Course Outline

Course Summary

Description

This Linux security course covers a range of topics essential for system administrators and system security specialists needing to harden and secure Linux systems.

Objectives

At the end of this course, students will be able to:

- Using services as firewalls, managing permissions, and using access control and connection limiting
- Monitor filesystems for intrusion detection using AIDE
- Manage system users with account permissions, password security, and authentication
- Configure remote system access with SSH and logging administration
- Utilize access control through SELinux
- Audit the system with kernel audit
- Secure system services; Apache
- Scan, probe, and map system vulnerabilities
- Apply and maintain security and software updates

Topics

- Security Concepts
- Securing Services
- Manage The Filesystem
- Securing The Filesystem
- Manage Special Permissions
- Monitor For Filesystem Changes
- Manage User Accounts
- Password Security and Pam
- Automating Tasks with Ssh
- Log File Administration
- Accountability With Kernel Auditd
- Selinux
- Securing Apache
- Scanning, Probing, And Mapping Vulnerabilities
- Tracking Security Updates and Software Maintenance

Audience

This course is designed for system administrators and system security specialists.

Prerequisites

Knowledge equivalent to "Linux Fundamentals" and "Enterprise Linux Systems Administration".

Duration

Five days

Course Outline

I. SECURITY CONCEPTS

- A. Basic Security Principles
- B. RHEL7 Default Install
- C. RHEL7 Firewall
- D. Minimization – Discovery
- E. Service Discovery
- F. Hardening
- G. Security Concepts
- H. LAB TASKS
    1. Removing Packages Using RPM
    2. Firewall Configuration
    3. Process Discovery
    4. Operation of the setuid() and capset() System Calls
    5. Operation of the chroot() System Call

II. SECURING SERVICES

- A. Xinetd
- B. Xinetd Connection Limiting and Access Control
- C. Xinetd: Resource limits, redirection, logging
- D. TCP Wrappers
- E. The /etc/hosts.allow & /etc/hosts.deny Files
- F. /etc/hosts.{allow,deny} Shortcuts
- G. Advanced TCP Wrappers
- H. FirewallD
- I. Netfilter: Stateful Packet Filter Firewall
- J. Netfilter Concepts
- K. Using the iptables Command
- L. Netfilter Rule Syntax
- M. Targets
- N. Common match_specs
- O. Extended Packet Matching Modules
- P. Connection Tracking
- Q. LAB TASKS
    1. Securing xinetd Services
    2. Enforcing Security Policy with xinetd
    3. Securing Services with TCP Wrappers
    4. Securing Services with Netfilter
    5. FirewallD
    6. Troubleshooting Practice

III. MANAGE THE FILESYSTEM

- A. Partitioning Disks with fdisk & gdisk
- B. Resizing a GPT Partition with gdisk
- C. Partitioning Disks with parted
- D. Non-Interactive Disk Partitioning with sfdisk
- E. Filesystem Creation
- F. Persistent Block Devices
- G. Mounting Filesystems
- H. Filesystem Maintenance
- I. Swap
- J. LAB TASKS
    1. Creating and Managing Filesystems
    2. Hot Adding Swap

IV. SECURING THE FILESYSTEM

- A. Configuring Disk Quotas
- B. Setting Quotas
- C. Viewing and Monitoring Quotas
- D. Filesystem Attributes
- E. Filesystem Mount Options
- F. GPG – GNU Privacy Guard
- G. File Encryption with OpenSSL
- H. File Encryption With encfs
- I. Linux Unified Key Setup (LUKS)
- J. LAB TASKS
    1. Setting User Quotas
    2. Securing Filesystems
    3. Securing NFS
    4. File Encryption with GPG
    5. File Encryption With OpenSSL
    6. LUKS-on-disk format Encrypted Filesystem

V. MANAGE SPECIAL PERMISSIONS

- A. File and Directory Permissions
- B. File Creation Permissions with umask
- C. SUID and SGID on files
- D. SGID and Sticky Bit on Directories
- E. Changing File Permissions
- F. User Private Group Scheme
- G. MANAGE FILE ACCESS CONTROLS
- H. File Access Control Lists
- I. Manipulating FACLs
- J. Viewing FACLs
- K. Backing Up FACLs
- L. LAB TASKS
    1. Using Filesystem ACLs

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Course Outline (cont’d)

VI. MONITOR FOR FILESYSTEM CHANGES

A. Host Intrusion Detection Systems
B. Using RPM as a HIDS
C. Introduction to AIDE
D. AIDE Installation
E. AIDE Policies
F. AIDE Usage
G. LAB TASKS

1. File Integrity Checking with RPM
2. File Integrity Checking with AIDE

VII. MANAGE USER ACCOUNTS

A. Approaches to Storing User Accounts
B. User and Group Concepts
C. User Administration
D. Modifying Accounts
E. sudo
F. Group Administration
G. RHEL DS Client Configuration
H. System Security Services Daemon (SSSD)
I. LAB TASKS

