Hands-On Ethical Hacking and Network Defense, 3rd Edition

Chapter 1

Ethical Hacking Overview

Objectives

After completing this chapter, 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

© Cengage Learning 2017

Introduction to Ethical Hacking

- Ethical hackers
  - Hired by companies to perform penetration tests
- Penetration test
  - Attempt to break into a company's network to find the weakest link
- Vulnerability assessment
  - Tester attempts to enumerate all vulnerabilities found in an application or on a system
- Security test
  - Besides a break in attempt; includes analyzing company's security policy and procedures

© Cengage Learning 2017

The Role of Security and Penetration Testers

- Hackers
  - Access computer system or network without authorization
    - Breaks the law; can go to prison
- Crackers
  - Break into systems to steal or destroy data
    - U.S. Department of Justice calls both hackers
- Ethical hacker
  - Performs most of the same activities with owner's permission

© Cengage Learning 2017

The Role of Security and Penetration Testers

- Script kiddies or packet monkeys
  - Younger, inexperienced hackers who copy codes from knowledgeable hackers
- Programming languages used by experienced penetration testers
  - Python, Ruby, Practical Extraction and Report Language (Perl), C language
- Script
  - Set of instructions
  - Runs in sequence to perform tasks

© Cengage Learning 2017

The Role of Security and Penetration Testers

- Hacktivist
  - A person who hacks computer systems for political or social reasons
- Penetration testers usually have:
  - A laptop computer with multiple OSs and hacking tools

© Cengage Learning 2017

The Role of Security and Penetration Testers

- Job requirements for a penetration tester might include:
  - Perform vulnerability, attack, and penetration assessments in Intranet and wireless environments
  - Perform discovery and scanning for open ports
  - Apply appropriate exploits to gain access
  - Participate in activities involving application penetration
  - Produce reports documenting discoveries
  - Debrief with the client at the conclusion

© Cengage Learning 2017

Penetration-Testing Methodologies

- White box model
  - Tester is told about network topology and technology
    - May be given a floor plan
  - Tester is permitted to interview IT personnel and company employees
    - Makes tester's job a little easier
- Black box model
  - Staff does not know about the test
  - Tester is not given details about technologies used
    - Burden is on tester to find details
  - Tests security personnel's ability to detect an attack

