



FIFTH EDITION

COMPUTER SECURITY FUNDAMENTALS

DR. CHUCK EASTTOM

Computer Security Fundamentals

Fifth Edition

Dr. Chuck Easttom



Pearson

Computer Security Fundamentals

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Table of Contents

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

Assessing the Likelihood of an Attack on Your Network

Basic Security Terminology

Hacker Slang

Professional Terms

Concepts and Approaches

Table of Contents

How Do Legal Issues Impact Network Security?

Online Security Resources

CERT

Microsoft Security Advisor

F-Secure

SANS Institute

Summary

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

Basic Network Utilities

IPConfig

Ping

Tracert

Netstat

NSLookup

ARP

Table of Contents

Route

PathPing

Other Network Devices

Advanced Network Communications Topics

The OSI Model

Media Access Control (MAC) Addresses

The TCP/IP Model

Cloud Computing

Summary

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

Protecting Against Identity Theft

Secure Browser Settings

Protecting Against Auction Fraud

Protecting Against Online Harassment

Summary

Table of Contents

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

Login DoS Attacks

Land Attacks

DDoS Attacks

Yo-Yo Attack

Login Attacks

CLDAP Reflection

Degradation of Service Attacks

Table of Contents

Challenge Collapsar Attack

EDoS

Real-World Examples of DoS Attacks

Google Attack

AWS Attack

Boston Globe Attack

Memcache Attacks

DDoS Blackmail

Mirai

How to Defend Against DoS Attacks

Summary

Chapter 5: Malware

Introduction

Viruses

How a Virus Spreads

Types of Viruses

Virus Examples

The Impact of Viruses

Machine Learning and Malware

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?

Pegasus

Obtaining Spyware Software

Table of Contents

Other Forms of Malware

- Rootkits

- Malicious Web-Based Code

- Logic Bombs

- Spam

- Advanced Persistent Threats

- Deep Fakes

Detecting and Eliminating Viruses and Spyware

- Antivirus Software

- Anti-Malware and Machine Learning

- Remediation Steps

Summary

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

- Command Injection

- Wireless Attacks

- Cell Phone Attacks

- Password Cracking

Table of Contents

Malware Creation

- Windows Hacking Techniques

Penetration Testing

- NIST 800-115

- The NSA Information Assessment Methodology

- PCI Penetration Testing Standard

The Dark Web

Summary

Chapter 7: Industrial Espionage in Cyberspace

Introduction

What Is Industrial Espionage?

Information as an Asset

Real-World Examples of Industrial Espionage

- Example 1: Hacker Group

- Example 2: Company Versus Company

- 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

- Spy for Hire

Protecting Against Industrial Espionage

Trade Secrets

Table of Contents

The Industrial Espionage Act

Spear Phishing

Summary

Chapter 8: Encryption

Introduction

Cryptography Basics

History of Encryption

 The Caesar Cipher

 Atbash

 Multi-Alphabet Substitution

 Rail Fence

 Scytale

 Polybius Cipher

 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

Table of Contents

Steganography

- Historical Steganography

- Steganography Methods and Tools

Cryptanalysis

- Frequency Analysis

- Modern Cryptanalysis Methods

Cryptography Used on the Internet

Quantum Computing Cryptography

Summary

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

- Types of Firewalls

- Commercial and Free Firewall Products

- Firewall Logs

Antispyware

IDSs

- IDS Categorization

- Identifying an Intrusion

- IDS Elements

- Snort

Table of Contents

Honey Pots

Database Activity Monitoring

SIEM

Other Preemptive Techniques

Authentication

Digital Certificates

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

Chapter 10: Security Policies

Introduction

What Is a Policy?

Important Standards

ISO 17999

NIST SP 800-53

ISO 27001

ISO 27002

ISO 17799

Defining User Policies

Passwords

Table of Contents

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

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

Zero Trust

Important Laws

HIPAA

Table of Contents

Sarbanes-Oxley

Payment Card Industry Data Security Standards

Summary

Chapter 11: Network Scanning and Vulnerability Scanning

Introduction

Basics of Assessing a System

Patch

Ports

Protect

Policies

Probe

Physical

Securing Computer Systems

Securing an Individual Workstation

Securing a Server

Securing a Network

Scanning Your Network

NESSUS

OWASP Zap

Shodan

Kali Linux

Vega

OpenVAS

Testing and Scanning Standards

NIST 800-115

NSA-IAM

PCI -DSS

National Vulnerability Database

Getting Professional Help

Table of Contents

Summary

Chapter 12: Cyber Terrorism and Information Warfare

Introduction

Actual Cases of Cyber Terrorism

Chinas Advanced Persistent Threat

India and Pakistan

Russian Hackers

IranSaudi Tension

Weapons of Cyber Warfare

Stuxnet

Flame

StopGeorgia.ru Malware

FinFisher

BlackEnergy

Regin

NSA ANT Catalog

Economic Attacks

Military Operations Attacks

General Attacks

Supervisory Control and Data Acquisitions (SCADA)

Information Warfare

Propaganda

Information Control

Disinformation

Actual Cases of Cyber Terrorism

Future Trends

Machine Learning/Artificial Intelligence

Positive Trends

Table of Contents

Negative Trends

Defense Against Cyber Terrorism

Terrorist Recruiting and Communication

TOR and the Dark Web

Summary

Chapter 13: Cyber Detective

Introduction

General Searches

Email Searches

Company Searches

Court Records and Criminal Checks

Sex Offender Registries

Civil Court Records

Other Resources

Usenet

Google

Maltego

Summary

Chapter 14: Introduction to Forensics

Introduction

General Guidelines

Dont Touch the Suspect Drive

Imaging 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

Table of Contents

- U.S. Secret Service Forensics Guidelines
- EU Evidence Gathering
- Scientific Working Group on Digital Evidence
- Locards Principle of Transference
- The Scientific Method
- Standards
- Forensics Reports
- Tools

Finding Evidence on a PC

- Finding Evidence in a 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

- Specific Entries

Mobile Forensics: Cell Phone Concepts

- Cell Phone State
- Cell Phone Components
- Cellular Networks
- iOS
- Android
- What You Should Look For

The Need for Forensic Certification

Table of Contents

Expert Witnesses

- Federal Rule 702

- Daubert

Additional Types of Forensics

- Network Forensics

- Virtual Forensics

Summary

Chapter 15: Cybersecurity Engineering

Introduction

Defining Cybersecurity Engineering

- Cybersecurity and Systems Engineering

- Applying Engineering to Cybersecurity

Standards

- RMF

- ISO 27001

- ISO 27004

- NIST SP 800-63B

SecML

- SecML Concepts

- Misuse-Case Diagram

- Security Sequence Diagram

- Data Interface Diagram

- Security Block Diagram

Modeling

- STRIDE

- PASTA

- DREAD

Summary

Table of Contents

Glossary

Appendix A: Resources

Appendix B: Answers to the Multiple Choice Questions

Index