



TCM
SECURITY

PENTESTER ROADMAP



academy.tcm-sec.com



TCM
SECURITY





TCM
SECURITY

PRACTICAL ETHICAL HACKING COURSE (PEH)

- 1. Introduction:** Accessible to all with enthusiasm for learning; no previous hacking experience required.
- 2. Prerequisites:** Basic IT knowledge essential; specific hardware recommendations for intensive tasks.
- 3. Foundational Skills:** Gain proficiency in networking, Linux basics, and Python programming.
- 4. Specialized Techniques:** Dive into reconnaissance, scanning, enumeration, and direct system exploitation.
- 5. Hands-On Projects:** Practical exercises including Active Directory exploitation and wireless network hacking.
- 6. Professional Skills:** Learn to write detailed reports and navigate legal documentation in cybersecurity.
- 7. Career Pathways:** Guidance on leveraging course learnings for advancement in cybersecurity careers.



academy.tcm-sec.com



TCM
SECURITY



PRACTICAL JUNIOR PENETRATION TESTER(PJPT)

- 1. Certification Overview:** Beginner-level exam for those aiming to master internal network penetration testing at an associate level.
- 2. Exam Structure:** Four-day challenge including a two-day penetration test and two days for report writing.
- 3. Key Competencies:**
 - Mastery of Active Directory to navigate and control network domains.
 - Crafting a comprehensive, professional report on findings.
- 4. Intended Participants:** Designed for aspiring hackers, IT professionals, students in tech, and those advancing their cybersecurity careers.
- 5. Outcomes:** Gain certification by demonstrating practical penetration testing skills and reporting capabilities.





TCM
SECURITY



OPEN-SOURCE INTELLIGENCE (OSINT) FUNDAMENTALS

- 1. Focus:** Master OSINT techniques for enhanced investigative skills and personal security.
- 2. Requirements:** Basic Linux and virtualization knowledge; enthusiasm to learn.
- 3. Skills Gained:**
 - Fundamentals of OSINT, advanced search tactics, and secure account creation.
 - Analyzing images, emails, social media, and more for intelligence gathering.
- 4. Application:** Use OSINT tools for automation and efficient data analysis.
- 5. Deliverables:** Develop the ability to write comprehensive OSINT reports.



academy.tcm-sec.com



TCM
SECURITY



EXTERNAL PENTEST PLAYBOOK

- 1. Course Focus:** Enhance your external pentest skills, from understanding attack methodologies to improving client interactions and acing job interviews.
- 2. Prerequisites:** Basic pentest and security knowledge recommended, along with a keen desire to learn.
- 3. Learning Outcomes:**
 - Master external pentest objectives, documentation, and effective communication with clients.
 - Develop advanced attack strategies, including vulnerability scanning and OSINT techniques.
- 4. Practical Skills:** Learn to attack O365/OWA, login portals, bypass MFA, and escalate access.
- 5. Professional Development:** Gain expertise in report writing, pentest findings, client debriefs, retests, and attestations.



academy.tcm-sec.com



TCM
SECURITY



WINDOWS PRIVILEGE ESCALATION

- 1. Course Goals:** Master Windows Privilege Escalation to enhance your skills in security and prepare for major certifications.
- 2. Requirements:** Basic hacking and virtualization knowledge
- 3. Key Learnings:**
 - Techniques for enumerating Windows systems using manual methods and tools.
 - Diverse privilege escalation tactics, from kernel exploits to service permissions.
- 4. Experience:** Engage with 13 vulnerable machines and a comprehensive capstone challenge.
- 5. Ideal For:** aiming to improve Capture the Flag abilities and PNPT certification preparation.



academy.tcm-sec.com



TCM
SECURITY



LINUX PRIVILEGE ESCALATION

- 1. Course Goals:** Enhance your cybersecurity prowess with Linux Privilege Escalation, tailored for upskilling in security practices and aiding certification achievements.
- 2. Requirements:** Basic hacking and virtualization knowledge; Hack the Box/TryHackMe recommended.
- 3. Key Learnings:**
 - Linux system enumeration techniques.
 - Various privilege escalation methods, including kernel exploits and specific CVEs.
- 4. Experience:** Tackle 11 machines and a capstone in a custom lab.
- 5. Ideal For:** Aspiring to advanced cybersecurity professionals focusing on Linux environments.





TCM
SECURITY

TCM SECURITY CERTIFIED

Practical Network Penetration Tester

PNPT

PRACTICAL NETWORK PENETRATION TESTER (PNPT)

- 1. Overview:** The PNPT offers an intermediate-level certification focusing on network penetration testing skills at a professional level.
- 2. Exam Details:** Candidates have 5 days for the assessment plus 2 days for report writing.
- 3. Certification Requirements:**
 - Use OSINT for attack planning.
 - Exploit networks via Active Directory.
 - Provide a report and a 15-minute live debrief.
- 4. Key Skills:** Emphasizes OSINT, Active Directory exploitation, and effective communication.
- 5. Ideal For:** Individuals aiming to certify their ability to conduct high-level network penetration tests.



academy.tcm-sec.com