



Z X 3 0 1

PRACTITIONER • LEVEL 3

Penetration Testing

9

MODULES

213

LAB TASKS

108

CTF CHALLENGES

85

TOPICS

9

COURSE BOOKS

146

SLIDES

9 COURSE BOOKS INCLUDED

Penetration Testing

Z X 3 0 1



This program transforms students into versatile security professionals by teaching the full lifecycle of a cyber attack. You will start by mastering reconnaissance and enumeration, learning how to map out a target's digital footprint. From there, the focus shifts to the "break-in," where students practice identifying and exploiting vulnerabilities to understand how systems fall. The journey continues with post-exploitation tactics—learning how attackers maintain access and extract data—before concluding with a deep dive into web application security to ensure digital platforms are hardened against real-world threats.

CURRICULUM & WHAT EACH MODULE COVERS

MODULE	TASKS
01 Information Gathering Leaked Credential and Data Breach Databases · Shodan · Device and Vulnerability Search Engine · Network Range and Host Reconnaissance · +5 more	20
02 Scanning Controlling Nmap Scan Scope and Speed · Analyzing Scan Traffic with Wireshark · Netdiscover for LAN Host Discovery · +4 more	24
03 Enumeration Scanning Fundamentals with Nmap · Nmap Scripting Engine (NSE) · Metasploit Framework for Enumeration · +5 more	20
04 Exploitation SMB Share Enumeration and Symlink Traversal · Credential Attacks and Remote Login Exploitation · Exploiting Vulnerable Network Services via... · +6 more	25
05 Meterpreter Reading Network Configuration of a Compromised Host · File System Operations Through Meterpreter · Reconstructing Attacks from Meterpreter Session Logs · +8 more	20
06 Payloads Connection Models: Bind vs Reverse Shells · Inspecting Generated Payload Files · Automated and Web-Delivered Payload Generation · +12 more	26
07 Post Exploitation Credential Harvesting and Lateral Movement · What Post-Exploitation Actually Is · Getting a Foothold on Linux · +8 more	32
08 Social Engineering Malicious Office Documents and NTLM Hash Capture · Recognizing and Defending Against Social Engineering · Browser Hooking and Exploitation with BeEF · +4 more	15
09 WebApp Security File Upload Vulnerabilities & Remote Code Execution · Web Application Fundamentals for Security Testing · Web Vulnerability Scanning and Directory Enumeration · +6 more	31

GOOD TO KNOW

Best after a level 1–2 programme · Self-paced or trainer-led · Cy, the AI helper, answers in the student's own language

HOW EVERY MODULE RUNS

Lab



Extra at 80%



Timed test at 85%



Slides at 90%

A REAL TASK FROM MODULE 7 — POST EXPLOITATION

"In the Windows VM session, escalate privileges and run the hashdump post-module, then identify the full hash entry for the Administrator account."

Finish with a capstone project · interview preparation · City & Guilds Assured certificate

DATA AS OF 2026-09-30 · V260930