

MODUL 4

SNIFFING, SPOOFING DAN SESSION HIJACKING

SERTA COUNTERMEASURENYA

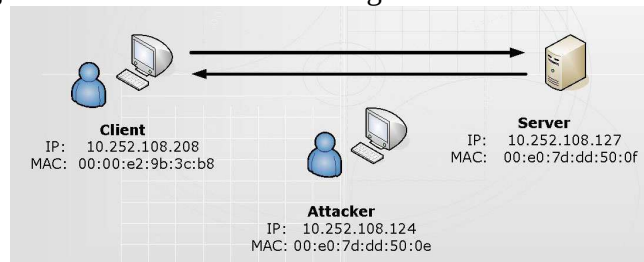
TUJUAN PEMBELAJARAN:

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

DASAR TEORI

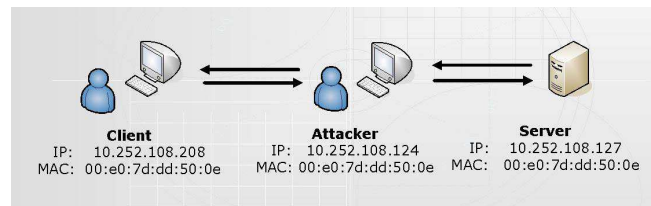
Sniffer adalah program yang membaca dan menganalisa setiap protokol yang melewati mesin di mana program tersebut diinstal. Secara default, sebuah komputer dalam jaringan (workstation) hanya mendengarkan dan merespon paket-paket yang dikirimkan kepada mereka. Namun demikian, kartu jaringan (network card) 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 attacker. Biasa disebut serangan spoofing. Attacker 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.

```

Stream Content
aalllicce
Password: alice06
Last login: Mon Jul 31 17:39:03 2006 from 10.252.108.208 on pts/2
Linux client 2.6.8-2-386 #1 Thu May 19 17:40:50 JST 2005 i686 GNU/Linux

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
alice@client:~$ ffiiinggeerr

Login      Name      Tty      Idle   Login Time   Office   Office Phone
alice      alice     *pts/2   Jul 31 17:52 (10.252.108.208)
root      root      *:0      Jul 31 17:02
root      root      pts/0    1 Jul 31 17:15 (:0.0)
root      root      pts/1    31 Jul 31 17:15 (:0.0)
alice@client:~$ wwhooaammi

alice
alice@client:~$ ssuu
Password: root
client:/home/alice# ffiiinggeerr

Login      Name      Tty      Idle   Login Time   Office   Office Phone
alice      alice     *pts/2   Jul 31 17:52 (10.252.108.208)
root      root      *:0      Jul 31 17:02
root      root      pts/0    2 Jul 31 17:15 (:0.0)
root      root      pts/1    31 Jul 31 17:15 (:0.0)
client:/home/alice# eexxiitt
  
```

Follow TCP Stream yang dijalankan attacker

Ada dua macam serangan spoofing yang terjadi :

1. ARP Spooofing,

ARP sppoofing yang bekerja dalam satu jaringan dan 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 merupakan serangan yang 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 *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

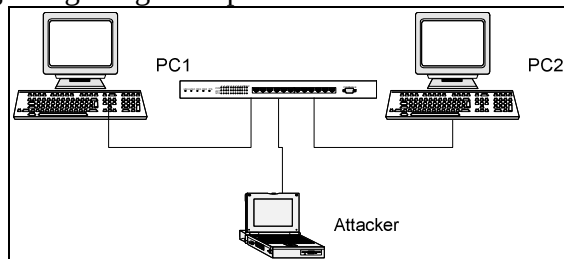
IP spoofing adalah membuat paket IP menggunakan *source IP address* orang lain. Orang yang melakukan serangan DoS (Denial Of Service) biasanya mengelabui target dengan menyamar/IP Headernya diganti dengan IP Header orang lain. Beberapa serangan yang biasa digunakan Ping Of Death, Syn Flood, Land Attack,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

TUGAS PENDAHULUAN

1. Dalam arp spoofing ada istilah yang disebut dengan arp cache poisoning, jelaskan dengan singkat apa itu arp cache poisoning !
2. Carilah command untuk melakukan bloking terhadap ip spoofing menggunakan iptables.

