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 and SELinux 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.

Course Objectives:

- Understand security techniques and principles
- Learn to secure filesystems and common services
- Detect system compromise
- Understand system vulnerabilities
- Generate detailed audit reports
- Learn Discretionary Access Control (DAC)
- Manage Port Contexts
- Activating and Deactivating Apache Modules
- Securing email systems

Audience: System and network administrators working with wide network security and authentication.

Prerequisites: Experienced systems administrators with current Linux or UNIX systems administration.

Number of Days: 5 days

1 Security Concepts

Basic Security Principles
RHEL6 Default Install
RHEL6 Firewall
SLES11 Default Install
SLES11 Firewall
SLES11: File Security
Minimization - Discovery
Service Discovery
Hardening
Security Concepts

2 Scanning, Probing, and Mapping Vulnerabilities

The Security Environment
Stealth Reconnaissance
The WHOIS database
Interrogating DNS
Discovering Hosts
Discovering Reachable Services
Reconnaissance with SNMP
Discovery of RPC Services
Enumerating NFS Shares
Nessus Insecurity Scanner
Configuring OpenVAS

3 Password Security and PAM

UNIX Passwords
Password Aging
Auditing Passwords
PAM Overview
PAM Module Types
PAM Order of Processing
PAM Control Statements
PAM Modules
pam_unix
pam_cracklib.so
pam_pwcheck.so