



Z X 3 0 5

ADVANCED • LEVEL 4

Network Security

10

MODULES

329

LAB TASKS

122

CTF CHALLENGES

68

TOPICS

10

COURSE BOOKS

175

SLIDES

10 COURSE BOOKS INCLUDED

This program transforms students into experts in securing complex corporate infrastructures. You will start by mastering advanced networking and attacking frameworks, gaining a deep understanding of how protocols can be both used and abused. From there, the focus shifts to the heart of the modern office: Active Directory. You'll learn the ins and outs of domain services and event logging before mastering PowerShell to automate and manage Windows environments at scale. The journey continues with hands-on domain exploitation, where you'll learn to identify and neutralize vulnerabilities before they can be leveraged. The program concludes with a study of cryptography, providing you with the encryption skills needed to keep sensitive data truly private.

CURRICULUM & WHAT EACH MODULE COVERS

MODULE	TASKS
01 Subnetting Variable Length Subnet Masking (VLSM) · Subnet Design for Network Topologies · IP Addressing Fundamentals · +3 more	23
02 Network Attacks ARP and Man-in-the-Middle Attacks · DNS and Local Name Resolution · Windows Target Configuration · +4 more	41
03 Domain Setup Active Directory Domain Fundamentals · DNS Integration with Active Directory · LDAP Directory Access Protocol · +4 more	21
04 Domain Events Configuring Audit Policies with Group Policy · Windows Event Logging Fundamentals · Security Group Management Events · +5 more	21
05 PowerShell PowerShell Environment and Core Navigation · Object Pipeline and Member Inspection · File Content Analysis and Hashing · +6 more	42
06 Domain Enumeration PowerShell Active Directory Module Enumeration · Windows Built-in Enumeration Commands · Network Discovery with PowerShell · +5 more	31
07 Domain Exploitation Remote Windows Enumeration with RPC and SMB · MS17-010 Exploitation and Defense Bypass · Network Reconnaissance and Vulnerability Scanning · +3 more	31
08 Domain Post Initial Access and Hash Extraction · Domain User Manipulation and Persistence · Pass-the-Hash and Lateral Movement · +3 more	45
09 Domain Security PowerShell for Domain Security Analysis · NTLM Authentication and Pass-the-Hash Detection · Windows Security Event Logs · +2 more	21
10 Cryptography Number Systems and Data Encoding · Mathematical Foundations for Modern Cryptography · Cryptographic Hash Functions · +3 more	53

GOOD TO KNOW

Best after a level 2–3 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 8 — DOMAIN POST

"Configure the Web Delivery exploit target to be PowerShell, choose an x64 architecture payload, and determine the PowerShell command to execute on the victim machine."

Finish with a capstone project · interview preparation

DATA AS OF 2026-10-12 · V261012

