

# Chapter 1: Ethical Hacking Overview

## Objectives

Describe the role of an ethical hacker

Describe what you can do legally as an ethical hacker

Describe what you cannot do as an ethical hacker

## Introduction to Ethical Hacking

### ■ Ethical hackers

- Employed by companies to perform penetration tests

### ■ Penetration test

- Legal attempt to break into a company's network to find its weakest link
- Tester only reports findings, does not solve problems

### ■ Security test

- More than an attempt to break in; also includes analyzing company's security policy and procedures
- Tester offers solutions to secure or protect the network

## 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 but with owner's permission

## The Role of Security and Penetration Testers

Script kiddies or packet monkeys

- Young inexperienced hackers
- Copy codes and techniques from knowledgeable hackers

Experienced penetration testers write programs or scripts using these languages

- Practical Extraction and Report Language (Perl), C, C++, Python, JavaScript, Visual Basic, SQL, and many others

Script

- Set of instructions that runs in sequence

## It Takes Time to Become a Hacker

- This class alone won't make you a hacker, or an expert  
It might make you a script kiddie
- It usually takes years of study and experience to earn respect in the hacker community
- It's a hobby, a lifestyle, and an attitude  
A drive to figure out how things work

## The Role of Security and Penetration Testers

Tiger box

- Collection of OSs and hacking tools
- Usually on a laptop
- Helps penetration testers and security testers conduct vulnerabilities assessments and attacks

## Penetration-Testing Methodologies

White box model

# Chapter 1: Ethical Hacking Overview

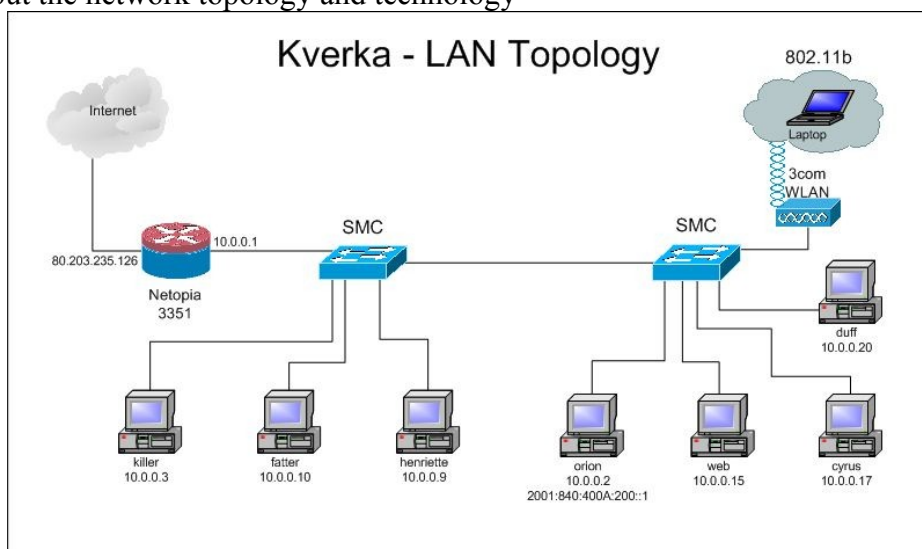
- Tester is told everything about the network topology and technology

## Network diagram

- Tester is authorized to interview IT personnel and company employees
- Makes tester's job a little easier

## Network Diagram

- From



ratemynetworkdiagram.com (Link Ch 1g)

