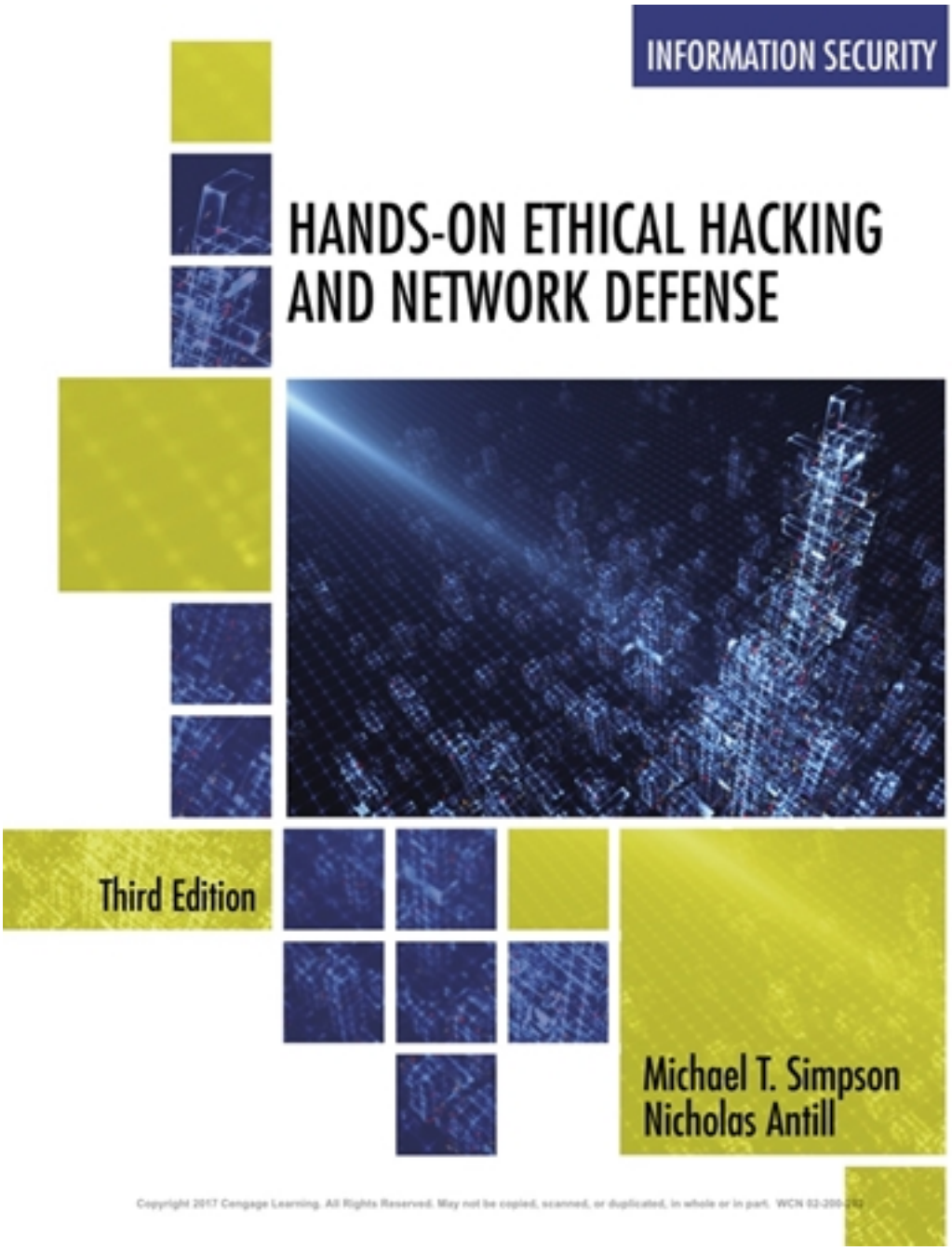
Solutions for Hands-On Ethical Hacking and Network Defense 3rd Edition by Simpson

