



N X 2 0 1

APPLIED • LEVEL 2

Network Research

10

MODULES

297

LAB TASKS

164

CTF CHALLENGES

73

TOPICS

10

COURSE BOOKS

144

SLIDES

10 COURSE BOOKS INCLUDED

Network Research

N X 2 0 1



This program provides a deep dive into the architecture of modern networks and the security measures that protect them. Students master Linux administration and virtualization, building a strong foundation in scripting and system management. After gaining a thorough understanding of core networking protocols, the focus shifts to network security, where participants learn to identify vulnerabilities using advanced scanning tools and testing strategies. The journey concludes with hands-on experience in cyber defense, including firewall operations and payload manipulation with industry-standard tools like Msfvenom and Metasploit, ensuring a comprehensive grasp of robust network protection.

CURRICULUM & WHAT EACH MODULE COVERS

MODULE	TASKS
01 Intro to Linux Getting Oriented in the Shell · Installing and Running Software · System and Process Monitoring · +3 more	39
02 Text Manipulation Applying Text Tools to Real Investigations · Locating and Viewing Specific Lines · Setting Up: Redirection and Pipes · +5 more	27
03 Network Services Browsing Web Servers and Inspecting Pages · Standing Up and Monitoring Network Services on Linux · Remote Shell Access with SSH · +2 more	35
04 Scanning Basic Nmap Port Scanning · Masscan: High-Speed Port Scanning · Investigating Discovered Services · +3 more	30
05 Wireshark The TCP/IP Model and Packet Encapsulation · Telnet, SSH, and Cleartext Credential Exposure · SMB File Sharing Traffic · +7 more	35
06 Online Attacks Authentication Logs and Detecting Brute Force On the Host · Detecting Brute-Force Attacks in Network Traffic · ARP and Man-in-the-Middle Attacks · +5 more	34
07 Offline Brute-Force Chained Cracking and Building Wordlists from Cracked Content · Custom Wordlists with Cupp and CeWL · Cracking Hashes with John the Ripper · +5 more	22
08 Linux Scripting Filtering and Comparing Data with Command-Line Tools · File Permissions and Executing Scripts · Building a Log Analysis Script · +6 more	30
09 Intro to Trojans Reading and Analysing a Meterpreter Log · How Trojans Work · Payload Creation with msfvenom · +4 more	29
10 Intro to Firewalls Applied Rule Scenarios — Locking Down Common Services · Firewall State Management and Backup · netsh advfirewall — Introducing the Tool · +3 more	16

GOOD TO KNOW

Best after a foundation (level 1) 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 6 — ONLINE ATTACKS

"Use Hydra to brute-force the NR-BOX SSH service with the user 'ghost', which does not exist. Find the line in /var/log/auth.log that records the failed attempt and write it."

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

DATA AS OF 2026-10-12 · V261012