

PEARSON IT

CYBERSECURITY CURRICULUM



FOURTH EDITION

COMPUTER SECURITY FUNDAMENTALS

DR. CHUCK EASTTOM

Computer Security Fundamentals

Fourth Edition

Dr. Chuck Easttom



Pearson

Computer Security Fundamentals

Table of Contents

Cover

Title Page

Copyright Page

Credits

Contents

About the Author

About the Technical Reviewer

Dedication

Acknowledgments

Introduction

Chapter 1: Introduction to Computer Security

Introduction

How Seriously Should You Take Threats to Network Security?

Identifying Types of Threats

Malware

Compromising System Security

DoS Attacks

Web Attacks

Session Hijacking

Insider Threats

DNS Poisoning

New Attacks

Table of Contents

Assessing the Likelihood of an Attack on Your Network

Basic Security Terminology

Hacker Slang

Professional Terms

Concepts and Approaches

How Do Legal Issues Impact Network Security?

Online Security Resources

CERT

Microsoft Security Advisor

F-Secure

SANS Institute

Summary

Test Your Skills

Chapter 2: Networks and the Internet

Introduction

Network Basics

The Physical Connection: Local Networks

Faster Connection Speeds

Wireless

Bluetooth

Other Wireless Protocols

Data Transmission

How the Internet Works

IP Addresses

Uniform Resource Locators

What Is a Packet?

Basic Communications

History of the Internet

Table of Contents

Basic Network Utilities

IPConfig

Ping

Tracert

Netstat

NSLookup

ARP

Route

Other Network Devices

Advanced Network Communications Topics

The OSI Model

Media Access Control (MAC) Addresses

Summary

Test Your Skills

Chapter 3: Cyber Stalking, Fraud, and Abuse

Introduction

How Internet Fraud Works

Investment Offers

Auction Fraud

Identity Theft

Phishing

Cyber Stalking

Real Cyber Stalking Cases

How to Evaluate Cyber Stalking

Crimes Against Children

Laws About Internet Fraud

Protecting Yourself Against Cybercrime

Protecting Against Investment Fraud

Table of Contents

Protecting Against Identity Theft

Secure Browser Settings

Protecting Against Auction Fraud

Protecting Against Online Harassment

Summary

Test Your Skills

Chapter 4: Denial of Service Attacks

Introduction

DoS Attacks

Illustrating an Attack

Distributed Reflection Denial of Service Attacks

Common Tools Used for DoS Attacks

Low Orbit Ion Cannon

XOIC

TFN and TFN2K

Stacheldraht

DoS Weaknesses

Specific DoS Attacks

TCP SYN Flood Attacks

Smurf IP Attacks

UDP Flood Attacks

ICMP Flood Attacks

The Ping of Death

Teardrop Attacks

DHCP Starvation

HTTP POST DoS Attacks

PDoS Attacks

Registration DoS Attacks

Table of Contents

Login DoS Attacks

Land Attacks

DDoS Attacks

Real-World Examples of DoS Attacks

Boston Globe Attack

Memcache Attacks

MyDoom

DDoS Blackmail

Mirai

How to Defend Against DoS Attacks

Summary

Test Your Skills

Chapter 5: Malware

Introduction

Viruses

How a Virus Spreads

Types of Viruses

Virus Examples

The Impact of Viruses

Rules for Avoiding Viruses

Trojan Horses

The Buffer-Overflow Attack

The Sasser Virus/Buffer Overflow

Spyware

Legal Uses of Spyware

How Is Spyware Delivered to a Target System?

Obtaining Spyware Software

Other Forms of Malware

Table of Contents

Rootkits

Malicious Web-Based Code

Logic Bombs

Spam

Advanced Persistent Threats

Detecting and Eliminating Viruses and Spyware

Antivirus Software

Remediation Steps

Summary

Test Your Skills

Chapter 6: Techniques Used by Hackers

Introduction

Basic Terminology

The Reconnaissance Phase

Passive Scanning Techniques

Active Scanning Techniques

Actual Attacks

SQL Script Injection

Cross-Site Scripting

Cross-Site Request Forgery

Directory Traversal

Cookie Poisoning

URL Hijacking

Wireless Attacks

Cell Phone Attacks

Password Cracking

Malware Creation

Windows Hacking Techniques

Penetration Testing

Table of Contents

NIST 800-115

The NSA Information Assessment Methodology

PCI Penetration Testing Standard

The Dark Web

Summary

Test Your Skills

Chapter 7: Industrial Espionage in Cyberspace

Introduction

What Is Industrial Espionage?

Information as an Asset

Real-World Examples of Industrial Espionage

Example 1: Houston Astros

Example 2: University Trade Secrets

Example 3: Nuclear Secrets

Example 4: Uber

Example 5: Foreign Governments and Economic Espionage

Trends in Industrial Espionage

Industrial Espionage and You

How Does Espionage Occur?

