LPIC3-303 (temario)

Cryptography

- X.509 Certificates and Public Key Infrastructures
    - 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
- X.509 Certificates for Encryption, Signing and Authentication
    - 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
- 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
- DNS and Cryptography
    - 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

Host Security

- Host Hardening
  - 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
  - Terms and Utilities:
    - grub.cfg
    - chkconfig, systemctl
    - ulimit
    - /etc/security/limits.conf
    - pam_limits.so
    - chroot
    - sysctl
    - /etc/sysctl.conf
- Host Intrusion Detection
  - 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

        - /etc/auditd/auditd.conf
        - /etc/auditd/auditd.rules
        - pam_tty_audit.so
        - chkrootkit
        - rkhunter
        - /etc/rkhunter.conf
        - maldet
        - conf.maldet
        - aide
        - /etc/aide/aide.conf
- User Management and Authentication
    - 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
    - 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

- FreeIPA Installation and Samba Integration
    - 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

Access Control

- Discretionary Access Control
    - 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
- Mandatory Access Control
    - 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, setsebol, togglesebool
        - fixfiles, restorecon, setfiles
        - newrole, runcon
        - semanage
        - sestatus, seinfo
        - apol
        - seaudit, seaudit-report, audit2why, audit2allow
        - /etc/selinux/*
- Network File Systems
    - 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

Network Security

- Network Hardening
    - 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
- Network Intrusion Detection
    - 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
- Packet Filtering
    - 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
- Virtual Private Networks
    - 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