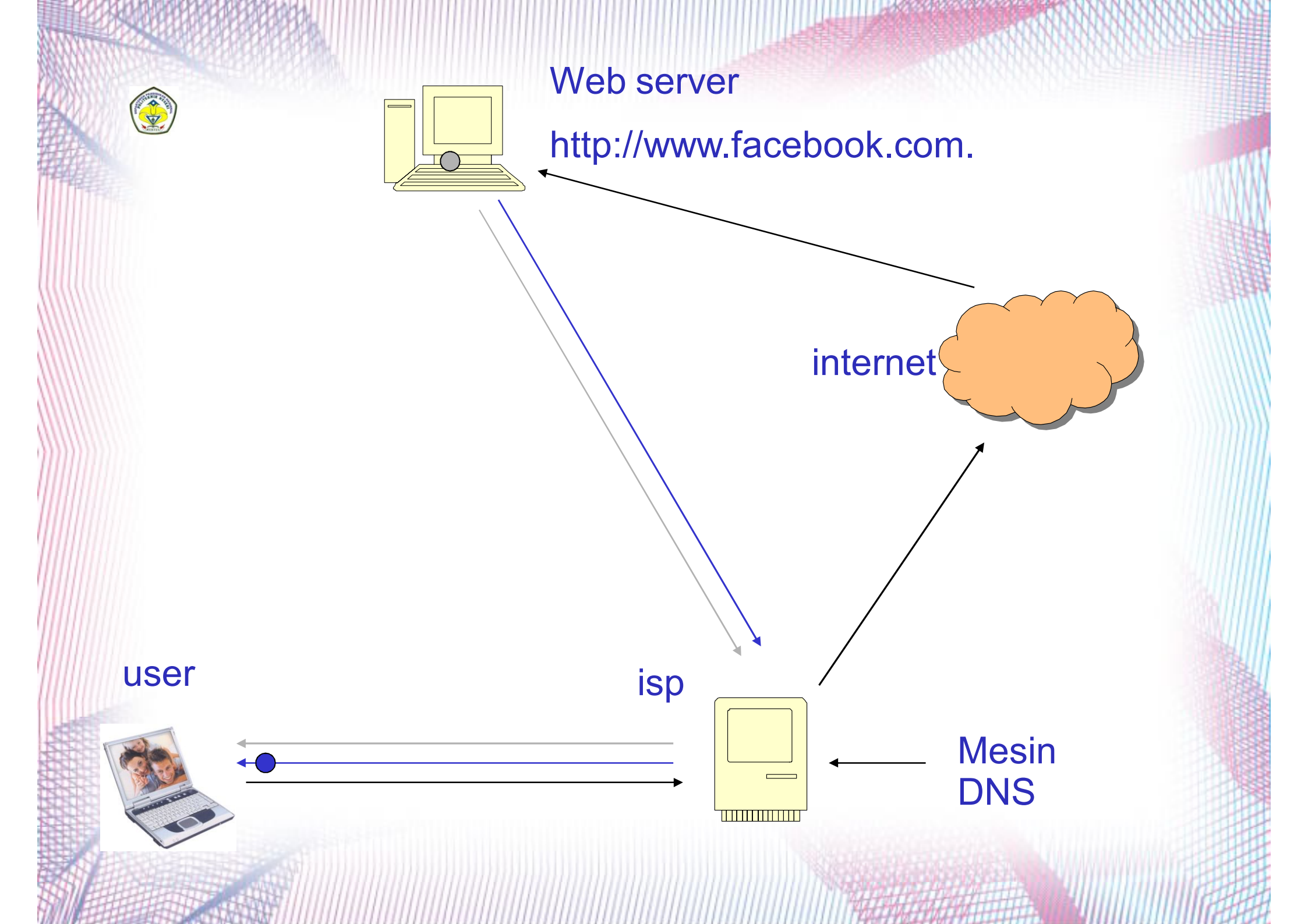
Antonius P.G Manginsela
antonpgm@gmail.com, antonpgm@polimdo.ac.id

Administrasi & Keamanan Jaringan Komputer

Layanan Jaringan Komputer

Modul No.3

- Pengenalan layanan jaringan
- Layanan jaringan fundamental


Web server
http://www.facebook.com.
internet
user
isp
Mesin
DNS

Pemeriksaan keamanan dan Pencegahan.