Low-Tech Industrial Espionage

Spyware Used in Industrial Espionage

Steganography Used in Industrial Espionage

Phone Taps and Bugs

Protecting Against Industrial Espionage

The Industrial Espionage Act

Spear Phishing

Summary

Test Your Skills

Table of Contents

Chapter 8: Encryption

Introduction

Cryptography Basics

History of Encryption

The Caesar Cipher

Atbash

Multi-Alphabet Substitution

Rail Fence

Enigma

Binary Operations

Modern Cryptography Methods

Single-Key (Symmetric) Encryption

Modification of Symmetric Methods

Public Key (Asymmetric) Encryption

PGP

Legitimate Versus Fraudulent Encryption Methods

Digital Signatures

Hashing

MD5

SHA

RIPEMD

MAC and HMAC

Rainbow Tables

Steganography

Historical Steganography

Steganography Methods and Tools

Cryptanalysis

Frequency Analysis

Table of Contents

Modern Cryptanalysis Methods

Cryptography Used on the Internet

Quantum Computing Cryptography

Summary

Test Your Skills

Chapter 9: Computer Security Technology

Introduction

Virus Scanners

How Does a Virus Scanner Work?

Virus-Scanning Techniques

Commercial Antivirus Software

Firewalls

Benefits and Limitations of Firewalls

Firewall Types and Components

Firewall Configurations

Commercial and Free Firewall Products

Firewall Logs

Antispyware

IDSs

IDS Categorization

Identifying an Intrusion

IDS Elements

Snort

Honey Pots

Database Activity Monitoring

Other Preemptive Techniques

Authentication

Digital Certificates

Table of Contents

SSL/TLS

Virtual Private Networks

Point-to-Point Tunneling Protocol

Layer 2 Tunneling Protocol

IPsec

Wi-Fi Security

Wired Equivalent Privacy

Wi-Fi Protected Access

WPA2

WPA3

Summary

Test Your Skills

Chapter 10: Security Policies

Introduction

What Is a Policy?

ISO 17999

Defining User Policies

Passwords

Internet Use

Email Usage

Installing/Uninstalling Software

Instant Messaging

Desktop Configuration

Bring Your Own Device

Final Thoughts on User Policies

Defining System Administration Policies

New Employees

Departing Employees

Table of Contents

Change Requests

Security Breaches

Virus Infection

DoS Attacks

Intrusion by a Hacker

Defining Access Control

Development Policies

Standards, Guidelines, and Procedures

Data Classification

DoD Clearances

Disaster Recovery

Disaster Recovery Plan

Business Continuity Plan

Impact Analysis

Disaster Recovery and Business Continuity Standards

Fault Tolerance

Important Laws

HIPAA

Sarbanes-Oxley

Payment Card Industry Data Security Standards

Summary

Test Your Skills

Chapter 11: Network Scanning and Vulnerability

Scanning

Introduction

Basics of Assessing a System

Patch

Ports

Table of Contents

Protect

Policies

Probe

Physical

Securing Computer Systems

Securing an Individual Workstation

Securing a Server

Securing a Network

Scanning Your Network

MBSA

NESSUS

OWASP Zap

Shodan

Getting Professional Help

Summary

Test Your Skills

Chapter 12: Cyber Terrorism and Information Warfare

Introduction

Actual Cases of Cyber Terrorism

The Chinese Eagle Union

Chinas Advanced Persistent Threat

India and Pakistan

Russian Hackers

Weapons of Cyber Warfare

Stuxnet

Flame

StopGeorgia.ru Malware

FinFisher

Table of Contents

BlackEnergy

NSA ANT Catalog

Economic Attacks

Military Operations Attacks

General Attacks

Supervisory Control and Data Acquisitions (SCADA)

Information Warfare

Propaganda

Information Control

Disinformation

Actual Cases

Future Trends

Positive Trends

Negative Trends

Defense Against Cyber Terrorism

Terrorist Recruiting and Communication

TOR and the Dark Web

Summary

Test Your Skills

Chapter 13: Cyber Detective

Introduction

General Searches

Facebook

Court Records and Criminal Checks

Sex Offender Registries

Civil Court Records

Other Resources

Usenet

Table of Contents

Summary

Test Your Skills

Chapter 14: Introduction to Forensics

Introduction

General Guidelines

Dont Touch the Suspect Drive

Image a Drive with Forensic Toolkit

Can You Ever Conduct Forensics on a Live Machine?

Document Trail

Secure the Evidence

Chain of Custody

FBI Forensics Guidelines

U.S. Secret Service Forensics Guidelines

EU Evidence Gathering

Scientific Working Group on Digital Evidence

Locards Principle of Transference

Tools

Finding Evidence on the PC

Finding Evidence in the Browser

Finding Evidence in System Logs

Windows Logs

Linux Logs

Getting Back Deleted Files

Operating System Utilities

net sessions

openfiles

fc

netstat

The Windows Registry

Table of Contents

Specific Entries

Mobile Forensics: Cell Phone Concepts

Cell Concepts Module

Cellular Networks

iOS

Android

Windows

What You Should Look For

The Need for Forensic Certification

Expert Witnesses

Federal Rule 702

Daubert

Additional Types of Forensics

Network Forensics

Virtual Forensics

Summary

Test Your Skills

Chapter 15: Cybersecurity Engineering

Introduction

Defining Cybersecurity Engineering

Cybersecurity and Systems Engineering

Applying Engineering to Cybersecurity

SecML

SecML Concepts

Misuse Case Diagram

Security Sequence Diagram

Data Interface Diagram

Security Block Diagram

Table of Contents

Summary

Test Your Skills

Glossary

A

B

C

D

E

F

G

H

I

K

M

N

P

R

S

T

V

W

Appendix A: Resources

Appendix B: Answers to the Multiple Choice Questions

Index