

GL550 - Enterprise Linux Security Administration

This highly technical course focuses on properly securing machines running the Linux operating systems. A broad range of general security techniques such as packet filtering, password policies, and file integrity checking are covered. Advanced security technologies such as Kerberos are taught. Special attention is given to securing commonly deployed network services. At the end of the course, students have an excellent understanding of the potential security vulnerabilities -- know how to audit existing machines, and how to securely deploy new network services.

Prerequisites:

This class covers advanced security topics and is intended for experienced systems administrators. Candidates should have current Linux or UNIX systems administration experience equivalent to the Linux Fundamentals, Enterprise Linux Systems Administration, and Enterprise Linux Network Services

Supported Distributions:

- Red Hat Enterprise Linux 5
- Fedora Core 6
- SUSE Linux Enterprise Server 10
- SUSE Linux 10.1

Recommended Class Length:

5 days

Detailed Course Outline:

1. Security Concepts
 1. Basic Security Principles
 2. Linux Default Install
 3. Installer Firewall Options
 4. Post-Install Firewall
 5. Minimization - Discovery
 6. Service Discovery
 7. Hardening
 8. Security Concepts

Lab Tasks

9. Removing Packages Using RPM
10. Firewall Configuration
11. Process Discovery

12. Operation of the setuid() and capset() System Calls
13. Operation of the chroot() System Call

2. Scanning, Probing, and Mapping Vulnerabilities
 1. The Security Environment
 2. Stealth Reconnaissance
 3. The WHOIS database
 4. Interrogating DNS
 5. Discovering Available Hosts and Apps
 6. Reconnaissance with SNMP
 7. Discovery of RPC Services
 8. Enumerating NFS Shares
 9. Nessus Insecurity Scanner
 10. Configuring OpenVAS

Lab Tasks

11. NMAP
12. OpenVAS
13. Advanced NMAP Options

3. Password Security and PAM
 1. Unix Passwords
 2. Password Aging
 3. Auditing Passwords
 4. PAM Implementation, Management, and Control Statements
 5. PAM Modules
 6. pam_unix.so
 7. pam_cracklib.so
 8. pam_pwcheck.so
 9. pam_env.so
 10. pam_xauth.so
 11. pam_tally.so
 12. pam_wheel.so
 13. pam_limits.so
 14. pam_nologin.so
 15. pam_deny.so
 16. pam_securetty.so
 17. pam_time.so
 18. pam_access.so
 19. pam_listfile.so
 20. pam_lastlog.so
 21. pam_warn.so
 22. pam_console.so
 23. pam_resmgr.so
 24. pam_devperm.so

Lab Tasks

25. John the Ripper
 26. Cracklib
 27. Using pam_listfile to Implement Arbitrary ACLs
 28. Using pam_limits to Restrict Simultaneous Logins
 29. Using pam_nologin to Restrict Logins
 30. Using pam_access to Restrict Logins
 31. su & pam
4. Secure Network Time Protocol (NTP)
 1. The Importance of Time
 2. Time Measurements
 3. Terms and Definitions
 4. Synchronization Methods
 5. NTP Evolution
 6. Time Server Hierarchy
 7. Operational Modes
 8. NTP Clients
 9. Configuring NTP Clients and Servers
 10. Securing NTP
 11. NTP Packet Integrity
 12. Useful NTP Commands

Lab Tasks

13. Configuring and Securing NTP
 14. Peering NTP With Multiple Systems
5. Kerberos Concepts
 1. Common Security Problems
 2. Account Proliferation
 3. The Kerberos Solution
 4. Kerberos History, Implementations, and Concepts
 5. Kerberos Principals, Safeguards, and Components
 6. Authentication Process
 7. Identification Types
 8. Logging In
 9. Gaining and Using Privileges
 6. Kerberos Components
 1. Kerberos Components
 2. KDC
 3. Kerberos Principal Review
 4. Kerberized Services Review
 5. Kerberized Clients
 6. KDC Server Daemons
 7. Configuration Files
 8. Utilities Overview
 9. Kerberos SysV Init Scripts

