LPI 303-300

LPI LPIC-3 Certification Questions & Answers

Exam Summary – Syllabus –Questions

303-300
LPIC-3 Security
60 Questions Exam – 500 / 800 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your 303-300 Certification Well:

The 303-300 is best suitable for candidates who want to gain knowledge in the LPI Linux System Administration. Before you start your 303-300 preparation you may struggle to get all the crucial LPIC-3 materials like 303-300 syllabus, sample questions, study guide.

But don't worry the 303-300 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the 303-300 syllabus?
- How many questions are there in the 303-300 exam?
- Which Practice test would help me to pass the 303-300 exam at the first attempt?

Passing the 303-300 exam makes you LPIC-3 Security. Having the LPIC-3 certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

LPI 303-300 LPIC-3 Certification Details:

Exam Name	LPIC-3 Security
Exam Code	303-300
Exam Price	$200 (USD)
Duration	90 mins
Number of Questions	60
Passing Score	500 / 800
Schedule Exam	**LPI Marketplace**
Sample Questions	**LPI LPIC-3 Sample Questions**
Practice Exam	**LPI 303-300 Certification Practice Exam**

303-300 Syllabus:

Topic	Details
Cryptography	
X.509 Certificates and Public Key Infrastructures	**Weight:** 5 **Description:** 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, including certificate transparency • 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 • Basic feature knowledge of Let's Encrypt, ACME and certbot • Basic feature knowledge of CFSSL **Partial list of the used files, terms and utilities:** • openssl (including relevant subcommands) • OpenSSL configuration • PEM, DER, PKCS • CSR • CRL • OCSPSP

Topic	Details
X.509 Certificates for Encryption, Signing and Authentication	**Weight:** 4 **Description:** Candidates should be able to use X.509 certificates for both server and client authentication. This includes implementing user and server authentication for Apache HTTPD. The version of Apache HTTPD covered is 2.4 or higher. **Key Knowledge Areas:** • Understand SSL, TLS, including protocol versions and ciphers • Configure Apache HTTPD with mod_ssl to provide HTTPS service, including SNI and HSTS • Configure Apache HTTPD with mod_ssl to serve certificate chains and adjust the cipher configuration (no cipher-specific knowledge) • 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 **Partial list of the used files, terms and utilities:** • httpd.conf • mod_ssl • openssl (including relevant subcommands)
Encrypted File Systems	**Weight:** 3 **Description:** Candidates should be able to set up and configure encrypted file systems. **Key Knowledge Areas:** • Understand block device and file system encryption • Use dm-crypt with LUKS1 to encrypt block devices • Use eCryptfs to encrypt file systems, including home directories and PAM integration

Topic	Details
	• Awareness of plain dm-crypt • Awareness of LUKS2 features • Conceptual understanding of Clevis for LUKS devices and Clevis PINs for TMP2 and Network Bound Disk Encryption (NBDE)/Tang **Partial list of the used files, terms and utilities:** • cryptsetup (including relevant subcommands) • cryptmount • /etc/crypttab • ecryptfsd • ecryptfs-* commands • mount.ecryptfs, umount.ecryptfs • pam_ecryptfs
DNS and Cryptography	**Weight:** 5 **Description:** 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:** • Understand the concepts of DNS, zones and resource records • Understand DNSSEC, including key signing keys, zone signing keys and relevant DNS records such as DS, DNSKEY, RRSIG, NSEC, NSEC3 and NSEC3PARAM • Configure and troubleshoot BIND as an authoritative name server serving DNSSEC secured zones • Manage DNSSEC signed zones, including key generation, key rollover and re-signing of zones • Configure BIND as an recursive name server that performs DNSSEC validation on behalf of its clients • Understand CAA and DANE, including relevant DNS records such as CAA and TLSA

