Training Course on Advanced Network Traffic Analysis (PCAP Analysis)

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s cybersecurity landscape, Advanced Network Traffic Analysis is a critical skill for identifying and mitigating sophisticated threats. Training Course on Advanced Network Traffic Analysis focuses on PCAP (Packet Capture) analysis, a foundational technique for understanding and interpreting network behavior. By diving deep into PCAP files using industry-standard tools like Wireshark, tcpdump, and Zeek, participants will gain hands-on expertise in analyzing network traffic, detecting anomalies, and tracing malicious activity with precision.

Designed for cybersecurity professionals, analysts, and IT engineers, this course integrates real-world case studies, cutting-edge techniques, and threat intelligence to transform raw packet data into actionable insights. Whether you're monitoring network performance, identifying threats, or responding to incidents, this training equips you with the analytical and technical skills required in today’s zero-trust, threat-hunting, and SOC-driven environments.

Programme Curriculum

Training Course on Advanced Network Traffic Analysis

Introduction

In today’s cybersecurity landscape, Advanced Network Traffic Analysis is a critical skill for identifying and mitigating sophisticated threats. Training Course on Advanced Network Traffic Analysis focuses on PCAP (Packet Capture) analysis, a foundational technique for understanding and interpreting network behavior. By diving deep into PCAP files using industry-standard tools like Wireshark, tcpdump, and Zeek, participants will gain hands-on expertise in analyzing network traffic, detecting anomalies, and tracing malicious activity with precision.

Designed for cybersecurity professionals, analysts, and IT engineers, this course integrates real-world case studies, cutting-edge techniques, and threat intelligence to transform raw packet data into actionable insights. Whether you're monitoring network performance, identifying threats, or responding to incidents, this training equips you with the analytical and technical skills required in today’s zero-trust, threat-hunting, and SOC-driven environments.

Course Objectives

1. Master the fundamentals and structure of PCAP files using Wireshark and tcpdump.
2. Identify anomalies, intrusions, and malware through deep packet inspection (DPI).
3. Correlate threat behavior using MITRE ATT&CK and kill chain models.
4. Apply network forensics techniques to real-time and historical traffic.
5. Analyze encrypted traffic and understand limitations and decryption techniques.
6. Perform incident response by interpreting log data and packet behavior.
7. Detect C2 (Command and Control) communications in PCAP traces.
8. Use Zeek (Bro) and Suricata for high-performance traffic analysis.
9. Build detection rules and threat indicators (IOCs) from raw traffic.
10. Integrate PCAP analysis into SIEM and EDR workflows.
11. Evaluate network segmentation, VLANs, and tunneling protocols.
12. Perform timeline reconstruction for attack investigations.
13. Document findings in a forensic report with clear evidence chain.

Target Audience

1. SOC Analysts
2. Cybersecurity Engineers
3. Incident Responders
4. Network Administrators
5. Digital Forensics Professionals
6. Malware Analysts
7. Penetration Testers
8. IT Security Consultants

Course Duration: 10 days

Course Modules

Module 1: Introduction to Network Traffic and PCAP Basics

- Overview of TCP/IP and OSI models
- Packet structure and common protocols (HTTP, DNS, TCP, UDP)
- Introduction to PCAP file format
- Capturing packets with Wireshark and tcpdump
- Filtering and displaying traffic
- **Case Study**: Analyzing a DNS tunneling attack in a corporate network

Module 2: Advanced Wireshark Techniques

- Customizing columns and coloring rules
- Advanced display filters and capture filters
- Protocol-specific analysis (HTTP, SSL/TLS)
- Exporting objects from PCAP files
- Profile creation for repeatable workflows
- **Case Study**: Identifying data exfiltration via HTTP POST

Module 3: Threat Detection with Deep Packet Inspection

- Layered traffic analysis
- Recognizing scanning, enumeration, and exploit traffic
- Detecting malformed and suspicious payloads
- Identifying anomalies and beaconing behavior

