

**Course Outline:** Linux Professional Institute-LPI 202

**Learning Method:** Instructor-led Classroom Learning

**Duration:** 5.00 Day(s)/ 40 hrs

**Overview:**

The LPI certification is a vendor-neutral Linux credential that measures critical Linux system and Network administration skills. LPI prides itself on delivering statistically valid exams and provides a quality testing experience for candidates around the globe. The LPIC Level II certification consists of two exams, LPI 201 and LPI 202. This 5-day course focuses on the LPI 202 exam and addresses the following knowledge areas

- Network configuration
- Mail and news
- DNS
- Web Services
- Network Client Management
- System Security

**Who Should Attend:**

This course is intended for individuals who are employed as a Systems Administrator, Systems Engineer and IT Manager.

Phone: +357 70002770  
[www.computrain.com.cy](http://www.computrain.com.cy)



## Outline:

### Module 1: Networking

- 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
- Implementing DNS Services

### Module 2: DNS

- 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 sub domains
- Delegating a DNS zone
- DNS utilities dig host nslookup
- Internal DNS
- Limiting negotiations
- Split DNS: stand-alone internal master
- Configuring the master on privdms
- Configuring DNS on liongate
- Alternatives Split DNS: two DNS servers on one machine
- Two name servers on one machine
- Configuring the internal name server
- Configuring the visible name server

### Module 3: DNS Security

- DNS security strategies
- Making information harder to obtain
- Hiding the version number
- Limiting access
- Limiting queries
- Limiting zone transfers
- Controlling requests
- Turning of glue
- Mitigating the effects of an intrusion

Phone: +357 70002770  
[www.computrain.com.cy](http://www.computrain.com.cy)



- 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

#### Module 4: DHCP and NIS

- What is DHCP?
- Configuring the server
- Global parameters
- Shared-network declarations
- Subnet declarations
- Group declarations
- 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 . ypserv.conf
- Pluggable authentication modules
- Authentication . Authentication via /etc/passwd and /etc/shadow . account . auth . password . session .
- Configuring authentication via NIS . Configuring authentication via LDAP

#### Module 5: Mail and news

- 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

#### Module 6: LDAP

- Installing and configuring an LDAP Server
- Obtaining the software
- Configuring a directory hierarchy
- Editing the Idif file
- Adding data to the hierarchy

Phone: +357 70002770  
[www.computrain.com.cy](http://www.computrain.com.cy)



- Changing data in the hierarchy
- Additional information

- Authentication
- Security issues
- Access policies
- Memory usage

### Module 7: Web services: Apache and Squid

- 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 . mod\_perl . 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 . authenticate\_program
- Redirectors

### Module 8: System security

- 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-chooted 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
- Testing for Open Mail relays Keeping track of security alerts
- Subscribing to the Bugtraq mailing list
- Cert

Phone: +357 70002770  
[www.computrain.com.cy](http://www.computrain.com.cy)



- Subscribing to the Cert Advisory Mailing List
- CIAC
- Subscribing to the mailing list

### Module 9: Security programs

- Kerberos
- Preparing the installation
- Kerberos realms
- Mapping hostnames on to Kerberos realms Ports for the KDC and administrative 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 configure the slave KDCs Create host keys for the Slave KDCs
- Extract host keytabs for the KDCs
- Setup 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 krbSkdc 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 and configuration
- The Tripwire configuration file twcfg.txt
- Required variables
- Other variables
- The Tripwire Policy file
- Comments
- Using the n map command

### Module 10: Secure shell

- 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
- Tunneling with ssh and port Mapping
- The .rhosts and .shosts files

### Module 11: IPCHAINS and IPTABLES

- Private network addresses
- IP masquerading with IPCHAINS
- IP forwarding with IPCHAINS
- Port redirection with IPCHAINS
- The firm's network with IPCHAINS
- IPTABLES
- Tables and chains
- The MANGLE table
- The NAT table

Phone: +357 70002770  
[www.computrain.com.cy](http://www.computrain.com.cy)



- 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

### Module 12: Troubleshooting

- Troubleshooting network issues
- Cost effectiveness
- Getting help
- Troubleshooting tools
- netstat . hostname . dmesg . lsdev  
lsmod . modprobe . insmod .  
uname . /proc . strace . ltrace .  
strings . fuser . lsof

Phone: +357 70002770  
[www.computrain.com.cy](http://www.computrain.com.cy)

