

## LINUX LPI-202 CERTIFICATION COURSE



The **Linux LPI-202 Course** is part two of an exam syllabus designed to lead to LPIC-2 Advanced Level Administration certification.

Linux Professional Institute (LPI) promote and certify essential skills on Linux and Open Source technologies through the global delivery of comprehensive, top quality, vendor-independent exams.

The **LPI certification** program is arranged into three main levels by job tasks. Distance Learning Centre offers LPI Approved Training Material for the LPIC-1 (Level 1) and LPIC-2 (Level 2) certifications.

Open-source operating systems, most notably Linux, are rapidly gaining ground on more popular proprietary software. Much of this success is due to the efforts of the Linux Professional Institute (LPI).

Besides promoting the use of Linux-based, open-source and free software, LPI seeks to advance the skills of professionals who use these systems through its LPI certification program.

### The LPI Certification Program is:

- Designed by a community of Linux professionals, volunteers, vendors and educators.
- Challenging: if you don't know the subjects you won't pass.
- Accessible and available at thousands of test centres around the world or at special events.
- Of high quality: relying on critical input from numerous Linux experts and employing scientific and industry-recognized psychometric processes.
- Distribution-neutral: verifying knowledge on any standard Linux system.
- Relevant: surveying thousands to determine the skills that need to be tested.
- Training-vendor independent: encouraging a variety of methods and approaches to test preparation.
- Supported and sponsored by a large number of Linux companies and projects.
- A certification the Linux community can respect and be proud of.

### ➤ **Linux LPI-202 Course Book:**

#### The course book covers the following Units:

##### • **Lesson One – Introduction**

The following topics are covered: Course Format; Product Development; Structure; Objectives; Conventions; Introduction to Labs; Introduction to Lab Solutions; and Lab Conventions.

##### • **Lesson Two – Networking**

The following topics are covered: Objectives; Configuring the Network Interface – (The Loopback Interface; Ethernet Interfaces) Routing Through a Gateway; Virtual Private Networks; What Is A VPN; VPN Types; SSH and PPP The Server; The Client; IPSEC; Authentication Over PPP Secrets Files; The CHAP Secrets File; Troubleshooting – (ifconfig; ping; route; traceroute; arp and arpwatc; tcpdump; nc); and Summary.

**Price:**  
£275.00

#### **Instalment Options:**

You can spread the payments for this course over 4 monthly payments. 1 initial payment of £110.00, followed by 3 monthly payments of £55.00.

**Course Format:**  
Linux LPI Course Book

**Assessment:**  
Linux Professional Institute  
LPI-202 Examination

**Approximate Study Time:**  
120 Hours of Self Study

- **Lesson Three – DNS**

The following topics are covered: Objectives; BIND 8; named.conf; Syntax; The options Statement; The directory Statement; The forwarders Statement; The forward Statement; The version Statement; The dialup Statement; The logging Statement; Predefined Zone Statements; Converting BIND Configurations; The named Name Server Daemon; The ndc Program; Signals to named; Controlling named with a Start/Stop Script; Zones and Reverse zones; The db.local File; The db.127 File; The hints File; Zone Definitions in named.conf; The \$TTL Statement; Resource Records; SOA Record; A Record; CNAME Record; NS Record; HINFO Record; MX Record; MXing a Domain; Reverse Zone Files; PTR Record; Master and Slave Servers; Configuring a Master; Configuring a Slave; Creating Subdomains; Delegating a DNS Zone; DNS Utilities – (dig; host; nslookup); Internal DNS; Limiting Negotiations; Split DNS: Stand-Alone Internal Master; Configuring the Master on privdns; Configuring DNS on liongate; Alternatives; Split DNS: Two DNS Servers On One Machine; Two Name Servers On One Host; Configuring the Internal Name Server; Configuring the Visible Name Server; A Problem; and Summary.

- **Lesson Four – DNS Security**

The following topics are covered: Objectives; DNS Security Strategies; Making Information Harder to Obtain; Hiding the Version Number; Limiting Access; Limiting Queries; Limiting Zone Transfers; Controlling Requests; Turning Off Glue; Mitigating the Effects of an Intrusion; Running BIND with Less Privileges; Running BIND in a chroot Jail; Preparing a chroot Jail; Running BIND chrooted; Configuration for a chrooted BIND; Combining Special User and chroot; Securing Name Server Connections; Using the dnskeygen Command; Generated Key Files; Using the Key; and Summary.