- Using Wireshark’s expert info and IO graphs
- **Case Study**: Detecting a SQL injection attempt through DPI

Module 4: PCAP Analysis Using Zeek and Suricata

- Introduction to Zeek scripts and logs
- Suricata rules and alerts configuration
- Session reassembly and file extraction
- Using signatures vs. behavior-based detection
- Integration with ELK stack for log correlation
- **Case Study**: Tracking malware download via Zeek HTTP logs

Module 5: Investigating Encrypted Traffic

- Understanding SSL/TLS handshake and certificates
- Indicators of compromise in encrypted sessions
- Decryption methods using session keys
- JA3 fingerprinting for threat hunting
- Limitations and legal considerations
- **Case Study**: Investigating malware over HTTPS using JA3 hash

Module 6: Analyzing Command and Control (C2) Traffic

- Common C2 techniques and protocols
- Beaconing and periodic callbacks
- Domain generation algorithms (DGAs)
- Detecting covert channels and tunneling
- Indicators and behaviors of known APT groups
- **Case Study**: Identifying Cobalt Strike C2 traffic

Module 7: Network Forensics and Incident Response

- Building a forensics timeline from PCAP
- Correlating events with logs and host data
- Identifying initial compromise vector
- Preserving evidence and metadata
- Reporting and documentation standards
- **Case Study**: Forensic investigation of ransomware outbreak

Module 8: Anomaly Detection and Machine Learning Integration

- Defining network baselines
- Using anomaly detection tools
- Introduction to ML for traffic classification
- Flow analysis and clustering techniques
- Data visualization for anomaly detection
- **Case Study**: Unsupervised ML detection of outlier traffic

Module 9: Integrating PCAP Analysis into SIEM Workflows

- Role of PCAP in layered defense
- Feeding PCAP metadata into SIEM
- Alert correlation and triage using PCAP
- Automating workflows with scripts
- Reducing false positives through context
- **Case Study**: Investigating SIEM alerts using PCAP evidence

Module 10: Malware Analysis via Network Traffic

- Identifying malware indicators in traffic
- Payload extraction and analysis
- Reverse engineering traffic behavior
- Malware sandbox integration
- Reporting and classification
- **Case Study**: Analyzing Emotet malware traffic from PCAP

Module 11: Investigating Insider Threats

- Recognizing lateral movement patterns
- Abnormal access patterns and data flow
- File transfers and protocol misuse
- Use of unauthorized remote tools
- Behavioral baselining techniques
- **Case Study**: Detecting insider data theft using NetFlow and PCAP

Module 12: Mobile and IoT Traffic Analysis

- Identifying mobile OS-specific traffic
- IoT protocol analysis (MQTT, CoAP)
- Detecting unencrypted data transmission
- Device fingerprinting via traffic
- Security considerations for smart devices
- **Case Study**: Tracing IoT botnet behavior in PCAP

Module 13: Working with VLANs, Tunnels & VPNs

- VLAN tagging and analysis
- GRE, IPsec, and SSL tunnels
- Traffic segmentation and encapsulation
- Detecting VPN misuse and policy violations
- Visibility challenges and solutions
- **Case Study**: Uncovering lateral movement through VPN tunnel

Module 14: Building Custom Detection Rules

- Writing Suricata rules
- Creating Zeek detection scripts
- Generating alerts from custom indicators
- Rule tuning for performance
- Testing and validation with PCAP samples
- **Case Study**: Building detection rules for credential harvesting

Module 15: Capstone Project and Certification Assessment

- End-to-end traffic investigation challenge
- Realistic attack simulation and analysis
- Report generation and peer review
- Live presentation of findings
- Feedback from instructors
- **Case Study**: Multi-stage attack analysis on enterprise network

Training Methodology

- Instructor-led hands-on sessions with real PCAP data

- Guided labs and simulations using Wireshark, Zeek, Suricata
- Group discussions and team analysis projects
- Quizzes, capstone project, and skill assessment
- Access to downloadable lab environments and toolkits

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com