Network Defense Fundamentals

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

Course Overview

Course Dates: August 19, 2024 – August 30, 2024
Duration: 14 days
Instructional Hours: 15 contact hours
Delivery Format: Asynchronous online
Target Audience: IT or Cybersecurity practitioners or staff
CEUs: 1.5, **CPEs:** 18
Level of Instruction: Undergraduate, Entry-level

Instructor/Contact Information:

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

Course Description

Course Overview

Prerequisites:
Participants should have a working knowledge of computers, basic knowledge of computer networks, familiarity with the usage and administration of Linux OS, and basic skills with programming/scripting.

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.

Learning Outcomes:

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

- Explain protocol functionalities and vulnerabilities in the TCP/IP stack (T0019)
- Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources (T0023)
- Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis (T0036)
- Define and interpret ethical, legal, and regulatory requirements pertaining to network defense (T0408)

Materials:

No Required Texts (Title, edition, ISBN)

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.

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. Discussion and test for understanding grades will be assigned based on participation.

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

NIST NICE Cybersecurity Workforce Framework Mapping

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

Cybersecurity Competencies and Work Roles:

Competencies

- Communications Security
- Cyber Resiliency

Work Roles

- Defensive Cybersecurity (PD-WRL-001)

Course NICE Framework Alignment and Credentials

NICE Cybersecurity Workforce Framework

Knowledge and Skills required to fulfill the above tasks mapped to the NICE Cybersecurity Workforce Framework:

- Knowledge of computer networking concepts and protocols, and network security methodologies (K0001)
- Knowledge of cyber threats and vulnerabilities (K0005) Knowledge of host/network access control mechanisms (K0033)
- Knowledge of information technology (IT) security principles and methods (K0049)
- Knowledge of network traffic analysis methods (K0058)
- Knowledge of how traffic flows across the network (K0061)
- Knowledge of defense-in-depth principles and network security architecture (K0112)
- Knowledge of cyber-attack stages (K0177)
- Knowledge of basic system, network, and OS hardening (K0205)
- Knowledge of the basics of network security (K0561)
- Knowledge of threat and/or target systems (K0604)
- Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities (K0106)
- Skill in using protocol analyzers (S0057)
- Skill in performing packet-level analysis (S0156)
- Skill in identifying cyber threats which may jeopardize organization and/or partner interests (S0229)
- Skill in creating and extracting important information from packet captures (S0199)

Digital Badges and Credentials Earned
Badge URL and or QR code

Course Versioning

Version 3.0

Student Accessibility Resources
If you have a disability that impacts your full participation in this course, please email Student Accessibility Resources at 850.474.2387 or by email, sar@uwf.edu.

Course Outline

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