© Cengage Learning 2017

Penetration-Testing Methodologies

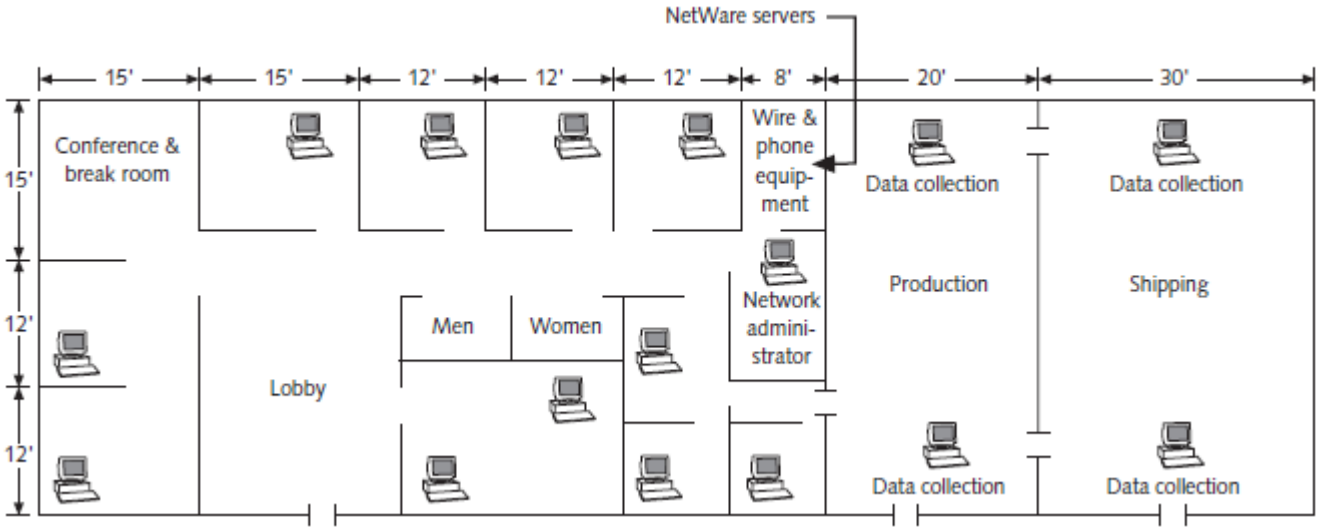

Figure 1-1 A sample floor plan

© Cengage Learning 2017

Penetration-Testing Methodologies

- Gray box model
  - Hybrid of the white and black box models
  - Company gives tester partial information (e.g., OSs are used, but no network diagrams)

© Cengage Learning 2017

Certification Programs for Network Security Personnel

- Certification programs
  - Available in almost every area of network security
- Minimum certification
  - CompTIA Security+ or equivalent knowledge
    - Prerequisite for Security+ certification is CompTIA Network+

© Cengage Learning 2017

Offensive Security Certified Professional

- OSCP
  - An advanced certification that requires students to demonstrate hands-on abilities to earn their certificates
  - Covers network and application exploits
  - Gives students experience in developing rudimentary buffer overflows, writing scripts to collect and manipulate data, and trying exploits on vulnerable systems

© Cengage Learning 2017

Certified Ethical Hacker

- Developed by the International Council of Electronic Commerce Consultants (EC-Council)
  - Based on 22 domains (subject areas)
  - Web site: *www.eccouncil.org*
- Most likely be placed on a team that conducts penetration tests
  - Called a Red team
    - Conducts penetration tests
    - Composed of people with varied skills
    - Unlikely that one person will perform all tests

© Cengage Learning 2017

OSSTMM Professional Security Tester (OPST)

- Open Source Security Testing Methodology Manual (OSSTMM) Professional Security Tester
  - Designated by the Institute for Security and Open Methodologies (ISECOM)
  - Based on Open Source Security Testing Methodology Manual (OSSTMM)
    - Written by Peter Herzog
  - Five main topics (i.e., professional, enumeration, assessments, application, and verification)
  - Web site: *www.isecom.org*

© Cengage Learning 2017

Certified Information Systems Security Professional

- CISSP
  - Issued by the International Information Systems Security Certification Consortium (ISC^2)
  - Not geared toward technical IT professionals
  - Tests security-related managerial skills
    - Usually more concerned with policies and procedures
  - Consists of ten domains
  - Web site: *www.isc2.org*

© Cengage Learning 2017

SANS Institute

- SysAdmin, Audit, Network, Security (SANS) Institute
  - Offers training and IT security certifications through Global Information Assurance Certification (GIAC)
- Top 25 Software Errors list
  - One of the most popular SANS Institute documents
  - Details most common network exploits
  - Suggests ways of correcting vulnerabilities
  - Web site: *www.sans.org*

© Cengage Learning 2017

Which Certification is Best?

- Penetration testers and security testers
  - Need technical skills to perform duties effectively
  - Must also have:
    - A good understanding of networks and the role of management in an organization
    - Skills in writing and verbal communication
    - Desire to continue learning
- Danger of certification exams
  - Some participants simply memorize terminology
    - Don’t have a good grasp of subject matter

© Cengage Learning 2017

What Can You Do Legally

- Laws involving technology change as rapidly as technology itself
  - Keep abreast of what's happening in your area
    - Find out what is legal for you locally
  - Be aware of what is allowed and what you should not or cannot do
    - Laws vary from state to state and country to country
  - Example: In some states, the possession of lockpicking tools constitutes a crime

© Cengage Learning 2017

Laws of the Land

- Some hacking tools on your computer might be illegal
  - Contact local law enforcement agencies before installing hacking tools
- Laws are written to protect society
  - Written words are open to interpretation
  - Example: In Hawaii, the state must prove the person charged had the “intent to commit a crime”
- Government is getting more serious about cybercrime punishment

