**EC7020: Computer and Network Security**

**Laboratory Experiment: 01**

**Basic Attack techniques and Defenses**

Reg No: \_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 04/10/2023, from 13:00 to 16:00

**AIM**: student will learn the fundamental principles of computer and network security by studying attacks on computer systems, network, and the Web. Students will learn how those attacks work and how to prevent and detect them.

**OBJECTIVES:**

* To understand the fundamentals of computer malware.
* To understand the Fundamentals about sandbox.
* Ability to use Sandbox for testing Computer Malwares.
* Ability to Create own malware for the windows operating system.

**Following are the tasks for this lab session.**

1. Briefly explain the following computer malware. (Not more than 4 lines)(8 Marks)
2. Worm

It is a subset of malware which can be capable for spreading copies itself from computer to computer, and it can replicate itself without any human interaction, it does not need to attach with software to damage a pc. The spread of worms happens with software vulnerabilities which do not update before any third-party software installation.

1. Ransomware

 Ransomware also some species of malware lock or encrypt the victim machines’ files or hardware aiming at ransom or payment from the victim. Usually businesses, bank systems, organizations or individual people become the target of the team. Unknown virus guard or third-party crack tools installation have some possibility to affect ransomware.

1. Briefly explain How you can create a simple Ransomware (12 Marks)

* Use our own virtual environment for ethically test the ransomware
* The program should look like a regular exe file of a pdf file which hides hidden bat or java scripts or any scripts.
* Then the scripts should encrypt the data with the public key, after encryption the files looks extensions should change.
* May use some popup with count down timer.

1. Briefly explain about Sandbox and its benefits (8 Marks)

Sandboxes provides lightweight desktop environment to safely run applications in isolated environments.

It runs separately from the environment. When the app closes all the sandbox resets and gives new environment.part of windows Disposable Secure Efficient are features of sandbox

1. Use Windows Sandbox to create a simple worm using windows DOS batch language.

**Instructions:**

1. Search Windows sand Box in the start menu. And click on Windows Sandbox
2. Copy the provided lab zip to the sand box desktop
3. Go through provided “DirectoryBomb.Bat” file in the folder “Lab1/SimpleWorm Example”

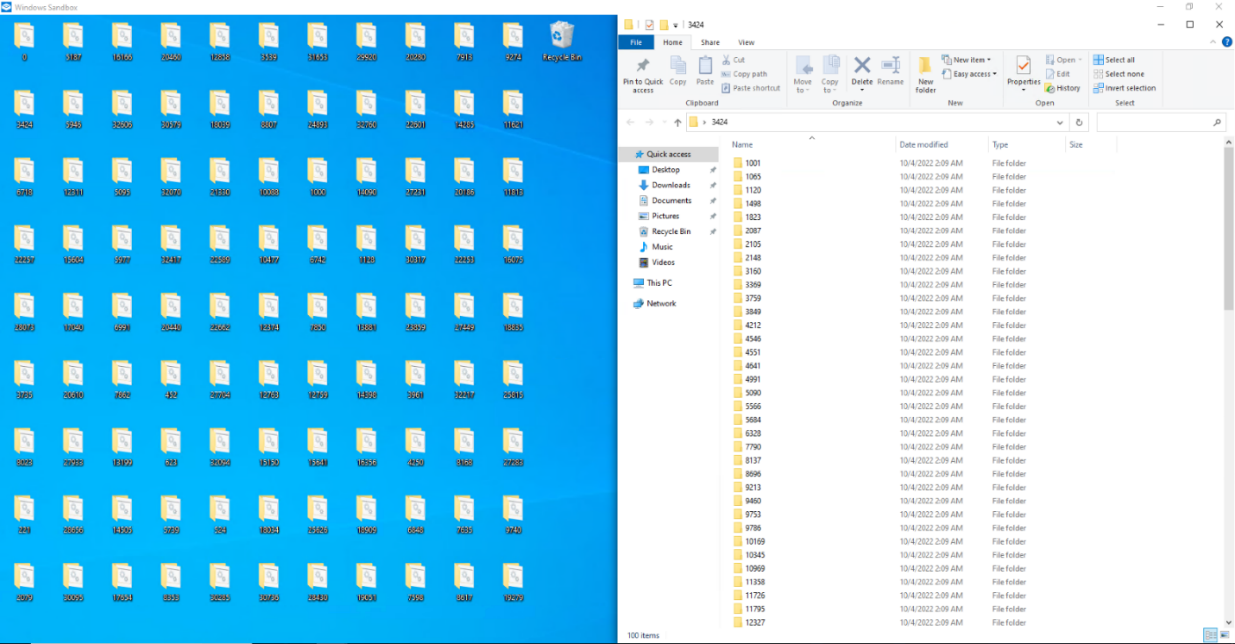
**Task:**

1. Briefly Explain how this program works:  (12 Marks)

Looping until the %val%=225 from random values ,if it equals the program done the job. Else make directorys in desktop and copy the bat file and past to the created directories %y% place.

1. Edit the “LAB1\SimpleWorm Task\ DirectoryBombHieracy.bat” file to create many folders

Inside every folder in the desktop. With the copy of .bat file. See the following images for references.   (30 Marks)



1. Explain How You changed the program (20 Marks)

 creating a second loop inside the given loop and create a sub directory variable which randomly Chage

1. Attach Your Screen shot of the folder in the desktop and Screen shot of folders inside

any one folder in the desktop  (5 Marks)

**Discussion**

**Conclusion**

**This is individual work. Write your answers in this Lab Instruction sheet with the file name EC7020\_L1\_YourRegNo. Submit it as a pdf document and archive all files and upload to the teams. Same name conversion applies for the Zip.**