Topic	Details
	• Use CAA and DANE to publish X.509 certificate and certificate authority information in DNS • Use TSIG for secure communication with BIND • Awareness of DNS over TLS and DNS over HTTPS • Awareness of Multicast DNS **Partial list of the used files, terms and utilities:** • named.conf • dnssec-keygen • dnssec-signzone • dnssec-settime • dnssec-dsfromkey • rndc (including relevant subcommands) • dig • delv • openssl (including relevant subcommands)
Host Security	
Host Hardening	**Weight:** 5 **Description:** Candidates should be able to secure computers running Linux against common threats. **Key Knowledge Areas:** • Configure BIOS and boot loader (GRUB 2) security • Disable unused software and services • Understand and drop unnecessary capabilities for specific systemd units and the entire system • Understand and configure Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP) and Exec-Shield • Black and white list USB devices attached to a computer using USBGuard

Topic	Details
	• Create an SSH CA, create SSH certificates for host and user keys using the CA and configure OpenSSH to use SSH certificates • Work with chroot environments • Use systemd units to limit the system calls and capabilities available to a process • Use systemd units to start processes with limited or no access to specific files and devices • Use systemd units to start processes with dedicated temporary and /dev directories and without network access • Understand the implications of Linux Meltdown and Spectre mitigations and enable/disable the mitigations • Awareness of polkit • Awareness of the security advantages of virtualization and containerization **The following is a partial list of the used files, terms and utilities:** • grub.cfg • systemctl • getcap • setcap • capsh • sysctl • /etc/sysctl.conf • /etc/usbguard/usbguard-daemon.conf • /etc/usbguard/rules.conf • usbguard • ssh-keygen • /etc/ssh/ • ~/.ssh/ • /etc/ssh/sshd_config • chroot

Topic	Details
Host Intrusion Detection	**Weight:** 5 **Description:** Candidates should be familiar with the use and configuration of common host intrusion detection software. This includes managing the Linux Audit system and verifying a system's integrity. **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 • Use RPM and DPKG package management tools to verify the integrity of installed files • Configure and use AIDE, including rule management • Awareness of OpenSCAP **Partial list of the used files, terms and utilities:** • auditd • auditctl • ausearch, aureport • auditd.conf • audit.rules • pam_tty_audit.so • chkrootkit • rkhunter • /etc/rkhunter.conf • maldet • conf.maldet • rpm • dpkg • aide • /etc/aide/aide.conf

Topic	Details
Resource Control	**Weight:** 3 **Description:** Candidates should be able to restrict the resources services and programs can consume. **Key Knowledge Areas:** • Understand and configure ulimits • Understand cgroups, including classes, limits and accounting • Manage cgroups and process cgroup association • Understand systemd slices, scopes and services • Use systemd units to limit the system resources processes can consume • Awareness of cgmanager and libcgroup utilities **Partial list of the used files, terms and utilities:** • ulimit • /etc/security/limits.conf • pam_limits.so • /sys/fs/group/ • /proc/cgroups • systemd-cgls • systemd-cgtop
Access Control	
Discretionary Access Control	**Weight:** 3 **Description:** Candidates should understand discretionary access control (DAC) and know how to implement it using access control lists (ACL). Additionally, candidates are required to understand and know how to use extended attributes. **Key Knowledge Areas:**

Topic	Details
	• Understand and manage file ownership and permissions, including SetUID and SetGID bits • Understand and manage access control lists • Understand and manage extended attributes and attribute classes **Partial list of the used files, terms and utilities:** • getfacl • setfacl • getfattr • setfattr
Mandatory Access Control	**Weight:** 5 **Description:** Candidates should be familiar with mandatory access control (MAC) 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 type enforcement, role based access control, mandatory access control and discretionary access control • Configure, manage and use SELinux • Awareness of AppArmor and Smack **Partial list of the used files, terms and utilities:** • getenforce • setenforce • selinuxenabled • getsebool • setsebool • togglesebool • fixfiles

