سرفصل آموزشی

پک پیشرفته مهندسی شبکه

فهرست سرفصل‌های دوره‌های آموزشی

سرفصل‌های دوره آموزشی

LPIC3-303

Topic 325: Cryptography

325.1 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
- 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

The following is a partial list of the used files, terms and utilities:

- openssl, including relevant subcommands
- OpenSSL configuration
- PEM, DER, PKCS
- CSR
- CRL
- OCSP

325.2 X.509 Certificates for Encryption, Signing and Authentication

Weight: 4

Description: 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

Terms and Utilities:

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

325.3 Encrypted File Systems

Weight: 3

Description: 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

Terms and Utilities:

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

325.4 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:

- 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

Terms and Utilities:

- 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

Topic 326: Host Security

326.1 Host Hardening

Weight: 3

Description: 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
- Exec-Shield and IP / ICMP configuration
- Limit resource usage
- Work with chroot environments
- Drop unnecessary capabilities
- Be aware of the security advantages of virtualization

Terms and Utilities:

- grub.cfg
- chkconfig, systemctl
- ulimit
- /etc/security/limits.conf
- pam_limits.so
- chroot
- sysctl
- /etc/sysctl.conf

326.2 Host Intrusion Detection

Weight: 4

Description: 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.

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

Terms and Utilities:

- 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

Weight: 5

Description: 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
- 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

Weight: 4

Description: 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

Terms and Utilities:

- 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

Topic 327: Access Control

327.1 Discretionary Access Control

Weight: 3

Description: 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

Terms and Utilities:

- getfacl
- setfacl
- getfattr
- setfattr

327.2 Mandatory Access Control

Weight: 4

Description: 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

Terms and Utilities:

- 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

Weight: 3

Description: 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

Terms and Utilities:

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

Topic 328: Network Security

328.1 Network Hardening

Weight: 4

Description: 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

Terms and Utilities:

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

328.2 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

Terms and Utilities:

- ntop
- Cacti
- snort
- snort-stat
- /etc/snort/*
- openvas-adduser, openvas-rmuser
- openvas-nvt-sync
- openvassd
- openvas-mkcert
- /etc/openvas/*

328.3 Packet Filtering

Weight: 5

Description: 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

Terms and Utilities:

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

328.4 Virtual Private Networks

Weight: 4

Description: 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

Terms and Utilities:

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

سرفصل‌های دوره آموزشی

LPIC3-305

Topic 351: Full Virtualization

351.1 Virtualization Concepts and Theory

Weight: 8

Description: Candidates should know and understand the general concepts, theory and terminology of virtualization. This includes Xen, QEMU and libvirt terminology.

Key Knowledge Areas:

- Understand virtualization terminology
- Understand the pros and cons of virtualization
- Understand the various variations of Hypervisors and Virtual Machine Monitors
- Understand the major aspects of migrating physical to virtual machines
- Understand the major aspects of migrating virtual machines between host systems
- Understand the features and implications of virtualization for a virtual machine, such as snapshotting, pausing, cloning and resource limits
- Awareness of oVirt, Proxmox, systemd-machined and VirtualBox
- Awareness of Open vSwitch

The following is a partial list of the used files, terms and utilities:

- Hypervisor
- Hardware Virtual Machine (HVM)
- Paravirtualization (PV)
- Emulation and Simulation
- CPU flags
- /proc/cpuinfo
- Migration (P2V, V2V)

351.2 Xen

Weight: 3

Description: Candidates should be able to install, configure, maintain, migrate and troubleshoot Xen installations. The focus is on Xen version 4.x.

Key Knowledge Areas:

- Understand architecture of Xen, including networking and storage
- Basic configuration of Xen nodes and domains
- Basic management of Xen nodes and domains
- Basic troubleshooting of Xen installations
- Awareness of XAPI
- Awareness of XenStore
- Awareness of Xen Boot Parameters
- Awareness of the xm utility

The following is a partial list of the used files, terms and utilities:

- in0 (Dom0), DomainU (DomU)Doma
- PV-DomU, HVM-DomU
- /etc/xen/
- xl
- xl.cfg
- xl.conf
- xentop

351.3 QEMU

Weight: 4

Description: Candidates should be able to install, configure, maintain, migrate and troubleshoot QEMU installations.