© Cengage Learning 2017

Laws of the Land

State and year	Description
Massachusetts, 2013	Aaron Swartz was charged with 13 felony counts under the Computer Fraud and Abuse Act after connecting to MIT's computer networks and downloading 2.7 million articles from JSTOR, a digital library of academic journals. *Note*: The movie *Internet's Own Boy*, the story of Aaron Swartz, is available free at *https://www.youtube.com/watch?v=vXr-2hwTk58*.
Massachusetts, 2014	Cameron Lacroix, 25, of New Bedford, Massachusetts, was sentenced to 4 years in prison and 3 years of supervised release for computer hacking and credit card theft. Lacroix, a community college student, hacked into law enforcement agencies' servers that contained sensitive information, such as arrest warrants, police reports, and sex offender information. He also accessed the Massachusetts chief of police's e-mail account and hacked into his college's server to change his grades and those of two other students.
Georgia, 2014	Sergei Nicolaevich Tsurikov, 30, of Tallinn, Estonia, was sentenced to 11 years in prison for conspiracy to commit wire fraud and computer intrusion. U.S. Attorney Sally Quillian Yates said the hack was one of the most sophisticated and organized computer fraud attacks ever conducted. It involved more than 44 counterfeit payroll debit cards and the withdrawal of more than $9 million.
Delaware, 2014	Nathan Leroux, 20, of Bowie, Maryland; Sanadodeh Nesheiwat, 28, of Washington, New Jersey; David Pokora, 22, of Mississauga, Ontario, Canada; and Austin Alcala, 18, of McCordsville, Indiana, were indicted for stealing gaming technology and Apache helicopter training software. The four hackers used SQL injection (covered in Chapter 10) and stolen usernames and passwords to hack into Microsoft Corporation, Epic Games Inc., Valve Corporation, Zombie Studios, and the U.S. Army. After they had access to computer systems, they stole unreleased software, trade secrets, source programming code, and other proprietary information. The cyber theft included the popular Xbox game *Call of Duty: Modern Warfare 3*.

Table 1-1 An overview of recent hacking cases (continues)

© Cengage Learning 2017

Laws of the Land

Texas, 2014	Fidel Salinas, 27, of Donna, Texas, an alleged member of the hacktivist group Anonymous, faces up to 10 years in federal prison for allegedly cyberstalking a female victim, attempting to gain unauthorized access to her Web site, and attempting to open user accounts in her name without her permission. The indictment also claims that Salinas made more than 14,000 hacking attempts on the administration page of the Hidalgo County Web site's server, causing a denial of service (discussed in Chapter 3) and incurring a cost of more than $10,000 to respond to the attack.
New York, 2014	Lauri Love, 30, of Suffolk, England, was charged with hacking into the Federal Reserve. He allegedly used SQL injection to exploit a vulnerability in the Federal Reserve's servers; stole confidential information, such as names, phone numbers, and e-mail addresses; and posted the information to a Web site he had already hacked. He's believed to have hacked into thousands of networks, including those of the U.S. Army and NASA. If convicted, he faces up to 10 years in a federal prison.
Wisconsin, 2014	James L Santelle, 24, of Postville, Iowa, was sentenced to 24 months' probation and ordered to pay $110,932.71 in restitution for participating in a distributed denial-of-service attack against the Angel Soft (bathroom tissue) Web site. The company claimed it lost several hundred thousand dollars over a 3-day period as a result.

Table 1-1 An overview of recent hacking cases

Table 1-1 An overview of recent hacking cases (cont'd)

© Cengage Learning 2017

Is Port Scanning Legal?

- Some states consider it legal
  - Not always the case
  - Be prudent before using penetration-testing tools
- Federal government does not see it as a violation
  - Allows each state to address it separately
    - Research state laws
- Read your ISP's "Acceptable Use Policy"

© Cengage Learning 2017

Is Port Scanning Legal?

Acceptable Use Policy

(a) PacInfo Net makes no restriction on usage provided that such usage is legal under the laws and regulations of the State of Hawaii and the United States of America and does not adversely affect PacInfo Net customers. Customer is responsible for obtaining and adhering to the Acceptable Use Policies of any network accessed through PacInfo Net services.

(b) PacInfo Net reserves the right without notice to disconnect an account that is the source of spamming, abusive, or malicious activities. There will be no refund when an account is terminated for these causes. Moreover, there will be a billing rate of $125 per hour charged to such accounts to cover staff time spent repairing subsequent damage.

