LPI – Linux Enterprise Professional – Security («LP6»)

Dieses Seminar dient zur Vorbereitung auf die LPIC-3-Zertifizierung, die LP303- oder «Security»-Prüfung. Im Kurs beschäftigen Sie sich von den Themen lokale Systemsicherheit bis hin zu Netzwerksicherheit, quer durch die Linux-Landschaft.

Dauer: 4 Tage
Preis: 3'200.– zzgl. 8.1% MWST
Kursdokumente: Digicomp Kursmaterial
Herstellercode: 303-300

Inhalt

Thema 331: Kryptographie

331.1 X.509-Zertifikate und Public-Key-Infrastrukturen (Gewichtung: 5)
Die Kandidaten sollten X.509-Zertifikate und Public-Key-Infrastrukturen verstehen. Sie sollten wissen, wie man OpenSSL konfiguriert und verwendet, um Zertifizierungsstellen zu implementieren und SSL-Zertifikate für verschiedene Zwecke auszustellen.
Wichtige Wissensgebiete:

- Verstehen von X.509-Zertifikaten, X.509-Zertifikatslebenszyklus, X.509-Zertifikatsfeldern und X.509v3-Zertifikatserweiterungen
- Verstehen von Vertrauensketten und Public-Key-Infrastrukturen, einschliesslich Zertifikatstransparenz
- Generieren und Verwalten von öffentlichen und privaten Schlüsseln
- Erstellen, Betreiben und Sichern einer Zertifizierungsstelle
- Beantragen, Signieren und Verwalten von Server- und Client-Zertifikaten
- Sperren von Zertifikaten und Zertifizierungsstellen
- Grundlegende Kenntnisse der Funktionen von Let's Encrypt, ACME und certbot
- Grundlegende Kenntnisse über die Funktionen von CFSSL

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- openssl (einschliesslich relevanter Unterbefehle)
- OpenSSL-Konfiguration
- PEM, DER, PKCS
- CSR
- CRL
- OCSP

331.2 X.509-Zertifikate für Verschlüsselung, Signierung und Authentifizierung (Gewicht: 4)
Kandidaten sollten in der Lage sein, X.509-Zertifikate sowohl für die Server- als auch für die Client-Authentifizierung zu verwenden. Dies beinhaltet die Implementierung von Benutzer- und Server-Authentifizierung für Apache HTTPD. Die behandelte Version von Apache HTTPD ist 2.4 oder höher.
Wichtige Wissensgebiete:

- Verstehen von SSL, TLS, einschliesslich Protokollversionen und Chiffren
- Konfigurieren von Apache HTTPD mit mod_ssl zur Bereitstellung von HTTPS-Diensten, einschliesslich SNI und HSTS
- Konfiguration von Apache HTTPD mit mod_ssl zur Bereitstellung von Zertifikatsketten und Anpassung der Verschlüsselungskonfiguration (keine verschlüsselungsspezifischen Kenntnisse)
- Konfigurieren Sie Apache HTTPD mit mod_ssl, um Benutzer mit Zertifikaten zu authentifizieren
- Konfigurieren Sie Apache HTTPD mit mod_ssl, um OCSP-Stapling bereitzustellen

- Verwendung von OpenSSL für SSL/TLS-Client- und -Server-Tests

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- httpd.conf
- mod_ssl
- openssl (einschliesslich relevanter Unterbefehle)

331.3 Verschlüsselte Dateisysteme (Gewichtung: 3)
Kandidaten sollten in der Lage sein, verschlüsselte Dateisysteme einzurichten und zu konfigurieren.
Wichtige Wissensgebiete:

- Verstehen der Verschlüsselung von Blockgeräten und Dateisystemen
- dm-crypt mit LUKS1 verwenden, um Blockgeräte zu verschlüsseln
- Verwendung von eCryptfs zur Verschlüsselung von Dateisystemen, einschliesslich Home-Verzeichnissen und PAM-Integration
- Kenntnis von einfachem dm-crypt
- Kennenlernen der LUKS2-Funktionen
- Konzeptuelles Verständnis von Clevis für LUKS-Geräte und Clevis-PINs für TMP2 und Network Bound Disk Encryption (NBDE)/Tang

