Training Course on Investigating DDoS Attacks and Mitigation

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 hyperconnected digital ecosystem, Distributed Denial-of-Service (DDoS) attacks pose one of the most serious threats to enterprise networks, public services, and online platforms. With attack methods becoming increasingly sophisticated—ranging from volumetric assaults to application-layer floods—cybersecurity professionals must be equipped with deep technical insights and investigative capabilities. Training Course on Investigating DDoS Attacks and Mitigation is designed to empower cybersecurity teams, digital forensic analysts, and network engineers with advanced tools, strategies, and methodologies for identifying, analyzing, and neutralizing DDoS threats across hybrid and cloud-based environments.

The course provides hands-on practical training in DDoS forensics, traffic pattern analysis, anomaly detection, cloud-based mitigation strategies, and incident response planning. Through interactive labs, real-world case studies, and threat simulation exercises, participants will gain critical skills in cyber defense, traffic filtering, and automated response systems. Learners will explore the full cycle of DDoS investigations—from attack identification to forensic reporting, ensuring organizational resilience and compliance with industry standards such as NIST, ISO 27001, and GDPR.

Programme Curriculum

Training Course on Investigating DDoS Attacks and Mitigation

Course Introduction

In today’s hyperconnected digital ecosystem, Distributed Denial-of-Service (DDoS) attacks pose one of the most serious threats to enterprise networks, public services, and online platforms. With attack methods becoming increasingly sophisticated—ranging from volumetric assaults to application-layer floods—cybersecurity professionals must be equipped with deep technical insights and investigative capabilities. Training Course on Investigating DDoS Attacks and Mitigation is designed to empower cybersecurity teams, digital forensic analysts, and network engineers with advanced tools, strategies, and methodologies for identifying, analyzing, and neutralizing DDoS threats across hybrid and cloud-based

environments.

The course provides hands-on practical training in DDoS forensics, traffic pattern analysis, anomaly detection, cloud-based mitigation strategies, and incident response planning. Through interactive labs, real-world case studies, and threat simulation exercises, participants will gain critical skills in cyber defense, traffic filtering, and automated response systems. Learners will explore the full cycle of DDoS investigations—from attack identification to forensic reporting, ensuring organizational resilience and compliance with industry standards such as NIST, ISO 27001, and GDPR.

Course Objectives

1. Understand the core types of DDoS attacks and their operational mechanics.
2. Identify and capture network traffic anomalies using packet sniffing and flow monitoring.
3. Perform in-depth DDoS forensics and reverse engineering of attack signatures.
4. Utilize SIEM tools and threat intelligence feeds for real-time attack correlation.
5. Implement cloud-native DDoS mitigation platforms (e.g., AWS Shield, Cloudflare).
6. Apply AI and machine learning in DDoS detection and prediction.
7. Build incident response playbooks for DDoS scenarios.
8. Harden network infrastructure with firewall, router, and CDN configurations.
9. Analyze attack vectors from botnets, IoT devices, and spoofed IP sources.
10. Assess the financial and operational impact of DDoS attacks on organizations.
11. Use threat hunting techniques to uncover persistent DDoS campaigns.
12. Conduct post-mortem attack reconstruction and legal documentation.
13. Integrate zero trust architecture for enhanced DDoS resilience.

Target Audiences

1. Cybersecurity Professionals
2. Network Security Engineers
3. Digital Forensic Analysts
4. System Administrators
5. IT Managers
6. Incident Response Teams
7. Cloud Security Architects
8. Law Enforcement and Government Cyber Units

Course Duration: 10 days

Course Modules

Module 1: Introduction to DDoS Attacks

- Understanding DDoS fundamentals
- Historical evolution of DDoS attacks
- Key terms: flood, amplification, reflection
- DDoS attack life cycle
- Real-time impact on critical systems
- **Case Study:** Mirai Botnet Attack on DynDNS

Module 2: Traffic Pattern Analysis

- Deep packet inspection (DPI)
- Flow-based traffic analytics (NetFlow, sFlow)
- Signature vs anomaly-based detection
- Identifying spoofed IP traffic
- Building custom traffic rules

