سرفصل آموزشی

پک پیشرفته مهندسی لینوکس

فهرست سرفصل‌های دوره‌های آموزشی

LPIC3-303 2

Ansible 17

Networking with Linux 23

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

Ansible

Introduction of DevOps

Understanding DevOps concepts

DevOps Automation

Continuous Integration

Continues Delivery

Continuous Deployment

The roles of Ansible in CI/CD

The benefit of CICD

What is Ansible?

Automation Deployment Pipeline

Need of Ansible

What Ansible can do?

Advantages of using Ansible?

Agent-Based VS Agentless systems

Ansible’s Agentless Architecture

Install Ansible

Validate Ansible Installation

Ansible Vs Puppet Vs Chef Vs SaltStack

Ansible Architecture

Host, Group and Host Inventory

Ansible Ad-Hoc commands

Playbooks, plays, tasks and modules

Ansible configuration

Ansible-playbook Structure

Taks, vars, files, templates, meta, defaults, handlers

Ansible-playbook Syntax

Run ansible playbook

Variables, variable types and priorities

Command, expect, script, shell and raw modules

file, copy and fetch modules

Group and user modules

zyper_repository, zypper, yum_repository and you modules

Template, lineinfile, replace and service module

Archive and unarchive module

Async actions and concurrent tasks

wait_for and wait_for_connection modules

Mail module

Subversion and git modules

get_url, timezone and iptables modules

Mariadb modules

Find module and local_action feature

Conditions

Loops

Standard loops

Nested loops

Import playbooks and tasks

Handlers

Ansible Vault

Encrypt files and strings

Vault ID

Implement an Ansible playBook to Setup a webserver

Integrate Jenkins & Ansible

CICD with Git, Jenkins and Ansible (Application Deployment)

Ansible & VMWare

Ansible & Cisco

Ansible & Mikrotik

Develop Custom Module

Module format

Module’s return value and error handling

Setup nginx servers behind haproxy via Ansible playBook

Ansible & Windows Hosts

Manage windows features

Manage windows services

Execute shell module on windows

Windows Package management

Package Silent Installation

Implement an Ansible PlayBook to Setup IIS

Integrate Ansible and Docker

Docker_image and docker_image modules

docker_container and docker_container modules

docker_network and docker_network_info modules

docker_volume and docker_volume_info modules docker_swarm module

Ansible Galaxy

Ansible Tower

Ansible AWX

AWX prerequisites and Installation

AWX Dashboard

AWX - organizations, teams and users

AWX - hosts, groups and inventory

AWX - credentials

AWX - projects and templates

AWX - Schedule templates, notification and permissions

سرفصل‌های دوره آموزشی

Networking with Linux

Switching

- Switching Concepts
- Mac Address Learning
- Mac Address flooding
- Switch vs. Bridges
- Layer 3 Switching
- Physical Switch vs. Virtual Switch
- Layer 2 Switch deployment in Linux
- Virtual LAN (VLan) and Trunk
- Dot1q tagging overview
- Layer 3 Switches and InterVlan Routing in Linux
- Link Aggregation and binding (Ether-channel)
- Load Balancing in L2 links
- Software-defined Networks (SDN) concepts
- Open V-Switch basic management and configuration

Routing

- What is routing
- Network Performance in L2 vs. L3 networks
- Bandwidth, Delay, Throughput in networks
- Delay mitigation techniques in Networks
- Network Performance Monitoring with Iperf
- Static routing
- Dynamic routing concepts
- Distance-vector and Link-state routing protocols
- Open Shortest Path First (OSPF)
- Implementing Ospfd with Linux kernel and management interface
- Single-area and multi-area routing with OSPF
- Routing inside Internet
- Is BGP only Required in ISPs?
- Why BGP is mandatory in not only ISPs?
- High Availability and BGP
- EIGRP, BGP, RIP support in linux

DHCP

- DHCP Concepts
- DHCP installation and configuration
- DHCP relay-agent
- Advanced features for DHCP server
- DHCP Advanced Options

CA (one time forever)

