

**NOVA COLLEGE-WIDE COURSE CONTENT SUMMARY**  
**ITN 261 - NETWORK ATTACKS, COMPUTER CRIME AND HACKING (4 CR.)**

**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.

**General Course Purpose**

This course introduces the student to the process and tools, including nmap and other port scanning tools, used to perform ethical hacking. A discussion of different network attacks, computer crime, and hacking is provided. The purpose of this course is to inform the student of common techniques used by attackers in order to increase awareness and assist the student learn how to effectively counter these attacks. This course also includes content, as indicated below in parenthesis behind each learning objective, which directly maps to DHS/NSA's Center of Academic Excellence – 2 Year (CAE2Y) criteria. Current information on NOVA's Cybersecurity Program is located at [www.nvcc.edu/cybersecurity](http://www.nvcc.edu/cybersecurity)

**Recommended Corequisites/Prerequisites**

Prerequisite: ITN 260

**Course Objectives**

Upon successful completion of this course, the student will have a working knowledge of:

- a) Hacker attack techniques, methodologies, and tools
- b) Network worms, viruses, and malicious code
- c) Computer crime
- d) Industrial espionage
- e) Information warfare

**Major Topics to be Included**

- a) Network Attacks
- b) Malicious Code
- c) Computer Crime
- d) Industrial Espionage
- e) Information Warfare

**Student Learning Outcomes**

1. **Attacks**
  - 1.1. Explain the professional hacker's methodology for attacking a network.
  - 1.2. Explain the script kiddie's methodology for attacking network.
  - 1.3. Explain network security vulnerabilities.
  - 1.4. Explain hackers, hacker techniques, tools and methodologies.
  - 1.5. Describe hacker motivation
  - 1.6. Describe and perform network reconnaissance
  - 1.7. Describe and perform network mapping and scanning
  - 1.8. Describe and perform gaining access to a network.
  - 1.9. Describe and perform maintaining access to a network.
  - 1.10. Describe and perform covering tracks after gaining access to a network.
  - 1.11. Describe the Adversary Model (resources, capabilities, intent, motivation, risk aversion, access).
  - 1.12. Be able to use a network mapping tool (e.g. Nmap) to identify open ports on a network.

## **2. Malicious Code**

- 2.1. Describe the general symptoms of a virus attack
- 2.2. Differentiate between viruses and worms.
- 2.3. Identify and describe the various categories of viruses and how they operate.
- 2.4. Identify and describe the virus attack categories.
- 2.5. Identify and describe the propagation of worms.
- 2.6. Learn the terms and definitions associated with viruses, worms and malicious code.
- 2.7. Describe the use of social engineering in the propagation of worms and viruses.
- 2.8. Describe the operation of a macro virus.
- 2.9. Define and describe the two basic approaches to antivirus software.
- 2.10. Describe how to defend against a worm and virus attack.

## **3. Computer Crime**

- 3.1. Describe the steps in planning for a computer incident.
- 3.2. Identify the difficulty in establishing who has jurisdiction over a computer crime.
- 3.3. Understand the legal issues with regard to preserving digital evidence.
- 3.4. Describe the various factors to consider in evaluating the financial loss due to a computer incident.
- 3.5. Identify and describe the incident response goals and priorities.
- 3.6. Describe the factors involved in identifying a computer incident.
- 3.7. Describe and use the various tools associated with identifying an intruder.
- 3.8. Specify the process for the initial response to an incident.
- 3.9. Identify the various factors involved in assessing an incident.
- 3.10. Identify the various types of documentation that should be examined in evaluating an incident.
- 3.11. Describe how to handle and evaluate a computer incident.
- 3.12. Recognize the role of law enforcement and rule of particularity in executing a search warrant.
- 3.13. Describe the role the network security specialist would play in assisting the law enforcement and prosecution effort.
- 3.14. Describe the difficulties in prosecuting a computer crime incident.

## **4. Industrial Espionage**

- 4.1. Differentiate between competitive intelligence, economic intelligence, and industrial espionage.
- 4.2. Differentiate between information, data, knowledge and intelligence.
- 4.3. Specify the advantages of intelligence in industrial espionage.
- 4.4. Describe the foreign intelligence organizations interested in economic intelligence and their general methodology.
- 4.5. Describe Industrial Control Systems (ICS) and security issues associated with ICS and SCADA.
- 4.6.
- 4.7. Describe personnel countermeasure factors.
- 4.8. Describe physical countermeasure factors.
- 4.9. Describe technical countermeasure factors.

## **5. Information Warfare**

- 5.1. Describe the history of warfare and its relationship to information warfare.
- 5.2. Describe the historical factors that lead to information warfare.
- 5.3. Explain the concerns of the US. Government with regard to the information infrastructure.
- 5.4. Identify the spectrum of threats against the information infrastructure.
- 5.5. Specify the role of offensive information warfare.
- 5.6. Identify the types and roles of information warfare weapons.
- 5.7. Specify the role of defensive information warfare.
- 5.8. Explain the information assurance factors relating to defensive information warfare.
- 5.9. Explain the military role in information warfare.
- 5.10. Explain the civilian role in information warfare.
- 5.11. Explain the law enforcement role in information warfare.

### **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.

<b>Topic</b>	<b>Time in Hours</b>	<b>Percentages</b>
Network Attacks	24	53%
Malicious Code	8	18%
Computer Crime	3	7%
Industrial Espionage	2	4%
Information Warfare	2	4%
Other Optional Content	3	7%
Exams and Quizzes	3	7%
Total	45	100%