Linux Security Administration Eğitimi

Eğitim Hakkında

Linux Security Administration kursu, katılımcılara Linux işletim sistemini çalıştıran makinelerin güvenliğini sağlamayı öğretir. Katılımcılar, paket filtreleme, parola ilkeleri ve dosya bütünlüğü denetimi gibi çok çeşitli genel güvenlik tekniklerinin yanı sıra Kerberos ve SELinux gibi gelişmiş güvenlik teknolojilerini öğrenirler.

Neler Öğreneceksiniz

Olası güvenlik açıklarını mükemmel şekilde anlamayı,

Mevcut makineleri denetlemeyi,

Yeni ağ hizmetlerini güvenli bir şekilde dağıtmayı.

Eğitim İçeriği

Introduction
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

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

Password Security and PAM
UNIX Passwords
Password Aging
Auditing Passwords
PAM Overview
PAM Module Types
PAM Order of Processing
PAM Control Statements
PAM Modules

Secure Network Time Protocol (NTP)
The Importance of Time
Hardware and System Clock
Time Measurements
NTP Terms and Definitions
Synchronization Methods
NTP Evolution
Time Server Hierarchy
Operational Modes
NTP Clients
Configuring NTP Clients
Enterprise Linux Security
Administration
Enterprise Linux Security Administration
Configuring NTP Servers
Securing NTP
NTP Packet Integrity
Useful NTP Commands

Kerberos Concepts and Components
Common Security Problems
Account Proliferation
The Kerberos Solution
Kerberos History
Kerberos Implementations
Kerberos Concepts
Kerberos Principals
Kerberos Safeguards
Kerberos Components
Authentication Process
Identification Types
Logging In
Gaining Privileges
Using Privileges
Kerberos Components and the KDC
Kerberized Services Review

Kerberized Clients
KDC Server Daemons
Configuration Files
Utilities Overview

Implementing Kerberos
Plan Topology and Implementation
Kerberos 5 Client Software
Kerberos 5 Server Software
Synchronize Clocks
Create Master KDC
Configuring the Master KDC
KDC Logging
Kerberos Realm Defaults
Specifying [realms]
Specifying [domain_realm]
Allow Administrative Access
Create KDC Databases
Create Administrators
Install Keys for Services
Start Services
Add Host Principals
Add Common Service Principals
Configure Slave KDCs
Create Principals for Slaves
Define Slaves as KDCs
Copy Configuration to Slaves
Install Principals on Slaves
Create Stash on Slaves
Start Slave Daemons
Client Configuration
Install krb5.conf on Clients
Client PAM Configuration
Install Client Host Keys

Administering and using
Kerberos
Administrative Tasks
Key Tables
Managing Keytabs
Managing Principals
Viewing Principals
Adding, Deleting, and Modifying
Principals
Principal Policy
Overall Goals for Users
Signing In to Kerberos
Ticket types
Viewing Tickets

Removing Tickets
Passwords
Changing Passwords
Giving Others Access
Using Kerberized Services
Kerberized FTP
Enabling Kerberized Services
OpenSSH and Kerberos

Securing the Filesystem
Filesystem Mount Options
NFS Properties
NFS Export Option
NFSv4 and GSSAPI Auth
Implementing NFSv4
Implementing Kerberos with
NFS
GPG - GNU Privacy Guard
File Encryption with OpenSSL
File Encryption with encfs
Linux Unified Key Setup
(LUKS)

AIDE
Host Intrusion Detection Systems
Using RPM as a HIDS
Enterprise Linux Security Administration
Introduction to AIDE
AIDE Installation
AIDE Policies
AIDE Usage Chapter Section

Accountability with Kernel Audit
Accountability and Auditing
Simple Session Auditing
Simple Process Accounting & Command History
Kernel-Level Auditing
Configuring the Audit Daemon
Controlling Kernel Audit System
Creating Audit Rules
Searching Audit Logs
Generating Audit Log Reports
Audit Log Analysis

SELinux
DAC vs. MAC
Shortcomings of Traditional Unix Security
AppArmor
SELinux Goals
SELinux Evolution

SELinux Modes
Gathering Information
SELinux Virtual File System
SELinux Contexts
Managing Contexts
The SELinux Policy
Choosing an SELinux Policy
Policy Layout
Tuning and Adapting Policy
Booleans
Permissive Domains
Managing File Contexts
Managing Port Contexts
SELinux Policy Tools
Examining Policy
SELinux Troubleshooting

Securing Apache
Apache Overview
httpd.conf - Server Settings
Configuring CGI
Turning Off Unneeded Modules
Delegating Administration
Apache Access Controls (mod_access)
HTTP User Authentication
Standard Auth Modules
HTTP Digest Authentication
Authentication via SQL
Authentication via LDAP
Authentication via Kerberos
Scrubbing HTTP Headers
Metering HTTP Band

Securing PostgreSQL
PostgreSQL Overview
PostgreSQL Default Config
Configuring SSL
Client Authentication Basics
Advanced Authentication
Ident-based Authentication