

Pen Tester Track

ISC² CC · CompTIA Network+ · CompTIA Security+ (SY0-701) · EC-Council CEH v13

Learn to think like an attacker — legally. The Pen Tester Track takes you from zero IT knowledge through networking foundations and security fundamentals to full-scale ethical hacking and penetration testing. Graduate with CEH v13 exam readiness and a portfolio of real p...

Kali Linux

Metasploit

Burp Suite

Nmap

Wireshark

Nessus

Hydra

Aircrack-ng

OWASP ZAP

260 hrs

Training

3

Modules

4

Certs Aligned

~3 mo

Full-Time

R28,000

Track Fee

WHAT'S IN THIS TRACK

Three Modules. One Career Path.

1

IT & Networking Foundations

OSI model, TCP/IP deep dive, DNS, DHCP, subnetting, Wireshark packet analysis and Kali Linux lab setup. The entry point for all tracks — no prior IT knowledge required.

R9,500

80 hrs · 4 wks FT

2

Core Security Fundamentals

Threats and vulnerabilities, cryptography, PKI, firewalls, IDS/IPS, vulnerability scanning, identity and access management, and POPIA/NIST compliance frameworks.

R10,500

80 hrs · 4 wks FT

3

Ethical Hacking & Pen Testing

Reconnaissance, scanning, exploitation, post-exploitation and professional report writing. Metasploit, Burp Suite, Nmap, OWASP Top 10 web app attacks and wireless penetration testing.

R12,000

100 hrs · 5 wks FT

CURRICULUM HIGHLIGHTS

Week-by-Week Training

WEEKS 1-2

Networking Foundations

OSI model, TCP/IP stack, IP addressing, DNS, DHCP, ARP. Understanding how data moves across networks — the foundation for everything that follows.

WEEKS 3-4

Network Tools & Lab Setup

Wireshark packet capture and analysis, Kali Linux installation and configuration, VirtualBox/VMware lab setup, basic Linux command line proficiency.

WEEKS 5-6

Security Concepts & Threat Landscape

CIA triad, threat actors, attack vectors, malware types, social engineering, risk assessment methodologies and the current South African threat landscape.

WEEKS 7-8

Cryptography, PKI & Access Control

Symmetric and asymmetric encryption, hashing, digital certificates, PKI infrastructure, multi-factor authentication, identity and access management.

WEEKS 9-10

Firewalls, IDS/IPS & Vulnerability Scanning

Firewall configuration and rule sets, intrusion detection and prevention systems, Nessus vulnerability scanning, security baselines and hardening.

WEEKS 11-12

Reconnaissance & Footprinting

Passive and active reconnaissance, OSINT techniques, Google dorking, Shodan, DNS enumeration, social engineering reconnaissance and information gathering.

WEEKS 13-14

Scanning, Enumeration & Exploitation

Nmap scanning techniques, service enumeration, Metasploit framework, exploit development basics, privilege escalation on Linux and Windows targets.

WEEKS 15-16

Web App Hacking & Wireless Attacks

OWASP Top 10 vulnerabilities, SQL injection, XSS, CSRF, Burp Suite interception, OWASP ZAP, wireless network attacks with Aircrack-ng, WPA2 cracking.

WEEKS 17-18

Post-Exploitation, Pivoting & Report Writing

Maintaining access, lateral movement, pivoting techniques, data exfiltration, covering tracks, professional penetration test report writing and client presentation.

CERTIFICATIONS ALIGNED

Industry Certifications

ISC² Certified in Cybersecurity

Entry-level security certification that validates foundational cybersecurity knowledge. Recognised globally and a strong first credential on your CV.

CompTIA Network+

Networking skills foundation for security professionals. Validates your understanding of how networks operate — essential knowledge for any penetration tester.

CompTIA Security+

The gold standard entry-level security certification. Required by US DoD 8570 and requested by most South African cybersecurity employers as a baseline requirement.

EC-Council CEH v13

The industry standard for penetration testing. Validates ethical hacking skills across reconnaissance, exploitation, web app attacks and report writing.

WHO IS THIS FOR

Built for Your Career Path

Aspiring Red Teamers

You're fascinated by how systems break. You want to learn reconnaissance, exploitation and post-exploitation — and get paid to do it legally. The Pen Tester Track is your structured path from curiosity to career.

