Reverse Engineering Malware
UWF Florida Cybersecurity Training Program
Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course Dates: December 2 - 13

Duration: 2 weeks

Estimated Time Commitment: 7.5 hours per week

Instructional Hours: 15 contact hours

Delivery Format: Asynchronous online

Target Audience: Courses: IT and Cybersecurity practitioners

Required Prerequisites / Background: Participants should have a basic familiarity with computer, network concepts and malware, familiarity with the usage and administration of Windows 10 Operating System, and a working knowledge of Linux OS to run simple scripts

CEUs: 1.5, **CPEs:** 18

Course Instructor(s):

Instructor	Email
Anthony Pinto	apinto@uwf.edu

Course Description

This course covers software reverse engineering of executable code (or malware) to determine its function and effect. The course lectures are supplemented with hands-on exercises to reinforce the learning process.

Student Learning Outcomes:
Upon completion of the course, students will be able to:

1. Understand basic analysis to determine software functionality.
2. Apply static analysis to determine software functionality.
3. Apply dynamic analysis to determine software functionality.

NIST NICE Cybersecurity Workforce Framework Mapping

The course prepares for the following cybersecurity work roles as defined by the NICE Cybersecurity Workforce Framework.

Cybersecurity Work Roles and Categories:

- Digital Forensics (PD-WRL-002)
- Threat Analysis (PD-WRL-006