PENETRATION TESTING FUNDAMENTALS

A Hands-On Guide to Reliable Security Audits

CHUCK EASTTOM

Penetration Testing Fundamentals

A Hands-On Guide to Reliable Security Audits

Chuck Easttom

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits

Table of Contents

Cover
Title Page
Copyright Page
Contents
Introduction
Chapter 1: Introduction to Penetration Testing
- What Is Penetration Testing?
  - Audits
  - Vulnerability Scans
  - Penetration Tests
  - The Hybrid Test
- Terminology
- Methodologies
  - Nature of the Test
  - Approaches
- Ethical Issues
  - Everything Is Confidential
  - Keep in Your Lane
  - If You Break It, You Bought It
- Legal Issues
  - Computer Fraud and Abuse Act (CFAA): 18 U.S. Code § 1030

Table of Contents

Unlawful Access to Stored Communications: 18 U.S. Code § 2701

Identity Theft Enforcement and Restitution Act

Fraud and Related Activity in Connection with Access Devices: 18 U.S. Code § 1029

State Laws

International Laws

Certifications

CEH

GPEN

OSCP

Mile2

CISSP

PPT

This Book and Certifications

Careers in Penetration Testing

Security Administrators

Commercial Penetration Testing

Government/National Defense

Law Enforcement

Building Your Skillset

Summary

Test Your Skills

Chapter 2: Standards

PCI DSS

The Actual Test

NIST 800-115

Planning

Execution

Post-Execution

Table of Contents

National Security Agency InfoSec Assessment Methodology (NSA-IAM)

PTES

CREST (UK)

A Synthesis (Putting Standards Together into a Single Unified Approach)

- Pre-Engagement
- The Actual Test
- Reporting

Related Standards

- OWASP

Other Standards

- ISO 27002
- NIST 800-12, Revision 1
- NIST 800-14

Summary

Test Your Skills

Chapter 3: Cryptography

Cryptography Basics

History of Encryption

- The Caesar Cipher
- Atbash
- Multi-Alphabet Substitution
- Rail Fence

Modern Methods

- Symmetric Encryption
- Modification of Symmetric Methods
- Practical Applications

Public Key (Asymmetric) Encryption

Table of Contents

- Digital Signatures
- Hashing
  - MD5
  - SHA
  - RIPEMD
  - Windows Hashing
- MAC and HMAC
  - Rainbow Tables
  - Pass the Hash
- Password Crackers
- Steganography
  - Historical Steganography
  - Methods and Tools
- Cryptanalysis
  - Frequency Analysis
  - Modern Methods
  - Practical Application
- Learning More
- Summary
- Test Your Skills

Chapter 4: Reconnaissance

- Passive Scanning Techniques
  - Netcraft
  - BuiltWith
  - Archive.org
  - Shodan
  - Social Media
  - Google Searching

Table of Contents

- Active Scanning Techniques
  - Port Scanning
  - Enumeration
- Wireshark
- Maltego
- Other OSINT Tools
  - OSINT Website
  - Alexa
  - Web Master Tips
- Summary
- Test Your Skills

Chapter 5: Malware

- Viruses
  - How a Virus Spreads
  - Types of Viruses
  - Virus Examples
- Trojan Horses
- Other Forms of Malware
  - Rootkit
  - Malicious Web-Based Code
  - Logic Bombs
- Creating Malware
  - Levels of Malware Writing Skill
  - GUI Tools
  - Simple Script Viruses
  - Creating a Trojan Horse
  - Altering Existing Viruses
- Summary

Table of Contents

Test Your Skills

Chapter 6: Hacking Windows

Windows Details

Windows History

The Boot Process

Important Windows Files

Windows Logs

The Registry

Volume Shadow Copy

Windows Password Hashing

Windows Hacking Techniques

Pass the Hash

chntpw

Net User Script

Login as System

Find the Admin

Windows Scripting

net users

net view

net share

net service

netshell

Windows Password Cracking

Offline NT Registry Editor

LCP

pwdump

ophcrack

John the Ripper

Detecting Malware in Windows

Table of Contents

- Cain and Abel
- Summary
- Test Your Skills

Chapter 7: Web Hacking

- Web Technology
- Specific Attacks on Websites
  - SQL Script Injection
  - XSS
  - Other Web Attacks
- Tools
  - Burp Suite
  - BeEF
- Summary
- Test Your Skills

