FOURTH EDITION

NETWORK DEFENSE AND COUNTERMEASURES

Principles and Practices

DR.CHUCK EASTTOM

Network Defense and Countermeasures

Principles and Practices

Fourth Edition

Dr. Chuck Easttom

PEARSON

Network Defense and Countermeasures: Principles and Practices

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Table of Conents

Preface

Chapter 1: Introduction to Network Security

- Introduction
- The Basics of a Network
  - Basic Network Structure
  - Data Packets
  - IP Addresses
  - Uniform Resource Locators
  - MAC Addresses
  - Protocols
- Basic Network Utilities
  - ipconfig
  - ping
  - tracert
  - netstat
- The OSI Model
- What Does This Mean for Security?

Table of Contents

Assessing Likely Threats to the Network
Classifications of Threats
Malware
Compromising System SecurityIntrusions
Denial of Service
Likely Attacks
Threat Assessment
Understanding Security Terminology
Hacking Terminology
Security Terminology
Choosing a Network Security Approach
Perimeter Security Approach
Layered Security Approach
Hybrid Security Approach
Zero Trust
Network Security and the Law
Using Security Resources
Summary
Endnotes
Chapter 2: Types of Attacks
Introduction
Understanding Denial of Service Attacks
DoS in Action
SYN Flood
Smurf Attack
Ping of Death
UDP Flood
ICMP Flood

Table of Contents

DHCP Starvation

Billion Laughs Attack

ZIP Bomb

HTTP Post DoS

PDoS

Distributed Reflection Denial of Service

DoS Tools

Real-World Examples

Defending Against DoS Attacks

Defending Against Buffer Overflow Attacks

Defending Against IP Spoofing

Defending Against Session Hijacking

Blocking Virus and Trojan Horse Attacks

Viruses

Types of Viruses

Trojan Horses

Summary

Endnotes

Chapter 3: Fundamentals of Firewalls

Introduction

What Is a Firewall?

Types of Firewalls

Packet Filtering Firewall

Stateful Packet Inspection

Connection Tracking

Application Gateway

Hybrid Firewalls

Blacklisting/Whitelisting

Table of Contents

- Implementing Firewalls
  - Host-Based
  - Dual-Homed Hosts
  - Router-Based Firewall
  - Screened Hosts
- Firewall Deployment
- Selecting and Using a Firewall
  - Using a Firewall
- Using Proxy Servers
  - The WinGate Proxy Server
  - NAT
- Summary

Chapter 4: Firewall Practical Applications

- Introduction
- Using Single Machine Firewalls
  - Web Application Firewalls
  - Database Firewalls
- Windows 10 Firewall
- User Account Control
- Linux Firewalls
  - Iptables
  - Symantec Norton Firewall
  - McAfee Personal Firewall
  - Windows Defender
- Using Small Office/Home Office Firewalls
  - SonicWall
  - D-Link DFL-2560 Office Firewall
- Using Medium-Sized Network Firewalls

Table of Contents

Check Point Firewall

Cisco Next-Generation Firewalls

Juniper Next-Generation Firewalls

Using Enterprise Firewalls

Summary

Endnotes

Chapter 5: Intrusion-Detection Systems

Introduction

Understanding IDS Concepts

Preemptive Blocking

Signature Matching

Anomaly Detection

IDS Components and Processes

SIEM

Specific SIEM Products

Evasion Techniques

Understanding and Implementing IDSs

Snort

Cisco Intrusion Detection and Prevention

Juniper IDS/IPS

Other IDS/IPS

Understanding and Implementing Honeypots

Specter

Symantec Decoy Server

Intrusion Deflection

Intrusion Deterrence

Summary

Chapter 6: Encryption Fundamentals

Table of Contents

Introduction

The History of Encryption

- The Caesar Cipher
- ROT 13
- Atbash Cipher
- Multi-Alphabet Substitution
- Rail Fence
- Vigenère
- Enigma
- Binary Operations