(c) Customers are forbidden from using techniques designed to cause damage to or deny access by legitimate users of computers or network components connected to the Internet. PacInfo Net reserves the right to disconnect a customer site that is the source of such activities without notice.

Figure 1-2 An example of an acceptable use policy

© Cengage Learning 2017

Is Port Scanning Legal?

- IRC “bot”
  - Program that sends automatic responses to users
  - Gives the appearance of a person being present
- Some ISP’s may prohibit the use of IRC bots

© Cengage Learning 2017

Federal Laws

Federal law	Description
The Computer Fraud and Abuse Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 47, Fraud and False Statements, Sec. 1030: Fraud and related activity in connection with computers	This law makes it a federal crime to access classified information or financial information without authorization.
Electronic Communication Privacy Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications, Sec. 2510: Definitions and Sec. 2511: Interception and disclosure of wire, oral, or electronic communications prohibited	These laws make it illegal to intercept any communication, regardless of how it was transmitted.
U.S. PATRIOT Act, Sec. 217. Interception of Computer Trespasser Communications	This act largely sought to amend previous privacy and surveillance laws and fund government surveillance programs. Among many other things, it created new ways for the government to monitor individuals and allowed victims of cybercrimes to monitor the activity of trespassers on their systems.
Homeland Security Act of 2002, H.R. 5710, Sec. 225: Cyber Security Enhancement Act of 2002	This amendment to the Homeland Security Act of 2002 specifies sentencing guidelines for certain types of computer crimes.
The Computer Fraud and Abuse Act. Title 18, Crimes and Criminal Procedure, Sec. 1029: Fraud and related activity in connection with access devices	This law makes it a federal offense to manufacture, program, use, or possess any device or software that can be used for unauthorized use of telecommunications services.

Table 1-2 Federal computer crime laws

© Cengage Learning 2017

Federal Laws

Federal law	Description
Stored Wire and Electronic Communications and Transactional Records Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 121, Stored Wire and Electronic Communications and Transactional Records Act, Sec. 2701: Unlawful access to stored communications (a) Offense. Except as provided in subsection of this section whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; Sec. 2702: Disclosure of contents	This law defines unauthorized access to computers that store classified information.

Table 1-2 **Federal computer crime laws (*continued*)**

© Cengage Learning 2017

What You Cannot Do Legally

- Illegal actions:
  - Accessing a computer without permission
  - Destroying data without permission
  - Copying information without permission
  - Installing viruses that deny users access to network resources
- Be careful your actions do not prevent client's employees from doing their jobs

© Cengage Learning 2017

Get It In Writing

- Using a contract is good business
  - May be useful in court
- Books on working as an independent contractor
  - *Getting Started as an Independent Computer Consultant* by Mitch Paioff and Melanie Mulhall
  - *The Consulting Bible: Everything You Need to Know to Create and Expand a Seven-Figure Consulting Practice* by Alan Weiss
- Internet can also be a helpful resource
  - Free modifiable templates
- Have an attorney read your contract before signing

© Cengage Learning 2017

Ethical Hacking in a Nutshell

- Skills needed to be a security tester
  - Knowledge of network and computer technology
  - Ability to communicate with management and IT personnel
  - An understanding of the laws in your location
  - Ability to apply necessary tools to perform your tasks

© Cengage Learning 2017

Summary

- Companies hire ethical hackers to perform penetration tests
  - Penetration tests discover vulnerabilities in a network
  - Security tests are performed by a team of people with varied skills
- Penetration test models
  - White box model
  - Black box model
  - Gray box model

© Cengage Learning 2017

Summary

- Security testers can earn certifications
  - CEH
  - CISSP
  - OPST
- As a security tester, be aware
  - What you are legally allowed or not allowed to do
- ISPs may have an acceptable use policy
  - May limit ability to use tools

© Cengage Learning 2017

Summary

- Laws should be understood before conducting a security test
  - Federal laws
  - State laws
- Get it in writing
  - Use a contract
  - Have an attorney read the contract
- Understand tools available to conduct security tests
  - Learning how to use them should be a focused and methodical process

© Cengage Learning 2017