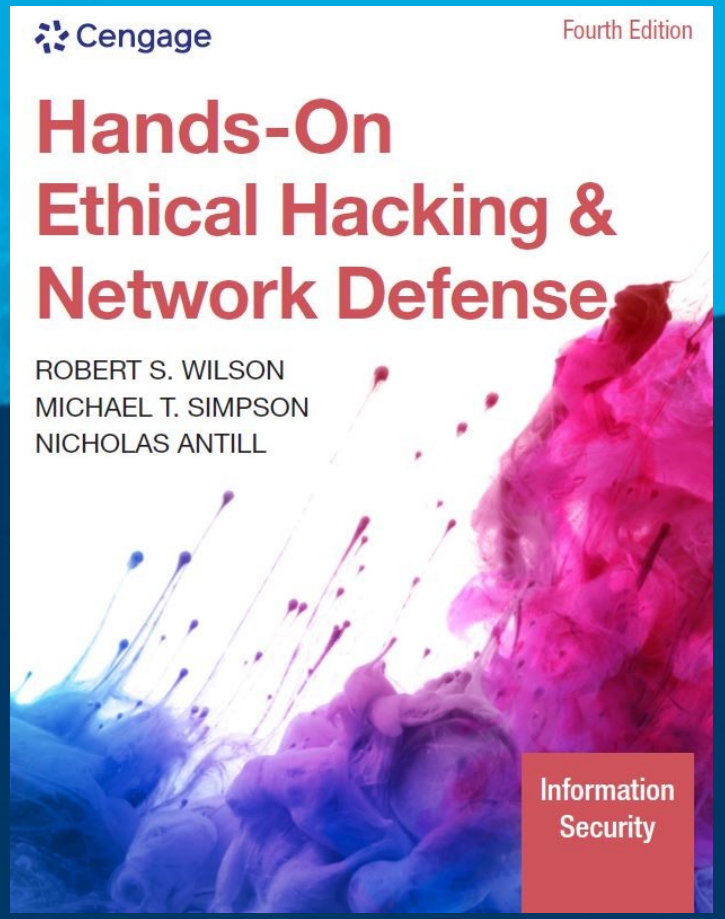

Hands-On Ethical Hacking and Network Defense, Edition 4

Module 1: Ethical Hacking Overview

CENGAGE

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 weak links
- **Vulnerability assessment**
  - Tester attempts to enumerate all vulnerabilities found in an application or on a system
- **Security test**
  - Tester analyzes a company's security policy and procedures
  - Reports any vulnerabilities to management

The Role of Security and Penetration Testers (1 of 5)

- **Hackers** access computer system or network
  - Without the authorization of the systems owner
    - Considered as breaking the law; can go to prison
- **Crackers**
  - Break into systems to steal or destroy data
  - The U.S. Department of Justice
    - Labels all illegal access to a computer or network systems as hacking
- Ethical hacker
  - Performs most of the same activities a hacker does
    - With the permission of the owner or company

The Role of Security and Penetration Testers (2 of 5)

- **Script kiddies** or **packet monkeys**
  - Derogatory terms to refer to younger, inexperienced people
  - They copy code or use tools created by knowledgeable programmers without understanding how they work
- Programs or scripts used by experienced penetration testers
  - To carry out attacks
  - Python, Ruby, Perl, or C
  - Script
    - A set of instructions
    - Runs in sequence to perform tasks on a computer system

The Role of Security and Penetration Testers (3 of 5)

- **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

The Role of Security and Penetration Testers (4 of 5)

- Job requirements for a penetration tester might include:
  - Perform vulnerability, attack, and penetration assessments
    - In Internet, Intranet, and wireless environments
  - Perform discovery and scanning
    - For open ports and services
  - Apply appropriate exploits
    - To gain access and expand access as necessary

The Role of Security and Penetration Testers (5 of 5)

- Participate in activities
  - Involving application penetration testing and application source code review
- Interact with the client as required throughout the engagement
- Produce reports documenting discoveries during the engagement
- Debrief with the client at the conclusion of each engagement
- Participate in research and provide recommendations
  - For continuous improvement
- Participate in knowledge sharing
- Demonstrate a good understanding of current country, state, and city cyber laws

Penetration-Testing Methodologies (1 of 3)

- **White box model**
  - The tester is told what network topology and technology the company is using
    - May be given a floor plan
  - Tester is permitted to interview IT personnel and company employees
    - Makes the penetration tester's job easier
- **Black box model**
  - Staff is not aware of the test
  - Tester is not given any diagrams or details about the technologies used
    - Burden is on the tester to find details using different techniques
  - Tests security personnel's ability to detect an attack

Penetration-Testing Methodologies (2 of 3)

- **Gray box model**
  - Hybrid of the white and black box models
  - Company gives tester only partial information
    - Example: OSs are used, but no network diagrams

Penetration-Testing Methodologies (3 of 3)