Key Knowledge Areas:

- Understand the architecture of QEMU, including KVM, networking and storage
- Start QEMU instances from the command line
- Manage snapshots using the QEMU monitor
- Install the QEMU Guest Agent and VirtIO device drivers
- Troubleshoot QEMU installations, including networking and storage
- Awareness of important QEMU configuration parameters

The following is a partial list of the used files, terms and utilities:

- Kernel modules: kvm, kvm-intel and kvm-amd
- /dev/kvm
- QEMU monitor
- qemu
- qemu-system-x86_64
- ip
- brctl
- tunctl

351.4 Libvirt Virtual Machine Management

Weight: 9

Description: Candidates should be able to manage virtualization hosts and virtual machines (‘libvirt domains’) using libvirt and related tools.

Key Knowledge Areas:

- Understand the architecture of libvirt
- Manage libvirt connections and nodes
- Create and manage QEMU and Xen domains, including snapshots
- Manage and analyze resource consumption of domains
- Create and manage storage pools and volumes
- Create and manage virtual networks
- Migrate domains between nodes
- Understand how libvirt interacts with Xen and QEMU
- Understand how libvirt interacts with network services such as dnsmasq and radvd
- Understand libvirt XML configuration files
- Awareness of virtlogd and virtlockd

The following is a partial list of the used files, terms and utilities:

- irtdlibv
- /etc/libvirt/
- virsh (including relevant subcommands)

351.5 Virtual Machine Disk Image Management

Weight: 3

Description: Candidates should be able to manage virtual machines disk images. This includes converting disk images between various formats and hypervisors and accessing data stored within an image.

Key Knowledge Areas:

- Understand features of various virtual disk image formats, such as raw images, qcow2 and VMDK
- Manage virtual machine disk images using qemu-img
- Mount partitions and access files contained in virtual machine disk images using libguestfish
- Copy physical disk content to a virtual machine disk image
- Migrate disk content between various virtual machine disk image formats
- Awareness of Open Virtualization Format (OVF)

The following is a partial list of the used files, terms and utilities:

- u-imgqem
- guestfish (including relevant subcommands)
- guestmount
- guestumount
- virt-cat
- virt-copy-in
- virt-copy-out
- virt-diff
- virt-inspector
- virt-filesystems
- virt-rescue
- virt-df
- virt-resize
- virt-sparsify
- virt-p2v
- virt-p2v-make-disk
- virt-v2v
- virt-sysprep

Topic352: Container Virtualization

352.1 Container Virtualization Concepts

Weight: 7

Description: Candidates should understand the concept of container virtualization. This includes understanding the Linux components used to implement container virtualization as well as using standard Linux tools to troubleshoot these components.

Key Knowledge Areas:

- Understand the concepts of system and application container
- Understand and analyze kernel namespaces
- Understand and analyze control groups
- Understand and analyze capabilities
- Understand the role of seccomp, SELinux and AppArmor for container virtualization
- Understand how LXC and Docker leverage namespaces, cgroups, capabilities, seccomp and MAC
- Understand the principle of runc
- Understand the principle of CRI-O and containerd
- Awareness of the OCI runtime and image specifications
- Awareness of the Kubernetes Container Runtime Interface (CRI)
- Awareness of podman, buildah and skopeo
- Awareness of other container virtualization approaches in Linux and other free operating systems, such as rkt, OpenVZ, systemd-nspawn or BSD Jails

The following is a partial list of the used files, terms and utilities:

- nsenter
- unshare
- ip (including relevant subcommands)
- capsh
- /sys/fs/cgroups
- /proc/[0-9]+/ns
- /proc/[0-9]+/status

352.2 LXC

Weight: 6

Description: Candidates should be able to use system containers using LXC and LXD. The version of LXC covered is 3.0 or higher.

Key Knowledge Areas:

- Understand the architecture of LXC and LXD
- Manage LXC containers based on existing images using LXD, including networking and storage
- Configure LXC container properties
- Limit LXC container resource usage
- Use LXD profiles
- Understand LXC images
- Awareness of traditional LXC tools

Partial list of the used files, terms and utilities:

- dlx
- lxc (including relevant subcommands)

352.3 Docker

Weight: 9

Description: Candidate should be able to manage Docker nodes and Docker containers. This include understand the architecture of Docker as well as understanding how Docker interacts with the node's Linux system.

