



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

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 2026-10-12 · V261012