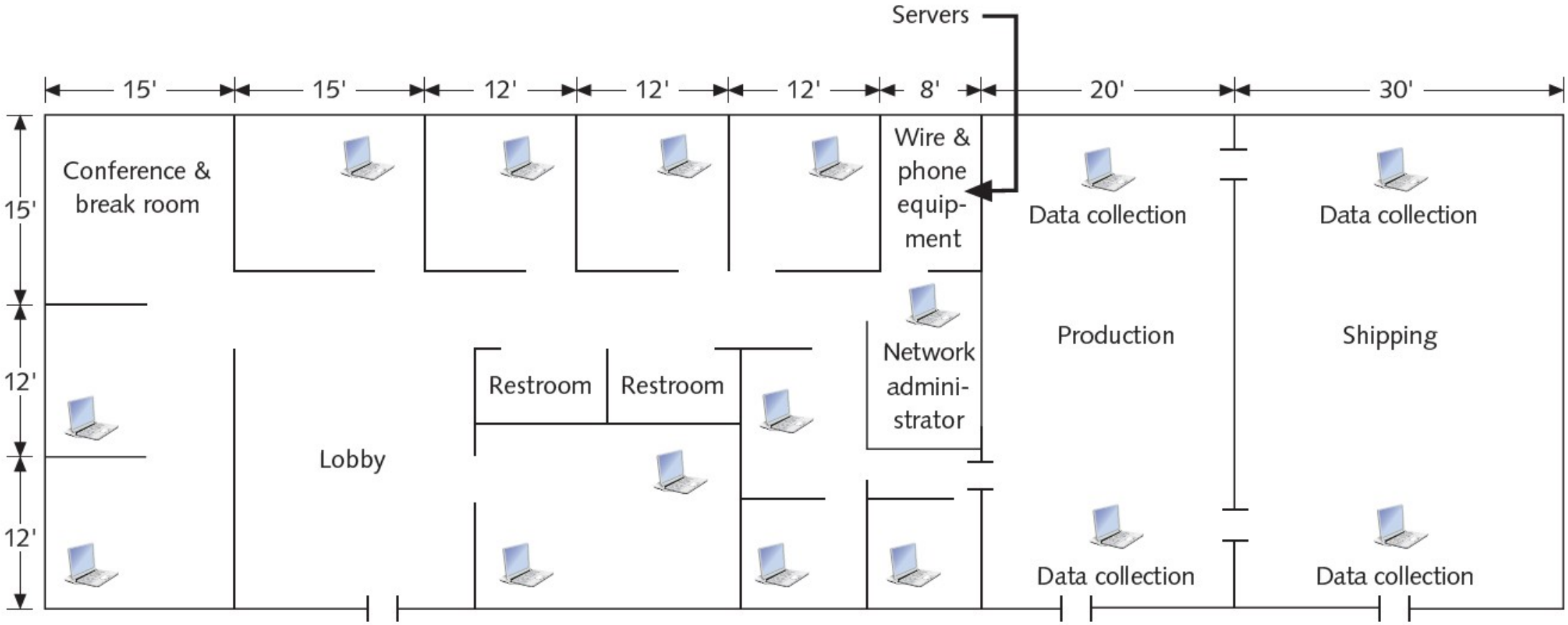

Figure 1-1 A sample floor plan

Certification Programs for Network Security Personnel

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

CompTIA PenTest+

- Advanced certification that verifies successful candidates have the knowledge and skills required to:
  - Plan and scope an assessment
  - Understand legal and compliance requirements
  - Perform vulnerability scanning and penetration testing
  - Analyze data
  - Effectively report and communicate results

Offensive Security Certified Professional (OSCP)

- 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
    - Trying exploits on vulnerable systems

Certified Ethical Hacker

- Developed by the International Council of Electronic Commerce Consultants (EC-Council)
  - The multiple-choice **Certified Ethical Hacker** (CEH) exam is based on 22 domains the tester must be familiar with
  - EC-Council website
- Most likely to be placed on a team that conducts penetration tests
  - Called a **Red team**
    - Composed of people with varied skills who perform the tests
    - Unlikely that one person will perform all tests

O S S T M M Professional Security Tester (OPST)

- Open Source Security Testing Methodology Manual (O S S T M M) Professional Security Tester
  - Designated by the **Institute for Security and Open Methodologies (ISECOM)**
  - The OPST certification uses the **O S S T M M** as its standardized methodology
  - Written by Peter Herzog
  - Five main topics (i.e., professional, enumeration, assessments, application, and verification)
  - ISECOM website

Certified Information Systems Security Professional (C I S S P)

- C I S S P
  - 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 questions from ten domains
  - ISECOM website

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
  - SANS website

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 or complex concepts

What You Can Do Legally

- Laws involving technology change as rapidly as technology itself:
  - As a security tester, you should:
    - 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

Laws of the Land

- Having 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 that the person charged with committing a crime on a computer had the “intent to commit a crime”
- Make sure you’re aware of the dangers of being a security tester

Overview of Recent Hacking Cases (1 of 3)

State and Year	Description
Kansas, 2021	A resident of Ellsworth County, Kansas, was charged with one count of tampering with a public water system and one count of reckless damage to a protected computer during unauthorized access. The indictment alleged that a former employee knowingly accessed the Ellsworth County Rural Water District's protected computer system without authorization. During this unauthorized access, the accused allegedly performed activities that shut down the processes at the facility, which affected cleaning and disinfecting procedures, with the intention of harming the public drinking water system. If found guilty, the accused faces up to 25 years in prison and a fine of up to $500,000 for illegally accessing the protected computer and tampering with the water system.
California, 2021	A former employee of an IT consulting firm accessed the server of a company in Carlsbad, California, and deleted more than 1,200 of the company's 1,500 Microsoft user accounts. The employee was apparently retaliating for being fired. The attack affected most of the Carlsbad company's employees so that they could not access email or other network services, effectively shutting down the company for days and causing continuous IT problems for three months. The former contractor was sentenced in federal court to two years in prison and ordered to pay the company more than $560,000.