Learning About Modern Encryption Methods

- Symmetric Encryption
- Symmetric Methods
- Key Stretching
- PRNG
- Public Key Encryption
- Digital Signatures

Identifying Good Encryption

Understanding Digital Signatures and Certificates

- Digital Certificates
- PGP Certificates
- MD5
- SHA
- RIPEMD
- Tiger
- HAVAL
- SWIFFT
- MAC and HMAC

Understanding and Using Decryption

Table of Contents

Cracking Passwords

John the Ripper

Using Rainbow Tables

Using Other Password Crackers

General Cryptanalysis

Steganography

Steganalysis

Quantum Computing and Quantum Cryptography

Summary

Endnote

Chapter 7: Virtual Private Networks

Introduction

Basic VPN Technology

Using VPN Protocols for VPN Encryption

PPTP

PPTP Authentication

L2TP

L2TP Authentication

L2TP Compared to PPTP

IPsec

SSL/TLS

Other VPN Protocols

DTLS

WireGuard

SSTP

Implementing VPN Solutions

VPN Concentrator

Cisco Solutions

Table of Contents

Juniper Solutions

Huawei Solutions

Service Solutions

Openswan

SoftEther VPN

Other Solutions

Summary

Endnotes

Chapter 8: Operating System Hardening

Introduction

Configuring Windows Properly

Accounts, Users, Groups, and Passwords

Setting Security Policies

Registry Settings

Services

Encrypting File System

Security Templates

Configuring Windows Server 2019 Properly

Configuring Linux Properly

Patching the Operating System

Configuring Browsers

Securing Browser Settings for Microsoft Edge

Secure Settings for Firefox

Secure Settings for Chrome

Other Browsers

Summary

Chapter 9: Defending Against Virus Attacks

Introduction

Table of Contents

Understanding Virus Attacks

What Is a Virus?

What Is a Worm?

How a Virus Spreads

The Virus Hoax

Types of Viruses

Malware Techniques

Virus Scanners

Virus Scanning Techniques

When Antivirus Causes a Problem

Commercial Antivirus Software

Antivirus Policies and Procedures

Additional Methods for Defending Your System

What to Do If Your System Is Infected by a Virus

Stopping the Spread of the Virus

Removing the Virus

Finding Out How the Infection Started

Machine Learning and Malware

Summary

Endnotes

Chapter 10: Defending Against Trojan Horses and Phishing

Introduction

Trojan Horses

Types of Trojan Horses

Identifying Trojan Horses

Symptoms of a Trojan Horse

Why So Many Trojan Horses?

Preventing Trojan Horses

Table of Contents

Phishing

Phishing Examples

Defending Against Phishing

Threat Intelligence

Summary

Endnotes

Chapter 11: Security Policies

Introduction

ISO 27002

Security Policy

Organization of Information Security

Asset Management

Human Resources Security

Physical and Environmental Security

Communications and Operations Management

Access Control

Information Systems Acquisition, Development, and Maintenance

Information Security Incident Management

Business Continuity Management

Compliance

Important Standards

NIST SP 800-53

ISO 27001

ISO 27002

Defining User Policies

Passwords

Internet Use Policy

E-mail Attachments

Software Installation and Removal

Table of Contents

- Instant Messaging
- Desktop Configuration
- Final Thoughts on User Policies

Defining System Administration Policies

- New Employees
- Leaving Employees
- Change Requests
- Security Breaches

Defining Access Control

Defining Developmental Policies

Disaster Recovery

Summary

Chapter 12: Assessing System Security

Introduction

Risk Assessment Concepts

Evaluating the Security Risk

Conducting the Initial Assessment

- Patches
- Ports
- Protect
- Physical

Probing the Network

- NetCop
- NetBrute
- Cerberus
- Port Scanner for Unix: SATAN
- SAINT
- Nessus

Table of Contents

- NetStat Live
- Active Ports
- Other Port Scanners
- NSAuditor
- Nmap
- OWASP ZAP
- Shodan
- Kali Linux
- Vega
- OpenVAS