7. Implementing Kerberos
 1. Plan Topology
 2. Plan Implementation
 3. Kerberos 5 Client Software
 4. Kerberos 5 Server Software
 5. Synchronize Clocks
 6. Creating and Configuring the Master KDC
 7. KDC Logging
 8. Kerberos Realm Defaults
 9. Specifying [realms]
 10. Specifying [domain_realm]
 11. Allow Administrative Access
 12. Create KDC Databases and Administrators
 13. Install Keys for Services
 14. Start Services
 15. Add Host Principals
 16. Add Common Service Principals
 17. Configure Slave KDCs
 18. Create Principals for Slaves
 19. Define Slaves as KDCs
 20. Copy Configuration to Slaves
 21. Install Principals on Slaves
 22. Synchronization of Database
 23. Propagate Data to Slaves
 24. Create Stash on Slaves
 25. Start Slave Daemons
 26. Client Configuration
 27. Install krb5.conf on Clients
 28. Client PAM Configuration
 29. Install Client Host Keys

Lab Tasks

30. Implementing Kerberos
8. Administrating and Using Kerberos
 1. Administrative Tasks
 2. Key Tables
 3. Managing Keytabs
 4. Principals
 5. Managing Principals
 6. Principal Policy
 7. Viewing Principals
 8. Managing Policies
 9. Overall Goals for Users
 10. Signing Into Kerberos
 11. Ticket types
 12. Viewing Tickets
 13. Removing Tickets
 14. Passwords

15. Changing Passwords
16. Giving Others Access
17. Using Kerberized Services
18. Kerberized FTP
19. Enabling Kerberized Services
20. OpenSSH and Kerberos

Lab Tasks

21. Using Kerberized Clients
22. Forwarding Kerberos Tickets
23. OpenSSH with Kerberos

9. Securing The Filesystem

1. Filesystem Mount Options
2. NFS Properties
3. NFS Export Option
4. NFSv4 and GSSAPI Auth
5. Implementing NFSv4
6. File Encryption with GPG and OpenSSL
7. Linux Unified Key Setup (LUKS)

Lab Tasks

8. Securing Filesystems
9. Securing NFS
10. Implementing NFSv4
11. File Encryption With GPG
12. File Encryption With OpenSSL
13. LUKS-on-disk format Encrypted Filesystem

10. AIDE

1. Host Intrusion Detection
2. Using RPM as an HIDS
3. Introduction to AIDE
4. Concepts of AIDE
5. AIDE Installation
6. AIDE Policies
7. AIDE Usage

Lab Tasks

8. File Integrity Checking with RPM
9. File Integrity Checking with AIDE

11. Securing APACHE

1. Apache Overview
2. Default Configuration
3. Configuring CGI
4. Turning Off Unneeded modules
5. Configuration Delegation and Scope
6. ACL by IP Address
7. HTTP User Authentication
8. Standard Auth Modules
9. HTTP Digest Authentication
10. Authentication via SQL, LDAP, and Kerberos
11. Scrubbing HTTP Headers
12. Metering HTTP Bandwidth

Lab Tasks

13. Hardening Apache by Minimizing Loaded Modules
14. Scrubbing Apache & PHP version headers
15. Protecting Web Content
16. Using the suexec mechanism
17. Enabling SSO in Apache with mod_auth_kerb

12. Securing PostgreSQL

1. PostgreSQL Overview and Default Configuration
2. Configuring SSL
3. Client Authentication Basics
4. Authentication Methods
5. Advanced Authentication
6. Ident-based Authentication

Lab Tasks

7. Configure PostgreSQL
8. PostgreSQL with SSL
9. PostgreSQL with Kerberos Authentication
10. Securing PostgreSQL with Web Based Applications

13. Securing Email Systems

1. SMTP Overview
2. SMTP Implementations
3. Selecting an MTA
4. Security Considerations
5. Postfix Overview
6. Chrooting Postfix
7. Connections and Relays
8. SMTP AUTH & StartTLS/SSL
9. Secure Cyrus IMAP Config
10. Using GSSAPI/Kerberos Auth

Lab Tasks

11. Configuring Postfix
12. Postfix Network Configuration
13. Postfix In a Chrooted Environment
14. Postfix SMTP AUTH Configuration
15. Postfix STARTTLS Configuration
16. Configuring Cyrus IMAP
17. Kerberos with Postfix and Cyrus

14. Accountability with Kernel auditd
 1. Accountability and Auditing
 2. Simple Audit Tools
 3. Kernel-Level Auditing
 4. Configuring the Audit Daemon
 5. Controlling Kernel Audit System
 6. Creating Audit Rules
 7. Searching Audit Logs
 8. Generating Audit Log Reports
 9. Audit Log Analysis

Lab Tasks

10. Auditing Login/Logout
11. Auditing File Access
12. Auditing Command Execution