Overview of Recent Hacking Cases (2 of 3)

State and Year	Description
Nevada, 2021	A Russian national offered $1 million to an employee of Tesla's electric battery plant in Nevada in a scheme to have the insider introduce malicious software into the company's computer network. The malware attack was designed to extract data from the company's network and then demand a ransom for its return. The ransomware case is considered unusual because it involves face-to-face bribery rather than anonymous hacking via the Internet. Such an attack typically carries a penalty of up to five years in prison and a $250,000 fine.
Atlanta, 2021	A Cypriot national hacked into major websites as a teenager and threatened that he would release stolen user information unless the websites paid a ransom. The hacker identified vulnerable websites, including those for sports news and online games, and then stole personally identifiable information from user and customer databases. He became the first Cypriot national extradited from Cyprus to the United States, and paid nearly $600,000 in restitution to his victims. In addition, he has been sentenced to federal prison for at least three years.

Overview of Recent Hacking Cases (3 of 3)

State and Year	Description
New Jersey, 2021	While employed at a data analytics and risk assessment firm based in New Jersey, a resident of Moorefield, Nebraska, obtained confidential information that belonged to the firm—including names, passwords, email addresses, and telephone numbers of clients—and then attempted to sell the information. Nearly two years after his arrest, the hacker was sentenced to three years of supervised release and ordered to pay restitution of more than $290,000.
Florida, 2021	A Florida high school conducted online voting to select a homecoming queen but found out that an assistant principal in the school district manipulated the vote electronically. She accessed a network database storing confidential student information—including grades, medical history, and credentials—and then used the credentials to cast ballots in favor of her daughter. The pair were arrested and charged with fraudulently accessing confidential student information. The daughter was expelled from the high school, and her mother was suspended from her job as they awaited sentencing.

Is Port Scanning Legal? (1 of 3)

- Some states consider it noninvasive or nondestructive in nature and deem it legal
  - Not always the case
  - Be prudent before using penetration-testing tools
- Federal government does not see infringements, such as port scanning, as a violation of the U.S. Constitution
  - Allows each state to address them separately
    - Research your state laws before using what you learn
- Read your ISP's "Acceptable Use Policy"

Is Port Scanning Legal? (2 of 3)

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 1-3 Sample acceptable use policy

Is Port Scanning Legal? (3 of 3)

- Internet Relay Chat (IRC) bot
  - Program that sends automatic responses to users
  - Gives the appearance of a person on the other side of a connection
- Virtual private network (VPN)
  - Consider whether your computer is connected to your business network by a VPN
    - Many people work from home using a VPN to connect to their work network
    - May end up scanning work computers, which could be problematic

Federal Computer Crime Laws (1 of 4)

Federal law	Description
The No Electronic Theft Act (P.L. 105 to 147)	Extends the reach of criminal copyright law to specifically include electronic means as one method for committing the crime (17 U.S.C. § 501(a)(1)). The act also expands the scope of the criminal conduct covered under this crime, allowing for prosecutions without showing that the distributor of the copyrighted material profited from the activity.
The Economic Espionage Act (EEA)	The EEA offers trade secret protection to both businesses and the government. The significance of information to society and the problems that are attached to protecting this information make the EEA an important step in how the law can provide protection from computer crime.
The Computer Fraud and Abuse Act (CFAA). 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.

Federal Computer Crime Laws (2 of 4)

Federal law	Description
The Identity Theft and Assumption Deterrence Act (ITADA) [18 U.S.C. Section 1028(a)(7)]	This act criminalizes identity theft and allows courts to assess the losses suffered by individual consumers. While the CFAA covers certain aspects of identity theft, the ITADA addresses restitution and relief for the victims.
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 seeks to amend previous privacy and surveillance laws and fund government surveillance programs. It also specifies ways for the government to monitor individuals and allows victims of cybercrimes to monitor the activity of trespassers on their systems.

Federal Computer Crime Laws (3 of 4)

Federal law	Description
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.

Federal Computer Crime Laws (4 of 4)

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.

What You Cannot Do Legally

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

Get It in Writing

- Using a contract is good business
  - May be useful in court
- Books on working as an independent contractor
  - *Getting Started in Consulting* by Alan Weiss
  - *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
  - Will find free modifiable contract templates
- Have an attorney read your contract before signing

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 applicable in your location
  - Ability to apply necessary tools to perform your tasks