CENTER FOR CYBERSECURITY

AT THE UNIVERSITY OF WEST FLORIDA

Penetration Testing

UWF--CISA CyberSkills2Work Training Program
Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course Dates: August 5-16, 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. Hossain Shahriar	hshahriar@uwf.edu
Dr. Elizabeth Rasnick	erasnick@uwf.edu

Course Description

Course Overview

Prerequisites:

Participants should have a basic familiarity with computer and network concepts, familiarity with the usage and administration of Linux OS.

Course Description

This course focuses on various activities in the pentesting including but not limited to reconnaissance, enumeration, evasion, attacks and defending. The course will provide hands on experience towards discovering vulnerabilities and detecting attacks within enterprise network, operating systems, software and application and infrastructure. Topics may include ethics and laws in pentesting, risk analysis, analyzing and preventing exploitations. The course lectures are supplemented with hands-on exercises to reinforce the learning process. The lectures build upon the National Institute of Standards and Technology (NIST) guidelines documented in the following Special Publications (SP): 800-181 rev 1 (NICE Cybersecurity Workforce Framework).

The course is divided into 5 modules. Each module includes assessment, or hands-on exercises as appropriate. Each student is expected to participate actively in the course.

Student Learning Outcomes: At the end of this course, students will be able to:

- Differentiate what an ethical hacker can and cannot do legally.
- Evaluate security threats and vulnerabilities.
- Use hacking tools to locate and fix security leaks.
- Assess potential operating systems vulnerabilities.
- Configure security devices to secure systems against attacks.

NIST NICE Cybersecurity Workforce Framework Mapping

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 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

Cybersecurity Work Roles and Categories:

- Exploitation Analyst (Analyze, AN-TWA-001)
- Target Network Analyst (Analyze Targets, AN-TGT-002)
- Threat/Warning Analyst (Analyze, AN-TWA-001)
- Cyber Defense Analyst (Protect and Defend, PR-CDA-001)

Learning Outcomes mapped to the NICE Cybersecurity Workforce Framework Tasks:

- Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile (T0019)
- Develop content for cyber defense tools (T0020)
- Build, test, and modify product prototypes using working models or theoretical models (T0021)
- Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion (T0027)
- Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis (T0036)
- Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications (T0042)
- Provide subject matter expertise to the development of cyber operations specific indicators (T0585)
- Identify threat tactics, and methodologies (T0708)

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

- Knowledge of cyber threats and vulnerabilities (K0005)
- Knowledge of computer programming principles (K0016)

- Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions (K0046)
- Knowledge of current and emerging cyber technologies (K0335)
- Knowledge of access authentication methods (K0336)
- Explain various concepts of host hardening (K0205, S0121))
- Explain concepts and techniques of perimeter security (K0561, S0192)
- 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 identifying cyber threats which may jeopardize organization and/or partner interests (S0229)
- Knowledge of attack methods and techniques (K0362)
- 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)
- Knowledge of cyber attackers (K0162)

Materials:

No Required Books and Materials. NDG Netlab can be accessed via Florida Cyber range https://mercury.floridacyberrange.org/, you will get access at the beginning of the course.

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. A UWF Continuing Education certificate and a UWF digital badge will be awarded to each successful participant.

Assessment	**Percentage**
Hands on Labs	60%

Quizzes	20%
Discussion	20%
Total:	**100%**

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: Overview of Pentesting Topics: ▪ Ethical hacking ▪ Network security ▪ Packet analysis	▪ Discussion, Lab – Network analysis, packet crafting
Module 2- Reconnaissance Topics: ▪ Port scanning ▪ Foot printing ▪ Social Engineering ▪ Netlab practices	▪ Lab - Nmap, Hping, Social engineering attacks)
Module 3: Embedded system and web app security Topics: ▪ Embedded systems security ▪ Web application security ▪ Programming security	▪ Quiz ▪ Discussion ▪ Lab – OpenVas, Metasploit
Module 4: Secure programming, Operating systems security Topics: ▪ Operating system security ▪ Buffer overflow, SQL injection ▪ Password cracking	▪ Lab – buffer overflow, web scanning, password cracking

Module 5: Intrusion detection, Firewall, Backdoor Topics: ▪ Intrusion detection systems ▪ Firewall ▪ Rootkit, Backdoor	▪ Discussion ▪ Lab – Evading IDS, Netcat