Enterprise Linux Security Administration Eğitimi

Eğitim Hakkında

Enterprise Linux Security Administration eğitim kursu, katılımcılara Linux işletim sistemini çalıştıran makinelerin güvenliğini nasıl sağlayacaklarını öğretir. Katılımcılar, potansiyel güvenlik açıkları hakkında mükemmel bir anlayış kazanır ve çok çeşitli genel güçlendirme tekniklerini öğrenirler.

Neler Öğreneceksiniz

Olası güvenlik açıklarını mükemmel bir şekilde anlamayı,

Paket filtreleme, şifre politikaları ve dosya bütünlüğü denetimini,

Mevcut makinelerin nasıl denetleneceğini,

Yeni ağ hizmetlerinin güvenli bir şekilde nasıl dağıtılacağını,

Kerberos ve SELinux gibi gelişmiş güvenlik teknolojileri nasıl kullanılır?

Eğitim İçeriği

Security Concepts
Basic Security Principles
RHEL7 Default Install
RHEL7 Firewall
SLES12 Default Install
SUSE Basic Firewall Configuration
SLES12: 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/OpenVAS Insecurity Scanner
Configuring OpenVAS
Intrusion Detection Systems
Snort Rules
Writing Snort Rules

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
pam_env.so
pam_xauth.so
pam_tally2.so
pam_wheel.so
pam_limits.so
pam_nologin.so
pam_deny.so
pam_warn.so
pam_securetty.so
pam_time.so
pam_access.so
pam_listfile.so
pam_lastlog.so
pam_console.so

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
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
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
Synchronization of Database
Propagate Data to 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 Into 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
Introduction to AIDE
AIDE Installation
AIDE Policies
AIDE Usage

Accountability with Kernel Auditd
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 SELinux Information
SELinux Virtual Filesystem
SELinux Contexts
Managing Contexts
The SELinux Policy
Choosing an SELinux Policy
Policy Layout
Tuning and Adapting Policy
Booleans
Permissive Domains
Managing File Context Database
Managing Port Contexts
SELinux Policy Tools
Examining Policy
SELinux Troubleshooting
SELinux Troubleshooting Continued

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
TLS Using mod_ssl.so
Authentication via SQL
Authentication via LDAP
Authentication via Kerberos
Scrubbing HTTP Headers

Metering HTTP Bandwidth

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

Securing Email Systems
SMTP Implementations
Security Considerations
chrooting Postfix
Email with GSSAPI/Kerberos Auth