1. Memeriksa daemon apa saja yang berjalan sebagai default, kita dapat menggunakan netstat untuk hal tersebut.
   - *# netstat -a*
   - Active Internet connections (servers and established)

     Proto Recv-Q Send-Q Local Address Foreign Address State
     tcp 0 0 *:ftp *:* LISTEN
     tcp 0 0 *:ssh *:* LISTEN
     tcp 0 0 *:telnet *:* LISTEN
     tcp 0 0 *:smtp *:* LISTEN
     tcp 0 0 *:finger *:* LISTEN
     tcp 0 0 *:www-http *:* LISTEN
     tcp 0 0 *:pop3 *:* LISTEN
     tcp 0 0 *:shell *:* LISTEN
     raw 0 0 *:icmp *:* 7
     raw 0 0 *:tcp *:* 7
     #

Pemeriksaan keamanan dan Pencegahan.

Segera matikan daemon finger dan shell yang berjalan seperti :

- *Daemon Finger memberikan info kepada siapa saja yang memintanya, walaupun tidak cukup banyak, tetapi memberikan username yang sah yang memungkinkan usaha brute force, maupun usaha sosial engineering.*
- *Daemon Shell, adalah sesuatu yang disebut sebagai service r* , karakteristiknya adalah semua service dalam kategori ini tidak membutuhkan authentikasi. Semuanya didasarkan kepada trusted host. Jika anda tetap ingin menjalankannya, pastikan anda mengaktifkan identifikasi kerberos.*
- *service r* yang berjalan tanpa kerberos atau metode authentikasi lainnya:*
- *Ada suatu file (.rhosts) yang mana akan memberikan trusted IPs yang mana login dilakukan dari salah satu ip yang ada dalam file, akan mendapat akses ke sistem. Suatu serangan dengan menggunakan IP Spoffing dapat memanipulasi ip, dan anda akan mendapat masalah dengan sistem anda.*

Pemeriksaan keamanan dan Pencegahan

- Membuka/menutup port dengan mengedit file /etc/inetd.conf. Jika service yang ingin anda tutup tidak terdaftar disana, periksa pada script init yang dapat ditemukan pada direktori /etc/rc.d atau /etc/init.d tergantung pada distribusi yang anda gunakan.
- Cari informasi berkala atau berlangganan mailing list BugTraq di (http://www.securityfocus.com)

Web Server

- Web server merupakan servis yang memuat informasi web, sehingga dapat diakses melalui jaringan internet.
- Proses pengaksesan informasi dari web server dilakukan dengan menggunakan web browser.
  - Internet Explorer, Mozilla Firefox,Google Chrome
  - Safari,Opera,Maxthon,Dll.
- Permintaan informasi dari web server oleh web browser tidak langsung mendapatkan informasi segera. Namun perlu konfirmasi dari pihak web server kepada web browser tentang valid tidaknya permintaan. Jika permintaan valid, maka web server akan mengirim paket informasi kepada web browser sesuai yang diminta.

Web Server

- Proses pengiriman permintaan atau informasi dari atau ke web browser melalui berbagai cara.
  - Secara langsung (Direct Access) melalui gateway atau routing
  - Filtering (Proxy/ firewall)
- Jenis-jenis web server berdasarkan namanya.
  - Apache
  - Apache Tomcat
  - Personal Web Server (PWS)
  - Internet Information Server (IIS)
  - Dll.
- Jenis-jenis web server berdasarkan prinsip kerjanya
  - Standalone
  - Inetd

Langkah-langkah pengamanan Server

1. ***Shell Provider*** :
   - Jangan memperbolehkan root untuk login secara remote
   - Buang, atau paling tidak ganti password untuk account default.
   - Jangan memperbolehkan pemakai ftp anonymous untuk login, demikian juga untuk root, dan user berkemampuan tinggi lainnya untuk login dengan ftp, bin, daemon, dan pseudo user lainnya dari root.
   - Periksa semua file dengan SUID bit, dan periksa halaman manual mereka, jika dikatakan mereka dapat dijalankan tanpa SUID bit hilangkan saja. File seperti at, mount, umount selalu tanpa SUID bit. Jika pada sistem anda ada, hilangkan saja
   - Chroot() user pada home masing-masing ketika login dengan ftp.
   - Gunakan password shadow
   - Hapus **su** dari sistem anda dan gunakan **sudo** sebagai pengantinya, jika anda benar-benar ingin anda atau hanya anda saja sebagai **sysadmin** buang saja keduanya.

Langkah-langkah pengamanan Web Server

- Lakukan upgrade dan patch hole secara berkala.
- Tidak memperbolehkan **upload ke direktori** jika **web server** dengan daemon ftp.INGAT **chroot()** ftp dan **chroot() http** PADA DIREKTORI YANG BERBEDA, mereka tidak dapat mengakses satu sama yanglain. Kecuali scripts dapat mengupload ke root pada server anda.
- Jika mengunakan script CGI **periksa bahwa script CGI** tersebut tidak memiliki kelemahan, jika ada hapus saja.
- Jika menggunakan suatu *world writable ftp directory* seperti */incoming* periksalah secara *berkala, misalnya setiap 3 hari*, atau *setiap minggu*, jangan *lebih dari 1 minggu*, setelah periode tersebut hapuslah segala sesuatu yang berada didalam direktori tersebut.

