
Table of Contents

Chapter 1 Getting Started

Audience

How to Use This Book

Chapter 2 Setting the Stage

Perspectives of Value

Where Does Ethical Hacking Fit?

What Constitutes a Success?

 Note 1: Digging for the Hole

A Quick Look Back

 Note 2: Foreign Internet Hackers Extort Domestic Companies

Hacking Impacts

Security Industry Reports

Notable Facts

The Hacker

 Type of Hacker

 Script Kiddies

 Note 3: Sophisticated Tools Will Cover for the Unsophisticated

 Hackers

 Über Hacker

 Extortionists

 Espionage

 Note 4: The Value of Seemingly Basic Manufacturing Techniques

 Sociology

 Motives

Chapter 3 The Framework

Planning the Test

Sound Operations

Reconnaissance

Enumeration

Vulnerability Analysis

Exploitation

Final Analysis

Deliverable

Integration

Chapter 4 Information Security Models

Computer Security

Harden a System

Physically Secure It

Installing the Operating System

Get It Running

Set System Policies

Accessing the System

Cleanup

Network Security

Transmission Security

Protocol Security

Routing Protocol Security

Network Access Controls

Service Security

Application Security

Security Architecture

Resource Layer

Control

Perimeter

Extended

Chapter 5 Information Security Program

Scope of Information Security Programs

The Process of Information Security

Identify Risk

Risk Analysis Process

Quantify Risk

Inherent Risk

Control Risk

Detection Risk

Handling Risk

Address Risk

Mitigate Risk

Measure Effectiveness

Component Parts of Information

Security Programs

Risk Assessment

Management System

Controls

Maintenance Plan

Risk Analysis and Ethical Hacking

Chapter 6 The Business Perspective

Business Objectives

Security Policy

Previous Test Results

Building a Roadmap

Business Challenges

Security Drivers

Increasing Network Complexity

Ensuring Corporate Value

Lower Management Investment

Business Consolidation

Mobile Workforce

Government Regulations and Standards

Why Have the Test?

Proof of Issue

Note 5: Presenting Only the Problem Is Not Always the Solution

Limited Staffing and Capability

Third-Party Perspective

It's All About Perspective

Overall Expectations

How Deep Is Deep Enough?

One-Hole Wonder

Today's Hole

Chapter 7 Planning for a Controlled Attack

Inherent Limitations

Imposed Limitations

Note 6: Imposed Limitations Can Cause Problems for Everyone

Timing Is Everything

Attack Type

Source Point

Required Knowledge

Timing of Information

Internet

Web Authenticated

Application Service

Direct Access

Multi-Phased Attacks

Parallel Shared

Parallel Isolated

Series Shared

Series Isolated

Value of Multi-Phase Testing

Employing Multi-Phased Tests

- Teaming and Attack Structure
 - Red Team
 - White Team
 - Blue Team
 - Note 7: Incident Management Is More Than Just Technology
 - Team Communications
- Engagement Planner
- The Right Security Consultant
 - Technologists
 - Architects
 - Ethics
- The Tester
- Logistics
 - Agreements
 - Note 8: Example Legal Agreement for Testing Services
 - Note 9: Legal Document Supporting Exhibit A
 - Downtime Issues
 - System and Data Integrity
 - Get Out of Jail Free Card
 - Intermediates
 - Partners
 - Customers
 - Service Providers
 - Law Enforcement

Chapter 8 Preparing for a Hack

- Technical Preparation
 - Attacking System
 - Operating System
 - Tools
 - Data Management and Protection
 - Note 10: The Hunter Becoming the Hunted
 - Attacking Network
 - Attacking Network Architecture
- Managing the Engagement
 - Project Initiation
 - Note 11: White Team Problems Affecting the Test
 - During the Project
 - Concluding the Engagement

Chapter 9 Reconnaissance

- Social Engineering
 - Note 12: The Physicality of Social Engineering
 - E-Mail

Note 13: Trusting E-Mail

Value

Controlling Depth

Helpdesk Fraud

Note 14: Good Helpdesk Practices Gone Wrong

Value

Controlling Depth

Prowling and Surfing

Internal Relations and Collaboration

Corporate Identity Assumption

Physical Security

Observation

Dumpster Diving

Wardriving and Warchalking

Theft

Internet Reconnaissance

General Information

Web Sites

Newsgroups

Technical Reconnaissance

Ping Sweeps

Scans

Passive Scan

Active Scan

Interactive Scan

Chapter 10 Enumeration

Enumeration Techniques

Soft Objective

Looking Around or Attack?

Note 15: Is It Scanning or Exploitation?

Elements of Enumeration

Preparing for the Next Phase

Chapter 11 Vulnerability Analysis

Weighing the Vulnerability

Note 16: Hacking an Old Hole Is Bad Business

Source Points

Obtained Data

Note 17: The Needle in the Haystack

The Internet

Note 18: Nasty Tools and the Difficulty in Finding Them

Vendors

Alerts

Service Packs

Reporting Dilemma

Note 19: Reporting Problems Is Not Always Easy

Chapter 12 Exploitation

Intuitive Testing

Evasion

Threads and Groups

Threads

Groups

Operating Systems

Windows

UNIX

Password Crackers

Rootkits

Applications

Web Applications

Distributed Applications

Customer Applications

Wardialing

Network

Perimeter

Network Nodes

Services and Areas of Concern

Services

Services Started by Default

Windows Ports

Null Connection

Remote Procedure Calls (RPC)

Simple Network Management Protocol (SNMP)

Berkeley Internet Name Domain (BIND)

Common Gateway Interface (CGI)

Cleartext Services

Network File System (NFS)

Domain Name Service (DNS)

File and Directory Permissions

FTP and Telnet

Internet Control Message Protocol (ICMP)

IMAP and POP

Network Architecture

Chapter 13 The Deliverable

Final Analysis

Potential Analysis

The Document

Executive Summary

- Present Findings
- Planning and Operations
- Vulnerability Ranking
- Process Mapping
- Recommendations
- Exceptions and Limitations
- Final Analysis
- Conclusion
- Overall Structure
- Aligning Findings
 - Technical Measurement
 - Severity
 - Exposure
 - Business Measurement
 - Cost
 - Risk
- Presentation
 - Remedial
 - Tactical
 - Strategic

Chapter 14 Integrating the Results

- Note 20: Fixing the Problem Cannot Always Be Done from the Outside
- Integration Summary
- Mitigation
 - Test
 - Pilot
 - Implement
 - Validate
- Defense Planning
 - Architecture Review
 - Architecture Review Structure
 - Awareness Training
 - Awareness Program
- Incident Management
 - Building a Team
 - People
 - Note 21: Food and Beverage
 - Mission
 - Constituency
 - Organizational Structure
 - Defining Services and Quality
 - CERT Forms
- Security Policy

Data Classification
Organizational Security
Conclusion