MODULE 8:
Operating System Security & Network Forensics

Module Objective:
Harden Windows + Linux, investigate firewall/IDS logs, and validate suspicious activity using PCAP and Wireshark. Build SOC-ready skills that translate directly to real incidents.
6 hours • Practical labs • Investigation workflow

Curriculum

SEGMENT 8.1 Windows Security Hardening

Topics Covered

- Windows security architecture
- Local vs Domain Group Policies
- Password and account lockout policies
- User privilege management
- USB and device control
- BitLocker encryption
- Windows Defender advanced security
- Audit policy configuration

Practical Lab

- Configuring Group Policy Objects (GPO)
- Hardening checklist implementation

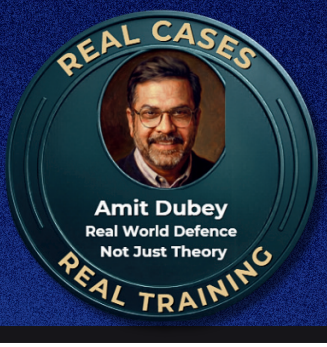
SEGMENT 8.2 Linux Security & Access Control

Topics

- Linux file system permissions (rwx)
- Ownership and groups
- chmod, chown, umask
- Sudo policies
- SELinux / AppArmor basics
- SSH hardening
- Log file analysis

Practical Lab

- Permission misconfiguration detection
- SSH security hardening



SEGMENT 8.3 Network Forensics (PCAP Analysis)

Intelligence from a Mobile Number

- Country & telecom circle
- Messaging app linkage
- Business listings
- Social media associations
- Fraud database presence

Practical Use-Cases

- Scam & extortion investigations
- Fake profiles & impersonation
- Threat actor attribution
- Victim–suspect linkage

Common Pitfalls

- Number recycling by telecom operators
- False attribution due to shared devices
- Over-reliance on a single source

SEGMENT 8.4 Firewalls & Intrusion Detection Systems

Topics

- Firewall types (Stateful, NGFW, WAF)
- IDS vs IPS
- Log formats
- Alert correlation
- False positives
- Attack signature identification
- Incident response workflow

Practical Lab

- Firewall log investigation
- IDS alert interpretation
- What you get (participant takeaways)
- Windows hardening checklist (GPO + audit policy baseline)
- Linux security checklist (permissions, sudo policy, SSH hardening starter baseline)
- Wireshark filter starter set + protocol quick guide
- Firewall/IDS log interpretation cheat-sheet (including false-positive reduction basics)
- Incident workflow template: detect → validate → contain → document
- Certificate of Completion (non-degree)
- **Primary CTA**: Enroll Now
- **Secondary CTA**: Download Curriculum
- For teams: Group / SME Training