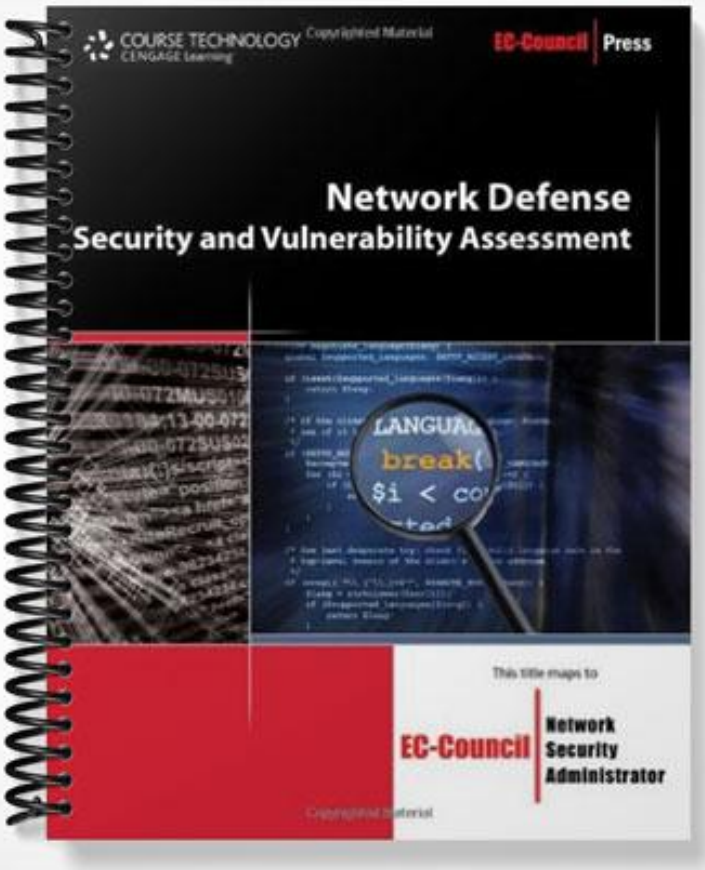
SOLUTIONS MANUAL



Network Defense Book 5: Security and Vulnerability Assessment Instructor Guide

Fact Sheet

Title of the course: Security and Vulnerability Assessment

About this course

The EC-Council Network Defense is a very advanced security-training program. Proper preparation is required before conducting the Network Defense class.

Instructor pre-requisites

You must have advanced knowledge of networking and system administration skills. MCSE and CCNA certifications are preferred.

- You must have worked on Firewalls, IDS and Anti-virus systems
- Excellent presentation skills
- Knowledge on hacking tools and their usage
- The ability to handle students effectively in the class
- Manage lecture / labs time effectively

The audience

You will find different types of audience sitting in your Network Defense class. They are:

• Forensic Investigators

• System Administrators

• Programmers

• Students

• IT Security Professionals

• IT Managers

Please DO NOT under-estimate the students' expectations. Do not assume everyone sitting in the class has knowledge on Linux skills, C++ knowledge, or TCP/IP concepts. You will find students who have never used Linux before, seen a Trojan in action, or knows how a virus works, etc. You will need to pitch your class based on the students' knowledge.

Why is the student sitting in your Network Defense class?

They want to learn about network defense methodologies and practice their knowledge with the various security tools.

Showcase of tools

You will find that every module is showcased with numerous tools. The students are exposed to many of the tools in that category. You are demonstrating the concept of each tool and not necessarily recommending their usage. The students are free to choose any tool that fits their task but they MUST be familiar with the complete showcase of tools that are available to them.

Book 5: Security and Vulnerability Assessment Content

The Security and Vulnerability Assessment book contains the following chapters:

Chapter 1: Web Security

Chapter 2: E-Mail Security

Chapter 3: Authentication, Encryption, and Digital Signatures

Chapter 4: Virtual Private Networks

Chapter 5: Creating Fault Tolerance

Chapter 6: Incident Response

Chapter 7: Disaster Recovery Planning and Risk Analysis

Chapter 8: Network Vulnerability Assessment

Security and Vulnerability Assessment Classroom Timing

Chapter 01 - How to Teach This Module

Web Security

Instructor notes:

Discuss why Web sites are often the easiest places for an attacker to enter the internal network.

Show how to secure Web servers, clients, and networks.

Chapter 02 - How to Teach This Module

E-Mail Security

Instructor notes:

Describe the main characteristics of e-mail.

Explain how to send and receive e-mails safely and securely.

Chapter 03- How to Teach This Module

Authentication, Encryption, and Digital Signatures

Instructor notes:

Discuss several technologies being used to authenticate users and encrypt data.

Introduce the concept of digital signatures.

Chapter 04 - How to Teach This Module

Virtual Private Networks

Instructor notes:

Discuss the basics of VPNs, including how they work and how to implement them.

Chapter 05 - How to Teach This Module

Creating Fault Tolerance

Instructor notes:

Describe how to make sure your systems are fault tolerant in order to better ensure the availability and reliability of resources.

Chapter 06 - How to Teach This Module

Incident Response

Instructor notes:

Explain how to recognize, report, and respond to incidents in order to minimize damage and resume normal operations.

Chapter 07 - How to Teach This Module

Disaster Recovery Planning and Risk Analysis

Instructor notes:

Discuss how to plan and execute effective disaster recovery, as well as how to analyze risk.

Chapter 08 - How to Teach This Module

Network Vulnerability Assessment

Instructor notes:

Describe various techniques to perform network vulnerability assessment.