Training Course on Network Intrusion Detection and Analysis

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

As cyber threats grow in complexity, Network Intrusion Detection and Analysis (NIDA) has become a critical pillar in securing IT infrastructure. Training Course on Network Intrusion Detection and Analysis equips cybersecurity professionals, system administrators, and IT managers with the skills to detect, analyze, and respond to network-based attacks in real-time. With the increasing reliance on cloud services, IoT devices, and mobile networking, organizations require robust intrusion detection mechanisms to mitigate vulnerabilities and maintain secure environments.

In this comprehensive program, participants will gain hands-on experience using open-source and commercial intrusion detection systems (IDS), explore modern threat intelligence techniques, and apply deep packet inspection tools to evaluate and interpret suspicious activities. By combining real-world case studies with lab-based exercises, this course ensures learners are equipped with actionable knowledge to fortify enterprise networks against advanced persistent threats (APTs), zero-day attacks, and lateral movement within systems.

Programme Curriculum

Training Course on Network Intrusion Detection and Analysis

Introduction

As cyber threats grow in complexity, Network Intrusion Detection and Analysis (NIDA) has become a critical pillar in securing IT infrastructure. Training Course on Network Intrusion Detection and Analysis equips cybersecurity professionals, system administrators, and IT managers with the skills to detect, analyze, and respond to network-based attacks in real-time. With the increasing reliance on cloud services, IoT devices, and mobile networking, organizations require robust intrusion detection mechanisms to mitigate vulnerabilities and maintain secure environments.

In this comprehensive program, participants will gain hands-on experience using open-source and commercial intrusion detection systems (IDS), explore modern threat intelligence techniques, and apply deep packet inspection tools to evaluate

and interpret suspicious activities. By combining real-world case studies with lab-based exercises, this course ensures learners are equipped with actionable knowledge to fortify enterprise networks against advanced persistent threats (APTs), zero-day attacks, and lateral movement within systems.

Course Objectives

1. Understand network intrusion detection system (NIDS) architecture and components.
2. Identify and analyze signature-based vs anomaly-based detection techniques.
3. Use tools like Snort, Suricata, and Zeek for real-time monitoring.
4. Perform packet capture and traffic analysis using Wireshark and tcpdump.
5. Apply threat hunting techniques using threat intelligence feeds.
6. Understand MITRE ATT&CK Framework for mapping attack vectors.
7. Develop skills in network forensics and incident response planning.
8. Detect and mitigate zero-day exploits and advanced persistent threats (APTs).
9. Conduct SIEM integration with IDS tools for automated analysis.
10. Deploy honeypots and deception technologies for threat detection.
11. Evaluate network logs for suspicious behavior patterns.
12. Build and maintain custom rules for IDS/IPS environments.
13. Simulate real-world cyberattacks and analyze their lifecycle.

Target Audience

1. Cybersecurity Analysts
2. Network Engineers
3. System Administrators
4. SOC (Security Operations Center) Staff
5. IT Security Consultants
6. Digital Forensics Experts
7. Government and Military IT Staff
8. Cybersecurity Students and Educators

Course Duration: 5 days

Course Modules

Module 1: Introduction to Intrusion Detection Systems (IDS)

- Overview of IDS and IPS
- Types of intrusion detection: Host-based vs Network-based
- Components and architecture of IDS
- Common attack signatures and behaviors
- IDS configuration and deployment scenarios
- **Case Study**: How a financial firm blocked SQL injection via Snort IDS

Module 2: Packet Analysis and Network Traffic Monitoring

- Capturing packets using Wireshark and tcpdump
- Understanding TCP/IP layers and protocols
- Analyzing normal vs suspicious traffic
- Flow analysis and data reconstruction
- Network monitoring strategies and baselines
- **Case Study**: Identifying DNS tunneling in a compromised environment

Module 3: Signature-Based vs Anomaly-Based Detection

- Strengths and weaknesses of each approach

- Using Snort for rule-based detection
- Creating and modifying detection rules
- Identifying false positives and negatives
- Combining detection methods for effectiveness
- **Case Study**: Detecting ransomware using hybrid detection techniques

Module 4: Threat Intelligence and Threat Hunting

- Sources of threat intelligence feeds
- Indicators of Compromise (IoCs)
- Integrating threat intel into IDS
- Developing threat hunting hypotheses
- Tools and frameworks for proactive defense
- **Case Study**: Using threat feeds to detect command-and-control activity

Module 5: Deep Dive into Snort, Suricata, and Zeek

- Installation and setup of IDS tools
- Configuration and tuning for optimal detection
- Custom rule writing and alert management
- Performance considerations and resource tuning
- Comparison of features across IDS tools
- **Case Study**: Comparing Suricata vs Zeek in detecting brute-force attacks

Module 6: Network Forensics and Incident Response

- Preserving evidence and chain of custody
- Analyzing PCAP files post-incident
- Timeline reconstruction of attacks
- Collaborating with IR teams and legal entities
- Reporting and documenting forensic findings
- **Case Study**: Forensic investigation of an insider data breach

Module 7: SIEM and IDS Integration

- Overview of SIEM platforms (Splunk, ELK)
- Log correlation and alert management
- Centralized dashboards for monitoring
- Setting thresholds and notifications
- Automated response workflows
- **Case Study**: Integrating Zeek logs with ELK to identify port scanning

Module 8: Real-World Intrusion Simulation and Defense

- Simulating common network attacks (DDoS, MITM, ARP poisoning)
- Using tools like Metasploit and Kali Linux
- Defensive response drills
- Analysis and reporting of simulated incidents
- Red team vs blue team scenarios
- **Case Study**: Company-wide simulation of phishing attack and IDS response

Training Methodology

- Interactive Lectures to explain theoretical concepts and tools
- Hands-on Lab Exercises using open-source and commercial IDS tools
- Case Study Analysis to apply theory to real-world scenarios

- Simulation-based Learning for practicing detection and response
- Group Discussions and Q&A to enhance understanding and peer learning
- Assessments and Quizzes after each module to track progress
- Capstone Project involving a full-cycle intrusion detection and analysis exercise

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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