Advanced Network Defense

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

Course Overview

Course Dates: September 9-20, 2024

Duration: 2 weeks

Estimated Time Commitment: 10-15 hours per week

Instructional Hours: 15 contact hours

Delivery Format: Asynchronous online

Target Audience: IT and Cybersecurity practitioners

Required Prerequisites / Background: Prior knowledge of Network Packet inspection and Protocols

CEUs: 1.5, **CPEs:** 18

Course Instructor(s):

Instructor	Email
Dr. Guillermo Francia, III	gfranciaiii@uwf.edu
Mr. Amador (JR) Avila	aavila@uwf.edu

Course Description

This course serves as an intermediate-level course on network defense following the Network Defense Fundamentals course. It focuses on advanced knowledge, skills, and abilities of network defense, covering topics from intrusion detection and prevention mechanisms, wireless network security, network defense tactics and tools, and security incident and event management (SIEM). The course lectures are supplemented with hands-on exercises to reinforce the learning process. The learning components are loosely based on those found in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181 rev 1.

The course is divided into 5 modules. The modules are mapped to information common to all cybersecurity work roles defined in the Framework. Each module includes a discussion segment, and hands-on exercises as appropriate. Each student is expected to participate actively in the course. The course will culminate with incident management using SIEMs.

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:

- Cyber Defense Analyst (Protect and Defend, PR-CDA-001)

Course Information

Materials:

No Required Textbook

Technical Specifications:

Participants need access to a computer with stable internet connection. They will be required to access the course Leaning Management System (LMS) portal, Canvas. Participants will be logging in to the Florida Cyber Range (FCR) to do all hands-on activities (logins and instructions will be provided before session starts). The course will require internet connection for logging in to FCR.

Each module will have a discussion board that participants will use to post questions and comments related to that module. Instructors will look at the questions and comments and respond as needed.

By enrolling for this course, you agree to abide by the Computing Resources Usage Agreement provided to you.

Grading:

Participants will be assigned a pass/fail grade. Participants must earn a total of 70% or higher on graded assessments to earn a passing grade.

Assessment	**Percentage**
Discussions/Test for Understanding	40%
Projects/Exercises	60%
Total:	**100%**

Course Overview / Schedule

Modules and Lessons	**Assessment**

Module 1: Overview of network protocols and vulnerabilities • TCP/IP protocol stack analysis • Vulnerabilities revisited	• Discussion
Module 1 Lab • Network packet capture and in-depth analysis	• Completion of lab
Module 2: Wireless Network Security • Wireless technologies • Wireless threats and attacks • Securing wireless networks	• Discussion • Hands-on exercise
Module 2 Lab • Wireless Reconnaissance	• Completion of lab (optional)
Module 3: **Network Intrusion Detection and Prevention** • Signature based systems • Behavior based systems (anomaly)	• Discussion • Hands-on exercise
Module 3 Lab 1 • Writing Snort rules and creating signatures	• Completion of lab
Module 3 Lab 2 • Creating rules in Zeek NSM to detect network anomaly	• Completion of lab
Module 4: Network defense tactics and tools • Honeypots and Honeynets • Software Defined Networks (SDN) • Packet crafting for network security testing	• Discussion • Hands-on exercise
Module 4 Lab • Packet crafting and testing with Scapy	• Completion of lab
Module 5: Security Incident and Event Management (SIEM)	• Discussion • Hands-on exercise
Module 5 lab 1 • Incident management with Splunk	• Completion of lab
Module 5 lab 2 • Managing incidents with ElasticStack	• Completion of lab