

UTAH

LPIC-3 – 303-200

Enterprise Security

LPIC-3 - 303-200 - ES

SOBRE O CURSO:

Entre as Certificações Internacionais exigidas pelo mercado de trabalho certamente a LPI se destaca nas carreiras onde habilidade com Linux devem ser comprovadas.

Independente de você ter ou nas as certificações anteriores, os conhecimentos que a LPIC-3-303-200 exige são essências para qualquer pessoa que deseja trabalhar na Área de Cyber Security no Mundo Corporativo.

Nesse contexto independente ou não de você ter as certificações anteriores, seria negligência achar que um conhecimento como este deve ser deixado de lado, vale ressaltar que no mundo moderno, onde as pessoas estão constantemente atuando em suas casas, trabalhando em um ambiente onde a segurança não pode ser medida, cada vez mais esse tópico requer atenção.

Pensando nisso, o Grupo Utah desenvolveu um treinamento exclusivo para você que atua ou quer atuar na área de Segurança da Informação e dominar todos os conceitos necessários na Área de Segurança de Serviços.

Este Treinamento também possui um módulo adicional o de DEVSECOPS onde você será inserido em um ambiente ágil que os aspectos de segurança não poderão ser deixados de lado.

Este é o nível máximo de um profissional de segurança da Informação. A Certificação LPI-C-303.

Este é o passo final rumo a uma carreira de 5 dígitos.

Seja bem-vindo a sua nova profissão. Você agora é um especialista.

CARGA HORÁRIA:

44 Horas.
Sendo **4 horas** 100% com foco na prova **LPIC-303-200**

APÓS ESTE CURSO VOCÊ ESTARÁ APTO A:

- ✓ **Prestar a Prova Internacional de Certificação LPIC-3-303-200**
- ✓ Atuar na área de segurança da informação.
- ✓ **Compreender certificados X.509 e infraestruturas de chave pública.**
- ✓ Implementar autoridades de certificação e emitir certificados SSL para vários fins.
- ✓ **Implementar autenticação de usuário e servidor para Apache HTTPD.**
- ✓ Instalar e configurar sistemas de arquivos criptografados.
- ✓ **Conhecer criptografia no contexto de DNS e sua implementação usando BIND.**
- ✓ Proteger computadores com Linux contra ameaças comuns.
- ✓ **Usa e configurar de software de detecção de intrusão de host comum.**
- ✓ Gerenciar autenticação de contas de usuário. NSS, PAM, SSSD e Kerberos

LPIC-3 - 303-200 - ES

- ✓ **Familizar-se com o FreeIPA v4.x.**
- ✓ Implantar domínio FreeIPA, bem como a integração do FreeIPA com o Active Directory.
- ✓ **Controlar de Acesso Discricionário e saber como implementá-lo usando ACLS.**
- ✓ Familiarizar-se com os sistemas de controle de acesso obrigatório para Linux.
- ✓ **Dominar do SELinux.**
- ✓ Experiência e conhecimento de segurança no uso de clientes e servidores NFSv4
- ✓ **Proteger as redes contra ameaças comuns.**
- ✓ Usar e configurar software de varredura de segurança de rede, monitoramento de rede e detecção de intrusão de rede.
- ✓ **netfilter, iptables e ip6tables, bem como conhecimento básico de nftables, nft e ebtables.**
- ✓ Usar e Implantar OpenVPN e IPsec.

PRÉ-REQUISITOS:

- ✓ Conhecimentos de informática básica
- ✓ Conhecimentos em Linux.
- ✓ Conhecimentos em redes de Computadores.
- ✓ Conhecimentos em Segurança da Informação.
- ✓ Para a Certificação Internacional, Obrigatório as Certificações **LPIC-I e LPIC-2.**

EMENTA:

- **325.1 X.509 CERTIFICATES AND PUBLIC KEY INFRASTRUCTURES**
  - 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
  - openssl, including relevant subcommands
  - OpenSSL configuration
  - PEM, DER, PKCS
  - CSR
  - CRL
  - OCSP

325.2 X.509 CERTIFICATES FOR ENCRYPTION, SIGNING AND AUTHENTICATION

- 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
- Intermediate certification authorities
- Cipher configuration (no cipher-specific knowledge)
- httpd.conf
- mod_ssl
- openssl

325.3 ENCRYPTED FILE SYSTEMS

- 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
- cryptsetup
- cryptmount
- /etc/crypttab
- ecryptfsd
- ecryptfs-* commands
- mount.ecryptfs, umount.ecryptfs
- pam_ecryptfs

