Future Cert

LPIC-3: Linux Enterprise Professional Certification

LPIC-3 303: Security

LPIC-3 is a professional certification program program that covers enterprise Linux specialties. LPIC-3 303 covers administering Linux enterprise-wide with an emphasis on Security.

To become LPIC-3 certified, a candidate with an active LPIC-1 and LPIC-2 certification must pass at least one of the following specialty exams. Upon successful completion of the requirements, they will be entitled to the specialty designation: LPIC-3 Specialty Name. For example, LPIC-3 Virtualization & High Availability.

Specialties:

- 300: Mixed Environment
- 303: Security
- 304: Virtualization and High Availability

TOPIC 325: CRYPTOGRAPHY

325.1 X.509 Certificates and Public Key Infrastructures (5)

Candidates should understand X.509 certificates and public key infrastructures. They should know how to configure and use OpenSSL to implement certification authorities and issue SSL certificates for various purposes.

Key knowledge areas:

- Understand X.509 certificates, X.509 certificate lifecycle, X.509 certificate fields and X.509v3 certificate extensions
- Understand trust chains and public key infrastructures
- Generate and manage public and private keys
- Create, operate and secure a certification authority
- Request, sign and manage server and client certificates
- Revoke certificates and certification authorities

325.2 X.509 Certificates for Encryption, Signing and Authentication (4)

Candidates should know how to use X.509 certificates for both server and client authentication. Candidates should be able to implement user and server authentication for Apache HTTPD. The version of Apache HTTPD covered is 2.4 or higher.

Key knowledge areas:

- Understand SSL, TLS and protocol versions
- Understand common transport layer security threats, for example Man-in-the-Middle
- Configure Apache HTTPD with mod_ssl to provide HTTPS service, including SNI and HSTS
- Configure Apache HTTPD with mod_ssl to authenticate users using certificates
- Configure Apache HTTPD with mod_ssl to provide OCSP stapling
- Use OpenSSL for SSL/TLS client and server tests

325.3 Encrypted File Systems (3)

Candidates should be able to setup and configure encrypted file systems.

Key knowledge areas:

- Understand block device and file system encryption
- Use dm-crypt with LUKS to encrypt block devices
- Use eCryptfs to encrypt file systems, including home directories and
- PAM integration
- Be aware of plain dm-crypt and EncFS

325.4 DNS and Cryptography (5)

Candidates should have experience and knowledge of cryptography in the context of DNS and its implementation using BIND. The version of BIND covered is 9.7 or higher.

Key knowledge areas:

- Understanding of DNSSEC and DANE
- Configure and troubleshoot BIND as an authoritative name server serving DNSSEC secured zones
- Configure BIND as an recursive name server that performs DNSSEC validation on behalf of its clients
- Key Signing Key, Zone Signing Key, Key Tag
- Key generation, key storage, key management and key rollover
- Maintenance and re-signing of zones
- Use DANE to publish X.509 certificate information in DNS
- Use TSIG for secure communication with BIND

TOPIC 326: HOST SECURITY

326.1 Host Hardening (3)

Candidates should be able to secure computers running Linux against common threats. This includes kernel and software configuration.

Key knowledge areas:

- Configure BIOS and boot loader (GRUB 2) security
- Disable useless software and services
- Use sysctl for security related kernel configuration, particularly ASLR,
- Exec-Shield and IP / ICMP configuration
- Limit resource usage
- Work with chroot environments
- Drop unnecessary capabilities
- Be aware of the security advantages of virtualization

326.2 Host Intrusion Detection (4)

Candidates should be familiar with the use and configuration of common host intrusion detection software. This includes updates and maintenance as well as automated host scans.

Exam Objectives Version: Version 2.0 (last major update: September 2015)

Exam Covered: LPIC-3 (303-200); Exam 1 of 1 to obtain LPIC-3 Linux Enterprise Professional: Security certification

Objectives Reflected in Published Exam: January 2016

Required Prerequisite: Successfully pass LPIC-1 101 and 102 and LPIC-2 201 and 202 exams

About objective weights: Each objective is assigned a weighting value (x). The weights range roughly from 1 to 10 and indicate the relative importance of each objective. Objectives with higher weights will be covered in the exam with more questions.

Key knowledge areas:

- Use and configure the Linux Audit system
- Use chkrootkit
- Use and configure rkhunter, including updates
- Use Linux Malware Detect
- Automate host scans using cron
- Configure and use AIDE, including rule management
- Be aware of OpenSCAP

326.3 User Management and Authentication (5)

Candidates should be familiar with management and authentication of user accounts. This includes configuration and use of NSS, PAM, SSSD and Kerberos for both local and remote directories and authentication mechanisms as well as enforcing a password policy.

