

Virginia Western Community College

ITN 261

Network Attacks, Computer Crime, and Hacking

Prerequisites

ITN 260

VCCS Course Description

Encompasses in-depth exploration of various methods for attacking and defending a network. Explores network security concepts from the viewpoint of hackers and their attack methodologies. Includes topics about hackers, attacks, Intrusion Detection Systems (IDS) malicious code, computer crime and industrial espionage.

Semester Credits: 3

Lecture Hours: 3

Required Materials

Textbook

- Jones & Bartlett Learning Ethical Hacking: Techniques, Tools, and Countermeasures, fourth edition ISBN: 978-1-284-24899-9 Authors: Sean-Phillip Oriyano | Michael G. Solomon

Other Required Materials:

- Students enrolled in this course will be given access to the Virginia Western NetLab and Virginia Tech Cyber Range environments. This will require the student to have access to the internet.

VCCS COURSE OUTCOMES

- Explain ethical hacking and its value to the security professional.
- Understand the goals of information security: Confidentiality, Integrity, Availability
- Discuss the history of computer hacking and evolution from technical curiosity to high crime.
- Describe the protocols and services provided by the layers in the OSI and TCP/IP models.
- Explain the primary ports, protocols, and services in data networks.
- Employ the use of Wireshark and demonstrate through protocol analysis.

- Describe the usage of cryptography and the advantages and disadvantages of symmetric algorithms versus asymmetric algorithms.
- Describe some forms that cryptography may take in the future.
- Describe basic physical security controls and its role in information security.
- Explain and perform port scanning against a network system security boundary.
- Explain the processes of host enumeration, system hacking, and password cracking.
- Describe significance of network security to defend and observe malicious behavior on networks.
- Perform cross-site scripting (XSS) attacks and understand SQL injection attacks.
- Identify security issues associated with cloud computing.
- Describe threats posed by malware, viruses, Trojans.
- Explain what Kali-Linux is and the basics of working with Linux.
- Explain what social engineering is and how it is used to exploit weaknesses in people.
- Analyze an incident and apply incident handling processes based on the type of attack.
- Use the concepts of defense technologies to outline methods that can detect and mitigate the types of attacks described in this course.
- Describe the importance of using a secure benchmark such as the Center for Internet Security (CIS) to configure systems and devices.
- Reference frameworks and guidance such as the Risk Management Framework and OWASP Top 10 to build and validate secure systems.

Note to Instructors

None

TOPICAL DESCRIPTIONS

Discussed Topics
Threat Landscape & Discovery
Ethics & Compliance
Network Defense - Ports, Protocols, and Services
Applying Cryptography
Common Vulnerabilities and Exposures
Vulnerability Scanning
Application Security
Web Application Security

Host Hardening & Secure Benchmarks
Social Engineering
Incident Handling/Response
Cloud Computing Security Concepts
Final Project Presentation

[TITLE IX STATEMENT](#)

[ADA STATEMENT](#)

