

- Memory Attacks, Buffer Overflows
- File System Attacks, Race Conditions
- Trojan Horse Programs and Rootkits
- Monitoring and Alerting Tools
- Unix Logging and Kernel-Level Auditing
- Building a Centralized Logging Infrastructure
- Network Security Tools
- SSH for Secure Administration
- Server Lockdown for Linux and Unix
- Controlling Root Access with sudo
- SELinux and chroot() for Application Security
- DNSSEC Deployment and Automation
- mod_security and Web Application Firewalls
- Secure Configuration of BIND and Apache
- Forensics Investigation of Linux Systems

Memory Attacks and Overflows

- Stack and Heap Overflows
- Format String Attacks
- Stack Protection

Vulnerability Minimization

- Minimization vs. Patching
- OS Minimization
- Patching Strategies

Boot-Time Configuration

- Reducing Services
- systemd vs init
- Email Configuration
- Legacy Services

Encrypted Access

- Session Hijacking Exploits
- The Argument For Encryption
- SSH Configuration

Host-Based Firewalls

- IP Tables and Other Alternatives
- Simple Single-Host Firewalls
- Managing and Automating Rule Updates

Rootkits and Malicious Software

- Backdoors and Rootkits
- Kernel Rootkits
- chkrootkit and rkhunter

File Integrity Assessment

- Overview of AIDE
- Basic Configuration
- Typical Usage

Physical Attacks and Defenses

- Known Attacks
- Single User Mode Security
- Boot Loader Passwords

User Access Controls

- Password Threats and Defenses
- User Access Controls
- Environment Settings

Root Access Control With Sudo

- Features and Common Uses
- Configuration
- Known Issues and Work-Arounds

Warning Banners

- Why?
- Suggested Content
- Implementation Issues

Kernel Tuning For Security

- Network Tuning
- System Resource Limits
- Restricting Core Files

Automating Tasks With SSH

- Why and How
- Public Key Authentication
- ssh-agent and Agent Forwarding

AIDE Via SSH

- Conceptual Overview
- SSH Configuration
- Tools and Scripts

Linux/Unix Logging Overview

- Syslog Configuration
- System Accounting
- Process Accounting
- Kernel-Level Auditing

SSH Tunneling

- X11 Forwarding
- TCP Forwarding
- Reverse Tunneling Issues

Centralized Logging With Syslog-NG

- Why You Care
- Basic Configuration
- Hints and Hacks for Tunneling Log Data
- Log Analysis Tools and Strategies

chroot() for Application Security

- What is chroot()?
- How Do You chroot()?
- Known Security Issues

The SCP-Only Shell

- What It Is and How It Works
- Configuring chroot() directory
- Automounter Hacks for Large-Scale Deployments

SELinux Basics

- Overview of Functionality
- Navigation and Command Interface
- Troubleshooting Common Issues

SELinux and the Reference Policy

- Tools and Prerequisites
- Creating and Loading an Initial Policy
- Testing and Refining Your Policy
- Deploying Policy Files

BIND

- Common Security Issues
- Split-horizon DNS
- Configuration for Security
- Running BIND chroot()ed

DNSSEC

- Implementation Issues
- Generating Keys and Signing Zones
- Key "Rollover"
- Automation Tools

Apache

- Secure Directory Configuration
- Configuration/Installation Choices
- User Authentication
- SSL Setup

Web Application Firewalls with mod_security

- Introduction to Common Configurations
- Dependencies and Prerequisites
- Core Rules
- Installation and Debugging

Tools Throughout

- The Sleuth Kit
- Foremost
- chkrootkit
- Isot and Other Critical OS Commands

Forensic Preparation and Best Practices

- Basic Forensic Principles
- Importance of Policy
- Forensic Infrastructure
- Building a Desktop Analysis Laboratory

Incident Response and Evidence Acquisition

- Incident Response Process
- Vital Investigation Tools
- Taking a Live System Snapshot
- Creating Bit Images

Media Analysis

- File System Basics
- MAC Times and Timeline Analysis
- Recovering Deleted Files
- Searching Unallocated Space
- String Searches

Incident Reporting

- Critical Elements of a Report
- Lessons Learned
- Calculating Costs