- **Lesson Five – DHCP & NIS**

The following topics are covered: Objectives; What is DHCP?; Configuring the Server; Global Parameters; Shared-network Declarations; Subnet Declarations; Group Declaration; Host Declaration; Sample DHCP Scenario; Available Network Services; Subnet Independent Services; Subnet Dependent Services; Building the DHCP Server's Configuration File; The Global Parameters for Services; The Company's Shared Networks and Subnets; Static Hosts; Static BOOTP Hosts; Controlling the DHCP Server's Behavior; Leases; Interfaces; Restarting the DHCP Server After Making Changes; DHCP Relaying; Configuring a System as a NIS Client; Setting Up NIS Master and Slave Servers; Configuring Master and Slave Servers; Creating NIS Maps; NIS Related Commands; NIS Related Files – (nis.conf; nsswitch.conf; yperv.conf); Pluggable Authentication Modules; Authentication; Authentication via /etc/passwd and /etc/shadow – (Account; auth; password; and session); Configuring Authentication via NIS; Configuring Authentication via LDAP; and Summary.

- **Lesson Six – Mail & News**

The following topics are covered: Objectives; Majordomo; Creating a Mailing List; Aliases; Majordomo Files; Maintaining a Mailing List; Configuring Sendmail; Mail Aliases; Procmail; Recipes; Internet News; Installing INN; Configuring INN; Creating News Groups; Newsfeeds; and Summary.

- **Lesson Seven – LDAP**

The following topics are covered: Objectives; LDAP; Installing and Configuring an LDAP Server; Obtaining the Software; Configuring a Directory Hierarchy; Editing the Idif File; Adding Data to the Hierarchy; Changing Data in the Hierarchy; Additional Information; and Summary.

- **Lesson Eight – Web Services: Apache & Squid**

The following topics are covered: Objectives; Installing the Apache Web Server; Configuring Apache Server Options; Modularity; Run-time Loading of Modules (DSO); APache eXtenSion (APXS) Support Tool; Encrypted Web Servers: SSL; Public Key Cryptography; Various Apache and SSL Related Projects; Apache-SSL; Apache with mod\_ssl; Monitoring Apache Load and Performance; Restricting Access; The access\_log File; Restricting Client User Access; Configuring Authentication; User Files; Group Files; Configuring mod\_perl and mod\_php; Virtual Hosting; Name-based Virtual Hosting; IP-based Virtual Hosting; Setting Up Multiple Daemons; Setting Up a Single Daemon; Customizing File Access; How to Create a SSL Server Certificate; Proxy Servers: Squid; The squid.conf File; Sections in the squid.conf File – (http\_port; cache\_dir; http\_access, acl; and authenticate\_program); Redirectors Authentication; Security Issues; Access Policies; Memory Usage; and Summary.

- **Lesson Nine – System Security**

The following topics are covered: Objectives; Denial of Service (DoS) Attacks; Protecting Against DoS Attacks; routed; Sentry Tools and PortSentry: Preventing Port Scans; Installation and Configuration; Securing FTP Servers; Installing ftpd; Creating an “ftp” User For Anonymous FTP; Welcome Message For All FTP Users; Successful Login Messages; Directory Specific Messages; Preventing All FTP Connections; Preventing Specific Users From Using FTP; Restricting Specific Users to Their Home Directories; Restricting Groups; The Washington University FTP Server; Creating an “ftp” User For Anonymous FTP; Welcome Message For All FTP Users; Login Message For All Non-privileged Users; Directory Specific Messages; Preventing All FTP Connections; Preventing Specific Users Or Groups From Using FTP; Restricting Specific Users To Their Home Directories; Additional Precautions; TCP Wrappers; Configuring TCP Wrappers; xinetd; Testing for Open Mail Relays; Keeping Track of Security Alerts; Bugtraq; Subscribing to the Bugtraq Mailing List; CERT; Subscribing to the CERT Advisory Mailing List; CIAC; Subscribing to the Mailing List; and Summary.