CLICK HERE TO ACCESS COMPLETE Solutions



Solutions

Chapter 1 Solutions

Review Questions

1. The U.S. Department of Justice defines a hacker as which of the following?

a. A person who accesses a computer or network without the owner's permission

2. A penetration tester is which of the following?

c. A security professional who's hired to hack into a network to discover vulnerabilities

3. Some experienced hackers refer to inexperienced hackers who copy or use prewritten scripts or programs as which of the following? (Choose all that apply.)

c. Packet monkeys

d. Script kiddies

4. What three models do penetration or security testers use to conduct tests?

white box, black box, gray box

5. A team composed of people with varied skills who attempt to penetrate a network is referred to as which of the following?

d. Red team

6. How can you find out which computer crime laws are applicable in your state?

a. Contact your local law enforcement agencies.

7. What portion of your ISP contract might affect your ability to conduct a penetration test over the Internet?

c. Acceptable use policy

8. If you run a program in New York City that uses network resources to the extent that a user is denied access to them, what type of law have you violated?

d. Federal

9. Which federal law prohibits unauthorized access of classified information?

a. Computer Fraud and Abuse Act, Title 18

10. Which federal law prohibits intercepting any communication, regardless of how it was transmitted?

b. Electronic Communication Privacy Act

11. Which federal law amended Chapter 119 of Title 18, U.S. Code?

d. U.S. Patriot Act, Sec. 217: Interception of Computer Trespasser Communications

12. To determine whether scanning is illegal in your area, you should do which of the following?

c. Refer to state laws.

13. What organization offers the Certified Ethical Hacker (CEH) certification exam?

b. EC-Council

14. What organization designates a person as a CISSP?

a. International Information Systems Security Certification Consortium (ISC^2)

15. What is an OSCP?

b. Offensive Security Certified Professional

16. As a security tester, what should you do before installing hacking software on your computer?

a. Check with local law enforcement agencies.

17. Before using hacking software over the Internet, you should contact which of the following? (Choose all that apply.)

a. Your ISP

c. Local law enforcement authorities to check for compliance

18. Which organization issues the Top 20 list of current network vulnerabilities?

a. SANS Institute

19. A written contract isn't necessary when a friend recommends a client. True or False?

False

20. A penetration tester should possess which of the following attributes? (Choose all that apply.)

a. Good listening skills

b. Knowledge of networking and computer technology

c. Good verbal and written communication skills

d. An interest in securing networks and computer systems

Hands-On Activities

Activity 1-3: Identifying Computer Statutes in Your State or Country

Answers will vary. The memo should include state laws that might affect how a penetration test could be conducted as well as problems that might arise because of state laws. The memo could also ask that management draw up a contract addressing any risks or possible network degradation that might occur during testing.

Activity 1-4: Examining Federal Computer Crime Laws

Answers will vary. The summary should mention some key elements, such as (a)(2) "…intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains …." Section (g) states: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator…" The summary might also mention the possibility of a lawsuit. Students need to understand that this federal law addresses government computers and financial systems.

Activity 1-5: Understanding a Consulting Contract

Answers will vary. The summary could discuss the portions of the contract pertaining to confidential information and liability. An attorney could assist a consultant in adding verbiage to Section 4, stating that any passwords obtained during the penetration tests will not be disclosed, or Section 10 might be modified to include the possibility of loss of time caused by using scanning software.

Case Projects

Case Project 1-1: Determining Legal Requirements for Penetration Testing

The report could include the following possible steps:

1. Prepare a statement of work detailing what the penetration tests would include.
2. Verify that a contract exists between both companies authorizing you to perform the penetration test.
3. Review state laws for Hawaii and any applicable federal laws.
4. Discuss with management the formation of a red team.

Case Project 1-2: Hacktivist at Work

The paper is subjective in nature. The simple answer to the questions posed would be hacking is never justified. However, this should generate discussion and debates amongst the students.
Answers to questions:

1. Subjective question. Some might reference hacktivisim as civil disobedience.
2. Subjective. What is too far for someone might be not far enough for someone else.
3. The simple answer is no. Hacking is illegal.