325.4 DNS AND CRYPTOGRAPHY

- 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
- DNS, EDNS, Zones, Resource Records
- DNS resource records: DS, DNSKEY, RRSIG, NSEC, NSEC3, NSEC3PARAM, TLSA
- DO-Bit, AD-Bit
- TSIG
- named.conf
- dnssec-keygen
- dnssec-signzone
- dnssec-settime
- dnssec-dsfromkey
- rndc
- dig
- delv
- openssl

LPIC-3 - 303-200 - ES

326.1 HOST HARDENING

- 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
- Exec-Shield and IP / ICMP configuration
- Limit resource usage
- Work with chroot environments
- Drop unnecessary capabilities
- Be aware of the security advantages of virtualization
- grub.cfg
- chkconfig, systemctl
- ulimit
- /etc/security/limits.conf
- pam_limits.so
- chroot
- sysctl
- /etc/sysctl.conf

326.2 HOST INTRUSION DETECTION

- 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
- auditd
- auditctl
- ausearch, aureport
- auditd.conf
- auditd.rules
- pam_tty_audit.so
- chkrootkit
- rkhunter
- /etc/rkhunter.conf
- maldet
- conf.maldet
- aide
- /etc/aide/aide.conf

326.3 USER MANAGEMENT AND AUTHENTICATION

- 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
- Kerberos and local domains
- Obtain and manage Kerberos tickets
- **Terms and Utilities:**
- nsswitch.conf
- /etc/login.defs
- pam_cracklib.so
- chage
- pam_tally.so, pam_tally2.so
- faillog
- pam_sss.so
- sssd
- sssd.conf
- sss_* commands
- krb5.conf
- kinit, klist, kdestroy

326.4 FREEIPA INSTALLATION AND SAMBA INTEGRATION

- 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
- 389 Directory Server, MIT Kerberos, Dogtag Certificate System, NTP, DNS, SSSD, certmonger
- ipa, including relevant subcommands
- ipa-server-install, ipa-client-install, ipa-replica-install
- ipa-replica-prepare, ipa-replica-manage

LPIC-3 - 303-200 - ES

327.1 DISCRETIONARY ACCESS CONTROL

- 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
- getfacl
- setfacl
- getfattr
- setfattr

327.2 MANDATORY ACCESS CONTROL

- Understand the concepts of TE, RBAC, MAC and DAC
- Configure, manage and use SELinux
- Be aware of AppArmor and Smack
- getenforce, setenforce, selinuxenabled
- getsebool, setsebool, togglesebool
- fixfiles, restorecon, setfiles
- newrole, runcon
- semanage
- sestatus, seinfo
- apol
- seaudit, seaudit-report, audit2why, audit2allow
- /etc/selinux/*

327.3 NETWORK FILE SYSTEMS

- 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
- /etc/exports
- /etc/idmap.conf
- nfs4acl
- mount.cifs parameters related to ownership, permissions and security modes
- winbind
- getcifsacl, setcifsacl

328.1 NETWORK HARDENING

- 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
- radiusd
- radmin
- radtest, radclient
- radlast, radwho
- radiusd.conf
- /etc/raddb/*
- nmap
- wireshark
- tshark
- tcpdump
- ndpmon

328.2 NETWORK INTRUSION DETECTION

- Implement bandwidth usage monitoring
- Configure and use Snort, including rule management
- Configure and use OpenVAS, including NASL
- ntop
- Cacti
- snort
- snort-stat
- /etc/snort/*
- openvas-adduser, openvas-rmuser
- openvas-nvt-sync
- openvassd
- openvas-mkcert
- /etc/openvas/*

328.3 PACKET FILTERING

- 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
- iptables
- ip6tables
- iptables-save, iptables-restore
- ip6tables-save, ip6tables-restore
- ipset
- nft
- ebtables

328.4 VIRTUAL PRIVATE NETWORKS

- 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
- /etc/openvpn/*
- openvpn server and client
- setkey
- /etc/ipsec-tools.conf
- /etc/racoon/racoon.conf

LPIC-3 - 303-200 - ES

FORMA DE PAGAMENTO:

- ✓ Em até **12 vezes** sem juros no **Cartão de Crédito** ou Boleto.
- ✓ Em até 18 vezes com juros de 0.69% a.m.
- ✓ Em até 24 vezes com juros de 1.29% a.m.

Atenciosamente,

GRUPO UTAH - SECURITY
Sales Training – Grupo Utah
55 11 2649-4410
comercial@utah.com.br
www.utah.com.br