# CLEVELAND INSTITUTE OF ELECTRONICS SYLLABUS

**Course Number**: S375

**Course Name**: Network Defense and Countermeasures

**Course Clock Hours**: 90

**Course Prerequisites**: S370

**Course Co-requisites**: None

**Course Contact Information**: www.cie-wc.edu faculty@cie-wc.edu
1-800-243-6446 (216) 781-9400 (216) 781-0331 (fax)

**Course Description**: This course will cover concepts related to protecting a network against an attack. A review of network operation is accompanied by theoretical threats to networks and the best possible countermeasures are shown. Administrative policies that keep networks secure are discussed along with threats to virtual private networks (VPNs) and network intrusions are described. Methods of detection and action will be explained as well as the use of a variety of firewalls.

**Course Objectives**: Upon completion of this course the student will:

- Describe how to develop a security policy
- Discuss the countermeasures needed to prevent intrusions
- Discuss the steps in setting up packet filters
- Describe the policies used to secure networks
- Explain network security defenses commonly used in organizations

**Course Readings**: The required readings will be drawn from the textbook Guide to Network Defense and Countermeasures, 2nd Edition (ISBN: 1-4188-3679-6). The author is Randy Weaver and the publisher is Course Technology / Cengage Learning. The study guide will discuss the required readings and provide an outline of the topics explored in the textbook.

**Student Evaluation and Grading**: There are ten lessons in this course. The lessons are broken into nine exams and one case study. The nine lessons conclude with an examination; all examinations are open book. The Case Study explores real-world scenarios through written responses. The minimum passing score of 70% must be achieved but if the score is less than 70%, the lesson must be retaken to earn a passing score of 70% overall. The ten scores are averaged together and constitute 100% of the course grade.

| | | |
|---|---|---|
| 93% - 100% | A | The final grade for this course will be determined as follows: |
| 86% - 92.9% | B | 9 examinations + 1 Case Study = 100% |
| 78% - 85.9% | C | |
| 70% - 77.9% | D | |

**Course Schedule**: You should complete the following lessons in the order shown in the table. It is best to complete 1-2 lessons per week to maintain your schedule.

| Lesson Number | Title of Lesson | Topics Covered |
|---|---|---|
| 3751C | Network Defense Fundamentals | • Threats to network security<br>• Network security defenses |
| 3752C | Security Policy Design | • Risk analysis<br>• Techniques to minimize risk |
| 3753C | Security Policy Implementation | • Best practices in security policies<br>• Ongoing risk analysis and incident-handling procedures |
| 3754C | Network Traffic Signatures | • Concepts of signature analysis<br>• Identifying suspicious events and traffic signatures |
| 3755C | Virtual Private Network Concepts | • Encapsulation, encryption and authentication in VPNs |
| 3756C | VPN Implementation | • Design considerations for a VPN<br>• Setting up VPNs with firewalls |
| 3757C | Intrusion Detection System Concepts | • The components of an intrusion detection system<br>• Types of IDS products |
| 3758C | Intrusion Detection: Incident Response | • Configure an IDS and develop filter rules<br>• Six-step incident response process |
| 3759C | Choosing and Designing Firewalls | • Rules and restrictions for a firewall<br>• Common firewall configurations |
| 3760C | Case Study | • Selected Case Projects |