PERCOBAAN

1. Percobaan arp spoofing
 - a. Bangun topologi dengan tiga komputer sbb :

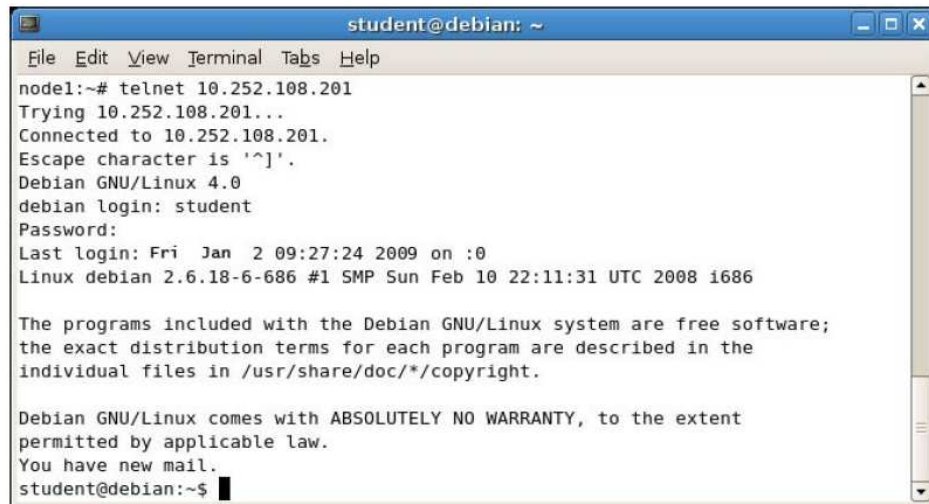


- b. Bekerjalah dengan teman sebelah untuk melakukan percobaan ini, setiap kelompok minimal 3 orang. Satu berfungsi sebagai penyerang,
- c. Install telnet, ftp dan ssh pada PC1,
 - Untuk install telnet lakukan apt-get install telnetd, pilih standalone

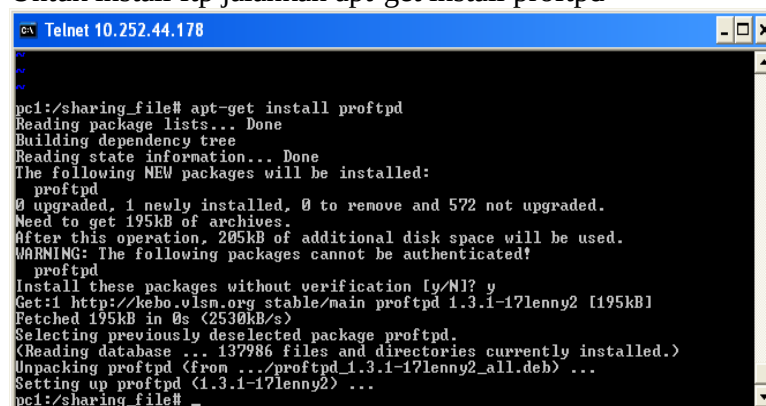
```
Terminal
File Edit View Terminal Tabs Help
debian:~# apt-get install telnetd
Reading package lists... Done
Building dependency tree... Done
The following NEW packages will be installed:
telnetd
0 upgraded, 1 newly installed, 0 to remove and 137 not upgraded.
Need to get 41.9kB of archives.
After unpacking 98.3kB of additional disk space will be used.
Get:1 http://kebo.vlsm.org etch/main telnetd 0.17-34 [41.9kB]
Fetched 41.9kB in 0s (253kB/s)
Selecting previously deselected package telnetd.
(Reading database ... 75890 files and directories currently installed.)
Unpacking telnetd (from .../telnetd_0.17-34_i386.deb) ...
Setting up telnetd (0.17-34) ...
debian:~#
```

Untuk mencoba telnet, buka terminal dan jalankan telnet localhost/no_ip_server_telnet, masukkan user dan password.

