



FIVE-DAY PRACTITIONER COURSE

Ethical Computer Hacking

Pure hands-on hacking — the techniques real attackers use, taught legally and ethically.

www.computertrainingwales.co.uk



THE COURSE

Hacking, done right

Five days of practical penetration testing — from reconnaissance through exploitation to the professional report clients pay for. Mornings are taught; afternoons are hands-on labs.

5

DAYS

5

LIVE LABS

1

CAPSTONE



COURSE ROADMAP

Five days. Five outcomes.

Each day builds on the last — by Friday you have run a full penetration test end to end.

01

Methodology & Setup

Ethics, law, Kali

02

Recon & Scanning

OSINT to Nmap

03

Exploitation

Metasploit & privesc

04

Web App Security

OWASP Top 10

05

Reporting

Report & present

Mornings taught · Afternoons hands-on labs · One transformed career

HOW A DAY WORKS

Learn it, then do it

MORNING

Taught session

Concepts, methodology and live demonstrations from a practising tester. You see the technique performed before you touch it.

AFTERNOON

Hands-on lab

You work in your own isolated lab environment, running the tools yourself against deliberately vulnerable targets.

09:00

Taught session

11:00

Technique demo

13:00

Lab time

16:00

Debrief & review

Hacking Methodology & Setup

The ethical framework, legal boundaries, and the Kali Linux toolkit that forms the basis of every penetration test.

- Ethical hacking vs criminal hacking

- Legal frameworks & authorisation

- Penetration testing methodology

- Kali Linux setup & tools

- Virtual lab environment

- Scope & rules of engagement

LAB

Set up your Kali Linux environment and practice lab

Reconnaissance & Scanning

Before you hack, you gather intelligence. OSINT, port scanning, service enumeration — the art of finding targets.

- OSINT (open-source intelligence)

- DNS enumeration

- Nmap port scanning

- Service version detection

- Vulnerability scanning (OpenVAS)

- Mapping the attack surface

LAB

Conduct a full reconnaissance and vulnerability scan of a target

Vulnerability Exploitation

The core of ethical hacking. Exploit real vulnerabilities in practice systems — safely, legally, and methodically.

- **Exploitation frameworks (Metasploit)**

- **Buffer overflows (conceptual)**

- **Lateral movement**

- **Common vulnerability types**

- **Privilege escalation**

- **Post-exploitation basics**

LAB

Exploit multiple vulnerabilities in a practice environment

Web Application Security

Most attacks target web applications. SQL injection, XSS, authentication flaws — the OWASP Top 10 in practice.

- OWASP Top 10 overview

- Cross-site scripting (XSS)

- Burp Suite introduction

- SQL injection

- Authentication & session attacks

- Secure coding principles

LAB

Find and exploit vulnerabilities in a practice web application

Reporting & Remediation

The hack is only half the job. Professional penetration testers live or die by the quality of their reports.

- Report structure & standards

- Evidence documentation

- Executive summary writing

- Risk rating methodologies

- Remediation recommendations

- Client presentation skills

CAPSTONE

Write and present a full penetration test report

THE TOOLKIT

Tools you will actually use

Kali Linux

The penetration tester's operating system and lab base

Nmap

Port scanning, service and version detection

OpenVAS

Automated vulnerability scanning and reporting

Metasploit

Exploitation framework and post-exploitation

Burp Suite

Intercepting and attacking web applications

OWASP Top 10

The industry standard web vulnerability set

Every tool is used inside a legal, isolated lab — never against live systems.

WHAT YOU LEAVE WITH

One transformed career

- 1 Run a penetration test from scope to report
- 2 Think like an attacker — and defend like one
- 3 Work confidently inside legal and ethical boundaries
- 4 Produce a client-ready report that stands up to scrutiny





READY WHEN YOU ARE

Book your place

Five days. Five outcomes. Pure hands-on ethical hacking with Reskill Wales.

01656 737349 · hello@reskillwales.co.uk

www.computertrainingwales.co.uk