Chapter 8: Vulnerability Scanning

- Vulnerabilities
  - CVE
  - NIST
  - OWASP
- Packet Capture
  - tcpdump
  - Wireshark
- Network Scanners
  - LanHelper
- Wireless Scanners/Crackers
  - Aircrack
- General Scanners
  - MBSA

Table of Contents

Nessus

Nexpose

SAINT

Web Application Scanners

OWASP ZAP

Vega

Cyber Threat Intelligence

Threatcrowd.org

Phishtank

Internet Storm Center

OSINT

Summary

Test Your Skills

Chapter 9: Introduction to Linux

Linux History

Linux Commands

ls Command

cd Command

Pipe Output

finger Command

grep Command

ps Command

pstree Command

top Command

kill Command

Basic File and Directory Commands

chown Command

chmod Command

bg Command

Table of Contents

fg Command
useradd Command
userdel Command
usermod Command
users Command
who Command

Directories

/root
/bin
/sbin
/etc
/dev
/boot
/usr
/var
/proc

Graphical User Interface

GNOME
KDE

Summary

Test Your Skills

Chapter 10: Linux Hacking

More on the Linux OS

sysfs
Crond
Shell Commands

Linux Firewall

Iptables
iptables Configuration

Table of Contents

- Syslog
- Syslogd
- Scripting
- Linux Passwords
- Linux Hacking Tricks
  - Boot Hack
  - Backspace Hack
- Summary
- Test Your Skills

Chapter 11: Introduction to Kali Linux

- Kali Linux History
- Kali Basics
- Kali Tools
  - recon-ng
  - Dmitry
  - Sparta
  - John the Ripper
  - Hashcat
  - macchanger
  - Ghost Phisher
- Summary
- Test Your Skills

Chapter 12: General Hacking Techniques

- Wi-Fi Testing
  - Create a Hotspot
  - Using Kali as a Hotspot
  - Testing the WAP Administration
  - Other Wi-Fi Issues

Table of Contents

- Social Engineering
- DoS
  - Well-known DoS Attacks
  - Tools
- Summary
- Test Your Skills

Chapter 13: Introduction to Metasploit

- Background on Metasploit
- Getting Started with Metasploit
- Basic Usage of msfconsole
  - Basic Commands
  - Searching
- Scanning with Metasploit
  - SMB Scanner
  - SQL Server Scan
  - SSH Server Scan
  - Anonymous FTP Servers
  - FTP Server
- How to Use Exploits
- Exploit Examples
  - Cascading Style Sheets
  - File Format Exploit
  - Remote Desktop Exploit
  - More Exploits
  - Common Error
- Post Exploits
  - Get Logged-on Users
  - Check VM

Table of Contents

Enumerate Applications

Going Deeper into the Target

Summary

Test Your Skills

Chapter 14: More with Metasploit

Meterpreter and Post Exploits

ARP

NETSTAT

PS

Navigation

Download and Upload

Desktops

Cameras

Key Logger

Other Information

msfvenom

More Metasploit Attacks

Formatting All Drives

Attacking Windows Server 2008 R2

Attacking Windows via Office

Attacking Linux

Attacking via the Web

Another Linux Attack

Linux Post Exploits

Summary

Test Your Skills

Chapter 15: Introduction to Scripting with Ruby

Getting Started

Table of Contents

- Basic Ruby Scripting
  - A First Script
  - Syntax
  - Object-Oriented Programming
- Summary
- Test Your Skills

Chapter 16: Write Your Own Metasploit Exploits with Ruby

- The API
- Getting Started
- Examine an Existing Exploit
- Extending Existing Exploits
- Writing Your First Exploit
- Summary
- Test Your Skills

Chapter 17: General Hacking Knowledge

- Conferences
- Dark Web
- Certification and Training
- Cyber Warfare and Terrorism
- Nation State Actors
- Summary
- Test Your Skills

Chapter 18: Additional Pen Testing Topics

- Wireless Pen Testing
  - 802.11
  - Infrared
  - Bluetooth

Table of Contents

Other Forms of Wireless

Wi-Fi Hacking

Mainframe and SCADA

SCADA Basics

Mainframes

Mobile Pen Testing

Cellular Terminology

Bluetooth Attacks

Bluetooth/Phone Tools

Summary

Test Your Skills

Chapter 19: A Sample Pen Test Project

Pen Test Outline

Pre-Test Activities

External

Internal

Optional Items

Report Outline

Summary

Appendix A: Answers to Chapter Multiple Choice Questions

Index