C-ID Descriptor
Introduction to Cybersecurity: Ethical Hacking

Descriptor Details

- **Descriptor Title**: Introduction to Cybersecurity: Ethical Hacking
- **C-ID Number**: 164
- **Units**: 3.0
- **Date of Last Revision**: 2/26/2025 07:20:53 PM GMT+0000

General Description

This course introduces the network security specialist to the various methodologies for attacking a network. Students will be introduced to the concepts, principles, and techniques, supplemented by hands-on exercises, for attacking and disabling a network within the context of properly securing a network. The course will emphasize network attack methodologies with the emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Students will receive course content information through a variety of methods: lecture and demonstration of hacking tools will be used in addition to a virtual environment. Students will experience a hands-on practical approach to penetration testing measures and ethical hacking.

Prerequisites

None

Corequisites

None

Advisories

ITIS 150 - Computer Network Fundamentals
AND ITIS 160 - Introduction to Information Systems Security

Content

1. Ethical Hacking Overview
2. Ethics and Legal Aspects for Cybersecurity Professionals
3. Information Security Frameworks
4. Transmission Control Protocol/Internet Protocol (TCP/IP) Concepts Review
5. Network and Computer Attacks
6. Passive Intelligence Gathering: Footprinting and Social Engineering
7. Network Reconnaissance
8. Port Scanning
9. Enumeration
10. Fundamentals of Exploitation
11. Denial of Service
12. Session Hijacking
13. Evading Intrusion Detection Systems (IDS), Firewalls, and Honeypots
14. Vulnerability Analysis
15. Linux Operating System Vulnerabilities
16. Internet of Things (IoT) Vulnerabilities and Hacking
17. Hacking Web Servers
18. Hacking Wireless Networks
19. Covering Tracks
20. Cryptography Fundamentals
21. Protecting Networks with Security Devices
22. Cloud Computing
23. Programming/Scripting for Security Professionals
24. Embedded Operating Systems

Lab Activities

No information provided

Objectives

At the conclusion of this course, the student should be able to:

1. Describe the tools and methodology a "hacker" uses to break into a computer or network.
2. Defend a computer and a Local Area Network (LAN) against a variety of different types of security attacks using several hands-on techniques.
3. Describe the legal and ethical aspects of hacking networked systems.

Evaluation Methods

Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.

Textbooks

- Simpson, M. T., Backman, K. & Corley, J., *Hands-On Ethical Hacking and Network Defense*, Cengage
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. & Williams, T., *Gray Hat Hacking: The Ethical Hacker's Handbook*, McGraw-Hill Education