Syllabus: Complete Linux Security and Hardening with Practical Examples:

There are total of 10 sections in this course

Section 1 – Introduction and Course Overview

- Course Overview
- Download Syllabus

Section 2 – Security Concepts

- What is Security and OS Hardening?
- Comparing House Security with Computer Security
- Securing All Operating Systems
- Importance of Linux Security
- Security Implementation Tools
- Type of Security Breach
- Quiz, Handouts and Homework

Section 3 - Lab Setup *(optional)*

- What is VirtualBox?
- Installing Oracle VirtualBox
- Creating First Virtual Machine
- Linux Installation

Section 4 - Securing User Environment

- Understanding /etc/passwd
- /etc/group
- /etc/shadow
- The /etc/login.def File
- Create User Account and Change Password
- Change Password Parameters
- Set Password Policy
- Lock or Disable User Accounts Automatically
- Lock or Disable User Accounts Manually
- Lock User Account After 3 Failed Attempts
- Restrict root Login

- Disable SSH Access for a Specific User
- Implement UID/GID Policy
- Centralized Authentication Service
- sudo Access
- Monitor User Activity
- Quiz, Handouts and Homework

Section 5 - PAM (Pluggable Authentication Module)

- What is PAM?
- The Importance of PAM
- The PAM Configuration Files Format
- PAM Config File – Module Interfaces
- Account Access Through PAM
- PAM Config File – Control Flags
- PAM Config File – Modules (SO)
- PAM Aware Services and Stacks
- Quiz, Handouts and Homework

Section 6 - Securing Linux Filesystem

- Linux File Types
- Linux File Attributes
- Linux File Ownership and Permissions
- Changing File Permission
- Changing File Ownership
- Access Control List (ACL)
- Quiz, Handouts and Homework

Section 7 - Securing Linux System

- Message of the Day
- Customize message of the day
- Physical Server Security
- Remove Un-necessary or Orphan Packages
- Keep Kernel and System Up to Date
- Stop and Disable Unwanted Services
- Separate Disk Partitions
- Disable Ctrl+Alt+Delete
- Running One Service per System
- Change Default Console Passwords

- Disable USB Stick Detection
- Enable Network Time Protocol (NTP or Chronyd)
- Lockdown Cronjobs
- Change SSH Ports
- SELinux (longest lecture and lab)
- Backups
- Quiz, Handouts and Homework

Section 8 - Securing Linux System Network

- Introduction to Firewall
- iptables (tables, chains and targets)
- iptables (practical examples)
- Firewall (firewalld)
- firewalld (Practical Examples)
- firewalld (GUI)
- Encrypt Incoming and Outgoing Traffic
- SSH vs. Telnet
- Turn Off IPV6 (If not in use)
- Quiz, Handouts and Homework

Section 9 - Securing Environment Around Linux

- Hardware/Network Firewall
- Network Address Translation (NAT)
- VPN Tunnel
- Application and Database Encryption
- Quiz, Handouts and Homework

Section 10 - Additional Resources

- Getting Linux Commands Help
- Compress and Uncompress Files
- Changing Password
- sed Command Examples
- Talking to Users
- User Directory Authentication
- Difference AD, openLDAP, WinBind etc.
- System Log Monitor
- Recover Root Password
- File Transfer Commands

- NIC Bonding
- Advance Package Management