



Z X 3 1 0

SPECIALIST • LEVEL 6

Cyber Warfare

11

MODULES

799

LAB TASKS

119

CTF CHALLENGES

99

TOPICS

11

COURSE BOOKS

293

SLIDES

11 COURSE BOOKS INCLUDED

Cyber Warfare

Z X 3 1 0



This program transforms students into advanced security specialists by teaching the complete lifecycle of high-level cyber attacks. You will start with reconnaissance and manual enumeration, learning to gather critical intelligence without relying on automated tools. From there, the focus shifts to the "art of the invisible," where you will master crafting undetectable payloads and bypassing modern security systems through obfuscation. The journey continues through complex domain attacks, lateral movement, and advanced exploitation techniques like buffer overflows.

CURRICULUM & WHAT EACH MODULE COVERS

MODULE	TASKS
01 Recon & Targeting Credential Attacks and Password Lists · SMB Enumeration and Vulnerability Assessment · +8 more	66
02 IoT Exploitation Filesystem Inspection and Static Analysis · Passive Reconnaissance with Shodan · +8 more	69
03 Advanced Payloads I Netcat for Shells and File Transfers · Alternate Data Streams and forfiles Execution · +5 more	56
04 Advanced Payloads II PowerShell Reverse Shell Payloads · certutil.exe Payload Delivery · +6 more	70
05 Hands-On Exploitation Bash I/O Redirection and Reverse Shell Fundamentals · Exploit Research and Vulnerability Intelligence · +4 more	85
06 Active Directory Attacks Key Active Directory Services · Remote Execution and Lateral Movement · +10 more	125
07 Post (Windows) Privilege Escalation via Unquoted Service Paths · Sensitive Data Discovery in User Profiles · +12 more	67
08 Post (Linux) Initial Access and Basic Enumeration · Automated Enumeration Tools · +6 more	83
09 Social Engineering URL Obfuscation Through IP Address Encoding · URL Structure Exploitation and Deceptive Formatting · +6 more	44
10 Stealth & Evasion Windows Antimalware Scan Interface (AMSI) · Linux Audit Subsystem · +8 more	94
11 Red-Team Ops Malicious Autorun and PDF Action Chains · Malicious PDF Structure and Actions · +4 more	40

GOOD TO KNOW

Best after a level 4–5 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 (WINDOWS)

"Run the local exploit suggester on the current session, escalate privileges from intern to SYSTEM, and execute 'whoami /groups' in the cmd shell. Identify the builtin group listed."

Finish with a capstone project · interview preparation

DATA AS OF 2026-09-30 · V260930