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- cryptsetup (einschliessich relevanter Unterbefehle)
- cryptmount
- /etc/crypttab
- ecryptfsd
- ecryptfs-* Befehle
- mount.ecryptfs, umount.ecryptfs
- pam_ecryptfs

331.4 DNS und Kryptographie (Gewichtung: 5)
Die Kandidaten sollten Erfahrung und Wissen über Kryptographie im Zusammenhang mit DNS und dessen Implementierung mit BIND haben. Die behandelte Version von BIND ist 9.7 oder höher.
Wichtige Wissensgebiete:

- Verstehen der Konzepte von DNS, Zonen und Ressourceneinträgen
- Verstehen von DNSSEC, einschliesslich Signierschlüsseln, Zonensignierschlüsseln und relevanten DNS-Einträgen wie DS, DNSKEY, RRSIG, NSEC, NSEC3
- und NSEC3PARAM
- BIND als autoritativen Nameserver, der DNSSEC-gesicherte Zonen bedient, zu konfigurieren und Fehler zu beheben
- Verwalten von DNSSEC-signierten Zonen, einschliesslich Schlüsselgenerierung, Schlüssel-Rollover und Neusignierung von Zonen
- Konfigurieren von BIND als rekursiver Nameserver, der die DNSSEC-Validierung im Namen seiner Kunden durchführt
- CAA und DANE zu verstehen, einschlieslsich relevanter DNS-Einträge wie CAA und TLSA
- Verwendung von CAA und DANE zur Veröffentlichung von X.509-Zertifikaten und Zertifizierungsstelleninformationen im DNS
- Verwendung von TSIG für die sichere Kommunikation mit BIND
- Kenntnis von DNS über TLS und DNS über HTTPS
- Kenntnis von Multicast DNS

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- named.conf

- dnssec-keygen
- dnssec-signzone
- dnssec-settime
- dnssec-dsfromkey
- rndc (einschliesslich relevanter Unterbefehle)
- dig
- delv
- openssl (einschliesslich relevanter Unterbefehle)

Thema 332: Host-Sicherheit

332.1 Härtung des Hosts (Gewichtung: 5)

Kandidaten sollten in der Lage sein, Computer unter Linux gegen gängige Bedrohungen abzusichern.

Wichtige Wissensgebiete:

- Konfigurieren der BIOS- und Bootloader (GRUB 2) Sicherheit
- Deaktivieren nicht benötigter Software und Dienste
- Unnötige Fähigkeiten für bestimmte systemd-Einheiten und das gesamte System verstehen und abschalten
- Verstehen und Konfigurieren von Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP) und Exec-Shield
- USB-Geräte, die an einen Computer angeschlossen sind, mit USBGuard blacklisten und whitelisten
- Eine SSH-Zertifizierungsstelle erstellen, SSH-Zertifikate für Host- und Benutzerschlüssel unter Verwendung der Zertifizierungsstelle erstellen und OpenSSH für die Verwendung von SSH-Zertifikaten konfigurieren
- Arbeiten mit Chroot-Umgebungen
- systemd-Units verwenden, um die einem Prozess zur Verfügung stehenden Systemaufrufe und Fähigkeiten einzuschränken
- Verwenden Sie systemd-Units, um Prozesse mit eingeschränktem oder keinem Zugriff auf bestimmte Dateien und Geräte zu starten
- systemd-Einheiten verwenden, um Prozesse mit dedizierten temporären und /dev-Verzeichnissen und ohne Netzwerkzugang zu starten
- Die Auswirkungen der Meltdown- und Spectre-Abschwächungen von Linux verstehen und die Abschwächungen aktivieren/deaktivieren
- Kenntnis von Polkit
- Kenntnis der Sicherheitsvorteile von Virtualisierung und Containerisierung

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- 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 (Gewichtung: 5)

Die Kandidaten sollten mit der Verwendung und Konfiguration gängiger Host Intrusion Detection Software vertraut sein. Dies beinhaltet die Verwaltung des Linux Audit-Systems und die Überprüfung der Integrität eines Systems.