- Encryption Concepts overview
- Symmetric Vs. Asymmetric Encryption
- DES, 3DES, AES encryption
- RSA, Deffi-helman, ECC
- Integrity Control
- Hash concepts and implementation
- Attacks of Encrypted Communications
- Man in the Middle attacks
- PKI Infrastructure
- Authentication with asymmetric encryption
- Certificates and CA
- Enterprise, Standalone and Sub ordinary CA
- Open-SSL Concepts
- Open-SSL installation and basic management
- PKI and Open-SSL
- SAN (Subject Alternative Name)
- Open-SSL SAN Support
- Securing WEB, DNS, etc with Certificate
- Securing Remote-Access Communication with PKI
- Internet (globally valid) Certificates
- Free valid Certificate

Network Security Concepts and Overview

- What is Network Security?
- Network Security approaches
- Firewalls
- IDS/IPS
- VPN Concentrators

- Unified Treat management (UTM)
- UTM Performance tuning
- Other Network security platforms (WAF, Mail security gateway, etc.)
- SSL Decryption (HTTPS inspection) in Firewalls
- Snort Overview
- Can Linux be used as a UTM?
- Log gathering Management
- Syslog in Linux
- Security information and event management (SIEM)
- Open-sourced Centralized log management tools
- Network devices monitoring with SNMP
- SNMP implementation in Linux (both client and server)

Free-radius

- AAA Concepts and definitions
- Identity management
- Extensible Authentication Protocol (EAP)
- Radius vs. TACACS/TACACS+
- Centralized Access Management
- Port-based authentication
- Dynamic VLaning and Network Mobility
- Free-radius installation and basic management
- EAP with Free-radius
- 802.1x standard and deployment
- Certificate-based EAP Authentication
- Advanced Configs of Free-radius
- Database integration for Free-radius
- Benefits of using Database as data storing in Free-radius
- Database Cli manipulation for Free-radius

- Saving logs in Database
- Graphical (web) interface for Free-radius
- Device Administration with Free-radius
- User-based privilege management for Device administration

Tunneling in Linux

- Encapsulation and packet structure
- Tunneling Concepts and protocols
- Why/when, tunnel is required.
- Generic Routing Encapsulation (GRE) Protocol
- GRE configuration and management
- Routing over GRE
- Ipv6 in Ipv4 tunneling
- Ipv6 in Ipv4 Tunneling
- IP in IP Tunnels overview and deployment
- Layer 2 tunneling
- VXLAN Concepts and definitions
- Why/when VXLAN is required?
- Stretch Datacenter with VXLAN Tunnel
- Network tearing with VXLAN
- Vms mobility and VXLAN
- VXLAN in Virtualized environments
- VXLAN usage in Disaster Recovery
- VXLAN deployment and use-cases

Virtual Router Redundancy Protocol (VRRP)

- VRRP basic and definitions
- Why VRRP?
- Is VRRP only for routers?
- Layer2 and Layer3 VRRP
- Keepalived installation
- Redundancy with keepalived
- Advanced parameter in keepalived
- Data synchronization with rsync in VRRP
- Service-level HA with VRRP (Web, DNS, AAA, etc.)

Secure communications and VPN

- VPN definitions
- Remote-access Vs. Site-to-Site VPN
- What is IPsec?
- IPsec Performance and security
- Protocols, framework and stacks
- IPsec different Phases

- IKE overview and versions
- IPsec protocols
- Securing tunnels with IPsec
- Remote-access VPN
- Open-vpn

Network in Virtualized Environments

- Network approach in Type1 and 2 Hypervisors
- Layer 2 and Layer 3 networks in Virtualized environments
- Routing and Switching in Virtualized environments
- VNF vs. SDN in Virtualized Environments
- Networking in KVM, Xen, ESXI
- Networking in Containerized Environments (Docker)
- Site-Recover-Managment (SRM) with VXLAN

IPv6

- Concepts and definitions
- Binary, Decimal and Hexadecimal overview
- IPv6 communication types (Unicast, Multicast, Anycast)
- Why Broadcast is eliminated in IPv6?
- NAT in IPv6 and Backward compatibility in IPv4 networks
- Network and device discovery without Broadcast in IPv6
- IPv6 address Types (ULA, GUA, LLA, etc.)
- Subneting and planning approach in IPv6
- IPv6 built-in security mechanisms
- IPv6 in different Platforms (Linux, Cisco, Windows, VMware)
- IPv6 in practice (Routing, DNS, CDN, HA, etc.)
- Routing to nearest device in IPv6
- Cloud distributed networks (CDN) with anycast