## This is a Floor Plan

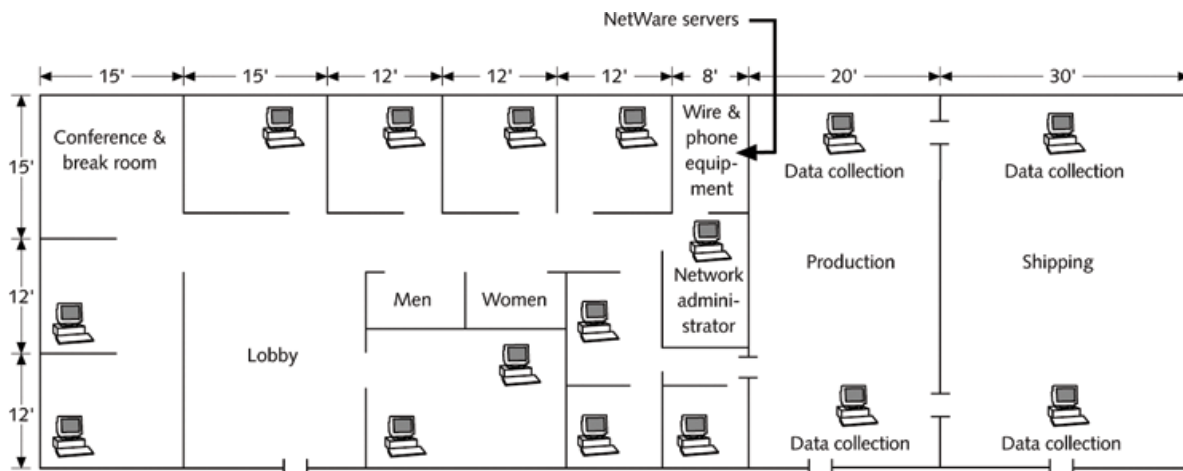


Figure 1-1 A sample network diagram

## Penetration-Testing Methodologies

### Black box model

- Company staff does not know about the test
- Tester is not given details about the network
- Burden is on the tester to find these details
  - Tests if security personnel are able to detect an attack

## Penetration-Testing Methodologies

### Gray box model

- Hybrid of the white and black box models
- Company gives tester partial information

## Chapter 1: Ethical Hacking Overview

### **Certification Programs for Network Security Personnel**

Certification programs available in almost every area of network security

Basics:

- CompTIA Security+ (CNIT 120)
- Network+ (CNIT 106 or 201)

## Chapter 1: Ethical Hacking Overview

### Take Certification Tests Here

CNIT is a Prometric Vue testing center

- Certification tests are given in S214
- CompTIA and Microsoft
- The next tests will be in the second week of April, right after Spring Break

—Email [sbowne@ccsf.edu](mailto:sbowne@ccsf.edu) if you want to take a test

### Certified Ethical Hacker (CEH)

#### •But see **Run Away From The CEH Certification**

- Link Ch 1e on my Web page

### OSSTMM Professional Security Tester (OPST)

Designated by the Institute for Security and Open Methodologies (ISECOM)

- Uses the Open Source Security Testing Methodology Manual (OSSTMM)
- Test is only offered in Connecticut and outside the USA, as far as I can tell
- See links Ch 1f and Ch 1h on my Web page

### Certified Information Systems Security Professional (CISSP)

Issued by the International Information Systems Security Certifications Consortium (ISC2)  
Usually more concerned with policies and procedures than technical details

Web site

- [www.isc2.org](http://www.isc2.org)

### SANS Institute

SysAdmin, Audit, Network, Security (SANS)

Offers certifications through Global Information Assurance Certification (GIAC)

Top 20 list

- One of the most popular SANS Institute documents
- Details the most common network exploits
- Suggests ways of correcting vulnerabilities

Web site

- [www.sans.org](http://www.sans.org) (links Ch 1i & Ch 1j)

### What You Can Do Legally

Laws involving technology change as rapidly as technology itself

Find what is legal for you locally

- Laws change from place to place

Be aware of what is allowed and what is not allowed

### Laws of the Land

Tools on your computer might be illegal to possess

Contact local law enforcement agencies before installing hacking tools

Written words are open to interpretation

Governments are getting more serious about punishment for cybercrimes



## Recent Hacking Cases

### Is Port Scanning Legal?

Some states deem it legal

Not always the case

Federal Government does not see it as a violation

- Allows each state to address it separately

Read your ISP's "Acceptable Use Policy"

- IRC "bots" may be forbidden
  - Program that sends automatic responses to users
  - Gives the appearance of a person being present