Wichtige Wissensgebiete:

- Verwendung und Konfiguration des Linux-Audit-Systems
- Verwendung von chkrootkit
- Verwendung und Konfiguration von rkhunter, einschliesslich Updates
- Verwendung von Linux Malware Detect
- Automatisieren von Host-Scans mit cron
- Verwendung von RPM- und DPKG-Paketverwaltungstools zur Überprüfung der Integrität der installierten Dateien
- Konfigurieren und Verwenden von AIDE, einschliesslich Regelmanagement
- Kenntnis von OpenSCAP

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- 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 Ressourcenkontrolle (Gewichtung: 3)

Kandidaten sollten in der Lage sein, die Ressourcen einzuschränken, die Dienste und Programme verbrauchen können.

Wichtige Wissensgebiete:

- Verstehen und Konfigurieren von ulimits
- Verständnis von cgroups, einschliesslich Klassen, Limits und Accounting
- Verwalten von cgroups und Verarbeiten von cgroup-Zuordnungen
- Verstehen von systemd-Slices, Scopes und Diensten
- systemd-Einheiten verwenden, um die Systemressourcen zu begrenzen, die Prozesse verbrauchen können
- Kenntnis von cgmanager und libcgroup-Dienstprogrammen

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- ulimit
- /etc/security/limits.conf
- pam_limits.so
- /sys/fs/group/
- /proc/cgroups
- systemd-cgls
- systemd-cgtop

Thema 333: Zugangskontrolle

333.1 Ermessensabhängige Zugangskontrolle (Gewichtung: 3)

Die Kandidaten sollten die diskretionäre Zugriffskontrolle (DAC) verstehen und wissen, wie man sie mit Hilfe von Zugriffskontrolllisten (ACL) implementiert. Darüber hinaus müssen Kandidaten die erweiterten Attribute verstehen und wissen, wie sie zu verwenden sind.

Wichtige Wissensgebiete:

- Verstehen und Verwalten von Dateibesitz und Berechtigungen, einschliesslich SetUID- und SetGID-Bits
- Verstehen und Verwalten von Zugriffskontrolllisten
- Verstehen und Verwalten von erweiterten Attributen und Attributklassen

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- getfacl
- setfacl
- getfattr
- setfattr

333.2 Obligatorische Zugriffskontrolle (Gewicht: 5)

Kandidaten sollten mit den Systemen der obligatorischen Zugriffskontrolle (MAC) für Linux vertraut sein. Insbesondere sollten die Kandidaten gründliche Kenntnisse über SELinux haben. Die Kandidaten sollten auch mit anderen Systemen zur obligatorischen Zugriffskontrolle für Linux vertraut sein. Dazu gehören die wichtigsten Funktionen dieser Systeme, nicht aber deren Konfiguration und Verwendung.

Wichtige Wissensgebiete:

- Verstehen der Konzepte von Type Enforcement, rollenbasierter Zugriffskontrolle, obligatorischer Zugriffskontrolle und diskretionärer Zugriffskontrolle
- Konfigurieren, Verwalten und Verwenden von SELinux
- Kenntnis von AppArmor und Smack

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- getenforce
- setenforce
- selinuxenabled
- getsebool
- setsebool
- togglesebool
- fixfiles
- restorecon
- setfiles
- newrole
- setcon
- runcon
- chcon
- semanage
- sestatus
- seinfo
- apol
- seaudit
- audit2why
- audit2allow
- /etc/selinux/*

