Topic 331: Cryptography

331.1 X.509 Certificates and Public Key Infrastructures (weight: 5)

Weight 5

Description Candidates should understand X.509 certificates and public key infrastructures. They should know how to configure and use Op 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
- OCSP

331.2 X.509 Certificates for Encryption, Signing and Authentication (weight: 4)

Weight 4

Description Candidates should be able to use X.509 certificates for both server and client authentication. This includes implementing user a 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)

331.3 Encrypted File Systems (weight: 3)

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
- 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

The following is a 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

331.4 DNS and Cryptography (weight: 5)

Weight	5
Description	Candidates should have experience and knowledge of cryptography in the context of DNS and its implementation using BIND. T 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
- 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)

Topic 332: Host Security

332.1 Host Hardening (weight: 5)

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
- 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

332.2 Host Intrusion Detection (weight: 5)

Weight	5
Description	Candidates should be familiar with the use and configuration of common host intrusion detection software. This includes mana 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

332.3 Resource Control (weight: 3)

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

Topic 333: Access Control

333.1 Discretionary Access Control (weight: 3)

Weight	3
Description	Candidates should understand discretionary access control (DAC) and know how to implement it using access control lists (ACL) candidates are required to understand and know how to use extended attributes.

Key Knowledge Areas:

- 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

333.2 Mandatory Access Control (weight: 5)

Weight	5
Description	Candidates should be familiar with mandatory access control (MAC) systems for Linux. Specifically, candidates should have a th SELinux. Also, candidates should be aware of other mandatory access control systems for Linux. This includes major features o 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
- restorecon
- setfiles
- newrole
- setcon
- runcon
- chcon
- semanage
- sestatus
- seinfo
- apol
- seaudit
- audit2why
- audit2allow
- /etc/selinux/*

Topic 334: Network Security

334.1 Network Hardening (weight: 4)

Weight	4

Description Candidates should be able to secure networks against common threats. This includes analyzing network traffic of specific node

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

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

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

334.2 Network Intrusion Detection (weight: 4)

Weight 4

Description Candidates should be familiar with the use and configuration of network security scanning, network monitoring and network in 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
- openvas-nvt-sync
- openvassd
- openvas-mkcert
- openvas-feed-update
- /etc/openvas/*

334.3 Packet Filtering (weight: 5)

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

334.4 Virtual Private Networks (weight: 4)

Weight 4

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

Topic 335: Threats and Vulnerability Assessment

335.1 Common Security Vulnerabilities and Threats (weight: 2)

Weight 2

Description Candidates should understand the principle of major types of security vulnerabilities and threats.

Key Knowledge Areas:

- 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

The following is a 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

335.2 Penetration Testing (weight: 3)

Weight	3
Description	Candidates understand the concepts of penetration testing, including an understand of commonly used penetration testing toc candidates 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