Chapter 01 – Ethical Hacking Overview

Notes

Overview

This chapter provides an introduction to ethical hacking concepts, including the term ethical hacker, as well as penetration and security tests and the differences between them. You will learn the differences between the terms hacker, cracker, and script kiddies. Next, you will learn about the white box, black box, and gray box models for conducting penetration testing. Certifications are an important part of the professional life of any security tester; this chapter presents an overview of the major certification programs available for security professionals. Finally, you will learn about the legal aspect of ethical hacking; specifically, what they can and cannot do legally.

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to:

- Describe the role of an ethical hacker
- Describe what you can do legally as an ethical hacker
- Describe what you can’t do as an ethical hacker

Tips

Introduction to Ethical Hacking

1. Understand the following concepts: ethical hacking, penetration test, vulnerability assessment, and security test.

2. Understand the differences between penetration tests and security tests. This book will explain things from a security testing perspective.

The Role of Security and Penetration Testers

1. Understand the role of security and penetration testers by defining concepts such as hacker, cracker, ethical hacker, and script kiddies (i.e., packet monkeys).

2. Define the term script. The programming languages that are often used by penetration and security tester to write scripts include:
   a. Practical Extraction and Report Language (Perl)
   b. C language

3. The term “hacktivist” is used to define a person who hacks computer systems for political or social reasons.

Tip	What is a script? Look at the following Web site to learn more: http://frontier.userland.com/tutorial/whatIsAScript.

4. The requirements for a typical penetration tester.
    a. Perform vulnerability, attack, and penetration assessments in Internet, intranet, and wireless environments.
    b. Perform discovery and scanning for open ports and services.
    c. Apply appropriate exploits to gain access and expand access as necessary.
    d. Participate in activities involving application penetration testing and application source code review.
    e. Interact with the client as required throughout the engagement.
    f. Produce reports documenting discoveries during the engagement.
    g. Debrief with the client at the conclusion of each engagement.
    h. Participate in research and provide recommendations for continuous improvement.
    i. Participate in knowledge sharing.

Penetration-Testing Methodologies

1. See Figure 1-1 for the characteristics of the white box model and a network diagram that can be used during a white-box-based penetration test.
    a. The tester is told everything about the network topology and technology.
    b. The tester is authorized to interview IT personnel and company employees.
    c. The job of the tester is a little easier than in the black box model.

2. The black box model.
    a. The company staff does not know about the test.
    b. The tester is not given details about the network, so the burden is on the tester to find these details.
    c. The test can help determine whether the company's security personnel are able to detect an attack.

3. The gray box model.
    a. A hybrid of the white and black box models.
    b. The company gives the tester partial information.

4. Consider the main advantages and disadvantages of each model, as well as how to choose which model to use.

Certification Programs for Network Security Personnel

1. There are certification programs available in almost every area of network security.

2. The CompTIA's Security+ certification can help prepare an IT professional for a security certification.

3. Consider also the following certification programs:
    - Offensive Security Certified Professional (OSCP)
    - Certified Ethical Hacker (CEH) from the International Council of Electronic Commerce Consultants (EC-Council)
    - Open Source Security Testing Methodology Manual (OSSTMM) Professional Security Tester (OPST)
    - Certified Information Systems Security Professional (CISSP)

- SANS Institute offering training and certifications through Global Information Assurance Certification (GIAC)
    i. GIAC Certified Penetration Tester (GPEN)
    ii. GIAC Certified Web Application Tester (GWAPT)

4. Find out more about these certifications and pursue one or more of them.

What You Can Do Legally

1. The legal aspect of network security. Any penetration or security tester must always be aware of the legal consequences of his or her actions as a professional.

2. Laws change from state to state, and country to country. Always investigate and understand local laws before starting any ethical hacking job.

Laws of the Land

1. Consider the risk of having hacking tools installed on your computer. You should contact local law enforcement agencies before installing those tools.

2. See Table 1-1 for some of the most infamous recent hacking cases and how the U.S. government handled each case.

Is Port Scanning Legal?

1. Depending on your state laws, port scanning is either legal or illegal. The federal government does not consider port scanning a violation of the U.S. Constitution and allows each state to address these issues independently.

2. Research the current legal status of port scanning (and other similar activities) in your state. You might need to ask your local law enforcement agency for information.

3. The term “Acceptable Use Policy” is issued by your ISP. See Figure 1-2 for an example.

Federal Laws

1. Consider the computer hacking and intellectual property branch of the government and its role in computer crime.

2. See Table 1-2 for some federal laws regarding computer crimes.

Tip	Consider local laws regarding computer hacking and intellectual property issues versus federal laws.

What You Cannot Do Legally

1. Some actions that are not considered legal, include the following:
    a. Accessing a computer, destroying data, and copying information without the owner’s permission
    b. Installing worms or viruses
    c. Denying users access to network resources

2. It is important that you clearly understand that preventing the client’s employees from doing their jobs can be considered a criminal act, even for security testers.

Get It in Writing

1. Consider the problems associated with using (or not using) a contract that defines the purpose of your business as an independent contractor.

2. Generally, a written contract is just good business.

3. If you decide to use a contract, ask an attorney to look at the contract before sending or signing it.

Ethical Hacking in a Nutshell

1. The different skills required for any security tester:
   a. Knowledge of network and computer technology
   b. Ability to communicate with management and IT personnel
   c. An understanding of the laws that apply to your location
   d. Ability to apply the necessary tools to perform your tasks

Additional Resources

1. EC Council Website: https://www.eccouncil.org/
2. Certification for Ethical Hackers: http://www.gocertify.com/articles/ceh.html
3. Benefits of Penetration Testing: http://www.secmgmt.com/benefits-of-penetration-testing
4. The Pros and Cons of Ethical Hacking: http://www.cioupdate.com/trends/article.php/3303001
5. Hacking Laws: http://www.protectivehacks.com/hackinglaws.html

Key Terms

- **black box model**
- **Certified Ethical Hacker (CEH)**
- **Certified Information Systems Security Professional (CISSP)**
- **crackers**
- **ethical hackers**
- **Global Information Assurance Certification (GIAC)**
- **gray box model**
- **hacker**
- **hacktivist**
- **Institute for Security and Open Methodologies (ISECOM)**
- **Offensive Security Certified Professional (OCSP)**
- **Open Source Security Testing Methodology Manual (OSSTMM)**
- **OSSTMM Professional Security Tester (OPST)**
- **packet monkeys**
- **penetration test**
- **red team**
- **script kiddies**
- **security test**
- **SysAdmin, Audit, Network, Security (SANS) Institute**
- **vulnerability assessment**
- **white box model**