Thema 334: Netzwerksicherheit

334.1 Netzwerk-Härtung (Gewichtung: 4)
Kandidaten sollten in der Lage sein, Netzwerke gegen gängige Bedrohungen abzusichern. Dazu gehört die Analyse des Netzwerkverkehrs bestimmter Knoten und Protokolle.
Wichtige Wissensgebiete:

- Verstehen der Sicherheitsmechanismen drahtloser Netzwerke
- FreeRADIUS konfigurieren, um Netzwerkknoten zu authentifizieren
- Verwendung von Wireshark und tcpdump zur Analyse des Netzwerkverkehrs, einschliesslich Filter und Statistiken
- Kismet verwenden, um drahtlose Netzwerke zu analysieren und drahtlosen Netzwerkverkehr zu erfassen
- Identifizierung von und Umgang mit Rogue-Router-Anzeigen und DHCP-Nachrichten
- Kenntnis von aircrack-ng und bettercap

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

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

334.2 Erkennung von Eindringlingen in das Netzwerk (Gewicht: 4)
Die Kandidaten sollten mit der Verwendung und Konfiguration von Netzwerksicherheitsscanner-, Netzwerküberwachungs- und Netzwerkeindringungserkennungssoftware vertraut sein. Dazu gehört auch die Aktualisierung und Wartung der Sicherheitsscanner.
Wichtige Wissensgebiete:

- Überwachung der Bandbreitennutzung implementieren
- Konfigurieren und Verwenden von Snort, einschliesslich Regelmanagement
- Konfigurieren und Verwenden von OpenVAS, einschliesslich NASL

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- 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 Paketfilterung (Gewichtung: 5)

Kandidaten sollten mit der Verwendung und Konfiguration des Linux-Paketfilters netfilter vertraut sein.

Wichtige Wissensgebiete:

- Verstehen gängiger Firewall-Architekturen, einschliesslich DMZ
- Verstehen und Verwenden von iptables und ip6tables, einschliesslich Standardmodule, Tests und Ziele
- Paketfilterung für IPv4 und IPv6 implementieren
- Implementierung von Verbindungsverfolgung und Netzwerkadressübersetzung
- IP-Sets verwalten und in Netzfilterregeln verwenden
- Kenntnis von nftables und nft
- Kenntnis von ebtables
- Kenntnis von conntrackd

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- iptables
- ip6tables
- iptables-save
- iptables-restore
- ip6tables-save
- ip6tables-restore
- ipset

334.4 Virtual Private Networks (Gewichtung: 4)

Kandidaten sollten mit der Verwendung von OpenVPN, IPsec und WireGuard vertraut sein, um Remote Access und Site-to-Site-VPNs einzurichten.

Wichtige Wissensgebiete:

- Verstehen der Prinzipien von Bridged und Routed VPNs
- Verstehen der Prinzipien und Hauptunterschiede der Protokolle OpenVPN, IPsec, IKEv2 und WireGuard
- Konfigurieren und Betreiben von OpenVPN-Servern und -Clients
- IPsec-Server und -Clients mit strongSwan konfigurieren und betreiben
- Konfigurieren und Betreiben von WireGuard-Servern und -Clients
- Kenntnis von L2TP

Teilweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- /etc/openvpn/
- openvpn
- /etc/strongswan.conf
- /etc/strongswan.d/
- /etc/swanctl/swanctl.conf
- /etc/swanctl/
- swanctl
- /etc/wireguard/
- wg
- wg-quick
- ip

Thema 335: Bedrohungen und Schwachstellenanalyse

335.1 Allgemeine Sicherheitsschwachstellen und Bedrohungen (Gewichtung: 2)

Die Kandidaten sollten das Prinzip der wichtigsten Arten von Sicherheitsschwachstellen und

Bedrohungen verstehen.
Wichtige Wissensgebiete:

- Konzeptuelles Verständnis von Bedrohungen gegen einzelne Knotenpunkte
- Konzeptuelles Verständnis von Bedrohungen gegen Netzwerke
- Konzeptuelles Verständnis von Bedrohungen gegen Anwendungen
- Konzeptuelles Verständnis von Bedrohungen gegen Anmeldeinformationen und Vertraulichkeit
- Konzeptuelles Verständnis von Honeypots