- **Case Study:** GitHub DDoS Attack (1.35 Tbps)

Module 3: DDoS Forensics

- Packet capture and preservation (PCAP)
- Chain of custody and digital evidence
- Time-based traffic correlation
- Payload analysis techniques
- Data sanitization and reporting
- **Case Study:** Cloudflare's Forensic Breakdown

Module 4: Types of DDoS Attacks

- Volumetric attacks (UDP floods)
- Protocol attacks (SYN flood, Ping of Death)
- Application layer attacks (Slowloris)
- Hybrid attack mechanisms
- Advanced persistent DDoS threats (APDoS)
- **Case Study:** AWS Cloud-Based Attack Vector

Module 5: Botnet Investigation

- Understanding botnet architecture
- Identifying command and control (C2) servers
- Botnet takedown methods
- Tracing infection paths
- Tools for botnet tracking (Maltego, Wireshark)
- **Case Study:** Avalanche Botnet Disruption

Module 6: Using SIEM for Detection

- Log correlation with Splunk/ELK
- Alert configuration and tuning
- Integrating external threat feeds
- Dashboards and visualizations
- Compliance-based reporting
- **Case Study:** Detection via Azure Sentinel

Module 7: AI in DDoS Detection

- AI-based anomaly detection models
- Training datasets and labeled traffic
- Reducing false positives
- Predictive modeling with ML algorithms
- Deployment challenges in live environments
- **Case Study:** ML Use in Akamai Defense Systems

Module 8: Cloud Mitigation Strategies

- Configuring AWS Shield/Cloudflare
- Traffic rerouting with Anycast
- Leveraging CDN caching
- Auto-scaling for traffic absorption
- Security automation in the cloud
- **Case Study:** Netflix’s Cloud Resilience Model

Module 9: On-Premise Infrastructure Hardening

- Router/firewall ACL configuration
- Rate limiting and blackhole routing
- IDS/IPS configuration
- BGP community setup for upstream filtering
- Redundancy and failover design
- **Case Study:** Bank DDoS Mitigation via Cisco ASA

Module 10: Incident Response Planning

- Crafting a DDoS-specific response plan
- Role assignments and response timelines
- Communication protocols (internal/external)
- Collaboration with ISPs and CERTs
- Post-incident reporting
- **Case Study:** Azure DDoS Protection Response Flow

Module 11: Legal and Regulatory Considerations

- Data privacy laws in cyber investigations
- Evidentiary standards in court
- GDPR, HIPAA, and NIST compliance
- Cross-border attack handling
- Reporting obligations to authorities
- **Case Study:** Legal Response to Estonia 2007 Attacks

Module 12: Threat Hunting for DDoS

- Indicators of compromise (IOCs)
- Behavioral analytics
- Automation with scripts and APIs
- Threat actor attribution
- Reconnaissance and pre-attack clues
- **Case Study:** Threat Hunt on Dark Web DDoS Offers

Module 13: Post-Attack Analysis

- Root cause analysis
- Recovery metrics and lessons learned
- Updating risk registers
- Refining mitigation plans
- Team debriefing and retraining
- **Case Study:** UK NHS DDoS Post-Incident Report

Module 14: Simulation & Red Teaming

- Setting up attack simulations
- Load testing tools (LOIC, Hping)
- Evaluating organizational readiness
- Monitoring and response testing
- Red vs. Blue team roles
- **Case Study:** Simulated Attack on Financial Institution

Module 15: Building Resilient Architecture

- Network segmentation
- Load balancing and failover

- Distributed traffic management
- Multi-region service deployment
- Integration with Zero Trust principles
- **Case Study:** Google's BeyondCorp Infrastructure

Training Methodology

- Instructor-led virtual sessions with real-time Q&A
- Hands-on labs with traffic analysis and attack simulation
- Group-based case study evaluations and team tasks
- Interactive dashboards and data analysis exercises
- Pre- and post-assessments to track learning outcomes
- Downloadable toolkits, cheat sheets, and configuration guides

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

Start Date	End Date	Location	Price
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

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

Register Online Now

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