



Essential Cyber Defenses

Course Overview

Course Dates: March 31 - April 11, 2025

Duration: 2 weeks

Instructional Hours: 15 contact hours

Delivery Format: Asynchronous online

Target Audience: IT and Cybersecurity practitioners

Recommended Background: Learners should have basic familiarity with computer concepts and operations.

CEUs: 1.5, **CPEs:** 1

Course Instructor:

Instructor	Email Address
Dr. Elizabeth Rasnick	erasnick@uwf.edu
Mrs. Sajida Shabanali	sshabanali

Course Description

Each module includes a quiz. Labs or other assessments are included as needed. Each learner is expected to actively participate in the course.

Learning Outcomes:

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

- Apply security policies to meet security objectives of the system (T0016)
- Employ secure configuration management processes (T0084)
- Identify and prioritize critical business functions in collaboration with the organization's stakeholders (T0108)
- Maintain baseline system security according to organizational policies (T0136)
- Administer accounts, network rights, and access to systems & equipment (T0494)

Materials:

No required textbooks. All relevant materials will be uploaded on Canvas.

Technical Specifications:

Participants need access to a computer with stable internet connection. They will be required to access the course Learning 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 an Internet connection for logging in to FCR.

NIST NICE Cybersecurity Workforce Framework Mapping

Work Roles

The course addresses cybersecurity work roles as identified in NIST’s Special Publication 800-181 rev 1, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework available at

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

The course is mapped to the following work roles:

- Network Operations Specialist (Operate and Maintain, OPM ID: 441)
- System Administrator (Operate and Maintain, OPM ID: 451)
- Systems Security Analyst (Operate and Maintain, OPM ID: 461)
- Enterprise Architect (Securely Provision, OPM ID: 651)

Knowledge and Skills required to fulfill tasks corresponding to the above work roles:

- Knowledge of computer networking concepts and protocols, and network security methodologies (K0001)
- Knowledge of cybersecurity and privacy principles (K0004)
- 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 defense-in-depth principles and network security architecture (K0112)
- Knowledge of cyber-attack stages (K0177)
- Knowledge of basic system, network, and OS hardening (K0205)
- K0302 Knowledge of the basic operation of computers (K0302)
- Knowledge of the basics of network security (K0561)

GRADING

The course is designed to introduce learners to foundational cybersecurity concepts. Quizzes reinforce the importance of key points. Lab assignments walk-through the application of the concepts covered in the module material.

Grading Scheme:

Assignment	Percentage of Grade
Quizzes	35.7%
Labs	64.3%
Total	100%

Course Details

- Course includes an online curriculum with instructor videos, online labs, and quizzes.



Course Schedule

Modules and Lessons	Assessment
Module 1: Cybersecurity Concepts <ul style="list-style-type: none">• NIST Cybersecurity Framework• Security Control Models (Bell-LaPadula; Biba)• The Lockheed Martin Cyber Kill Chain• Incident Response Lifecycle• System Lifecycle Process• Secure Software Development Lifecycle Lab 1: Application Least Privilege Lab 2: Cyber Kill Chain Reconnaissance Lab 3: Identify the incident	<ul style="list-style-type: none">• Quiz• Labs
Module 2: Networking <ul style="list-style-type: none">• Networking Concepts• The OSI Model• Commonly Used Network Protocols Lab 1: The OSI Model Lab 2: Types of Networks	<ul style="list-style-type: none">• Quiz• Labs
Module 3: Introduction to Risk Management <ul style="list-style-type: none">• Risk Management Concepts• The Role of Policies• Legal & Regulatory Compliance• The Risk Management Framework• Risk Management Mathematics Lab 1: Red Alert Gaming Risk Assessment Lab 2: Evaluating User Agreement Lab 3: Evaluating Risk	<ul style="list-style-type: none">• Quiz• Labs
Module 4: Implementing Access Controls <ul style="list-style-type: none">• Access Control Categories & Functions• Access control sources: NIST/CIS/STIGs• Security assessments• Choosing controls Lab 1: File Permissions	<ul style="list-style-type: none">• Quiz• Lab
Module 5: Authentication Methods <ul style="list-style-type: none">• Review of AAA• Authentication Methods	<ul style="list-style-type: none">• Quiz• Lab



Lab 1: Web-based Hacking	
Module 6: Cryptography <ul style="list-style-type: none">• Hashing• Encryption 101 Lab 1: Cryptography Concepts	<ul style="list-style-type: none">• Quiz• Lab