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- Trojaner
- Viren
- Rootkits
- Keylogger
- DoS and DDoS
- Man in the Middle
- ARP and NDP forgery
- Rogue Access Points, Routers und DHCP servers
- Link layer address und 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 Penetrationstests (Gewichtung: 3)
Die Kandidaten verstehen die Konzepte von Penetrationstests, einschliesslich der gängigen Penetrationstest-Tools. Darüber hinaus sollten die Kandidaten in der Lage sein, nmap zu verwenden, um die Wirksamkeit von Netzwerksicherheits-Massnahmen zu überprüfen.
Wichtige Wissensgebiete:

- Verstehen der Konzepte von Penetrationstests und Ethical Hacking
- Verständnis der rechtlichen Implikationen von Penetrationstests
- Verständnis der Phasen von Penetrationstests, wie z. B. aktive und passive Informationsbeschaffung, Enumeration, Zugangserlangung, Privilegienerweiterung, Zugangserhaltung, Verfolgung
- Verstehen der Architektur und der Komponenten von Metasploit, einschliesslich der Modultypen von Metasploit und wie Metasploit verschiedene Sicherheitstools integriert
- Verwendung von nmap zum Scannen von Netzwerken und Hosts, einschliesslich verschiedener Scan-Methoden, Versionsscans und Betriebssystemerkennung
- Verstehen der Konzepte der Nmap Scripting Engine und Ausführen vorhandener Skripte
- Kennenlernen von Kali Linux, Armitage und dem Social Engineer Toolkit (SET)

Teilweise Liste der verwendeten Dateien, Begriffe und Dienstprogramme:

- nmap

Key Learnings

- Erwerben der in der LPIC-3-Prüfung geforderten Fähigkeiten und Erfahrungen
- Entwurf und Implementierung kundenspezifischer Lösungen für komplexe Automatisierungs-Probleme, z. B. für Unternehmen mit mehreren Standorten und Hochleistungs-Internetseiten
- Initiieren von Projekten und Arbeiten im Rahmen eines Budgets
- Beaufsichtigung von Assistenten und Unterstützung bei der Problembehandlung
- Funktion als Berater für das höhere Management

Zielpublikum

LPIC-2-zertifizierte Administratoren erwerben mit diesem Kurs die Fähigkeit zur LPIC-3-Zertifizierung.

Anforderungen

Kenntnisse entsprechend dem LPIC2-Zertifikat und folgenden Kursen:

- LPI – Linux Engineer I («LP3»)
- LPI – Linux Enterprise Professional – Mixed Environments («LP5»)
- LPI – Linux Engineer II («LP4»)

Zertifizierung

Hinweis: Sie müssen ein gültiges LPIC-2 Zertifikat nachweisen, um neben der folgenden bestandenen Prüfung das LPIC-3 Zertifikat zu erhalten. Die Prüfungen der LPIC-2- und LPIC-3-Stufe können aber in beliebiger Reihenfolge absolviert werden.

Um das LPIC-3-Zertifikat zu erlangen, müssen Sie eine der folgenden drei Spezialisierungs-Prüfungen ablegen:

- «300: Mixed Environment»
- «303: Security»
- «305: Virtualization and Containerization»
- «306: High Availability and Storage Clusters»

Dieser Kurs bereitet Sie auf die «303: Security»-Prüfung zur Zertifizierung LPIC-3 vor.

Preisinformation: **Nicht inbegriffen** im Preis sind die Pearson-VUE-Prüfungsgebühren von ca. CHF 200.– pro Prüfung.

Weiterführende Kurse

- LPI – Linux Enterprise Professional – Virtualisierung und Containerisierung («LP7»)

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-it-provider/unix-linux/kurs-lpi-linux-enterprise-professional-security-303-300