dengan proses autentikasi pengguna lebih fleksibel dibandingkan dengan pengaturan akses berdasarkan *IP address* pengguna.

Ketika anda mencoba untuk mengakses suatu *resources* yang dilindungi oleh model autentikasi user semacam ini maka anda harus memasukan informasi login dan password yang sesuai dalam suatu form semacam ini :

Untuk mengimplementasikan mekanisme autentikasi ini perlu dilakukan perubahan-perubahan pada file **httpd.conf** ataupun pada file **.htaccess** yang diletakkan pada direktori yang bersangkutan. Informasi data login dibuat dengan menggunakan program **htpasswd**

Meminimalkan layanan publik pada mesin yang menjalankan web server

Pada umumnya mesin-mesin komputer yang terhubung dengan internet melayani beberapa program layanan sekaligus. Ada beberapa alasan yang mendasari hal tersebut antara lain :

• Keterbatasan alamat IP saat ini
• Keterbatasan sumber daya mesin komputer
• Keinginan memaksimalkan sumber daya komputer dengan menjalankan

TUGAS PENDAHULUAN

1. Sebutkan dan jelaskan dengan singkat apa kegunaan dari htaccess?
2. Sebutkan pula kegunaan dari SSL pada HTTP

PERCOBAAN

1. Instal HTTP

   Pastikan package develoment tools spt gcc sudah terinstall pada sistem anda

   Konfigurasi apache yang akan kita install

   - Menggunakan suEXEC untuk menjalankan web application
   - Menggunakan php untuk web application

   Login sebagai root dan masukkan password root (setiap komputer bisa berbeda-beda)

   Persiapan

   - Untuk keamanan sistem, instal program web server pada user tersendiri misal user apache
   - Untuk itu buatlah user apache sebagai user biasa yang sementara untuk installasi mempunyai hak bisa menulis di terminal, siapkan juga direktori untuk installasi webserver misal di /opt/apache

     [root@localhost conf]# /usr/sbin/useradd -s /bin/true -d /opt/apache apache
   - Siapkan source apache, bisa download.
   - Lakukan langkah installasi (dalam practice kali ini memakai tar.gz)

     Extract source httpd

     [apache@localhost src]$ tar xzf httpd-2.0.48.tar.gz

     masuk ke deirektori httpd hasil extract, mulai melaksanakan installasi

     [apache@localhost src]$ cd httpd-2.0.48
     [apache@localhost httpd-2.0.48]$ ./configure -prefix=/opt/apache -enable-suexec -with-suexec-caller=apache -enable-info
     [apache@localhost httpd-2.0.48]$ make
     [root@localhost httpd-2.0.48]# make install

     Konfigurasi file httpd.conf spt pada contoh :

     berikan tempat file berada kepada user apache

     [root@localhost httpd-2.0.48]# chown -R apache.apache /opt/apache/htdocs

     Siapkan source PHP, install php menggunakan apache,

     [root@localhost src]# tar xjf php-4.3.4.tar.bz2

[root@localhost php-4.3.4]# ./configure -prefix=/opt/php -enable-discard-path -enable-ftp
[root@localhost php-4.3.4]# make
[root@localhost php-4.3.4]# make install

Copy php.ini

[root@localhost php-4.3.4]# cp php.ini-recommended /opt/php/lib/php.ini

buat file php di /opt/apache/htdocs

[root@localhost zone]# vi /opt/apache/htdocs/phpinfo.php

dengan isi sbb :

```
#!/opt/php/bin/php
<? phpinfo() ?>
```

start browser untuk memastikan php sudah jalan http://10.252.20.225/phpinfo.php

Jika beres akan keluar spt diatas, jika tidak kembali lakukan installasi kemungkinan suexec yang belum beres.