Topic	Details
	• restorecon • setfiles • newrole • setcon • runcon • chcon • semanage • sestatus • seinfo • apol • seaudit • audit2why • audit2allow • /etc/selinux/*
Network Security	
Network	**Weight:** 4 **Description:** Candidates should be able to secure networks against common threats. This includes analyzing network traffic of specific nodes and protocols. **Key Knowledge Areas:** • Understand wireless networks security mechanisms • Configure FreeRADIUS to authenticate network nodes • Use Wireshark and tcpdump to analyze network traffic, including filters and statistics • Use Kismet to analyze wireless networks and capture wireless network traffic • Identify and deal with rogue router advertisements and DHCP messages • Awareness of aircrack-ng and bettercap **Partial list of the used files, terms and utilities:**

Topic	Details
	• radiusd • radmin • radtest • radclient • radlast • radwho • radiusd.conf • /etc/raddb/* • wireshark • tshark • tcpdump • kismet • ndpmon
Network Intrusion Detection	**Weight:** 4 **Description:** 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 **Partial list of the used files, terms and utilities:** • ntop • snort • snort-stat • pulledpork.pl • /etc/snort/* • openvas-adduser • openvas-rmuser

Topic	Details
	• openvas-nvt-sync • openvassd • openvas-mkcert • openvas-feed-update • /etc/openvas/*
Packet Filtering	**Weight:** 5 **Description:** Candidates should be familiar with the use and configuration of the netfilter Linux packet filter. **Key Knowledge Areas:** • Understand common firewall architectures, including DMZ • Understand and use iptables and ip6tables, including standard modules, tests and targets • Implement packet filtering for IPv4 and IPv6 • Implement connection tracking and network address translation • Manage IP sets and use them in netfilter rules • Awareness of nftables and nft • Awareness of ebtables • Awareness of conntrackd **Partial list of the used files, terms and utilities:** • iptables • ip6tables • iptables-save • iptables-restore • ip6tables-save • ip6tables-restore • ipset
Virtual Private Networks	**Weight:** 4

Topic	Details
	Description: Candidates should be familiar with the use of OpenVPN, IPsec and WireGuard to set up remote access and site to site VPNs. **Key Knowledge Areas:** • Understand the principles of bridged and routed VPNs • Understand the principles and major differences of the OpenVPN, IPsec, IKEv2 and WireGuard protocols • Configure and operate OpenVPN servers and clients • Configure and operate IPsec servers and clients using strongSwan • Configure and operate WireGuard servers and clients • Awareness of L2TP **Partial list of the used files, terms and utilities:** • /etc/openvpn/ • openvpn • /etc/strongswan.conf • /etc/strongswan.d/ • /etc/swanctl/swanctl.conf • /etc/swanctl/ • swanctl • /etc/wireguard/ • wg • wg-quick • ip
Threats and Vulnerability Assessment	
Common Security Vulnerabilities and Threats	**Weight:** 2 **Description:** Candidates should understand the principle of major types of security vulnerabilities and threats. **Key Knowledge Areas:**

Topic	Details
	• Conceptual understanding of threats against individual nodes • Conceptual understanding of threats against networks • Conceptual understanding of threats against application • Conceptual understanding of threats against credentials and confidentiality • Conceptual understanding of honeypots **Partial list of the used files, terms and utilities:** • Trojans • Viruses • Rootkits • Keylogger • DoS and DDoS • Man in the Middle • ARP and NDP forgery • Rogue Access Points, Routers and DHCP servers • Link layer address and IP address spoofing • Buffer Overflows • SQL and Code Injections • Cross Site Scripting • Cross Site Request Forgery • Privilege escalation • Brute Force Attacks • Rainbow tables • Phishing • Social Engineering
Penetration Testing	**Weight:** 3 **Description:** Candidates understand the concepts of penetration testing, including an understand of commonly used penetration testing tools. Furthermore, candidates

Topic	Details
	should be able to use nmap to verify the effectiveness of network security measures. **Key Knowledge Areas:** • Understand the concepts of penetration testing and ethical hacking • Understand legal implications of penetration testing • Understand the phases of penetration tests, such as active and passive information gathering, enumeration, gaining access, privilege escalation, access maintenance, covering tracks • Understand the architecture and components of Metasploit, including Metasploit module types and how Metasploit integrates various security tools • Use nmap to scan networks and hosts, including different scan methods, version scans and operating system recognition • Understand the concepts of Nmap Scripting Engine and execute existing scripts • Awareness of Kali Linux, Armitage and the Social Engineer Toolkit (SET) **Partial list of the used files, terms and utilities:** • nmap

LPI 303-300 Sample Questions:

Question: 1

What happens when the command getfattr afile is run while the file afile has no extended attributes set?

a) getfattr prints a warning and exits with a values of 0.
b) No output is produced and getfattr exits with a value of 0.
c) getfattr prints a warning and exits with a value of 1.
d) No outputs is produced and getfattr exits with a value of 1.