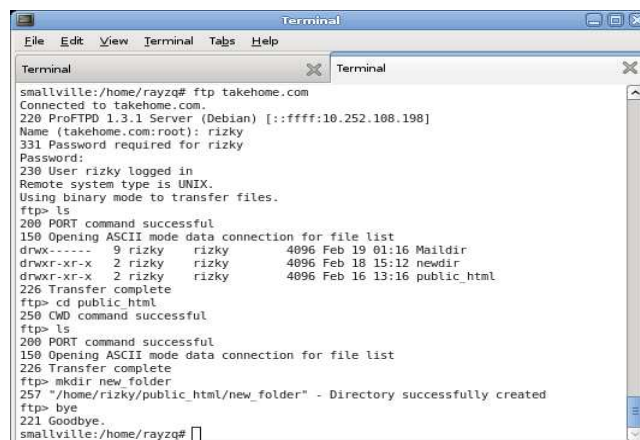
Untuk keluar ketikkan exit

A terminal window titled 'student@debian: ~' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The output shows a telnet session to 10.252.108.201. It displays the Debian GNU/Linux 4.0 login screen, including the login prompt, password prompt, last login time, and system version. It also shows the Debian GNU/Linux welcome message and the prompt 'student@debian:~\$'.

- Untuk install ftp jalankan apt-get install proftpd

A terminal window titled 'Telnet 10.252.44.178' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The output shows the command 'apt-get install proftpd' being executed. It displays the package list, dependency tree, and the installation of proftpd. It shows the disk space requirements and the installation progress, including the fetching of archives and the unpacking of the package. The prompt 'pci:/sharing_file#' is visible at the bottom.

Untuk menjalankan ftp jalankan ftp localhost/no_ip_pc1, masukkan user dan password

A terminal window titled 'Terminal' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The output shows an ftp session to localhost/no_ip_pc1. It displays the connection process, the user 'rizky' logging in, and the remote system type 'UNIX'. It shows the file list of the remote system, including 'Maildir', 'newdir', and 'public_html'. The user navigates to 'public_html' and creates a new folder named 'new_folder'. The session ends with a 'Goodbye' message. The prompt 'smallville:/home/rayzq#' is visible at the bottom.

- Untuk install ssh, jalankan apt-get install ssh

```

debian:/backup/student# apt-get install ssh
Reading package lists... Done
Building dependency tree... Done
The following extra packages will be installed:
  openssh-blacklist openssh-server
Suggested packages:
  ssh-askpass rssh molly-guard
The following NEW packages will be installed:
  openssh-blacklist openssh-server ssh
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 2347kB of archives.
After unpacking 4694kB of additional disk space will be used.
Do you want to continue [Y/n]? █

```

Untuk mencoba ssh, buka terminal dan jalankan ssh localhost/no_ip_server_telnet, masukkan user dan password. Untuk keluar ketikkan exit.

```

debian:/home/student# ssh student@10.252.108.65
Linux debian 2.6.18-6-686 #1 SMP Sat Dec 27 09:31:05 UTC 2008 i686

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Mon Dec 21 13:05:36 2009
student@debian:~$ █

```

Untuk mencoba secure ftp jalankan sftp localhost/ip_server_tujuan, masukkan user dan password.

- d. Dari komputer attacker, lakukan sbb :
 - Install dsniff dari komputer attacker, jalankan apt-get install dsniff.
 - Buka terminal baru Jalankan arpspoof -t IP_PC1 IP_PC2
 - Buka terminal baru jalankan arpspoof -t IP_PC2 IP_PC_1
 - Buka terminal baru jalankan dsniff, amati
- e. Dari komputer PC2 buka terminal, lakukan telnet ke PC1, amati hasil dnsiff apa output dari dsniff.
- f. Dari komputer PC2 buka terminal, lakukan ftp ke PC1, amati hasil dnsiff apa output dari dsniff
- g. Dari komputer PC2 buka terminal, lakukan ssh ke PC1, amati hasil dnsiff apa output dari dsniff.
- h. Dari komputer PC2 buka terminal, lakukan sftp ke PC1, amati hasil dnsiff apa output dari dsniff.
- i. Buat kesimpulan praktikum Anda.

- b. Percobaan packet Sniffing dengan Ettercap, buat topologi sama dengan percobaan 1
 - a. Diasumsikan PC1 sudah terinstall telnet, ftp dan ssh, PC2 sebagai client yang akan koneksi ke PC1
 - b. PC3 sebagai attacker lakukan instalasi ettercap dan konfigurasi :
 - Dari terminal jalan perintah apt-get install ettercap
 - Konfigurasi file /etc/etter.conf dan rubah sbb :

```

root@ubuntu: /home/isbat
#
# $Id: etter.conf,v 1.78 2004/10/12 15:28:38 alor Exp $
#
#####

[privs]
#ec_uid = 65534           # nobody is the default
#ec_gid = 65534           # nobody is the default

ec_uid = 0
ec_gid = 0
-- INSERT --
21,1

