Incident Response Technologies
Homework 3 (Malware Analysis)

Cliff C. Zou

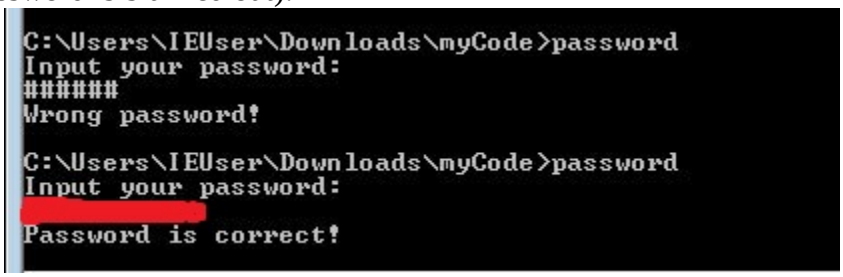
Question 1: In your Kali Linux VM, run 'strace' program to find out what system calls have been used by the command 'mkdir temp'. Make sure that this 'mkdir temp' can be successful. (if your Kali does not have strace, you need to install it by yourself)

(1). If you save the strace output into a text file, how many lines exist in this output file? Use screenshot image to show how you get this value.

(2). How many times the 'access()' system call has been called by mkdir command? Use screenshot image to show how you get this value.

(3). Show the complete 'execve(…)' system call executed by the mkdir command.

Question 2: I have made a very simple 32-bit Windows executable program called 'password.exe', which can be downloaded from the homework assignment page. The code can run on 32-bit or 64-bit Win7 or above Windows. When executed, the program asks for you to input a password. If your input password matches with the program's hardcoded password, then you are successful; otherwise it prints out that you input a wrong password. The execution is like this (the real password is blanked out):



Please use the free OllyDbg software to find out what is the correct password by dynamically analyzing this binary code. Provide the screenshot image to show your successful execution of this 'password.exe' code. In addition, use words and screenshot images to show how you find out this correct password.

Question 3: Malware Static Analysis: I have downloaded a 'malware.zip' from http://openmalware.org/. You can download this code from the assignment page. Now you need to provide static analysis of this code. Note that as I explained in lecture, this 'malware.zip' is compressed with password 'infected', and unzipping it will generate a file called 'malware.exe'. You probably *have to use your Windows VM* to download this malware code and analyze it, since the anti-virus software installed on your computer's host OS might prevent you from downloading or decompressing it out.

1). What is the real name of this malware? Explain how you determine its name. Since different malware detection systems provide different names, you need to provide the malware's name given by 'ClamAV' anti-virus software. Use screenshot image to show the part where ClamAV providing the name.

2). Use a screenshot image to show how you use a static analysis tool to determine that the malware is "packed".

3). Use a screenshot image to show how you unpack this malware. Give the unpacked malware program with the name as “malware-unpacked.exe”. What are the file size (in terms of number of bytes) of the ‘malware.exe’ and the ‘malware-unpacked.exe’, respectively?

4). Use a static analysis tool to analyze this unpacked malware code. Answer the following questions with support of corresponding screenshot images:

a). How many bytes are in the “File Header”? What are the value of the first 5 bytes in “File Header”?

b). Show the first three lines of assembly language instructions of the malware code.