Answer: b

Question: 2

An X509 certificate contains the following information:

X509v3 Basic Constraints: critical CA:TRUE, pathlen:0

Which of the following statements are true regarding the certificate?

(Choose THREE correct answers.)

a) This certificate belongs to a certification authority.
b) This certificate may be used to sign certificates of subordinate certification authorities.
c) This certificate may never be used to sign any other certificates.
d) This certificate may be used to sign certificates that are not also a certification authority.
e) This certificate will not be accepted by programs that do not understand the listed extension.

Answer: a, b, d

Question: 3

How does TSIG authenticate name servers in order to perform secured zone transfers?

a) Both servers mutually verify their X509 certificates.
b) Both servers use a secret key that is shared between the servers.
c) Both servers verify appropriate DANE records for the labels of the NS records used to delegate the transferred zone.
d) Both servers use DNSSEC to mutually verify that they are authoritative for the transferred zone.

Answer: b

Question: 4

Which of the following sections are allowed within the Kerberos configuration file krb5.conf?

(Choose THREE correct answers.)

a) [plugins]
b) [crypto]
c) [domain]
d) [capaths]
e) [realms]

Answer: a, b, e

Question: 5

What effect does the configuration SSLStrictSNIVHostCheck on have on an Apache HTTPD virtual host?

a) Despite its configuration, the virtual host is served only on the common name and Subject Alternative Names of the server certificates.
b) The virtual host is used as a fallback default for all clients that do not support SNI.
c) All of the names of the virtual host must be within the same DNS zone.
d) The virtual host is served only to clients that support SNI.
e) The clients connecting to the virtual host must provide a client certificate that was issued by the same CA that issued the server's certificate.

Answer: d

Question: 6

What is the purpose of IP sets?

a) They group together IP addresses that are assigned to the same network interfaces.
b) They group together IP addresses and networks that can be referenced by the network routing table.
c) They group together IP addresses that can be referenced by netfilter rules.
d) They group together IP and MAC addresses used by the neighbors on the local network.
e) They group together IP addresses and user names that can be referenced from /etc/hosts.allow and /etc/hosts.deny

Answer: c

Question: 7

Given a proper network and name resolution setup, which of the following commands establishes a trust between a FreeIPA domain and an Active Directory domain?

a) ipa trust-add --type ad addom --admin Administrator --password
b) ipa-ad –add-trust --account ADDOM\Administrator--query-password
c) net ad ipajoin addom –U Administrator -p
d) trustmanager add –-domain ad: //addom --user Administrator –w
e) ipa ad join addom -U Administrator -w

Answer: a

Question: 8

Which DNS label points to the DANE information used to secure HTTPS connections to https://www.example.com/?

a) example.com
b) dane.www.example.com
c) soa.example.com
d) www.example.com
e) _443_tcp.www.example.com

Answer: e

Question: 9

Linux Extended File Attributes are organized in namespaces. Which of the following names correspond to existing attribute namespaces?

(Choose THREE correct answers.)

a) default
b) system
c) owner
d) trusted
e) user

Answer: b, d, e

Question: 10

In which path is the data, which can be altered by the sysctl command, accessible?

a) /dev/sys/
b) /sys/
c) /proc/sys/
d) /sysctl/

Answer: c

Study Guide to Crack LPI LPIC-3 303-300 Exam:

- Getting details of the 303-300 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 303-300 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the LPI provided training for 303-300 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 303-300 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 303-300 practice tests is must. Continuous practice will make you an expert in all syllabus areas.