Training Course on Investigating DNS and Domain Name System Attacks

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 rapidly evolving cyber threat landscape, the Domain Name System (DNS) has become a prime target for sophisticated cyberattacks. Cybercriminals exploit DNS vulnerabilities to execute attacks such as DNS tunneling, cache poisoning, hijacking, and amplification. Training Course on Investigating DNS and Domain Name System Attacks equips cybersecurity professionals, forensic investigators, and IT security teams with the latest tools and techniques for identifying, analyzing, and mitigating DNS-based threats. With a focus on real-world attack vectors and forensic best practices, participants will gain hands-on experience and expert insights necessary for responding to DNS abuse in enterprise and cloud environments.

This course emphasizes threat intelligence, packet analysis, DNS logs, and anomaly detection to trace DNS misuse effectively. Leveraging SEO-focused cybersecurity tools and cutting-edge analytics, this training covers everything from DNS architecture to advanced incident response strategies. Whether you're defending against cyber espionage or managing enterprise DNS security policies, this program is designed to future-proof your DNS investigation capabilities using up-to-date methodologies, threat modeling, and scenario-based case studies.

Programme Curriculum

Training Course on Investigating DNS and Domain Name System Attacks

Introduction

In today’s rapidly evolving cyber threat landscape, the Domain Name System (DNS) has become a prime target for sophisticated cyberattacks. Cybercriminals exploit DNS vulnerabilities to execute attacks such as DNS tunneling, cache poisoning, hijacking, and amplification. Training Course on Investigating DNS and Domain Name System Attacks equips cybersecurity professionals, forensic investigators, and IT security teams with the latest tools and techniques for identifying, analyzing, and mitigating DNS-based threats. With a focus on real-world attack vectors and forensic best practices, participants will gain hands-on experience and expert insights necessary for responding to DNS abuse in

enterprise and cloud environments.

This course emphasizes threat intelligence, packet analysis, DNS logs, and anomaly detection to trace DNS misuse effectively. Leveraging SEO-focused cybersecurity tools and cutting-edge analytics, this training covers everything from DNS architecture to advanced incident response strategies. Whether you're defending against cyber espionage or managing enterprise DNS security policies, this program is designed to future-proof your DNS investigation capabilities using up-to-date methodologies, threat modeling, and scenario-based case studies.

Course Objectives

Participants will be able to:

1. Understand DNS infrastructure and its critical role in internet communication.
2. Identify and classify various DNS attack types, including DNS amplification and cache poisoning.
3. Utilize DNS logging and monitoring tools for forensic investigation.
4. Apply DNSSEC and advanced authentication protocols to secure DNS traffic.
5. Investigate DNS tunneling techniques used for data exfiltration.
6. Conduct threat hunting using DNS packet capture (PCAP) files.
7. Implement DNS filtering and response policies in enterprise networks.
8. Perform forensic analysis on malicious domains using threat intelligence platforms.
9. Analyze DNS hijacking and redirection attacks with real-world data sets.
10. Use cloud-native DNS logs from providers like AWS Route 53 and Azure DNS for cloud forensics.
11. Deploy open-source and commercial DNS forensic tools (e.g., Zeek, Splunk, Wireshark).
12. Develop and document DNS incident response and mitigation strategies.
13. Interpret domain reputation data and WHOIS records to identify malicious infrastructure.

Target Audiences

1. Cybersecurity Analysts
2. Digital Forensics Investigators
3. Incident Response Teams
4. Network Security Engineers
5. Cloud Security Specialists
6. IT Security Managers
7. Penetration Testers
8. Government and Law Enforcement Cyber Units

Course Duration: 5 days

Course Modules

Module 1: DNS Fundamentals and Attack Surfaces

- Understanding DNS architecture and protocols
- Common DNS vulnerabilities
- DNS amplification and reflection attack mechanics
- DNS over HTTPS (DoH) vs traditional DNS
- Identifying attack surface in DNS environments
- **Case Study**: Amplification attack on a financial services DNS server

Module 2: DNS Tunneling and Exfiltration Analysis

- What is DNS tunneling and how it works
- Detecting tunneling through behavior analysis
- Tools for analyzing DNS exfiltration

- Threat actor profiles using DNS tunnels
- Real-world tunneling malware indicators
- **Case Study**: Malware using DNS tunneling to bypass perimeter firewalls

Module 3: DNS Hijacking and Redirection Threats

- Mechanisms of DNS hijacking
- Detecting unauthorized DNS changes
- Securing registrar accounts and WHOIS data
- DNS redirection and fake landing page analysis
- Correlating hijacks with phishing attacks
- **Case Study**: Telecom provider compromised via DNS hijack

Module 4: DNS Log Analysis and Threat Hunting

- Configuring DNS logging (BIND, Unbound, Windows DNS)
- Aggregating and filtering logs with SIEM tools
- Identifying anomalies in DNS traffic
- Pivoting from DNS logs to endpoint forensics
- Automating threat hunting with DNS indicators
- **Case Study**: Investigating suspicious domain resolution patterns using Zeek

Module 5: Domain Intelligence and Threat Attribution

- Using WHOIS, Passive DNS, and domain age tools
- Mapping threat actor infrastructure
- Investigating registrars and hosting providers
- Enriching DNS data with external threat feeds
- Domain clustering and TTPs correlation
- **Case Study**: Attribution of phishing campaign using domain pivoting

Module 6: DNS Security Enhancements and DNSSEC

- Enabling DNSSEC validation
- Managing DNSSEC key lifecycles
- DNS sinkholing and RPZ deployment
- Cloud-based DNS security solutions
- Measuring DNS security posture
- **Case Study**: DNSSEC deployment in a government agency

Module 7: Cloud DNS Forensics (AWS, Azure, GCP)

- DNS service logging in cloud platforms
- Detecting malicious DNS in serverless environments
- Integrating cloud-native tools with forensics workflows
- Cross-referencing DNS and flow logs
- Investigating DNS abuse in multi-cloud architectures
- **Case Study**: DNS reconnaissance in AWS leading to lateral movement

Module 8: Incident Response and Reporting

- Building a DNS incident response plan
- Post-incident DNS configuration hardening
- Legal and compliance considerations in DNS investigations
- Documenting DNS-based attack findings
- Reporting formats for technical and executive teams

- **Case Study**: Full lifecycle analysis of DNS attack response in a healthcare firm

Training Methodology

- Hands-on Labs using live DNS traffic captures
- Simulated attack scenarios with DNS analysis
- Interactive sessions with case-based learning
- Tool walkthroughs (Wireshark, Zeek, Splunk, SecurityTrails, etc.)
- Collaborative exercises and guided threat hunting
- Quizzes and group activities to reinforce learning

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

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
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