CIS6395: Midterm Exam

University of Central Florida
Cliff C. Zou

1. **Virtual Machine Setup and Networking between VMs (20 points)**:

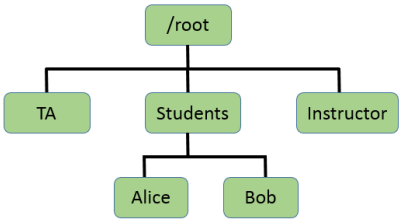
   Please install VirtualBox on your own computer, then import the following two VM images in your VirtualBox: Kali Linux VM, and Windows 7 (or Win10) VM.

   1). Set up these two VMs in "Nat Network" mode or 'Bridged Adapter' mode, so that they will be in the one VLAN and be able to reach each other. What are these two VMs IP addresses? Please use screenshot images to show how you find out each VM's IP address. **(10 points)**

   2). Use screenshot images to show that you can Ping from Windows VM to your Kali Linux VM successfully, and you can also Ping from Kali Linux VM to your Windows VM successfully ((Hint: you might need to disable firewall in your Windows VM for Ping to work). **(10 points)**

2. **Linux Basic Usage (15 points):**

   In your Kali Linux VM, login with the 'root' account (I explained in lecture how to create root account password for new Kali Linux VM). Then conduct the following operations. All operations must be conducted under Linux command line terminal window:
   1). Under your account home directory '/root', create the following directory tree. Use screenshot image to show how you do it. **(5 points)**



   2). Change the directory access property: Make the dir 'TA' to be read/write/executable by group and others; make the dir 'Instructor' to be un-readable and un-executable by others (writable property does not matter). Use sceenshot image to show your operations. **(5 points)**

   3). Copy '/etc/passwd' file under the 'Alice' directory. Then use one command line operation to show only the several lines in the passwd file under the Alice directory that contain 'systemd' keyword. Again use screenshot image to show your operation (Hint: you can try 'grep' command for text searching). **(5 points)**

3. **Malware Static Analysis (35 points):**

   I have downloaded a 'malware.zip' from http://openmalware.org/. You can download this code associated with this assignment. 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 the 'AVG' anti-virus software run on http://virustotal.com (don't run AVG software on your own computer to make this detection). Use screenshot image to show the part where AVG providing the name. **(5 points)**

2). Use a screenshot image to show how you use a static analysis tool to determine that the malware is "packed". **(7 points)**

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? **(10 points)**

4). Use a static analysis tool to analyze this unpacked malware code. Answer the following questions with support of corresponding screenshot images: **(13 points)**

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.

4. Wireshark Captured Traffic Analysis (30 points):

On the Windows computer in my UCF office, I opened Wireshark and captured network traffic while I did a few normal operations. The captured trace file is provided in association with this assignment. Your task is to download this captured file and analyze it by using Wireshark to answer the following questions (*you need to explain what display filters and operations you have done to derive your answers*):

1) How many TCP packets have 'reset' flag set as 1? In the Internet web traffic, what is the file name of the .jpg picture file? What are the IP addresses of the DNS servers that have been queried during this traffic capture? Please provide the list of IP addresses of local computers that have sent out 'Dropbox LAN sync Discovery' messages and have IP addresses between '10.173.214.0' to '10.173.214.99'? **(16 points)**

2) In command window, I used 'tracert' command to conduct a traceroute to an Internet server. I stopped the traceroute operation after I received "Request time out" messages from a few routers. **(14 points)**

   a. What is the IP address of the Internet server did I do the traceroute to? What is my own computer's IP address?

   b. How many routers within UCF campus network have responded to my traceroute operation (i.e., sent back notification messages)? Please provide their IP addresses in the order of the first router, second router, third router, etc.