COMP6016 (Malware Analysis)
Week 9- Practical Exercise: Dynamic Analysis

Today's labs will be done on Lubuntu VM. Create a new folder for each exercise.

1. Download the ***pp1*** malware executable from Moodle and store it on the folder created in Lubuntu VM. This is a malware executable whose source code is not available. You need to use Static and Dynamic analysis to learn what this malware does. Ideally, first thing to do, do not run the malware.
   a. Static Analysis: Use ***strings*** command with the filename to look for any strings in the binary. This may give you some clues on what the program does. Note: the strings may also be misleading.
   b. We will now familiarise ourselves with ***cutter-debugger*** available on Lubuntu VM `Password is 'pa$$wo'`
      - Open ***cutter-debugger***
      - Click File -> Open: Select your folder and the pp1; click Open
      - This will open the pp1 binary. It will be dissembled and the assembly will be shown
      - Static Analysis: Try to understand the assembly code to figure out what the code may be doing.
      - Dynamic Analysis: use the debugging option to carry out dynamic assembly. You may want to step-in or step over the lines of code. Keep monitoring the stack and the register values. You can always right click the register values and follow in the memory dump. This will should you the hex values.
   c. Answer the following:
      - Does the malware ask for a password? What is the password?
      - What does the executable do?
      - Is it harmful?

2. Download the ***pp2*** malware executable from Moodle and store it on the folder created in Lubuntu VM. This is a malware executable whose source code is not available. You need to use Static and Dynamic analysis to learn what this malware does. Ideally first thing to do, do not run the malware.
   a. Static Analysis: Use ***strings*** command with the filename to look for any strings in the binary. This may give you some clues on what the program does. Note: the strings may also be misleading.
   b. Dynamic Analysis: use cutter-debugger to carry out dynamic assembly. You may want to step-in or step over the lines of code. Keep monitoring the stack and the register values. You can always right click the register values and follow in the memory dump. This will should you the hex values.
   c. Answer the following:
      - What does the malware do?

Further Reading:

- Read Chapter 3 of Practical Malware Analysis. This chapter is on advanced dynamic analysis