Key knowledge areas:

- Understand and configure NSS
- Understand and configure PAM
- Enforce password complexity policies and periodic password changes
- Lock accounts automatically after failed login attempts
- Configure and use SSSD
- Configure NSS and PAM for use with SSSD
- Configure SSSD authentication against Active Directory, IPA, LDAP,
- Kerberos and local domains
- Obtain and manage Kerberos tickets

326.4 FreeIPA Installation and Samba Integration (4)

Candidates should be familiar with FreeIPA v4.x. This includes installation and maintenance of a server instance with a FreeIPA domain as well as integration of FreeIPA with Active Directory.

Key knowledge areas:

- Understand FreeIPA, including its architecture and components
- Understand system and configuration prerequisites for installing FreeIPA
- Install and manage a FreeIPA server and domain
- Understand and configure Active Directory replication and Kerberos cross-realm trusts
- Be aware of sudo, autofs, SSH and SELinux integration in FreeIPA

TOPIC 327: ACCESS CONTROL

327.1 Discretionary Access Control (3)

Candidates are required to understand Discretionary Access Control and know how to implement it using Access Control Lists. Additionally, candidates are required to understand and know how to use Extended Attributes.

Key knowledge areas:

- Understand and manage file ownership and permissions, including SUID and SGID
- Understand and manage access control lists
- Understand and manage extended attributes and attribute classes

327.2 Mandatory Access Control (4)

Candidates should be familiar with Mandatory Access Control systems for Linux. Specifically, candidates should have a thorough knowledge of SELinux. Also, candidates should be aware of other Mandatory Access Control systems for Linux. This includes major features of these systems but not configuration and use.

Key knowledge areas:

- Understand the concepts of TE, RBAC, MAC and DAC
- Configure, manage and use SELinux
- Be aware of AppArmor and Smack

327.3 Network File Systems (3)

Candidates should have experience and knowledge of security issues in use and configuration of NFSv4 clients and servers as well as CIFS client services. Earlier versions of NFS are not required knowledge.

Key knowledge areas:

- Understand NFSv4 security issues and improvements
- Configure NFSv4 server and clients
- Understand and configure NFSv4 authentication mechanisms (LIPKEY, SPKM, Kerberos)
- Understand and use NFSv4 pseudo file system
- Understand and use NFSv4 ACLs
- Configure CIFS clients
- Understand and use CIFS Unix Extensions
- Understand and configure CIFS security modes (NTLM, Kerberos)
- Understand and manage mapping and handling of CIFS ACLs and SIDs in a Linux system

TOPIC 328: NETWORK SECURITY

328.1 Network Hardening (4)

Candidates should be able to secure networks against common threats. This includes verification of the effectiveness of security measures.

Key knowledge areas:

- Configure FreeRADIUS to authenticate network nodes
- Use nmap to scan networks and hosts, including different scan methods
- Use Wireshark to analyze network traffic, including filters and statistics
- Identify and deal with rogue router advertisements and DHCP messages

328.2 Network Intrusion Detection (4)

Candidates should be familiar with the use and configuration of network security scanning, network monitoring and network intrusion detection software. This includes updating and maintaining the security scanners.

Key knowledge areas:

- Implement bandwidth usage monitoring
- Configure and use Snort, including rule management
- Configure and use OpenVAS, including NASL

328.3 Packet Filtering (5)

Candidates should be familiar with the use and configuration of packet filters. This includes netfilter, iptables and ip6tables as well as basic knowledge of nftables, nft and ebtables.

Key knowledge areas:

- Understand common firewall architectures, including DMZ
- Understand and use netfilter, iptables and ip6tables, including standard modules, tests and targets
- Implement packet filtering for both IPv4 and IPv6
- Implement connection tracking and network address translation
- Define IP sets and use them in netfilter rules
- Have basic knowledge of nftables and nft
- Have basic knowledge of ebtables
- Be aware of conntrackd

328.4 Virtual Private Networks (4)

Candidates should be familiar with the use of OpenVPN and IPsec.

Key knowledge areas:

- Configure and operate OpenVPN server and clients for both bridged and routed VPN networks
- Configure and operate IPsec server and clients for routed VPN networks using IPsec-Tools/racoon
- Awareness of L2TP