



SECURITY

Network Security Auditing

The complete guide to auditing network security,
measuring risk, and promoting compliance

Network Security Auditing

Chris Jackson, CCIE No. 6256 Cisco Press

Cisco Press

800 East 96th Street
Indianapolis, IN 46240

Network Security Auditing

Table of Contents

Contents

Introduction

Chapter 1 The Principles of Auditing

Security Fundamentals: The Five Pillars

- Assessment

- Prevention

- Detection

- Reaction

- Recovery

Building a Security Program

- Policy

- Procedures

- Standards

Security Controls

- Administrative Controls

- Technical Controls

- Physical Controls

Managing Risk

- Risk Assessment

- Risk Mitigation

- Risk in the Fourth Dimension

How, What, and Why You Audit

- Audit Charter

- Engagement Letter

- Types of Audits

Table of Contents

The Role of the Auditor

Places Where Audits Occur

The Auditing Process

Summary

References in This Chapter

Chapter 2 Information Security and the Law

IT Security Laws

Hacking, Cracking, and Fraud Laws

Computer Fraud and Abuse Act

Access Device Statute

Electronic Communications Privacy Act

Intellectual Property Laws

Digital Millennium Copyright Act

Economic Espionage Act

CAN-SPAM Act of 2003

State and Local Laws

Reporting a Crime

Regulatory Compliance Laws

SOX

HIPAA

GLBA

PCI DSS

Summary

References in This Chapter

Federal Hacking Laws

State Laws

Chapter 3 Information Security Governance, Frameworks, and Standards

Table of Contents

Understanding Information Security Governance

- People: Roles and Responsibilities

- Information Security Governance Organizational Structure

- Spotting Weaknesses in the People Aspect of Security

Process: Security Governance Frameworks

- COSO

- COBIT

- ITIL

Technology: Standards Procedures and Guidelines

- ISO 27000 Series of Standards

- NIST

- Center for Internet Security

- NSA

- DISA

- SANS

- ISACA

- Cisco Security Best Practices

Summary

References in This Chapter

Web Resources

Chapter 4 Auditing Tools and Techniques

- Evaluating Security Controls

- Auditing Security Practices

- Testing Security Technology

- Security Testing Frameworks

- OSSTMM

- ISSAF

- NIST 800-115

- OWASAP

Table of Contents

Security Auditing Tools

- Service Mapping Tools

- Vulnerability Assessment Tools

- Packet Capture Tools

- Penetration Testing Tools

- BackTrack

Summary

References in This Chapter

- Security Testing Frameworks

- Security Testing Tools

Chapter 5 Auditing Cisco Security Solutions

Auditors and Technology

Security as a System

Cisco Security Auditing Domains

- Policy, Compliance, and Management

- Infrastructure Security

- Perimeter Intrusion Prevention

- Access Control

- Secure Remote Access

- Endpoint Protection

- Unified Communications

Defining the Audit Scope of a Domain

Identifying Security Controls to Assess

Mapping Security Controls to Cisco Solutions

The Audit Checklist

Summary

Chapter 6 Policy, Compliance, and Management

Do You Know Where Your Policy Is?

Auditing Security Policies

Table of Contents

Standard Policies

- Acceptable Use
- Minimum Access
- Network Access
- Remote Access
- Internet Access
- User Account Management
- Data Classification
- Change Management
- Server Security
- Mobile Devices
- Guest Access
- Physical Security
- Password Policy
- Malware Protection
- Incident Handling
- Audit Policy
- Software Licensing
- Electronic Monitoring and Privacy

Policies for Regulatory and Industry Compliance

Cisco Policy Management and Monitoring Tools

- Cisco MARS
- Cisco Configuration Professional
- Cisco Security Manager
- Cisco Network Compliance Manager

Checklist

Summary

References in This Chapter

Chapter 7 Infrastructure Security

Table of Contents

Infrastructure Threats

- Unauthorized Access
- Denial of Service
- Traffic Capture
- Layer 2 Threats
- Network Service Threats

Policy Review

Infrastructure Operational Review

- The Network Map and Documentation
- Administrative Accounts
- Configuration Management
- Vulnerability Management
- Disaster Recovery
- Wireless Operations

Infrastructure Architecture Review

- Management Plane Auditing
- Control Plane Auditing
- Data Plane Auditing
- Layer 2 Security
- Wireless Security
- General Network Device Security Best Practices

Technical Testing

- Router Testing
- Switch Testing
- Wireless Testing

Checklist

Summary

References in This Chapter

Chapter 8 Perimeter Intrusion Prevention

Table of Contents

Perimeter Threats and Risk

Policy Review

Perimeter Operations Review

Management and Change Control

Monitoring and Incident Handling

Perimeter Architecture Review

What Are You Protecting?

