

# Module 3: Ethical Hacking & Penetration Testing

100 hrs · R12,000 · 5 weeks

Think like an attacker — legally. This ethical hacking and penetration testing course follows the EC-Council CEH v13 methodology from reconnaissance through exploitation to professional report writing. Run real attack...

**100 hrs**

Training Hours

**R12,000**

Module Fee

**5 weeks**

Full-Time

**10 weeks**

Part-Time

**JHB · Online**

Delivery

## WEEKLY CURRICULUM

## What You'll Learn

### Reconnaissance & Footprinting

Passive OSINT: Maltego, Shodan, theHarvester, WHOIS, Google dorks.  
Active scanning: Nmap host discovery, port scanning...

### Web Application Hacking

OWASP Top 10 hands-on: SQL injection (manual + sqlmap), XSS (reflected/stored/DOM), CSRF, IDOR, file inclusion (LFI/R...)

### Post-Exploitation & Report Writing

Post-exploitation: covering tracks, persistence, pivoting basics.  
Professional pen test report writing: executive summary...

### Exploitation — Systems & Passwords

Metasploit framework architecture, modules and payloads. Exploiting known CVEs against Metasploitable2. Password attacks...

### Wireless, Mobile & Social Engineering

WPA2/WPA3-PSK cracking, evil twin AP setup, deauthentication attacks, Bluetooth vulnerabilities. Social engineering methods...

## LEARNING OUTCOMES

## After This Module You Will Be Able To

- ✓ Execute a full penetration test following the CEH v13 methodology (recon → exploit → post-exploit → report)
- ✓ Use Kali Linux tools proficiently for scanning, exploitation and post-exploitation tasks
- ✓ Attack OWASP Top 10 web vulnerabilities against intentionally vulnerable applications in a legal lab
- ✓ Perform wireless network attacks (WPA2 cracking, evil twin) using an Alfa adapter
- ✓ Write a professional penetration test report with CVSS-scored findings and business-level recommendations
- ✓ Demonstrate EC-Council CEH v13 exam readiness across all 20 CEH domains

## TOOLS &amp; PLATFORMS

Kali Linux

Metasploit Framework

Burp Suite Community

Nmap / Zenmap

Hydra / John the Ripper

Aircrack-ng

Maltego

sqlmap

DVWA / Metasploitable2

TryHackMe (Jr Penetration Tester path)

### Certification Alignment

This module prepares you for the following internationally recognised exams. Exam fees are separate.

EC-Council CEH v13

## WHAT TO EXPECT

## Your Learning Experience



### Expert-Led Live Training

Live sessions, not recordings. Taught by industry practitioners with 20+ years of training experience.



### Hands-On VM Labs

Every topic has a lab exercise. You build, break and defend real systems in your own VM environment.



### Johannesburg & Online

In-person at Code College Woodmead or 100% live online from anywhere in South Africa.



### Digital Badge on Completion

Earn a Code College Digital Badge — shareable to LinkedIn. Stack badges toward the full bootcamp certificate.

## 2026 PRICING

## Investment

MODULE FEE

**R12,000**

One flat price — no hidden fees

TRACK BUNDLE (3 MODULES)

**From R26,500**

Save up to R4,500 vs individual prices

# Get in Touch

 [info@codecollege.co.za](mailto:info@codecollege.co.za)     +27 (0)10 970 7777     WhatsApp: +27 83 600 2765

 [codecollege.co.za/short-cybersecurity-courses/module-3-ethical-hacking/](https://codecollege.co.za/short-cybersecurity-courses/module-3-ethical-hacking/)

Payment plans available · Group rates on request · EFT & card accepted · B-BBEE Level 4

## FAQS

## Frequently Asked Questions

### Q Is it legal to learn these hacking techniques?

Yes — all practical work is performed in isolated, intentionally vulnerable lab environments that you own and control (VirtualBox VMs on your own machine) or in legal platforms like TryHackMe. The module includes a professional ethics session covering computer crimes legislation in South Africa (ECTA, Cybercrimes Act 2020) and the boundaries of lawful security testing.

### Q What about the wireless attack labs?

All wireless hacking labs run in your browser on Code College's Docker infrastructure. No Wi-Fi adapter, no local tools, no hardware needed. You get a simulated wireless environment that behaves exactly like real WPA2/WPA3 networks, allowing you to practice reconnaissance, password cracking, and packet injection attacks without special hardware.

### Q What is CEH v13 and how hard is the exam?

The EC-Council Certified Ethical Hacker v13 is a globally recognised offensive security certification. The exam is 125 multiple-choice questions over 4 hours. Pass rate for candidates who complete structured training is approximately 70%. This module maps to all 20 CEH v13 domains. The exam voucher is purchased separately from EC-Council (~R6,500–R8,500 depending on bundle).

### Q Can I take this module even if I don't plan to become a pen tester?

Absolutely. Understanding offensive techniques makes you a significantly better defender. SOC analysts and incident responders with Module 3 knowledge understand attacker behaviour at a level that improves detection quality and investigation speed. Many blue team professionals hold both CEH and CySA+.

### Q How much does the CEH exam cost in South Africa?

The CEH v13 exam (312-50) costs approximately USD 550 — around R10,000–R11,000 at current exchange rates — via Pearson VUE. It can be written at a Johannesburg test centre or online. A separate CEH Practical exam (also USD 550) is available; many employers value candidates who hold both. Module 3 prepares you for the theory exam and the practical lab hours count toward the Practical eligibility requirement.

### Next Step in Your Cybersecurity Journey

Next step: Module 4 (Blue Team/SOC) or Module 5 (Cloud Security) →