Revised Fall 2016

# ITN 261
# Network Attacks, Computer Crime, and Hacking

## COURSE OUTLINE

### Prerequisites:

Prerequisites: ITN 260

**Course Description:** This course will encompass an in-depth exploration of various methods for attacking and defending a network. Builds foundational understanding and application for TCP/IP Ports, Protocols, Services and Cryptography. Explores network security concepts from the mindset and viewpoint of various groups of hackers and their attack methodologies. Includes topics about network and system attacks, vulnerabilities, Intrusion Detection Systems (IDS) malicious code, computer crime, physical security, and industrial espionage.

This course is divided into three major parts. The first part will examine the landscape, key terms, and concepts that a security professional requires to understand hacking principles, computer crime, and history of hacking and ethical hacking. The second part will be a technical overview and application of ethical hacking. Review various methods attackers use, including footprinting, port scanning, enumeration, malware, sniffers, denial of service, and social engineering. The third part reviews incident response and defense technologies: how to respond to hacking attacks and defend them.

**Semester Credits: 4** Select Hours **Lecture Hours: 3** Select Hours
**Lab/Recitation Hours: 3** Select Hours

VIRGINIA WESTERN COMMUNITY COLLEGE
PO Box 14007
Roanoke, VA 24038
(540)-857-7273

Revised Fall 2016

# ITN 261
# Network Attacks, Computer Crime, and Hacking

## Course Outcomes

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

1. Explain ethical hacking and its value to the security professional.
2. Discuss the history of computer hacking and evolution from technical curiosity to high crime.
3. 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.
4. Explain the primary ports, protocols, and services in data networks.
5. Employ the use of Wireshark and demonstrate through protocol analysis TCP startup and shutdown.
6. Describe the usage of cryptography and the advantages and disadvantages of symmetric algorithms versus asymmetric algorithms.
7. Describe some forms that cryptography may take in the future.
8. Describe basic physical security and equipment controls combined with importance of safety.
9. Explain how to avoid common threats to physical security and mitigate vulnerabilities.
10. State the purpose of footprinting and identify associated sources on World Wide Web.
11. Explain and perform port scanning against a network system security boundary.
12. Explain the processes of enumeration, system hacking, and password cracking.
13. Describe significance of wireless security and defend wireless networks.
14. Describe a SQL Server injection.
15. Identify security issues associated with cloud computing.
16. Describe threats posed by malware, viruses, Trojans.
17. Describe the value of sniffers and how to evaluate packet captures.
18. Explain what Kali-Linux is and basics of working with Linux.
19. Explain what social engineering is and how to apply based on situational exploit.
20. Analyze an incident and apply incident handling processes based on type of attack.
21. Use the concepts of Defense Technologies to outline methods that can detect and mitigate the types of attacks described in this course.

**VIRGINIA WESTERN COMMUNITY COLLEGE**
**PO Box 14007**
**Roanoke, VA 24038**
**(540)-857-7273**

Revised Fall 2016

# ITN 261Network Attacks, Computer Crime, and Hacking

## Required Materials:

Primary Text: Hacking Techniques, Tools, and Incident Handling Second Edition, Sean-Philip Oriyano, Jones & Bartlett Learning, Information Systems Security & Assurance Series. ISBN:978-1-284-03171-3 Students enrolled in this course will have password-restricted access to the lab access. Internet Access Labs: www.jblcourses.com E-mail address.  The college-supplied email will be used to facilitate communications between instructor and student. All class communication must be through the VWCC-issued email address.

**VIRGINIA WESTERN COMMUNITY COLLEGE**
**PO Box 14007**
**Roanoke, VA 24038**
**(540)-857-7273**

# ITN 261 Network Attacks, Computer Crime and Hacking

Topical Description: (Outline chapters and sections to be covered in the book – may include timeline)

| Week | Topic | Reference (Chapter) |
|---|---|---|
| 1 | Hacking and TCP/IP | Ch 1-2 |
| 2 | Cryptographic Concepts and Physical Security | Ch 3-4 |
| 3 | Footprinting Tools and Techniques and Port Scanning | Ch 5-6 |
| 4 | Enumeration and Computer System Hacking Wireless Vulnerabilities | Ch 7-8 |
| 5 | Web and Database Attacks and Malware | Ch 9-10 |
| 6 | Sniffers, Session Hijacking, DoS and Linux Pen Tools | Ch 11-12 |
| 7 | Social Engineering and Incident Response | Ch13-14 |
| 8 | Defense Technologies | Ch-15 |
| Individual Lab Exam | | |

# ITN 261Network Attacks, Computer Crime and Hacking

## Notes to Instructors
(List information about optional topics, departmental exams, etc)

Suggested Grading Scheme:

| | |
|---|---|
| Scheduled Exams | 50% |
| Labs and Homework | 25% |
| Comprehensive Final Exam | 25% |

Grading Scale:
A = 91 – 100
B = 81 – 90
C = 71 – 80
D = 60 – 70
F = below 60

Required Time Allocation per Topic

In order to standardize the core topics of ITN 261 so that a course taught at one campus is equivalent to the same course taught at another campus, the following student contact hours per topic are required. Each syllabus should be created to adhere as closely as possible to these allocations. Of course, the topics cannot be followed sequentially. Many topics are taught best as an integrated whole, often revisiting the topic several times, each time at a higher level. There are normally 45 student-contact-hours per semester for a three credit course. (This includes 15 weeks of instruction and does not include the final exam week so 15* 3 = 45 hours. Sections of the course that are given in alternative formats from the standard 16 week section still meet for the same number of contact hours.) The final exam time is not included in the time table. The category, Other Optional Content, leaves ample time for an instructor to tailor the course to special needs or resources.