دوره جامع مهندسی لینوکس Linux Zero to Hero Pack

خلاصه دوره: سیستم عامل لینوکس شناخته شده ترین و پر استفاده ترین سیستم عامل متن باز (Open Source) در جهان است. لینوکس همه جا وجود دارد! از تلفن های همراه گرفته تا سیستم ها و سرور هایی که در جاهای مختلف استفاده میشود. لینوکس یکی از قابل اعتمادترین ، ایمن‌ترین و پایدارترین سیستم عامل‌های موجود در جهان است. در این پکیج آموزشی تمامی آن چیزی که برای تبدیل شدن به یک متخصص لینوکس نیاز است گنجانده شده است. دانشجویان در ابتدا با مفاهیم پایه و ابتدایی لینوکس در دوره Linux Essentials آشنا شده و سپس به ترتیب دوره های LPIC 1 ، LPIC 2 و LPIC 3 – 303 را طی میکنند. در طول این دوره از توزیع (Distro) های مختلف استفاده شده و یک لابراتوار نیز برای انجام تمرین های مختلف به دانشجویان داده خواهد شد.

مدت دوره : ۱۱۰ ساعت

پیش نیاز: Network+

مخاطبین دوره:

- کارشناسان و متخصصین شبکه
- کارشناسان و متخصصین امنیت شبکه

این پکیج شامل دوره‌های زیر می باشد:

- Linux Essentials
- LPIC 1
- LPIC 2
- LPIC 3 – 303 (Security)

سرفصل های دوره:

Linux Essentials:

1. The Linux Community and a Career in Open Source
    a. Linux Evolution and Popular Operating Systems
    b. Major Open Source Applications
    c. Open Source Software and Licensing
    d. ICT Skills and Working in Linux

2. Finding Your Way on a Linux System
    a. Command Line Basics
    b. Using the Command Line to Get Help
    c. Using Directories and Listing Files
    d. Creating, Moving and Deleting Files
3. The Power of the Command Line
    a. Archiving Files on the Command Line
    b. Searching and Extracting Data from Files
    c. Turning Commands into a Script
4. The Linux Operating System
    a. Choosing an Operating System
    b. Understanding Computer Hardware
    c. Where Data is Stored
    d. Your Computer on the Network
5. Security and File Permissions
    a. Basic Security and Identifying User Types
    b. Creating Users and Groups
    c. Managing File Permissions and Ownership
    d. Special Directories and Files

LPIC 1:

101: System Architecture

101.1 Determine and configure hardware settings

101.2 Boot the system

101.3 Change runlevels / boot targets and shutdown or reboot system

102: Linux Installation and Package Management

102.1 Design hard disk layout

102.2 Install a boot manager

102.3 Manage shared libraries

102.4 Use Debian package management

102.5 Use RPM and YUM package management

102.6 Linux as a virtualization guest

103: GNU and Unix Commands

103.1 Work on the command line

103.2 Process text streams using filters

103.3 Perform basic file management

103.4 Use streams, pipes and redirects

103.5 Create, monitor and kill processes

103.6 Modify process execution priorities

103.7 Search text files using regular expressions

103.8 Basic file editing

104: Devices, Linux Filesystems, Filesystem Hierarchy Standard

104.1 Create partitions and filesystems

104.2 Maintain the integrity of filesystems

104.3 Control mounting and unmounting of filesystems

104.5 Manage file permissions and ownership

104.6 Create and change hard and symbolic links

104.7 Find system files and place files in the correct location

105: Shells and Shell Scripting

105.1 Customize and use the shell environment

105.2 Customize or write simple scripts

106: Interfaces and Desktops

106.1 Install and configure X11

106.2 Graphical Desktops

107: Administrative Tasks

107.1 Manage user and group accounts and related system files

107.2 Automate system administration tasks by scheduling jobs

107.3 Localisation and internationalization

108: Essential System Services

108.1 Maintain system time

108.2 System logging

108.3 Mail Transfer Agent (MTA) basics

108.4 Manage printers and printing

109: Networking Fundamentals

109.1 Fundamentals of internet protocols

109.2 Persistent network configuration

109.3 Basic network troubleshooting

110: Security

109.4 Configure client side DNS

110.1 Perform security administration tasks

110.2 Setup host security

110.3 Securing data with encryption

LPIC 2:

200: Capacity Planning

200.1 Measure and Troubleshoot Resource Usage

200.2 Predict Future Resource Needs

201: Linux Kernel

201.1 Kernel Components

201.2 Compiling a kernel

201.3 Kernel runtime management and troubleshooting

202: System Startup

202.1 Customizing SysV-init system startup

202.2 System Recovery

202.3 Alternate Bootloaders

203: Filesystem and Devices

203.1 Operating the Linux filesystem

203.2 Maintaining a Linux filesystem

203.3 Creating and configuring filesystem options

204: Advanced Storage Device Administration

204.1 Configuring RAID

204.2 Adjusting Storage Device Access

204.3 Logical Volume Manager

205: Networking Configuration

205.1 Basic networking configuration

205.2 Advanced Network Configuration and Troubleshooting

205.3 Troubleshooting Network Issues

206: System Maintenance

206.1 Make and install programs from source

206.2 Backup operations

206.3 Notify users on system-related issues

207: Domain Name Server

207.1 Basic DNS server configuration

207.2 Create and maintain DNS zones

207.3 Securing a DNS server

208: Web Services

208.1 Implementing a web server

208.2 Apache configuration for HTTPS

208.3 Implementing a proxy server

208.4 Implementing Nginx as a web server and a reverse proxy

209: File Sharing

209.1 SAMBA Server Configuration

209.2 NFS Server Configuration

210: Network Client Management

210.1 DHCP configuration

210.2 PAM authentication

210.3 LDAP client usage

210.4 Configuring an OpenLDAP server

211: E-Mail Services

211.1 Using e-mail servers

211.2 Managing Local E-Mail Delivery

211.3 Managing Remote E-Mail Delivery

212: System Security

212.1 Configuring a router

212.2 Securing FTP servers

212.3 Secure shell (SSH)

212.4 Security tasks

212.5 OpenVPN

LPIC 3 (303):

325: Cryptography

325.1 X.509 Certificates and Public Key Infrastructures

325.2 X.509 Certificates for Encryption, Signing and Authentication

325.3 Encrypted File Systems

325.4 DNS and Cryptography

326: Host Security

326.1 Host Hardening

326.2 Host Intrusion Detection

326.3 User Management and Authentication

326.4 FreeIPA Installation and Samba Integration

327: Access Control

327.1 Discretionary Access Control

327.2 Mandatory Access Control

327.3 Network File Systems

328: Network Security

328.1 Network Hardening

328.2 Network Intrusion Detection

328.3 Packet Filtering

328.4 Virtual Private Networks