Virginia Western Community College
ITN 261
Network Attacks, Computer Crime, and Hacking

Prerequisites
ITN 260

Course Description
Encompasses in-depth exploration of various methods for attacking and defending a network. Explores network security concepts from the viewpoint 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 Lab/Clinical/Internship Hours: 0

Required Materials

Textbook:
Corporate Computer Security Fourth EditionAuthors: Randall J. Boyle & Raymond R. PankoISBN-13: 978-0-13-354519-7ISBN-10: 0-13-354519-9

Other Required Materials:
Students enrolled in this course will have password-restricted access to the lab access. Internet Access Labs: www.jblcourses.com

Course Outcomes

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

- Explain ethical hacking and its value to the security professional.
- Discuss the history of computer hacking and evolution from technical curiosity to high crime.
- Describe the protocols and services provided by the Application layer in the OSI and TCP/IP models and describe how this layer operates in various networks.
- Explain the primary ports, protocols, and services in data networks.
- Employ the use of Wireshark and demonstrate through protocol analysis TCP startup and shutdown.
- 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 and equipment controls combined with importance of safety.
- Explain how to avoid common threats to physical security and mitigate vulnerabilities.

- State the purpose of footprinting and identify associated sources on World Wide Web.
- Explain and perform port scanning against a network system security boundary.
- Explain the processes of enumeration, system hacking, and password cracking.
- Describe significance of wireless security and defend wireless networks.
- Describe a SQL Server injection.
- Identify security issues associated with cloud computing.
- Describe threats posed by malware, viruses, Trojans.
- Describe the value of sniffers and how to evaluate packet captures.
- Explain what Kali-Linux is and basics of working with Linux.
- Explain what social engineering is and how to apply based on situational exploit.
- Analyze an incident and apply incident handling processes based on 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.

Topical Description

Week #	Topic
1	Threat Landscape & Discovery
2	Ethics
3	Ports, Protocols, and Services
4	Applying Cryptography
5	Common Vulnerabilities and Exposures
6	Vulnerability Scanning
7	Application Security
8	Web Application Exploits - XSS
9	Web Application Exploits – SQL Injection
10	Host Hardening
11	Wireless Security Defense
12	Social Engineering
13	Incident Handling/Response
14	No Class
15	Cloud Computing Security Concepts
16	Final Project Presentation

Notes to Instructors

- none