Perimeter Design Review

Auditing Firewalls

Review Firewall Design

IOS Firewall Deployment

Review Firewall Configuration

Review Rule Base

Auditing IPS

How IPS Works

Review IPS Deployment

Review IPS Configuration

Review IPS Signatures

Technical Control Testing

Firewall Rule Testing

Testing the IPS

Checklist

Summary

References in This Chapter

Chapter 9 Access Control

Fundamentals of Access Control

Identity and Authentication

Access Control Threats and Risks

Access Control Policy

Table of Contents

Access Control Operational Review

- Identity Operational Good Practices
- Authorization and Accounting Practices
- Administrative Users
- Classification of Assets

Access Control Architecture Review

- Identity and Access Control Technologies
- Network Admission Control
- Identity-Based Networking Services
- NAC Guest Server
- NAC Profiler

Technical Testing

- Authentication and Identity Handling
- Posture Assessment Testing
- Testing for Weak Authentication

Checklist

Summary

References in This Chapter

Chapter 10 Secure Remote Access

Defining the Network Edge

VPN Fundamentals

- Confidentiality
- Integrity
- Authentication and Key Management
- IPsec, SSL, and dTLS

Remote Access Threats and Risks

Remote Access Policies

Remote Access Operational Review

- VPN Device Provisioning

Table of Contents

Mobile Access Provisioning

Mobile User Role-Based Access Control

Monitoring and Incident Handling

Remote Access Architecture Review

Site-to-Site VPN Technologies

Mobile User Access VPN

VPN Network Placement

VPN Access Controls

Remote Access Good Practices

Technical Testing

Authentication

IPsec

SSL

Site-to-Site Access Control Testing

Mobile User Access Control Testing

Monitoring and Log Review

Checklist

Summary

References in This Chapter

Chapter 11 Endpoint Protection

Endpoint Risks

Endpoint Threats

Malware

Web-Based Threats

E-Mail Threats

Data Loss Threats

Policy Review

Endpoint Protection Operational Control Review

Current Threat Intelligence

Table of Contents

Vulnerability and Patch Management

Monitoring and Incident Handling

Security Awareness Program

Endpoint Architecture Review

Cisco Security Intelligence Operations

Web Controls

E-Mail Controls

Data Loss Prevention

E-Mail

Monitoring

Technical Testing

Acceptable Use Enforcement

Malware Detection and Quarantine

SPAM, Phishing, and E-Mail Fraud

Encryption

Patch Management and Enforcement

Data Loss Prevention Testing

Detection and Response

Checklist

Summary

References in This Chapter

Chapter 12 Unified Communications

Unified Communications Risks

VoIP Threats

Denial of Service

Confidentiality

Fraud

UC Policy and Standards Review

UC Operational Control Review

Table of Contents

- User and Phone Provisioning
- Change Management
- Asset Management
- Call Detail Record Review
- Administrative Access
- Vulnerability Management
- Security Event Monitoring and Log Review
- Disaster Recovery

UC Architecture Review

- Unified Communications Fundamentals
- H.323
- MGCP
- SCCP
- SIP
- Session Border Controller
- RTP and SRTP
- Call Processing
- Infrastructure Controls
- ACLs and Firewalling
- Gateway Protection
- Site to Site
- Wireless
- Call Control Protection
- Application Controls
- Voice Endpoint Controls
- Monitoring and Management

Technical Testing

- VLAN Separation
- Eavesdropping
- Gateway

Table of Contents

Toll Fraud

Monitoring and Incident Detection

Checklist

Summary

References in This Chapter

Index