Key Knowledge Areas:

- Understand the architecture and components of Docker
- Manage Docker containers by using images from a Docker registry
- Understand and manage images and volumes for Docker containers
- Understand and manage logging for Docker containers
- Understand and manage networking for Docker
- Use Dockerfiles to create container images
- Run a Docker registry using the registry Docker image

Partial list of the used files, terms and utilities:

- rddocke
- /etc/docker/daemon.json
- /var/lib/docker/
- docker
- Dockerfile

352.4 Container Orchestration Platforms

Weight: 3

Description: Candidates should understand the importance of container orchestration and the key concepts Docker Swarm and Kubernetes provide to implement container orchestration.

Key Knowledge Areas:

- Understand the relevance of container orchestration
- Understand the key concepts of Docker Compose and Docker Swarm
- Understand the key concepts of Kubernetes and Helm
- Awareness of OpenShift, Rancher and Mesosphere DC/OS

Topic 353: VM Deployment and Provisioning

353.1 Cloud Management Tools

Weight: 2

Description: Candidates should understand common offerings in public clouds and have basic feature knowledge of commonly available cloud management tools.

Key Knowledge Areas:

- Understand common offerings in public clouds
- Basic feature knowledge of OpenStack
- Basic feature knowledge of Terraform
- Awareness of CloudStack, Eucalyptus and OpenNebula

Partial list of the used files, terms and utilities:

- IaaS, PaaS, SaaS
- OpenStack
- Terraform

353.2 Packer

Weight: 3

Description: Candidates should able to use cloud-init to configure virtual machines created from standardized images. This includes adjusting virtual machines to match their available hardware resources, specifically, disk space and volumes. Additionally, candidates should be able to configure instances to allow secure SSH logins and install a specific set of software packages. Furthermore, candidates should be able to create new system images with cloud-init support.

Key Knowledge Areas:

- Understanding the features and concepts of cloud-init, including user-data, initializing and configuring cloud-init
- Use cloud-init to create, resize and mount file systems, configure user accounts, including login credentials such as SSH keys and install software packages from the distribution's repository
- Integrate cloud-init into system images
- Use config drive datasource for testing

Partial list of the used files, terms and utilities:

- cloud-init
- user-data
- /var/lib/cloud/

353.4 Vagrant

Weight: 3

Description: Candidate should be able to use Vagrant to manage virtual machines, including provisioning of the virtual machine.

Key Knowledge Areas:

- Understand Vagrant architecture and concepts, including storage and networking
- Retrieve and use boxes from Atlas
- Create and run Vagrantfiles
- Access Vagrant virtual machines
- Share and synchronize folder between a Vagrant virtual machine and the host system
- Understand Vagrant provisioning, i.e. File and Shell provisioners
- Understand multi-machine setup

Partial list of the used files, terms and utilities:

- vagrant
- Vagrantfile

سرفصل‌های دوره آموزشی

OpenStack

Cloud Computing

Concept of Cloud Computing

- Learning IaaS, PaaS, SaaS
- Reviewing of Linux Command
- Install RDO OpenStack distribution with PackStack

Identity Management (Keystone)

- Architecture and Main Components of Keystone
- Managing Keystone Catalog Services and Endpoints
- Managing/Creating Projects, Users, and Roles

Image management (Glance)

- Architecture and Main Components of Glance
- Deploy Image
- Managing Images
- Managing Image Back Ends

OpenStack Compute (Nova)

- Architecture and Components of Nova
- Managing Flavors
- Managing Hypervisor
- Managing Key pairs
- Managing Quotas

OpenStack Networking (Neutron)

- Architecture and Components of Neutron
- Architecture of Open vSwitch
- Manage Network Resources (DHCP, Router, Floating IPs …)

OpenStack Dashboard (Horizon)

- Architecture of Horizon
- Managing Horizon

Block Storage (Cinder)

- Architecture and Components of Cinder
- Manage Volume
- Managing Volume on the LVM and NFS
- Manage Quotas
- Back Up and Restore Volumes and Snapshots

Object Storage (Swift)

- Architecture and Components Swift Object Storage
- Managing Storage backend
- Monitoring Swift Cluster

Orchestration of OpenStack (Heat)

- Architecture and Components of Heat
- Introducing the Heat OpenStack Template
- Launching a Stack Using a HOT

Troubleshooting

- The Main Principles of Troubleshooting
- How to Check the OpenStack Version
- Where to Find and How to Analyze Log Files
- Back Up the Database Used by an OpenStack Instance
- Analyze Network status