2. Instal SSL
   1. Masuk ke user apache
      [root@redhat root]# su -l apache
   2. Masuk ke home direktori apache
      [apache@redhat httpd]$ cd
   3. Buat direktori certs
      [apache@redhat httpd]$ mkdir certs
   4. lakukan langkah berikut :
      [apache@redhat httpd]$ cd certs/
      [apache@redhat certs]$ mkdir -p demoCA

[apache@redhat certs]$ touch demoCA/index.txt
[apache@redhat certs]$ echo 01 > demoCA/serial
[apache@redhat certs]$ openssl genrsa -des3 -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)

5. Masukkan password SSL min 4 karakter
   Enter pass phrase for ca.key:
   Verifying - Enter pass phrase for ca.key:

6. Buat Sertifikat
   [apache@redhat certs]$ openssl genrsa -des3 -out ca.key 1024
   Generating RSA private key, 1024 bit long modulus
   .....++++++
   .....++++++
   e is 65537 (0x10001)
7. Masukkan Password yang tadi kita masukkan
   Enter pass phrase for ca.key:
   Verifying - Enter pass phrase for ca.key:
   [apache@redhat certs]$ openssl req -new -x509 -key ca.key -out ca.crt
   Enter pass phrase for ca.key:
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
8. Masukkan data sbb :
   Country Name (2 letter code) [GB]:ID
   State or Province Name (full name) [Berkshire]:East Java
   Locality Name (eg, city) [Newbury]:Surabaya
   Organization Name (eg, company) [My Company Ltd]:EEPIS
   Organizational Unit Name (eg, section) []:IT
   Common Name (eg, your name or your server's hostname) []:isbat
   Email Address []:isbat@eepis-its.edu
9. Buat sertifikat
   [apache@redhat certs]$ cd ~/certs
   [apache@redhat certs]$ openssl genrsa -des3 -out aksi.co.id.key 1024
   Generating RSA private key, 1024 bit long modulus
   .....++++++
   .....++++++
   e is 65537 (0x10001)
   Enter pass phrase for aksi.co.id.key:
   Verifying - Enter pass phrase for aksi.co.id.key:
10. copy original

```
[apache@redhat certs]$ cp aksi.co.id.key aksi.co.id.key.original
[apache@redhat certs]$ openssl rsa -in aksi.co.id.key.original -out aksi.co.id.key
Enter pass phrase for aksi.co.id.key.original:
writing RSA key
```

11. jalankan open ssl

```
[apache@redhat certs]$ openssl req -new -key aksi.co.id.key -out aksi.co.id.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:ID
State or Province Name (full name) [Berkshire]:East Java
Locality Name (eg, city) [Newbury]:Surabaya
Organization Name (eg, company) [My Company Ltd]:EEPIS
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:Isbat
Email Address []:isbat@eepis-its.edu

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:redhat
An optional company name []:eepis
```

12. buat sertificate

```
[apache@redhat certs]$ openssl ca -in aksi.co.id.csr -out aksi.co.id.crt -keyfile
ca.key -cert ca.crt -outdir ./ -policy policy_anything
Using configuration from /usr/share/ssl/openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Nov 20 22:16:22 2006 GMT
            Not After : Nov 20 22:16:22 2007 GMT
        Subject:
            countryName               = ID
            stateOrProvinceName       = East Java
            localityName              = Surabaya
            organizationName          = EEPIS
            organizationalUnitName    = IT
            commonName                = Isbat
            emailAddress              = isbat@eepis-its.edu
```

X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
51:F5:B8:9A:FF:45:6F:2C:F9:D0:8D:37:EC:8B:88:13:B2:81:64:A9
X509v3 Authority Key Identifier:

keyid:F3:07:C2:DE:6A:36:28:D1:BE:30:37:1B:04:1F:76:5D:02:D4:9C:EB
DirName:/C=ID/ST=East Java/L=Surabaya/O=EEPIS/OU=IT/CN=isbat/emailAddress=isbat@eepis-its.edu
serial:00

Certificate is to be certified until Nov 20 22:16:22 2007 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

13. Buat direktori untuki certificate
[apache@redhat certs]$ mkdir /opt/httpd/certs/
mkdir: cannot create directory `/opt/httpd/certs/': File exists
[apache@redhat certs]$ cp aksi.co.id.crt aksi.co.id.key /opt/httpd/certs/
cp: `aksi.co.id.crt' and `/opt/httpd/certs/aksi.co.id.crt' are the same file
cp: `aksi.co.id.key' and `/opt/httpd/certs/aksi.co.id.key' are the same file
[apache@redhat certs]$ chown -R apache.apache /opt/httpd/certs/
[apache@redhat certs]$ chmod 600 /opt/httpd/certs/*