Vulnerabilities

- CVE
- NIST
- OWASP
- Common Vulnerability Scoring System
- OSSTMM

McCumber Cube

- Goals
- Information States
- Safeguards

Security Documentation

- Physical Security Documentation
- Policy and Personnel Documentation
- Probe Documents
- Network Protection Documents

Summary

Chapter 13: Security Standards

Introduction

COBIT

Table of Contents

ISO Standards

NIST Standards

- NIST SP 800-14
- NIST SP 800-35
- NIST SP 800-30 Rev. 1
- ISO 27002
- Cloud Security Standards
- Zero Trust Standards

U.S. DoD Standards

- DoD 8500.2
- RMF
- DoD 8140.01 Cyberspace Workforce Management

Using the Common Criteria

Using Security Models

- Bell-LaPadula Model
- Biba Integrity Model
- Clark-Wilson Model
- Chinese Wall Model
- State Machine Model

U.S. Federal Regulations, Guidelines, and Standards

- The Health Insurance Portability & Accountability Act of 1996 (HIPAA)
- HITECH
- Sarbanes-Oxley (SOX)
- Computer Fraud and Abuse Act (CFAA): 18 U.S. Code § 1030
- Fraud and Related Activity in Connection with Access Devices: 18 U.S. Code § 1029
- General Data Protection Regulation (GDPR)

Summary

Endnotes

Table of Contents

Chapter 14: Physical Security and Disaster Recovery

- Introduction
- Physical Security
  - Equipment Security
  - Securing Building Access
  - Monitoring
  - Biometrics
  - Fire Protection
  - General Premises Security
- Disaster Recovery
  - Disaster Recovery Plan
  - Business Continuity Plan
  - Determining Impact on Business
  - Testing Disaster Recovery
  - Disaster Recovery Related Standards
- Ensuring Fault Tolerance
- Summary

Chapter 15: Techniques Used by Attackers

- Introduction
- Preparing to Hack
  - Passively Searching for Information
  - Active Scanning
  - NSAuditor
  - Enumerating
  - Nmap
  - Shodan.io
  - Manual Scanning
- The Attack Phase

Table of Contents

- Physical Access Attacks
- Remote Access Attacks
- Session Hijacking
- Wi-Fi Hacking
- Bluetooth Hacking
- Summary

Chapter 16: Introduction to Forensics

- Introduction
- General Forensics Guidelines
  - EU Evidence Gathering
  - Scientific Working Group on Digital Evidence
  - U.S. Secret Service Forensics Guidelines
  - Dont Touch the Suspect Drive
  - Leave a Document Trail
  - Secure the Evidence
- FBI Forensics Guidelines
- Imaging a Drive
- Finding Evidence on the PC
  - In the Browser
  - In System Logs
  - Recovering Deleted Files
  - Open Source Forensic Tools
  - Operating System Utilities
  - The Windows Registry
  - The Scientific Method
  - Standards
  - Reports
- Gathering Evidence from a Cell Phone

Table of Contents

Logical Acquisition

Physical Acquisition

Chip-off and JTAG

Cellular Networks

Cell Phone Terms

iOS

Android

Forensic Tools to Use

AccessData Forensic Toolkit

EnCase

The Sleuth Kit

OSForensics

Forensic Science

To Certify or Not to Certify?

Expert Witnesses

Federal Rule 702

Daubert

Additional Types of Forensics

Network Forensics

Virtual Forensics

Summary

Endnote

Chapter 17: Cyber Warfare and Terrorism

Introduction

Defending Against Computer-Based Espionage

Defending Against Computer-Based Terrorism

Economic Attack

Compromising Defense

Table of Contents

- General Attacks
- Choosing Defense Strategies
  - Defending Against Information Warfare
  - Propaganda
  - Information Control
  - Actual Cases
  - Packet Sniffers
- Summary
- Endnotes

Appendix A: Answers

Glossary

- A
- B
- C
- D
- E
- F
- G
- H
- I
- K
- L
- M
- N
- O
- P
- Q

Table of Contents

R
S
T
V
W
X
Index

Pearson