



N X 2 1 6

ADVANCED • LEVEL 4

Network Forensics

14

MODULES

1064

LAB TASKS

127

CTF CHALLENGES

123

TOPICS

14

COURSE BOOKS

523

SLIDES

14 COURSE BOOKS INCLUDED



This program transforms cybersecurity professionals into elite investigators capable of deconstructing the most complex digital trail. You will start by mastering IPv6 forensics and advanced Wireshark techniques, learning to perform deep packet inspection and decrypt secure traffic. The journey continues through enterprise-level networking, where you will learn to extract forensic evidence from Cisco devices, routers, and switches. You will get hands-on experience in modern battlegrounds—from investigating email-based phishing to tracking anonymous activity on the DarkNet. The program concludes by mastering professional tools like Suricata and TShark, equipping you to automate threat detection and build robust defenses against sophisticated network attacks.

CURRICULUM & WHAT EACH MODULE COVERS

MODULE	TASKS
01 IPv6 IPv6 Network Simulation and Practical Application · IPv6 Address Structure and Representation · <i>+6 more</i>	62
02 Advanced Wireshark Cleartext Protocol Analysis and Credential Extraction · Network Service Discovery and Enumeration · <i>+5 more</i>	45
03 Advanced Networking Packet Capture and Traffic Analysis with Wireshark · DNS Reconnaissance and Web Application Discovery · <i>+6 more</i>	73
04 HTTPS Extracting and Analyzing Files from Decrypted HTTPS · Modern TLS Variants and Protocol Negotiation · <i>+5 more</i>	52
05 WiFi WiFi Frequency Bands and Channels · Wireless Adapters and Operating Modes · <i>+10 more</i>	113
06 TShark HTTP Traffic Analysis and Object Extraction · TLS Decryption and Encrypted Traffic Analysis · <i>+6 more</i>	65
07 Packet Crafting Scapy Utility Commands and Help System · Reading and Modifying Scapy Scripts · <i>+7 more</i>	56
08 Email Analysis Packet Capture Analysis of Email Traffic · DNS Records Supporting Email · <i>+9 more</i>	127
09 Routers Network Address Translation — Source NAT · Linux Packet Filtering Fundamentals · <i>+7 more</i>	48
10 Suricata Writing and Testing Suricata Rules · Detecting and Investigating HTTP Threats · <i>+8 more</i>	55
11 Cisco Securing Device Access and Configuration Persistence · Cisco IOS CLI Fundamentals · <i>+6 more</i>	104
12 Cloud Security EC2 Virtual Machines and Security Groups · Identity and Access Management (IAM) Core Concepts · <i>+7 more</i>	100
13 DarkNet VPN Fundamentals and Tunneling Protocols · SSH Tunneling for Secure Access · <i>+6 more</i>	87
14 Network Attacks ICMP Fundamentals and the Ping of Death Attack · ARP Spoofing and Man-in-the-Middle Attacks · <i>+7 more</i>	77

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 5 — WIFI

“In the Emulator, use the rockyou.txt wordlist to brute-force the network file generated during the handshake capture and crack the password for the 'teddy' Access Point.”

Finish with a capstone project · interview preparation

DATA AS OF 2026-10-12 · V261012