- ✓No prior IT experience required — start from scratch
- ✓Hands-on labs with real attack tools from week one
- ✓Build a portfolio of professional pen test reports
- ✓CEH v13 exam readiness upon completion

IT Professionals Pivoting to Security

You're already working in IT — networking, system admin, helpdesk — and you want to move into offensive security. The Pen Tester Track formalises your knowledge and adds the ethical hacking skills employers are hiring for.

- ✓Skip Module 1 if you pass the placement assessment
- ✓CompTIA Security+ and CEH to formalise what you know
- ✓Practical Metasploit, Burp Suite and Nmap lab work
- ✓Part-time option — keep your current role while upskilling

CAREER OUTCOMES

Where This Track Takes You

Junior Penetration Tester

Red Team Analyst

Vulnerability Assessor

Application Security Tester

Security Consultant

ENTRY LEVEL

R400K – R600K

0–2 years experience

MID LEVEL

R700K – R1.2M

2–5 years + CEH

SENIOR LEVEL

R1.2M – R2M+

PRICING

Track Pricing

Best Value

Pen Tester Track (Bundle)

R12,873,765,039

- ✓1: IT & Networking Foundations (80 hrs · 4 wks FT)
- ✓2: Core Security Fundamentals (80 hrs · 4 wks FT)
- ✓3: Ethical Hacking & Pen Testing (100 hrs · 5 wks FT)

1: IT & Networking Foundations

R9,500

2: Core Security Fundamentals

R10,500

3: Ethical Hacking & Pen Testing

R12,000

FAQS

Frequently Asked Questions

Q Do I need IT experience to start the Pen Tester Track?

No prior IT or cybersecurity experience is required. The track begins with Module 1 — IT & Networking Foundations — which starts from absolute zero. You'll learn networking concepts, Linux basics and set up your own security lab before moving into security and ethical hacking. If you already have an IT background, you may be able to skip Module 1 after a short placement assessment.

Q Which certifications does the Pen Tester Track prepare me for?

The Pen Tester Track prepares you for four industry-recognised certifications: ISC² CC (Certified in Cybersecurity), CompTIA Network+, CompTIA Security+ (SY0-701) and EC-Council CEH v13 (Certified Ethical Hacker). Each module's curriculum is directly aligned to the relevant exam objectives.

Q How long does the Pen Tester Track take?

The Pen Tester Track is 260 hours of training across three modules. Studied full-time, this takes approximately 3 months (13 weeks). A part-time option is available and roughly doubles the duration to about 6 months. All sessions are recorded so you can catch up if you miss a class.

Q Are certification exam fees included?

Certification exam fees are not included in the track fee of R28,000. Your tuition covers all training materials, lab environments and mock exams to prepare you fully before you sit the official exam. Exam vouchers can be purchased separately or are included as part of the Elite tier if you choose to enrol in the full bootcamp.

Q What equipment do I need?

You need a laptop or desktop with at least 8 GB of RAM (16 GB recommended), a modern processor (Intel i5 / AMD Ryzen 5 or better) and 100 GB of free disk space. You'll be running virtual machines with Kali Linux and target labs, so the more resources the better. A stable internet connection is required for online attendance and cloud lab access.

Q What does a penetration tester earn in South Africa?

Entry-level penetration testers and junior red team analysts in South Africa typically earn between R400,000 and R600,000 per year. Mid-level pen testers with CEH and 2–4 years of experience earn R700,000 to R1.2 million. Senior penetration testers, security consultants and red team leads earn R1.2 million to R2 million or more, with contract and consulting rates often exceeding salaried positions.

🚀 Want All Six Modules?

Complete all six modules across all three specialist tracks for the full Cybersecurity Bootcamp Certificate. Three tier options available.

STANDARD

R49,500

PROFESSIONAL

R59,000

ELITE

R79,000

Get in Touch

✉ info@codecollege.co.za

☎ +27 (0)10 970 7777

💬 WhatsApp: +27 83 600 2765

🌐 codecollege.co.za/cybersecurity-bootcamps/

Payment plans available · Group rates on request · EFT & card accepted · B-BBEE Level 4 · SDL eligible · Exam fees not included