Network Defense Fundamentals

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

Course Overview

Course Dates: February 12-23, 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: Participants should have a working knowledge of computers, basic knowledge of computer networks, familiarity with the usage and administration of Windows and Linux OS, and basic skills with text editing.

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 introductory course on network defense. It focuses on the fundamentals of network defense, covering topics from network protocol vulnerabilities, perimeter security, host hardening, and policies, legal and ethical aspects of network defense. 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 7 modules. Each module includes a discussion segment, assessment, or hands-on exercises as appropriate. Each participant is expected to participate actively in the course.

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: Principles of network defense • CIA Triad • Defense in depth • McCumber Cube • Business needs	• Discussion • Quiz
Module 2: Fundamentals of network protocol security and vulnerability • Protocol frame structures • Packet sniffing fundamentals • Packet analysis	• Discussion • Hands-on exercise using Wireshark
Module 2 Lab • Packet capture and analysis	• Completion of lab and report
Module 3: Perimeter defense • Firewalls and Access Control • Firewall deployment and DMZs • Firewall rules • Firewall log forensics	• Discussion • Quiz
Module 3 Lab • Firewall configuration and testing	• Completion of lab and report
Module 4: Host hardening • Operating System hardening • File integrity checking	• Discussion • Quiz
Module 4 Lab • Advanced Intrusion Detection System (AIDE) on host hardening	• Completion of lab and report
Module 5: Intrusion detection and prevention concepts	• Discussion • Quiz
Module 6: Security policy and threats • Concepts • Design and implementation	• Discussion • Table-top exercise on writing a network security policy
Module 7: Ethical, legal, and regulatory issues pertaining to network defense	• Discussion • Table-top exercise on ethical issues