Penetration Testing L4

Contents

What is this Qualification?

This qualification is designed to equip learners with the technical knowledge and practical capabilities required to launch a career in cyber security. Structured over 24 weeks, the course guides learners from core infrastructure and networking principles through to advanced penetration testing methodologies. Learners progress through three internationally recognised certifications: CompTIA Network+, CompTIA Security+, and CompTIA PenTest+, developing a complete skillset in defensive and offensive security operations.

Key aims and objectives of this course are:

- Focus on the progressive study of network engineering, cyber defence, and ethical hacking.
- Offer depth and breadth across the domains of networking protocols, secure architecture, risk management, and penetration testing.
- Provide learners with hands-on experience using industry-standard tooling and simulated labs to perform configuration, scanning, exploitation, and incident response tasks.
- Build the professional behaviours and legal awareness required to work in compliance with recognised security and ethical standards.

Who is this Course for?

Prior Knowledge and Suitability:

- Learners **must** complete a level 3 course such IT Support or other related IT course.

Why Should Learners Enrol?

Skills gained include:

- **Networking & infrastructure (Network+)**
  - Build and troubleshoot small to medium networks: addressing, subnetting (IPv4/IPv6), VLANs, routing basics, DHCP/DNS, wireless setup and fixes.
  - Configure and diagnose switches, routers, firewalls, NAT/PAT, and common SOHO services; understand WAN links and remote access options (VPN, SSH, RDP).
  - Work confidently with Linux VMs and the CLI for network configuration and testing.
- **Cyber security foundations (Security+)**
  - Apply core security concepts (CIA triad, control types), threat intelligence, and risk management to real scenarios.
  - Implement identity and access management (SSO, MFA, IAM models), secure architectures (on-prem, cloud), and operational security monitoring/SIEM.
  - Use cryptography and PKI in context; understand compliance and data protection (GDPR, ISO/NIST).
- **Penetration testing lifecycle (PenTest+)**
  - Plan & scope engagements legally and ethically: SOW, NDA, Rules of Engagement; map to frameworks (MITRE ATT&CK, PTES, NIST).
  - Information gathering & scanning: perform OSINT (WHOIS, metadata, Shodan), run
  - Attacks & exploits: execute network, web and wireless attacks in lab settings; practise on-path attacks, WPA2 handshake capture, and cloud misconfiguration exploits.
  - Post-exploitation: perform privilege escalation, lateral movement, pivoting and persistence safely in sandboxes.

Guided Learning Hours & Commitment

- **GLH:** 288 hours (taught sessions)
- Learners should expect to commit additional time outside of lessons for:
  - Research
  - Assignments
  - Portfolio building

Unit Breakdown

Module 1 — CompTIA Network+ (Weeks 1–8)

Focus: networking concepts, devices & cabling, virtualisation/cloud, network security essentials, and structured troubleshooting.

- **Models & data flow**: OSI vs TCP/IP mapping, encapsulation/decapsulation, PDUs, MTU/fragmentation, and where packet loss and latency occur on the path. Interpret ARP tables, MAC address learning and CAM tables on switches.
- **Cabling & media**: UTP categories and use cases, STP and when shielding matters, fibre (SMF/MMF, connectors), bend radius, attenuation, EMI/RFI, and testing with TDR/OTDR.
- **IP addressing & services**: IPv4/IPv6 addressing, CIDR, VLSM, default gateway logic, DHCP scopes, reservations and conflicts, DNS records (A/AAAA/CNAME/MX/TXT), split-horizon DNS, and name resolution order.
- **Switching & routing basics**L VLANs, trunking (802.1Q), inter-VLAN routing patterns, STP/RSTP concepts, static routes vs default routes on a SOHO edge.
- **Wireless & SOHO**: 802.11 standards, channels and interference, WPA2/WPA3 Personal/Enterprise, captive portals, guest segmentation, and IoT constraints on small networks.
- **Virtualisation & cloud connectivity**: Client VMs for testing, vSwitch/NAT/bridged adapters, and how on-prem networks connect securely to SaaS/PaaS/IaaS resources.
- **Troubleshooting method**: Structured steps from symptom capture → theory → test → fix → verify → document; bottom-up vs top-down vs divide-and-conquer.