```

Dan pada konfigurasi linux aktifkan sbb :

```

root@ubuntu: /home/isbat
#-----
#      Linux
#-----
# if you use ipchains:
#redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
#redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"

# if you use iptables:
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"

#-----
-- INSERT --
160,1      72%

```

- Jalankan ettercap sbb :
 ettercap -TqM ARP /IP_TARGET_PC2/
 T artinya mode Text, q artinya q = quiet mode, M = man in the middle
 ARP = tipe protocol man in the middle attack yang digunakan;
 Misal sbb :

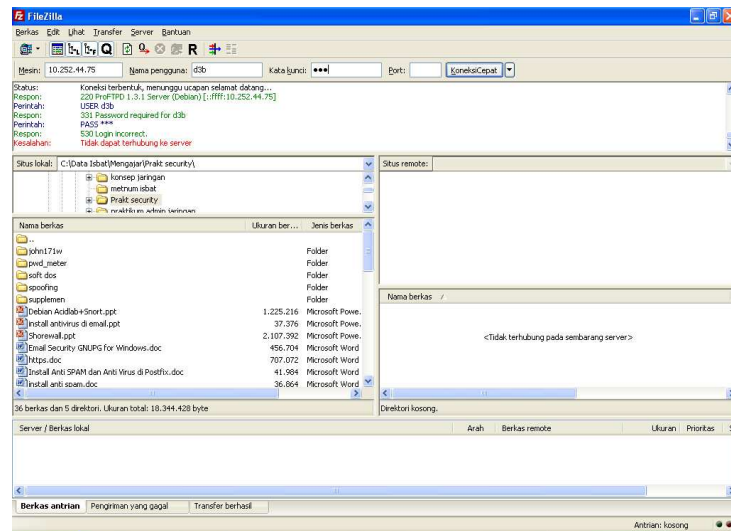
```

root@ubuntu: /home/isbat
root@ubuntu:/home/isbat# ettercap -TqM ARP /10.252.44.178/

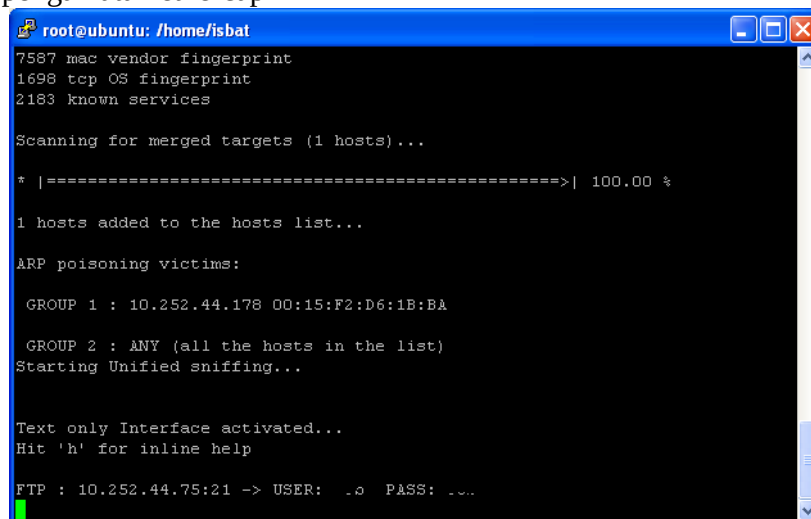
```

Amati hasilnya

- c. lakukan koneksi ftp dari PC2 ke PC1 dan amati dari ettercap, misal di sini dari windows



Hasil pengamatan ettercap



- Dari komputer PC2 buka terminal, lakukan telnet ke PC1, amati hasil ettercap apa outputnya
- Dari komputer PC2 buka terminal, lakukan ftp ke PC1, amati hasil ettercap apa outputnya
- Dari komputer PC2 buka terminal, lakukan ssh ke PC1, amati hasil ettercap apa outputnya
- Dari komputer PC2 buka terminal, lakukan sftp ke PC1, amati hasil dnsiff apa output
- Buat kesimpulan praktikum Anda

- b. Percobaan Session Hijacking, lakukan percobaan 1 dan 2 pada file prakt modul 5 sniffing spoofing session hijacking. pdf
- c. Lakukan percobaan jika PC1 menggunakan ssh apakah hunt masih bisa melakukannya ?
- d. Buat kesimpulan praktikum anda.

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