1. User Private Groups

VIII. PASSWORD SECURITY AND PAM

A. Unix Passwords
B. Password Aging
C. Auditing Passwords
D. PAM Overview
E. PAM Module Types
F. PAM Order of Processing
G. PAM Control Statements
H. PAM Modules
I. pam_unix
J. pam_cracklib.so
K. pam_env.so
L. pam_xauth.so
M. pam_tally2.so
N. pam_wheel.so
O. pam_limits.so
P. pam_nologin.so
Q. pam_deny.so
R. pam_warn.so
S. pam_securetty.so
T. pam_time.so
U. pam_access.so
V. pam_listfile.so
pam_lastlog.so
W. pam_console.so
X. LAB TASKS

1. John the Ripper
2. Cracklib
3. Using pam_listfile to Implement Arbitrary ACLs
4. Using pam_limits to Restrict Simultaneous Logins
5. Using pam_nologin to Restrict Logins
6. Using pam_access to Restrict Logins
7. su & pam

IX. AUTOMATING TASKS WITH SSH

A. OpenSSH Client & Server Configuration
B. Accessing Remote Shells
C. Transferring Files
D. SSH Key Management
E. ssh-agent
F. SSH Port Forwarding
G. LAB TASKS

1. SSH Key-based User Authentication
2. Using ssh-agent

X. LOG FILE ADMINISTRATION

A. System Logging
B. systemd Journal
C. systemd Journal's journalctl
D. Secure Logging with Journal's Log Sealing
E. gnome-system-log
F. Rsyslog
G. /etc/rsyslog.conf
H. Log Management
I. Log Anomaly Detector
J. Sending logs from the shell
K. LAB TASKS

1. Using the systemd Journal
2. Setting up a Full Debug Logfile
3. Remote Syslog Configuration
4. Remote Rsyslog TLS Configuration

Course Outline (cont'd)

XI. ACCOUNTABILITY WITH KERNEL AUDITD

A. Accountability and Auditing
B. Simple Session Auditing
C. Simple Process Accounting & Command History
D. Kernel-Level Auditing
E. Configuring the Audit Daemon
F. Controlling Kernel Audit System
G. Creating Audit Rules
H. Searching Audit Logs
I. Generating Audit Log Reports
J. Audit Log Analysis
K. LAB TASKS
  1. Auditing Login/Logout
  2. Auditing File Access
  3. Auditing Command Execution

XII. SELINUX

A. DAC vs. MAC
B. Shortcomings of Traditional Unix Security
C. SELinux Goals
D. SELinux Evolution
E. SELinux Modes
F. Gathering SELinux Information
G. SELinux Virtual Filesystem
H. SELinux Contexts
I. Managing Contexts
J. The SELinux Policy
K. Choosing an SELinux Policy
L. Policy Layout
M. Tuning and Adapting Policy
N. Booleans
O. Permissive Domains
P. Managing File Context Database
Q. Managing Port Contexts
R. SELinux Policy Tools
S. Examining Policy
T. SELinux Troubleshooting
U. LAB TASKS
  1. Exploring SELinux Modes
  2. SELinux File Contexts
  3. SELinux Contexts in Action
  4. Managing SELinux Booleans
  5. Creating Policy with Audit2allow
  6. Creating & Compiling Policy from Source

XIII. SECURING APACHE

A. Apache Overview
B. httpd.conf – Server Settings
C. Configuring CGI
D. Turning Off Unneeded Modules
E. Delegating Administration
F. Apache Access Controls (mod_access)
G. HTTP User Authentication
H. Standard Auth Modules
I. HTTP Digest Authentication
J. TLS Using mod_ssl.so
K. Authentication via SQL
L. Authentication via LDAP
M. Authentication via Kerberos
N. Scrubbing HTTP Headers
O. Metering HTTP Bandwidth
P. LAB TASKS
  1. Hardening Apache by Minimizing Loaded Modules
  2. Scrubbing Apache & PHP Version Headers
  3. Protecting Web Content
  4. Using the suexec Mechanism
  5. Create a TLS CA key pair
  6. Using SSL CA Certificates with Apache
  7. Enable Apache SSL Client Certificate Authentication
  8. Enabling SSO in Apache with mod_auth_kerb

XIV. SCANNING, PROBING, AND MAPPING VULNERABILITIES

A. The Security Environment
B. Stealth Reconnaissance
C. The WHOIS database
D. Interrogating DNS
E. Discovering Hosts
F. Discovering Reachable Services
G. Reconnaissance with SNMP
H. Discovery of RPC Services
I. Enumerating NFS Shares
J. Nessus/OpenVAS Insecurity Scanner
K. Configuring OpenVAS
L. Intrusion Detection Systems
M. Snort Rules
N. Writing Snort Rules
O. LAB TASKS
  1. NMAP
  2. OpenVAS

Course Outline (cont'd)

XV. TRACKING SECURITY UPDATES AND SOFTWARE MAINTENANCE

A. Security Advisories
B. Managing Software
C. RPM Features
D. RPM Architecture
E. RPM Package Files
F. Working With RPMs
G. Querying and Verifying with RPM
H. Updating the Kernel RPM
I. Dealing With RPM & Yum Digest Changes
J. Using the Yum command
K. Using Yum history
L. Yum Plugins & RHN Subscription Manager
M. Yum Version Lock Plugin
N. Yum Repositories
O. LAB TASKS
   1. Managing Software with RPM
   2. Creating a Custom RPM Repository
   3. Querying the RPM Database
   4. Using Yum