14. Buat file konfigurasi ssl
[apache@redhat conf]$ vim ssl.conf

15. Restart apache dan buka browser menggunakna https
[root@redhat root]# /opt/httpd/bin/apachectl restart

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Web Server Security

Dasar Teori :

Tugas Pendahuluan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Keamanan Data

Dasar Teori :

Desain Jaringan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Sebutkan beberapa jenis enkrip

MODUL 12
FINAL PROJECT

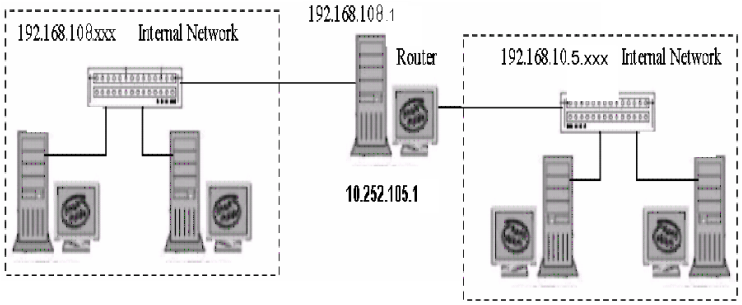
TUJUAN PEMBELAJARAN:

1. Memahami konsep security secara menyeluruh dan mengimplementasikan dalam desain jaringan yang disiapkan

DESAIN JARINGAN

PROJECT

1. Buatlah berkelompok dan bekerjasamalah dengan teman anda. Bagi tugas
2. Lakukan konfigurasi sesuai dengan desain yang sudah disiapkan pada bagian desain jaringan



3. Siapkan dua komputer pada jaringan 192.168.108.xxx, lakukan installasi mail beserta anti spam dan anti virus serta install ssh pada salah satu komputer, pada komputer yang lain instal apache dan ssl serta ssh.
4.
5. Pada komputer router install pula iptables, pada jaringan 192.168.105.xxx buat beberapa ip yang hanya bisa akses mail, web dan ssh. Juga buat rule ada yang bisa mengakses semua service dan buat rule salah satu IP tidak bisa akses sama sekali
6. Pada 192.168.108.xxx konfigurasi tcp wrapper mana yang boleh akses dan mana yang tidak.
7. Pada 192.168.108.xxx lakukan penutupan aplikasi yang bisa diakses kecuali web, mail dan ssh
8. Jika sudah selesai konfirmasikan hasil pekerjaan anda ke dosen/asisten praktikum.
9. Tulis semua langkah yang dikerjakan, rangkum semua menjadi satu laporan

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Final Project

Dasar Teori :

Desain Jaringan :

Hasil percobaan :

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Menurut anda security apa saja yang diperlukan bagi server internet?
3. Dan menurut anda security apa saja yang diperlukan untuk server local ?

DAFTAR PUSTAKA

[1] Joel Sklar, Principles of Web Design, Thonson Learning.

[2] http://fcit.usf.edu/network/

[3] CD Bonus: Video Info Komputer, September 2002

[4] http://www.IlmuKomputer.com

[5] http://artikel.WebGaul.com/Komputer/

[6] Raymond McLeod, Jr., George Schell, Arthur I. Stonehill, Michael H.Moffett, *Management Information System*, 8nd edition, Prentice Hall, 2001

[7] Budi Sutedjo Dharma Oetomo, S.Kom., M.M., *Perencanaan dan Pembangunan Sistem Informasi*, Andi Yogyakarta, 2002

[8] Peter Norton, *Peter Norton's Introduction To Computers Fifth Edition Student Edition*, 5th Edition, McGraw Hill Technology Education, 2002

[9] Peter Norton, *Computing Fundamentals Fifth Edition International Edition*, 5th edition , McGraw Hill Technology Education, 2003