LPIC-2 Linux Server Administration Exam 202

Duration:
5 Days

What is the course about?
LPIC-2 is the second certification in LPI's multi-level professional certification program. The LPIC-2 will validate the candidate's ability to administer small to medium–sized mixed networks. The candidate must have an active LPIC-1 certification to receive LPIC-2 certification, but the LPIC-1 and LPIC-2 exams may be taken in any order.

Duration
The course is run 5 days full time.

Technical Skill

To become LPIC-2 certified the candidate must be able to:

- perform advanced system administration, including common tasks regarding the Linux kernel, system startup and maintenance;
- perform advanced Management of block storage and file systems as well as advanced networking and authentication and system security, including firewall and VPN;
- install and configure fundamental network services, including DHCP, DNS, SSH, Web servers, file servers using FTP, NFS and Samba, email delivery; and
- supervise assistants and advise management on automation and purchases

Private Training
The course can be offered privately onsite or on our premises. A minimum of 4 delegates is required to schedule the course. The course price is R9 500 onsite and R12 500 on our premises. There is no set date to run the course; we schedule a date that suits your team.

Public Training
This course is also offered publicly. The course runs at our offices in Cape Town or Johannesburg. A minimum of 4 delegates is required to run the course. A tentative date is set but the course will only be confirmed to run once we have 4 confirmed bookings. There is no set date as the course is run on demand.

Course Topics

Basic DNS Server Configuration
BIND 9.x configuration files, terms and utilities
Defining the location of the BIND zone files in BIND configuration files
Reloading modified configuration and zone files
Awareness of dnsmasq, djbdns and PowerDNS as alternate name servers

Create and Maintain DNS Zones

BIND 9 configuration files, terms and utilities
Utilities to request information from the DNS server
Layout, content and file location of the BIND zone files
Various methods to add a new host in the zone files, including reverse zone

Securing a DNS server

BIND 9 configuration files
Configuring BIND to run in a chroot jail
Split configuration of BIND using the forwarders statement
Configuring and using transaction signatures (TSIG)
Awareness of DNSSEC and basic tool

Implementing a web server

Apache 2.x configuration files, terms and utilities
Apache log files configuration and content
Access restriction methods and files
mod_perl and PHP configuration
Client user authentication files and utilities
Configuration of maximum requests, minimum and maximum servers and clients
Apache 2.x virtual host implementation (with and without dedicated IP addresses)
Using redirect statements in Apache's configuration files to customize file access

Appache Configuration for HTTPS

SSL configuration files, tools and utilities
Ability to generate a server private key and CSR for a commercial CA
Ability to generate a self-signed Certificate from private CA
Ability to install the key and Certificate
Awareness of the issues with Virtual Hosting and use of SSL
Security issues in SSL use

Implementing a Proxy Server

Squid 3.x configuration files, terms and utilities
Access restriction methods
Client user authentication methods
Layout and content of ACL in the Squid configuration files

Implementing Nginx as a web server and a reverse proxy

Nginx
Reverse Proxy
Basic Web Server

SAMBA Server Configuration

Samba 3 documentation
Samba configuration files
Samba tools and utilities
Mounting Samba shares on Linux
Samba daemons
Mapping Windows usernames to Linux usernames
User-Level and Share-Level security

NFS Server Configuration
NFS version 3 configuration files
NFS tools and utilities
Access restrictions to certain hosts and/or subnets
Mount options on server and client
TCP Wrappers
Awareness of NFSv4

DHCP Configuration
DHCP configuration files, terms and utilities
Subnet and dynamically-allocated range setup

PAM Authentication
PAM configuration files, terms and utilities
passwd and shadow passwords

LDAP Client Usage
LDAP utilities for data management and queries
Change user passwords
Querying the LDAP directory

Configuring an OpenLDAP Server
OpenLDAP
Access Control
Distinguished Names
Changetype Operations
Schemas and Whitepages
Directories
Object IDs, Attributes and Classes
Awareness of System Security Services Daemon (SSSD)

Using E-mail Servers
Configuration files for postfix
Basic knowledge of the SMTP protocol
Awareness of sendmail and exim

Managing Local E-mail Delivery
procmail configuration files, tools and utilities
Usage of procmail on both server and client side

Managing Remote E-mail Delivery
Courier IMAP and Courier POP configuration
Dovecot configuration

Configuring a router
iptables configuration files, tools and utilities
Tools, commands and utilities to manage routing tables.
Private address ranges
Port redirection and IP forwarding
List and write filtering and rules that accept or block datagrams based on source or
Destination protocol, port and address

Save and reload filtering configurations
Awareness of ip6tables and filtering

Securing FTP Servers

Configuration files, tools and utilities for Pure-FTPd and vsftpd
Awareness of ProFTPd
Understanding of passive vs. active FTP connections

Secure Shell (SSH)

OpenSSH configuration files, tools and utilities
Login restrictions for the superuser and the normal users
Managing and using server and client keys to login with and without password
Usage of multiple connections from multiple hosts to guard against loss of connection to remote host following configuration changes

Security Tasks

Tools and utilities to scan and test ports on a server
Locations and organizations that report security alerts as Bugtraq, CERT or other sources
Tools and utilities to implement an intrusion detection system (IDS)
Awareness of OpenVAS and Snort

OpenVPN

Candidates should be able to configure a VPN (Virtual Private Network) and create secure point-to-point or site-to-site connections.