Penetration Testing - Malware

Linux and Windows will be involved.
Use a VM VirtualBox machine.

Fulfill whole no 1-4. Basically creating an exe program for victims to click on. Of course, you have to do stealthier approach it will be better.
Do All from Work 1 Whole (1.1-1.4)

Guidelines

- Complete all tasks outlined below.
- You may use the internet during the lab quiz, you are also allowed to use any code/script/tool/software available online, including chatGPT and alike tools.

Overview

You are tasked to create a multi-platform malware that affect hosts with different operating systems. You can design the malware to do anything you like, but it must adhere to the requirements outlined in the task below.

You are expected to conduct further research on topics as necessary to complete this research lab work.

Work 1: The Malware

First, give your malware a fancy name of your choice. It must do the following:

- Infect the specified **target** hosts
- Display malware **message**
- Exhibit the outlined malware **properties**
- **Exfiltrate** data from the target hosts

Your submission format is a report (only pdf will be accepted), followed by a live demo in the following week. So, think about how you might layout the information you want to present in the report, as your peer markers will also have access to your report when doing the peer marking.

Work 1.1 Target

Your malware must target multiple operating systems (OSes) and be functional on those targeted OSes. You can make assumptions about the configuration in each target OS as necessary for the malware to be functional – just make it clear.

Work 1.2 Message

The malware must display a message informing the target hosts' users that they are infected with the malware. Provide any other details in the message as appropriate.

Work 1.3 Properties

The malware must exhibit the following properties.

- It must behave like a virus.
- It must try to be evasive.
- It must mutate.
-

Work 1.4 Exfiltrate

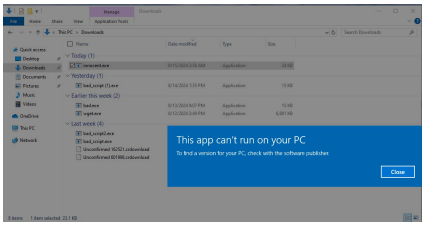
The malware is also able to exfiltrate data from the target host. What information to exfiltrate is up to you, but to receive Distinction or Higher Distinction grade, you must provide some reasoning behind which data is to be exfiltrated and how.

Make more stealthier data exfiltration techniques.

Special Instructions

1. Must infect the target host i.e Windows, or Mac, or Linux
2. When the user runs the program, it will pop up a message box and display the message(message of your choice).
3. The program would exfiltrate useful data, i.e user's credentials, ip address, etc.
4. The virus must be evasive and will mutate
5. Stealthier approach is required, how you want to do it is based on your expertise.
6. Rename the C++ file name as "innocent.cpp". Then also execute exe program. Rename "innocent.exe" for Same for exe program.
7. C++ program example, download here: https://we.tl/t-LlwGKfL1gL

I managed to create it but i can't run it on windows: https://we.tl/t-Zq7S8vSo52



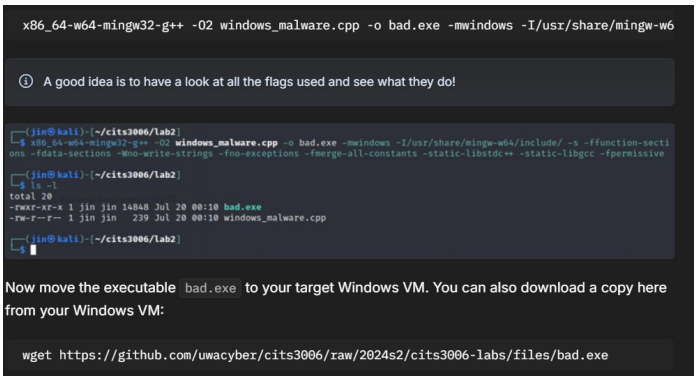
I have 2 files inside innocent2.cpp is able to create the exe program: https://we.tl/t-fF03UslE3F

Run this:

g++ -O2 innocent.cpp -o innocent.exe -lcurl

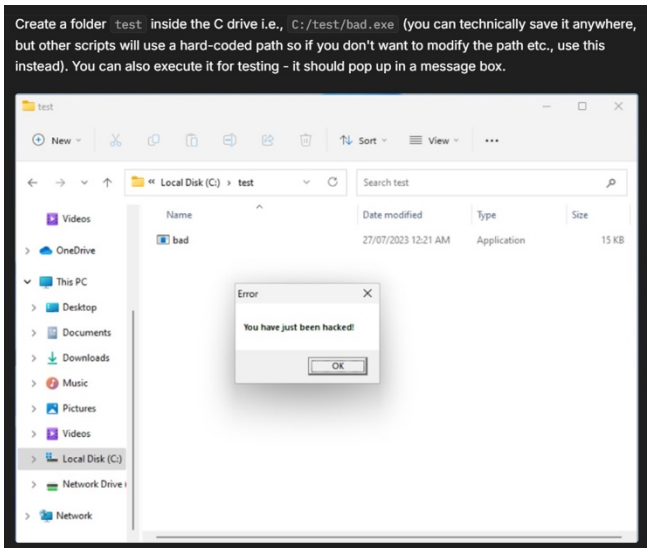
Expected Output:

Example from my lab question (but not necessary to follow): In my lab question, you run the above command to compile your program in Linux machine and then it would create example "bad.exe", then you maybe transfer it to a windows machine, which will be executed there.



Running this command would create the executable program below:

x86_64-w64-mingw32-g++ -O2 windows_malware.cpp -o bad.exe -mwindows -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive



And when the victim click on the exe program, then it would execute the function