



N X 2 1 5

ADVANCED • LEVEL 4

Linux Forensics

9

MODULES

442

LAB TASKS

69

CTF CHALLENGES

84

TOPICS

9

COURSE BOOKS

344

SLIDES

9 COURSE BOOKS INCLUDED



This program transforms students into elite forensic investigators by diving deep into the inner workings of Linux-based systems. You will start by mastering Linux fundamentals and scripting, building the foundation needed to automate complex tasks and manage services. From there, the focus shifts to advanced analysis techniques, where you will learn to uncover hidden evidence through log, file, and network analysis. The journey continues into evidence collection, where you will get hands-on experience in memory dumping, hard drive cloning, and working with professional tools like FTK. By the end of the course, you will be prepared to tackle real-world challenges—from malware detection to investigating sophisticated data breaches.

CURRICULUM & WHAT EACH MODULE COVERS

MODULE	TASKS
01 Intro to Linux SSH Service Configuration and Key-Based Authentication · Log Analysis Across Other Services · Getting Oriented in a Linux System · +7 more	57
02 Text Manipulation Core Text-Processing Toolkit for Log Analysis · Investigating Audit Logs (audit.log EXECVE records) · Investigating Web Server Access Logs · +5 more	30
03 File Analysis File Carving and Embedded File Recovery · Tracing System Calls and Library Calls · File Type Identification Fundamentals · +5 more	56
04 File Systems Data Carving and Recovering Hidden or Deleted Data · Examining Disk Images Without Mounting · Forensic Disk Imaging and Partition Analysis · +6 more	53
05 Log Analysis Web Traffic Log Analysis (access.log and http.log) · Audit Framework Deep Dive (audit.log) · Authentication Log Analysis (auth.log) · +4 more	52
06 User Activity Linux User Activity Artifacts on a Live System · Reconstructing User Activity from History Files · SSH Key-Based Authentication and Lateral Movement · +9 more	49
07 Network Forensics Extracting and Identifying Files from Captured Traffic · FTP Traffic Analysis and Credential Harvesting · Cracking Encrypted Archives Found in Traffic · +7 more	36
08 Intrusion Investigation Packet Capture Analysis of a Full Intrusion · Web Server Attack Log Analysis · Brute-Force Attacks and Credential Logging · +2 more	33
09 Live and Memory Forensics Live Socket and Process Investigation on a Running System · Live Disk Forensics Fundamentals · Fileless Process Execution Techniques · +12 more	76

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 — INTRUSION INVESTIGATION
"Use arpspoof to run a MiTM attack and capture the traffic with Wireshark. Find the opcode number in the malicious ARP packets."

Finish with a capstone project · interview preparation

DATA AS OF 2026-10-12 · V261012