### CCSF Computer Use Policy

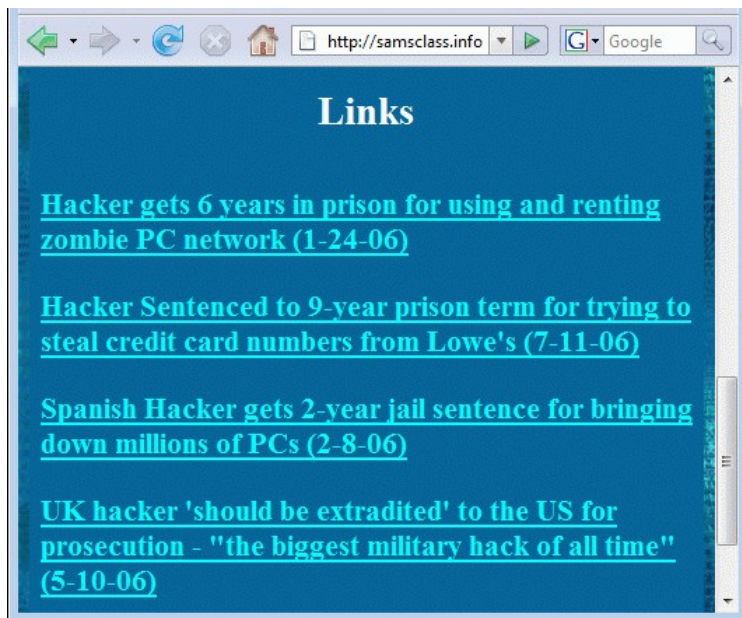
### Federal Laws

Federal computer crime laws are getting more specific

- Cover cybercrimes and intellectual property issues

Computer Hacking and Intellectual Property (CHIP)

- New government branch to address cybercrimes and intellectual property issues



**Table 1-2** Federal computer crime 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	This law prevents you from intercepting any communication, regardless of how it was transmitted.
U.S. Patriot Act Sec. 217. Interception of Computer Trespasser Communications	This law amends Chapter 119 of Title 18, U.S. Code.
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

Accessing a computer without permission is illegal

Other illegal actions

- Installing worms or viruses
- Denial of Service attacks
- Denying users access to network resources

Be careful your actions do not prevent customers from doing their jobs

### Anti-Spam Vigilantes: Lycos

- Ch 111: Lycos starts anti-spam screensaver plan: Dec 2, 2004
- Ch 112: Lycos Pulls Anti-Spam 'Vigilante' Campaign -- Dec 3, 2004

## Chapter 1: Ethical Hacking Overview

- Ch 113: Lycos's Spam Attack Network Dismantled -- Spammers sent the DOS packets back to Lycos -- Dec 6, 2004

### **Anti-Spam Vigilantes: Blue Frog**

- Ch 1m: Blue Frog begins its "vigilante approach" to fight spam -- July, 2005
- Ch 1n: Russian spammer fights back, claims to have stolen Blue Frog's database, sends threatening email -- DOS attack in progress -- May 2, 2006
- Ch 1o: Blue Frog compromised and destroyed by attacks, urgent instructions to uninstall it, the owners have lost control -- May 17, 2006

### **Anti-Spam Vigilantes: The Future**

- Ch 1p: Call for help creating distributed, open-source Blue Frog replacement -- May 17, 2006  
Not in textbook, see links on my page ([samsclass.info](http://samsclass.info))

### **Get It in Writing**

Using a contract is just good business

Contracts may be useful in court

Books on working as an independent contractor

- The Computer Consultant's Guide by Janet Ruhl
- Getting Started in Computer Consulting by Peter Meyer

Internet can also be a useful resource

Have an attorney read over your contract before sending or signing it

### **Ethical Hacking in a Nutshell**

What it takes to be a security tester

- Knowledge of network and computer technology
- Ability to communicate with management and IT personnel
- Understanding of the laws
- Ability to use necessary tools

Last modified 1-20-07 0:12