"**Practical Intrusion Analysis** *provides a solid fundamental overview of the art and science of intrusion analysis.*"

—**Nate Miller,** Cofounder, Stratum Security

PRACTICAL INTRUSION ANALYSIS

Prevention and Detection for the Twenty-First Century

RYAN TROST

Practical Intrusion Analysis

Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century

Table of Contents

Contents

Preface

Chapter 1 Network Overview

- Key Terms and Concepts
- Brief History of the Internet
- Layered Protocols
- TCP/IP Protocol Suite
- Internet Protocol
- Addressing
  - IP Addresses
  - IPv6
- Summary

Chapter 2 Infrastructure Monitoring

- Network-Analysis Tools
  - Packet Sniffing
- Accessing Packets on the Network
  - SPANs (Port Mirroring)
  - Network Taps
  - To Tap or to SPAN
- Defense-in-Depth
- Summary

Pearson

Table of Contents

Chapter 3 Intrusion Detection Systems

IDS Groundwork

From the Wire Up

DoS Attacks

IP Fragmentation

TCP Stream Issues

Target-Based Reassembly

Two Detection Philosophies: Signature and Anomaly Based

Snort: Signature-Based IDS

Two Signature Writing Techniques

Bro: An Anomaly-Based IDS

Similarities Between the Systems

Summary

Chapter 4 Lifecycle of a Vulnerability

A Vulnerability Is Born

FlashGet Vulnerability

Collecting a Sample Packet Capture

Packet Analysis and Signature-Writing

Signature Tuning

Detection Tuning

Performance Tuning

Advanced Examples

CitectSCADA ODBC Server Buffer Overflow: Metasploit

FastStone Image Viewer Bitmap Parsing

Libspf2 DNS TXT Record Size Mismatch

Summary

Chapter 5 Proactive Intrusion Prevention and Response via Attack Graphs

Table of Contents

Topological Vulnerability Analysis (TVA)

Overview of Approach

Illustrative Example

Limitations

Attack Modeling and Simulation

Network Attack Modeling

Attack Simulation

Optimal Network Protection

Vulnerability Mitigation

Attack Graph Visualization

Security Metrics

Intrusion Detection and Response

Intrusion Detection Guidance

Attack Prediction and Response

Summary

Acknowledgments

Endnotes

Chapter 6 Network Flows and Anomaly Detection

IP Data Flows

NetFlow Operational Theory

A Matter of Duplex

Cisco IOS NetFlow and Flexible NetFlow

sFlow: More Data, But Less Frequency

Internet Protocol Flow Information Export (IPFIX)

Its a Virtual World

Endless Streams of Data

Behavioral Analysis and Anomaly Detection

Compare and Contrast

IDS and NetFlow

Table of Contents

Signature Updates

IDS System Resources

Syslog and NetFlow

Technology Matrix

Summary

Endnotes

Chapter 7 Web Application Firewalls

Web Threat Overview

Why a WAF?

WAF Protection Models

Positive Security Model

Negative Security Model

Virtual Patching Model

Output Detection Model/Content Scrubbing

WAF Policy Models

Learning

Vulnerability Assessment Feedback

Manual Entry

ModSecurity

ModSecurity Rule Sets

VA+WAF

VA+WAF Example:WhiteHat Security and F5 Networks

WAFs and PCI Compliance

WAF Realities

IDS/IPS != WAF

False Positives

Misconfigured WAFs

WAFs Do Not Fix Bad Logic

Table of Contents

WAFs != Bad Code Patch

Summary

References

Chapter 8 Wireless IDS/IPS

Why a Wireless IDS?

Wireless Intrusion Detection/Prevention Realities

Types of Wireless IDSs/IPSs

Overlay

Combined AP/WIDS

Combined AP/WIDS/Access Controller

Wireless IDS Events

Unauthorized Activity

Active Recon/Cracking

DoS Attacks

Intrusion Prevention Techniques

Limitations

Isolation

WEP Cloaking (WEP Chaffing)

Location Detection

Honeypot

Other Wireless Threats

Legacy Wireless Technology

Bluetooth

Sniffers

Summary

Endnote

Chapter 9 Physical Intrusion Detection for IT

Origins of Physical Security

Table of Contents

Assumed, Yet Overlooked

A Parallel Universe to IT Security

Physical Security Background

Common Physical Access Control Components

This Is Not Your Fathers CCTV

Old Habits Die Hard

Convergence of Physical and Logical Security

How Convergence Works

HSPD-12: Convergence Trial by Fire

A Look at Some Vendor Offerings

Intrusion Detection Examples in a Converged Environment

Summary

Endnotes

Chapter 10 Geospatial Intrusion Detection

Current Uses of Geocoding

Introduction to Geographic Information Systems

GIS Basic Functions

Framework for Cooperation

Map Projection

Raster Versus Vector

Vector Data Model

Spatial Point Pattern Analysis

Classes of Spatial Analysis

Point Intensity

Point Process Statistics

Dynamics of a Professional Attack

Cornerstone Theory

Example of Attack Steps and Methods

Geocoding Techniques

Table of Contents

Geocoding Limitations

Accuracy

GeoLocation Intelligence Vendors

Case Study of Geographic Intrusion Detection

Case Outline

Breakdown of the Steps

Summary

Endnotes

References

Chapter 11 Visual Data Communications

Introduction to Visualization

Developing a Visualization Strategy

User Audiences

Statistical Graphing Techniques

Technological Considerations

Scalability

Installation and Support

Data Management

Security Event Visualization

Example Graphs

Starlight Visual Information System

ETRI: VisNet and VisMon

Use-Case: Security Audit

Summary

Terminology

Endnotes

Reference

Chapter 12 Return on Investment: Business Justification

Table of Contents

Not If, But When

Compliance Plays a Role

CoBIT Framework

ISO 27001/27002 Frameworks

ITIL Framework

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Payment Card Industry Data Security Standard (PCI-DSS)

Federal Information Security Management Act of 2002 (FISMA)/National Institute of Standards and Technology

Security Breaches

Breach Costs

Security Investment Within the Organization

Data Breaches and the Law

ROI as a Unifying Benchmark

Cost Breakdown

Cost-Benefit Analysis: Building an Economic Model

Gain from Investment

Cost of Investment

Return on Investment

Net Present Value

Internal Rate of Return

ROI Versus NPV Versus IRR

Security Investment: Should Security Operations Be Outsourced?

Benefits of MSSPs

Downfalls of MSSPs

The Financial Aspect of an MSSP

Cyber Liability Insurance (CLI)

CLI Coverage Types

Table of Contents

Privacy Liability Insurance

Network Security Liability Insurance

Property Loss Insurance

Loss of Revenue Insurance

Cyber Extortion Insurance

Notification Costs Insurance

Regulatory Defense Insurance

Media Liability Insurance

CLI Underwriting Process

Summary

Endnotes

Appendix: Bro Installation Guide

Compiling and Building Options

Operations Use

References

Index