- **Lesson Ten – Security Programs**

The following topics are covered: Objectives; Kerberos; Preparing the Installation; Kerberos Realms; Mapping Hostnames on to Kerberos Realms; Ports for the KDC and Administration Services; Slave KDCs; Hostnames for the Master and Slave KDCs; Database Propagation; Installation and Configuration; Installing and Configuring the Master KDC; Edit the Configuration Files; Create the Database; Add Administrators to the ACL File; Add Administrators to the Kerberos Database; Create a kadmind Keytab; Start the Kerberos Daemons on the Master KDC; Install and Configuring the Slave KDCs; Create Host Keys for the Slave KDCs; Extract Host Keytabs for the KDCs; Set Up the Slave KDCs for Database Propagation; Back on the Master KDC; Propagate the Database to Each Slave KDC; Finish Installing the Slave KDCs; Create Stash Files on the Slave KDCs; Start the krb5kdc Daemon on Each KDC; Add Kerberos Principals to the Database; Limiting Access to the KDCs; Switching Master and Slave KDCs; Snort; Installation and Configuration; Rules; Tripwire; Installation; The Tripwire Configuration File: twcfg.txt; Required Variables; Other Variables; The Tripwire Policy File; Comments; Directives; Variables; Rules; Nmap; Using the nmap Command; and Summary.

- **Lesson Eleven – Secure Shell**

The following topics are covered: Objectives; Secure Shell (ssh); Configuring sshd; Allow or Deny root Logins; Allow or Deny Non-root Logins; Enabling or Disabling X Forwarding; Keys and Their Purpose; Creating Public and Private User Keys with ssh-keygen; Using the Keys; Configuring the ssh-agent; ssh-add; Enabling X-sessions; Tunnelling with ssh and Port Mapping; The .rhosts and .shosts Files; and Summary.

- **Lesson Twelve – IPCHAINS and IPTABLES**

The following topics are covered: Objectives; Private Network Addresses; IP Masquerading with IPCHAINS; IP Forwarding with IPCHAINS; Port Redirection with IPCHAINS; IPCHAINS; The Firm's Network with IPCHAINS; IPTABLES; Tables and Chains; The MANGLE table; The NAT Table; The FILTER Table; Connection Tracking; Stateful Firewalling; Adding Extra Functionality; Adding Targets; Adding matching modules; The Firm's Network with IPTABLES; Creating the Firewall; Saving And Restoring Firewall Rules; and Summary.

- **Lesson Thirteen – Secure Shell**

The following topics are covered: Objectives; Troubleshooting Network Issues; Cost Effectiveness; Getting Help; Troubleshooting Tools – (netstat; hostname; dmesg; lsd; lsmod; modprobe; insmod; uname; /proc; strace; ltrace; strings; fuser; lsof); An Example Situation; and Summary.

### Pre-Requirements:

Students should have completed the LPI-1 Certification.

Students should be able to: Administer a small to medium-sized site; Plan, implement, maintain, keep consistent, secure, and troubleshoot a small mixed (MS, Linux) network, including a: LAN server (samba) Internet Gateway (firewall, proxy, mail, news) Internet Server (webserver, FTP server) Supervise assistants; and Advise management on automation and purchases.

### Course Duration & Support:

Students may register at any time. The courses are designed as self-study courses but if you have any problems you can email our email support. As the course is self study you can complete in as little or as long a time as you prefer, and we do not impose a cut-off date for study.

### Assessment:

Assessment is from the Linux LPI-202 Examination. Examinations are 120 minutes in length each and have 60 questions in multiple choice/multiple answer format. The Exam is graded on a scale of 200 - 800 with a minimum passing score of 500.

### Qualification:

On Completion of the Linux LPI-202 Course, you can apply for your **internationally recognised Linux Professional Institute LPI-202 Examination**.

Examinations must be sat at a registered Prometric or Pearson VUE testing centre and are currently £120.00 + VAT each.

You can locate testing centres and schedule appointments on their Websites:

**Prometric website** – <http://www.prometric.com/>

**Pearson VUE** - <http://pearsonvue.com/>

