Linux System Security

Duration: 4 Days **Course Code: LSS** **Delivery Method: Company Event**

Overview:

Linux System Security Course Overview

This highly practical instructor led Linux System Security course is aimed at Linux System Administrators who wish to enhance their knowledge of Linux security and increase the security level of their Linux systems.
The course covers detecting and restricting users and applications for Linux and Red Hat based Linux systems. Security compliance,logging and auditing are also covered along with hardening related tasks. The topics taught are relevant for all Linux distributions. The command line is demonstrated and used extensively throughout the course.
This Linux System Security course is based on the Red Hat/CentOS Linux distribution,the delegate will be able to apply the concepts covered on this course to other Linux based distributions.
Exercises and examples are used throughout the course to give practical hands-on experience with the techniques covered.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

Who will the Course Benefit?

The Linux System Security course is aimed at Linux System Administrators who wish to expand their knowledge of the many Linux security features and increase the security level of Linux systems.
Administrators who wish to increase the logging and auditing functionality of Linux systems will also find the techniques and subjects covered in this course useful.

Objectives:

- Course Objectives
- This course aims to provide the delegate with the knowledge to be able to query Linux systems for most security related events and harden many aspects of their systems.
- The course explains and demonstrates subjects such as the; Linux logging and auditing framework,SELinux,the firewall,certificate authorities,network time,Secure Shell,Pluggable Authentication Modules,Host Intrusion and Detection Systems (HIDS),detecting and removing malware,password cracking,administering Sudo and encrypting files.

Prerequisites:

Delegates attending this course should have experience of administering Linux in an Enterprise environment to the level covered on the pre-requisite courses.

Where Red Hat 9 courses are listed in the Pre-Requisite Courses section equivalent Red Hat 7 or Red Hat 8 courses would also suffice.

Follow-on-Courses:

Further Learning

- Linux Networking
- Linux Shell Programming
- Linux Advanced Shell Programming Tools
- Apache Web Server

Content:

Linux System Security Training Course Course Contents - DAY 1

Course Introduction

- Administration and Course Materials
- Course Structure and Agenda
- Delegate and Trainer Introductions

Session 1: INTRODUCTION TO LINUX SECURITY

- Linux Native Security
- Areas of Security
- Common Attack Methods
- Basic Security Precautions
- Standards and Compliance
- Security Technical Implementation Guides (STIGs)
- Exercise

Session 2: SECURING THE USER ENVIRONMENT

- Managing User Accounts and Security Options
- Configuring Account Defaults
- Default File and Directory Permissions
- Configuring History Variables
- Querying and Confining Command Line History
- Exercise

Session 3: LINUX LOGGING AND AUDITING

- Security Related Log Files
- Querying Login Activity
- Viewing and Configuring the Journal
- Viewing and Understanding Audit Records
- Generating Audit Queries
- Defining Auditing Rules
- Audit Performance
- Exercise

Session 4: SELINUX

- DAC vs MAC
- SELinux Policy
- SELinux Contexts
- SELinux Key Commands
- Viewing SELinux Decisions
- SELinux Booleans
- Permissive and Unconfined Domains
- Exporting SELinux Configuration
- Exercise Linux System Security Training Course Course Contents - DAY 2

Session 5: SELINUX MODULES

- SELinux Entities
- Listing and Administering SELinux Modules
- Creating Modules With audit2allow

Session 6: RED HAT FIREWALL

- Firewalld Overview
- Firewalld vs IPTables
- Configuring Firewall ports
- Creating a Firewall Service
- Creating and Configuring Firewall Zones
- Viewing and Creating Rich Rules
- Fail2ban Installation and Configuration
- Exercise

Session 7: SECURING SSH

- SSH Key Algorithms
- SSH Agents and Server Options
- Restricting Authentication Methods
- Viewing and Encrypting the known_hosts File
- Certificate Based Authentication
- Verifying Signed Certificates
- Exercise

Session 8: SECURING APPLICATIONS

- TCP Wrapper Access Checking
- TCP Wrapper Extended Syntax
- Configuring an NTP Server
- Securing chrony and Authenticating Clients
- Exercise Linux System Security Training Course Course Contents - DAY 3

Session 9: INTRUSION DETECTION AND PREVENTION

- Detecting Host Intrusions
- Limitations of AIDE
- Installing and Configuring AIDE
- Detecting Filesystem Changes
- Detecting and Removing Rootkits
- Rootkit Best Practices
- Installing and Configuring ClamAV
- Exercise

Session 10: CREATING AND SIGNING AN RPM PACKAGE

- Common Vulnerabilities and Exposures (CVE's)
- Red Hat Package Management
- Obtaining Detailed Update Information
- Post Update Considerations and Rolling Back Packages
- Details on Security Packages
- Package Management History
- Creating and Signing an RMP Package
- Creating a Package Repository
- Exercise

Session 11: PLUGGABLE AUTHENTICATION MODULES

- PAM File Format

Session 13: SUDO AND RESTRICTING LOGINS

- Basic Examples and Command Line Options
- Sudo Aliases,Tags and Groups
- Sudo Password Administration
- Running Sudo On Remote Systems
- Sudoedit
- Sudo Logging and Replay
- Include Statements
- Restricting root Access
- Configuring Timeouts
- Exercise

Session 14: SECURING THE LINUX FILESYSTEM

- Partitioning Considerations
- Protecting the Boot Menu
- Securely Erasing Data
- Data Sanitisation Methods
- Extended Permissions and File Attributes
- Creating and Modifying File Access Control Lists (ACLs)
- LUKS Encrypted Partitions
- Exercise

APPENDIX A: RED HAT IDENTITY MANAGEMENT

- IRed Hat Identity Management
- Identity Management Domain
- IDM Server and Client Installation and Configuration

APPENDIX B: CERTIFICATE BASED AUTHENTICATION

- Creating a Certificate Authority
- Configuring Logging with TLS
- Securing VSFTPD for SSL/TLS

APPENDIX C: AUDIT RECORDS

APPENDIX D: RESETTING A LOST ROOT PASSWORD

- Writing and Editing SELinux Modules
- Type Enforcement and File Context Files
- Exercise

- Restricting Services with PAM
- Restricting Access to SSH
- Increasing Password Complexity
- Delaying Failed Logins
- Controlling Access by Time
- Limiting user Resources
- Exercise

Session 12: LINUX PASSWORDS

- Password Hashing Methods
- Verifying Password Strength
- Password Attacks Types
- Password Cracking
- Installing a Password Cracking Utility
- Installing a Word List
- Exercise Linux System Security Training Course Course Contents - DAY 4

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/