



Hands-On Ethical Hacking and Network Defense

Chapter 1

Ethical Hacking Overview

Last modified 8-21-14

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

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

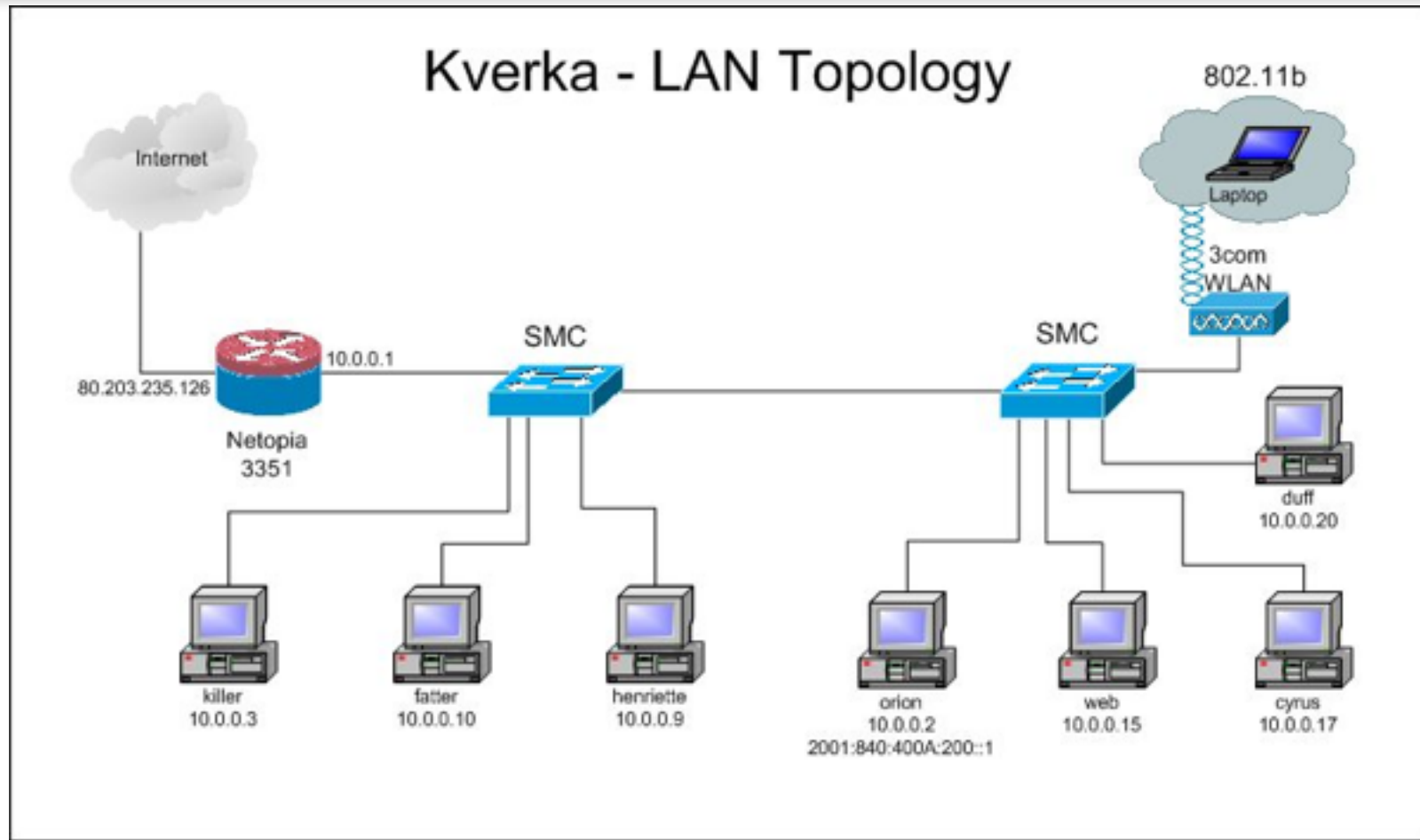
The Role of Security and Penetration Testers

- 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
 - 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)

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

Certification Programs

Certification Programs for Network Security Personnel

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



The screenshot shows the CompTIA website interface. At the top, the CompTIA logo is displayed with the tagline "the Computing Technology Industry Association". A navigation bar includes links for "Certification Home", "Certification Resources", "About CompTIA", "News", "Customer Support", "CompTIA Online Store", and "Search". The main content area features a sidebar with "CompTIA Certifications" and a list of links: "CompTIA Security+ Home", "CompTIA Security+ at a Glance", "CompTIA Security+ and Your Career", "Download Security+ Objectives", and "Prepare for Exam". The central focus is the "CompTIA Security+™ Certification" section, which includes a photo of a man in a light blue shirt and a quote from Steve Jordan, Vice President of System Engineering & Consulting at McAfee, Inc., praising the certification as a benchmark for foundational skills.

CompTIA Web sites : CompTIA Certifications | the Association | CompTIA Members

CompTIA
the Computing Technology Industry Association

Certification Home Certification Resources About CompTIA News Customer Support CompTIA Online Store Search

CompTIA Certifications

- > CompTIA Security+ Home
- > CompTIA Security+ at a Glance
- > CompTIA Security+ and Your Career
- > Download Security+ Objectives
- > Prepare for Exam

CompTIA Security+™ Certification

"Benchmarking foundational skills through the CompTIA Security+ certification and then adding progressive layers of expertise seems to us to be absolutely the right thing to do, from both the customer and employee standpoints."

- Steve Jordan
Vice President, System Engineering & Consulting, McAfee, Inc.

Certified Ethical Hacker (CEH)



- CNIT 123: Ethical Hacking and Network Defense
- CNIT 124: Advanced Ethical Hacking

OSSTMM Professional Security Tester (OPST)



Join the ISECOM Gold or Silver Team and get the latest OSSTMM Info at www.isecom.org - ACCREDITED TRAINING - OPST



OSSTMM
PROFESSIONAL
SECURITY TESTER
ACCREDITED
CERTIFICATION (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 If and Ch Ih 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
- CNIT 125: Information Security Professional Practices
- Web site: 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 (links Ch 1i & Ch 1j)

What You Can Do Legally

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

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



www.ccsf.edu/Policy/policy.shtml (link Ch 1k)

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 laws 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

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