Training Course on Network Deception and Honeypot Forensics

Professional Development Training Course Outline

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

Course Introduction

In today's ever-evolving cybersecurity landscape, proactive threat intelligence and detection mechanisms are critical. Training Course on Network Deception and Honeypot Forensics is designed to equip cybersecurity professionals with the knowledge and hands-on skills needed to deploy, manage, and analyze honeypot environments for detecting and investigating sophisticated cyber threats. With the surge in ransomware, APTs, and insider threats, organizations must go beyond traditional firewalls and adopt innovative deception strategies to stay ahead of attackers. This course blends advanced concepts in cyber deception, threat hunting, and forensic analysis, empowering participants to uncover malicious tactics, techniques, and procedures (TTPs) before they escalate.

Utilizing cutting-edge tools and real-world case studies, participants will learn how to configure, monitor, and extract digital evidence from honeypot systems. Whether defending enterprise networks or researching threat actor behavior, this course delivers actionable insights into adversary emulation, false asset generation, and network infiltration analysis. Professionals will gain in-demand expertise on deploying deception grids, conducting post-compromise forensics, and using threat intelligence feeds to enhance response efforts.

Programme Curriculum

Training Course on Network Deception and Honeypot Forensics

Introduction

In today's ever-evolving cybersecurity landscape, proactive threat intelligence and detection mechanisms are critical. Training Course on Network Deception and Honeypot Forensics is designed to equip cybersecurity professionals with the knowledge and hands-on skills needed to deploy, manage, and analyze honeypot environments for detecting and investigating sophisticated cyber threats. With the surge in ransomware, APTs, and insider threats, organizations must go beyond traditional firewalls and adopt innovative deception strategies to stay ahead of attackers. This course blends advanced concepts in cyber deception, threat hunting, and forensic analysis, empowering participants to uncover malicious

tactics, techniques, and procedures (TTPs) before they escalate.

Utilizing cutting-edge tools and real-world case studies, participants will learn how to configure, monitor, and extract digital evidence from honeypot systems. Whether defending enterprise networks or researching threat actor behavior, this course delivers actionable insights into adversary emulation, false asset generation, and network infiltration analysis. Professionals will gain in-demand expertise on deploying deception grids, conducting post-compromise forensics, and using threat intelligence feeds to enhance response efforts.

Course Objectives

By the end of this course, participants will be able to:

1. Design and implement interactive honeypots for enterprise environments.
2. Analyze attack vectors captured via honeypot infrastructure.
3. Deploy deception-based defense systems to detect lateral movement.
4. Integrate honeypots with SIEM and SOAR platforms for threat visibility.
5. Investigate attacker behavior using packet capture and log forensics.
6. Use threat intelligence to correlate honeypot data with known IOCs.
7. Develop deception playbooks to simulate attack surfaces.
8. Perform forensic triage of compromised honeypot environments.
9. Understand legal, ethical, and privacy issues in cyber deception.
10. Mitigate false positives while enhancing detection accuracy.
11. Apply AI/ML tools for behavioral anomaly detection in honeypot data.
12. Build low-interaction and high-interaction honeypots using open-source tools.
13. Craft deception layers across IT, OT, and IoT infrastructures.

Target Audiences

1. Cybersecurity Analysts
2. Threat Intelligence Professionals
3. Network Security Engineers
4. Digital Forensics Experts
5. Incident Response Teams
6. Penetration Testers
7. Cybersecurity Researchers
8. SOC Analysts

Course Duration: 5 days

Course Modules

Module 1: Introduction to Network Deception & Honeypots

- Understanding deception technology in cybersecurity
- History and evolution of honeypots
- Use cases of deception in modern networks
- Types of honeypots: Low, Medium, High interaction
- Threat landscape overview and deception benefits
- **Case Study**: Tracking a ransomware operator using a high-interaction honeypot

Module 2: Honeypot Architectures and Deployment Models

- Choosing the right honeypot for your network
- Open-source honeypot tools and frameworks
- Cloud-based vs on-premise honeypot deployment

- Integration with firewalls and intrusion detection systems
- Risk mitigation and security considerations
- **Case Study**: AWS honeypot trap for crypto mining attacks

Module 3: Data Collection and Analysis from Honeypots

- Capturing and parsing honeypot logs
- Deep packet inspection (DPI) techniques
- Visualizing attacker behaviors
- Forensic timeline reconstruction
- Using ELK Stack for honeypot log analysis
- **Case Study**: Detecting brute force attacks using Cowrie honeypot

Module 4: Forensic Investigation of Honeypot Breaches

- Preserving integrity of digital evidence
- Chain of custody and metadata validation
- Disk imaging and memory analysis tools
- Malware sandboxing and reverse engineering
- Extracting IOCs from honeypot breaches
- **Case Study**: Reverse engineering a credential-stealing malware

Module 5: Threat Intelligence Integration

- Leveraging honeypots for threat intelligence gathering
- IOC sharing and enrichment platforms (MISP, STIX/TAXII)
- Enabling real-time alerts via threat feeds
- Tagging TTPs to MITRE ATT&CK
- Operationalizing TI with deception outputs
- **Case Study**: Dark web correlation of honeypot-captured indicators

Module 6: Advanced Deception Strategies and AI Integration

- Creating believable decoys and breadcrumbs
- Behavioral analysis with machine learning
- Generating deception zones with automation
- Deception orchestration and playbooks
- Red team vs blue team simulations
- **Case Study**: AI-based threat detection using honeypot telemetry

Module 7: Legal, Ethical, and Policy Considerations

- Jurisdictional implications of deploying honeypots
- Privacy laws and data protection
- Ethical dilemmas in deception operations
- Evidence admissibility in court
- Best practices for responsible honeypot use
- **Case Study**: Legal implications of an entrapment accusation

Module 8: Capstone Project & Real-World Simulation

- End-to-end honeypot deployment
- Threat emulation scenario creation
- Full forensic chain documentation
- Analysis report preparation and presentation
- Peer review and feedback loop

- **Case Study**: Simulated insider threat investigation using honeypot artifacts

Training Methodology

- Instructor-led interactive lectures
- Hands-on labs with real-world attack simulation
- Group case study analysis
- Role-playing and adversary emulation exercises
- Practical assessments and capstone project

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	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 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