COURSE NUMBER: SEC 375

COURSE TITLE: Malware Analysis Techniques

I. MAJOR INSTRUCTIONAL OBJECTIVES:

Objective A: Fundamentals of malware analysis
A-1. Describe the key differences between the different forms of malware which are present in the real world
A-2. Identify and discuss the various methods which malware can use to infiltrate and alter a modern version of the Windows operating system
A-3. Describe the steps required to create a secured analysis lab in both a “bare metal” PC and virtual machine environment
A-4. Describe the key differences between the different analytical techniques associated with malware analysis

Objective B: Identify and recognize different malware analysis tools which are used in specific phases of the malware analysis process
B-1. Determine and explain the differences in static and dynamic analysis tools
B-2. Evaluate and defend decisions on which malware analysis tools to use for a specific form of malware
B-3. Understand the expected results which the various analysis tools will produce

Objective C: Strategies for protecting computer system(s) from a specific piece of malware
C-1. Organize, review, and analyze the data that was created as a result of utilizing numerous malware analysis tools
C-2. Explain the steps needed to protect a modern Windows environment from an analyzed piece of malware
C-3. Explain the steps needed to protect a networked environment from an analyzed piece of malware

Objective D: Findings discovered during a malware analysis procedure
D-1. Discuss and debate various malware-related questions and topics
D-2. Write a report, using a specific format/template, which accurately describes
   a. Findings regarding the behavior of a specific piece of malware
   b. Evidence that supports their findings
   c. Recommendations on how to prevent the malware from completing its mission
II. CLASS PARTICIPATION:

Students are expected to attend class and participate actively and in a positive way. Questions and relevant observations are encouraged and enrich the experience of the entire class. Computers in the classrooms are intended to be used as tools to enhance the students' learning experience. Instant messaging, gaming, emailing, and surfing the web are distractions to the student, the surrounding students, and the instructor and constitute inappropriate behavior. Students are ethically obliged to avoid these and similar practices.