Module 2 — CompTIA Security+ (Weeks 9–13)

Introduce risk-driven security, IAM, secure architectures and crypto/PKI so learners can select proportionate controls and operate them.The CompTIA troubleshooting methodology and the support mindset (documented steps from symptoms to verification and closure).

- **Threats, risk & controls**: Asset–threat–vulnerability triads, likelihood/impact, choosing technical/administrative/physical controls, change windows, and measuring residual risk.
- **Identity & access management**: Provisioning and de-provisioning flows, SSO/MFA factors, RBAC vs ABAC, password policies, account audit trails, and directory tie-ins (LDAP/Kerberos).
- **Secure network & cloud architecture**: Segmentation/DMZ, VPN types (IPsec/SSL; site-to-site vs client), bastion hosts, jump boxes, hardening patterns; shared-responsibility in cloud (IAM, KMS, groups/policies).
- **Operations & monitoring**: Log sources, normal vs abnormal baselines, alert triage, and linking findings to tickets.
- **Cryptography & PKI**: Symmetric vs asymmetric, hashing and signatures, TLS handshakes, certificates, CSRs, revocation/expiry, key escrow/rotation.

- **Resilience & site security**: RTO/RPO, backups and off-site copies, UPS/generators, physical access and media disposal.
- **Vulnerability management**: Prescan comms, credentialed vs uncredentialed scans, safe scan configs, triage, false positive reduction, risk-ranked remediation and re-test scheduling.

Module 3 — CompTIA PenTest+ (Weeks 14–24)
Execute the full penetration testing lifecycle legally and ethically in controlled labs, develop tool proficiency, and produce professional-grade reports.ITSM & ITIL fundamentals: the helpdesk as SPOC, ITIL guiding principles and the Service Value System (SVS).

- **Information Gathering & Vulnerability Scanning:** OSINT & recon: DNS/WHOIS lookups, metadata extraction, search operators, company footprinting. Tools: Shodan, recon-ng, Maltego, theHarvester; ethics and privacy guardrails.
- **Human/physical angles:** phishing, vishing, smishing patterns; badge/tailgate awareness; mitigations.
- **Scanning:** plan and run Nmap/NSE discovery, configure Nessus/OpenVAS policies, compare credentialed vs uncredentialed output, and capture packets with Wireshark/tcpdump to verify.
- **Web apps (OWASP Top 10):** SQLi, injection, XSS/CSRF, SSRF, path traversal; toolchain Burp Suite, SQLmap, DirBuster; practise against DVWA/Juice-Shop.
- **Protocol & session security:** TLS 1.2/1.3, HSTS, cookie flags, session fixation/timeout; safe downgrade demonstrations in lab only.
- **Evasion & covert channels:** IDS/IPS evasion concepts, rate-limiting, user-agent/IP rotation; tunnelling ideas explained with safeguards.
- **Specialised environments:** IoT and SCADA/ICS risks, VM-escape considerations; compensating controls and testing constraints.
- **Post-exploitation:** credential hunting and safe testing, privilege escalation, lateral movement (SMB/RDP/SSH), pivoting via tunnels, persistence (scheduled tasks/cron; services), and controlled exfiltration in a sandbox. Tools include Metasploit/C2 frameworks and PowerShell/Bash helpers.
- **During-test comms:** trigger points, stakeholder updates, and disciplined note-taking/versioning.
- **Professional reporting:** executive summary for non-technical readers, detailed methods and evidence, **CVSS-based prioritisation**, and clear remediation plans; secure storage/distribution; cleanup, retest and attestation.
- **Proficiency track:** Nmap/NSE & Zenmap, Nessus/OpenVAS, Wireshark/tcpdump, Metasploit—read outputs, correlate with logs, and reduce false positives.
    - **Scripting & automation:** Bash, PowerShell and Python for recon parsers, mass checks and evidence packaging; NASL basics for custom scanner plugins. Safe-by-design patterns (rate limits, logging, idempotence).

Assessment Method

- Learners will be assessed through a **portfolio of evidence x 4 projects** which includes:
    - Written reports
    - Presentations
    - Assignments
    - Case studies
- All assessments are:
    - **Internally assessed** by tutors.

Career Pathways

After completing the course, learners can progress to:

- Entry-level roles such as:
    - First Line IT Support
    - Junior Security Analyst
    - SOC Analyst
    - Junior Penetration Tester