Langkah-langkah pengamanan Web Serv

- Jangan menjalankan *daemon http sebagai root*, mungkin anda berkata bahwa port lebih rendah dari 1023 (yang standar) harus berjalan sebagai root, ya benar mereka harus di jalankan sebagai root, tetapi mereka dapat diturunkan permissionnya seperti pada *Apache*. Gunakan suatu *user khusus untuk httpd*, tentukan */bin/false* dan *shell dari user* dan tempatkan namanya dalam file */etc/ftpusers*.
- Jika anda ingin memiliki suatu web server, anda perlu *membiarkan daemon www-httpd daemon dan ftp. Atau lebih baik anda memiliki akses langsung ke web server sehingga daemon ftp-nya dapat* ditutup, dan *upload dilakukan secara lokal.*

Mail Server

- Mail Server juga disebut sebagai Mail Transfer Agent (MTA). Tugas dari mail server dapat diasosiasikan layaknya kantor pos. Mail server menerima email-email yang akan dikirim ketujuan dimasukkan ke dalam antrian server disebut queue. Alamat tujuan pengiriman email dapat diasosisikan layaknya PO BOX. Alamat email berada pada sebuah MTA yang dimudahkan dengan nama account kemudian diikuti dengan nama domain (mis. antonpqm@gmail.com) .
- Jenis-jenis MTA:
  - Qmail
  - Postfix
  - MDaemon
  - Exim
  - Dll

Mail Server

- Penggunaan email untuk menerima/membaca dan mengirim email dapat digunakan MUA (Mail User Agent). MUA dapat dikelompokkan:
  - Web Mail:
    - SquirrelMal
    - NeoMail
    - Horde/Imp
    - Basillix
    - NOCC
    - Dll.
  - Mail Client:
    - Microsoft Outlook
    - Mozilla Thunderbird
    - Opera Masil
    - Ximian Evolution
    - KMail
    - Dll.

Mailing List Server

- Server Mailing List memiliki proses kerja mirip sebuah forum diskusi. Server ini dapat memuat banyak forum yang biasa disebut sebagai group. Masing-masing group memiliki seorang atau lebih moderator untuk mengatur proses keanggotaan dan diskusi. Masing-masing group juga memiliki anggota diskusi yang proses pendafarannya harus menggunakan alamat email melalui subscribe ke group tersebut.
- Proses pengiriman masalah/argument ke dalam group disebut dengan posting. Setiap informasi yang diposting ke dalam group akann didistribusikan ke seluruh anggota dalam group, sehingga anggota lain bisa menanggapi informasi tersebut. Dengan demikian proses diskusi dapat interaktif melalui email.
- Jenis-jenis Mailing List Server
  - Ezmlm
  - Mailman, dll

Langkah-langkah pengamanan Mail Server

- Coba gunakan daemon **qmail** sebagai penganti sendmail.
- Periksa jika perintah **vrfy** dan **expn**, mungkin ada, jika tidak ada disable mereka.
- Pada POP3, jika mungkin, tentukan **lock account** jika suatu jangka waktu usaha login tetap gagal. Ingat untuk menggunakan mekanisme auto-unlock, misalnya setelah 30 menit account di lock. Jika tidak ada pilihan lain anda dapat senatiasa login ke account yang sedang di serang, dan tidak ada orang lain dapat melakukan login sampai anda logout (login pada pop3).

Pengaman Password.

- Gunakan algoritma pengacakan yang lebih baik. Algoritma MD5 menyediakan suatu password acak yang lebih baik dari pada yang normal
- Letakkan file password di tempat yang tidak diketahui user. (/etc/shadow)

Pengaman Password.

- Pluggable Authentication Modules : untuk menerapkan password shadow, yang perlu anda lakukan adalah konversi password dan group file serta mengubah PAM conf files (mudah bukan?). Link ke modul PAM:
  - .PAM cryptocard module http://www.jdimedia.nl/igmar/pam/
  - .PAM smartcard modulehttp://www.linuxnet.com/applications/applications.html
  - .PAM smb (samba) module http://rpmfind.net/linux/RPM/pam_smb.html
  - http://www.csn.ul.ie/~airlied/pam_smb/

Pengaman Password.

- Password cracking :
  - .John the Ripper, Ini tool password cracking yang paling terkenal, digunakan oleh semua pseudo hackers dan banyak black hats, karena mudah digunakan dan cepat. Homepage >> http://www.false.com/security/john/
  - .Crack tool Password cracking yang pertama yang benar-benar didefinsikan : http://www.users.dircon.co.uk/~crypto/

Terima Kasih