COMP 5350 / 6350 – Project #3

Schedule:

Project #2 Assigned: 11 November 2022
Project #2 Due: 3 December 2022

Students Project Requirements:

You will be provided a forensically collected copy of a Windows 10 registry named "Win10Reg.7z". Your task is to use any tool or technique discussed in class to find the following information:

- ✓ How many users and groups are associated with this system according to the Security Accounts Manager?
- ✓ What are the names of the users associated with this registry?
- ✓ When did the user aubie last log in to the system?
- ✓ What applications are automatically started when the user logs into the system and when was the last time the autostart was run?
- ✓ What was the private IP address associated with the system?
- ✓ What are the most recently executed commands from the Windows Run command window?

Final Report:

Each team will provide a final report that answers the questions from the grading rubric. The format of the final report will include the following sections:

1) Executive summary
2) Problem description
3) Description of analysis techniques utilized
4) Tables and screenshots
5) Conclusions and Recommendations

Grading Rubric:

The grading rubric that will be used to grade each disk image will be based on the following criteria:

Part I: File forensics using file signature analysis

Activity	%	Pts
Were the correct number of users and groups identified?	15%	30
Were the correct named of the users identified?	15%	30
Was the correct last login time specified?	15%	30
Were AutoStart applications identified and the last run time specified?	15%	30
Was the IP address of the system specified?	15%	30
Were the most recently executed commands specified?	15%	30
Did the final report effectively communicate the findings?	10%	20
Total		200

Project Grading:

Letter grades will be assigned based on a 10-point scale:

90 – 100 = A
80 - 89.9 = B
70 - 79.9 = C
60 - 69.9 = D
< 60 = F