PEARSON IT CYBERSECURITY CURRICULUM

THIRD EDITION

NETWORK DEFENSE AND COUNTERMEASURES

Principles and Practices

CHUCK EASTTOM

Network Defense and Countermeasures

Principles and Practices

Third Edition

Chuck Easttom

Pearson

800 East 96th Street, Indianapolis, Indiana 46240 USA

Network Defense and Countermeasures: Principles and Practices

Table of Contents

Cover

Title Page

Copyright Page

Contents

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?
- Assessing Likely Threats to the Network
- Classifications of Threats

Table of Contents

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

Network Security and the Law

Using Security Resources

Summary

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

DHCP Starvation

HTTP Post DoS

PDoS

Distributed Reflection Denial of Service

Table of Contents

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

Chapter 3: Fundamentals of Firewalls

Introduction

What Is a Firewall?

Types of Firewalls

Packet Filtering Firewall

Stateful Packet Inspection

Application Gateway

Circuit Level Gateway

Hybrid Firewalls

Blacklisting/Whitelisting

Implementing Firewalls

Host-Based

Dual-Homed Hosts

Router-Based Firewall

Screened Hosts

Selecting and Using a Firewall

Using a Firewall

Table of Contents

- Using Proxy Servers
  - The WinGate Proxy Server
  - NAT
- Summary

Chapter 4: Firewall Practical Applications

- Introduction
- Using Single Machine Firewalls
- Windows 10 Firewall
- User Account Control
- Linux Firewalls
  - Iptables
  - Symantec Norton Firewall
  - McAfee Personal Firewall
- Using Small Office/Home Office Firewalls
  - SonicWALL
  - D-Link DFL-2560 Office Firewall
- Using Medium-Sized Network Firewalls
  - Check Point Firewall
  - Cisco Next-Generation Firewalls
- Using Enterprise Firewalls
- Summary

Chapter 5: Intrusion-Detection Systems

- Introduction
- Understanding IDS Concepts
  - Preemptive Blocking
  - Anomaly Detection
- IDS Components and Processes

Table of Contents

Understanding and Implementing IDSs

Snort

Cisco Intrusion-Detection and Prevention

Understanding and Implementing Honeypots

Specter

Symantec Decoy Server

Intrusion Deflection

Intrusion Deterrence

Summary

Chapter 6: Encryption Fundamentals

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

Key Stretching

PRNG

Public Key Encryption

Digital Signatures

Identifying Good Encryption

Understanding Digital Signatures and Certificates

Table of Contents

- Digital Certificates
- PGP Certificates
- MD5
- SHA
- RIPEMD
- HAVAL

Understanding and Using Decryption

Cracking Passwords

- John the Ripper
- Using Rainbow Tables
- Using Other Password Crackers
- General Cryptanalysis

Steganography

Steganalysis

Quantum Computing and Quantum Cryptography

Summary

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

Implementing VPN Solutions

Table of Contents

Cisco Solutions

Service Solutions

Openswan

Other Solutions

Summary

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 Linux Properly

Patching the Operating System

Configuring Browsers

Securing Browser Settings for Microsoft Internet Explorer

Other Browsers

Summary

Chapter 9: Defending Against Virus Attacks

Introduction

Understanding Virus Attacks

What Is a Virus?

What Is a Worm?

How a Virus Spreads

The Virus Hoax

Types of Viruses

Table of Contents

Virus Scanners

Virus Scanning Techniques

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

Summary

Chapter 10: Defending Against Trojan Horses, Spyware, and Adware

Introduction

Trojan Horses

Identifying Trojan Horses

Symptoms of a Trojan Horse

Why So Many Trojan Horses?

Preventing Trojan Horses

Spyware and Adware

Identifying Spyware and Adware

Anti-Spyware

Anti-Spyware Policies

Summary

Chapter 11: Security Policies

Introduction

Defining User Policies

Passwords

Internet Use Policy

Table of Contents

E-mail Attachments

Software Installation and Removal

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

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

Table of Contents

Nessus

NetStat Live

Active Ports

Other Port Scanners

Microsoft Baseline Security Analyzer

NSAuditor

NMAP

Vulnerabilities

CVE

NIST

OWASP

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

ISO Standards

NIST Standards

NIST SP 800-14

NIST SP 800-35

Table of Contents

NIST SP 800-30 Rev. 1

U.S. DoD Standards

Using the Orange Book

D - Minimal Protection

C - Discretionary Protection

B - Mandatory Protection

A - Verified Protection

Using the Rainbow Series

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)

PCI DSS

Summary

Chapter 14: Physical Security and Disaster Recovery

Introduction

Physical Security

Table of Contents

Equipment Security

Securing Building Access

Monitoring

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

Physical Access Attacks

Remote Access Attacks

Wi-Fi Hacking

Summary

Table of Contents

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
- Finding Evidence on the PC
  - In the Browser
  - In System Logs
  - Recovering Deleted Files
  - Operating System Utilities
  - The Windows Registry
- Gathering Evidence from a Cell Phone
  - Logical Acquisition
  - Physical Acquisition
  - Chip-off and JTAG
  - Cellular Networks
  - Cell Phone Terms
- Forensic Tools to Use
  - AccessData Forensic Toolkit
  - EnCase
  - The Sleuth Kit
  - OSForensics
- Forensic Science
- To Certify or Not to Certify?

Table of Contents

Summary

Chapter 17: Cyber Terrorism

Introduction

Defending Against Computer-Based Espionage

Defending Against Computer-Based Terrorism

Economic Attack

Compromising Defense

General Attacks

China Eagle Union

Choosing Defense Strategies

Defending Against Information Warfare

Propaganda

Information Control

Actual Cases

Packet Sniffers

Summary

Appendix A: Answers

Glossary

Index