Training Course on Understanding Exploit Kits and Exploit 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 the ever-evolving landscape of cyber threats, Exploit Kits remain one of the most powerful tools in a threat actor’s arsenal. These toolkits automate the exploitation of known vulnerabilities, especially in browsers and plugins, to deliver malware payloads without user interaction. As organizations enhance their threat intelligence and incident response capabilities, it’s imperative for cybersecurity professionals to gain an in-depth understanding of Exploit Kit architectures, vulnerability exploitation chains, and exploit delivery mechanisms. Training Course on Understanding Exploit Kits and Exploit Analysis is designed to equip participants with the expertise to detect, analyze, and mitigate risks associated with exploit kits across multiple environments.

With hands-on labs and real-world malware analysis scenarios, learners will dissect popular exploit kits like Rig, Magnitude, and Fallout, exploring their evolution, obfuscation techniques, and payload strategies. The training integrates the latest industry techniques in reverse engineering, sandboxing, dynamic analysis, and exploit lifecycle management—crucial skills for digital forensics investigators, SOC analysts, and penetration testers. Whether you're defending enterprise networks or conducting forensic investigations, this course will deepen your knowledge of how cybercriminals weaponize vulnerabilities for gain.

Programme Curriculum

Training Course on Understanding Exploit Kits and Exploit Analysis

Introduction

In the ever-evolving landscape of cyber threats, Exploit Kits remain one of the most powerful tools in a threat actor’s arsenal. These toolkits automate the exploitation of known vulnerabilities, especially in browsers and plugins, to deliver malware payloads without user interaction. As organizations enhance their threat intelligence and incident response capabilities, it’s imperative for cybersecurity professionals to gain an in-depth understanding of Exploit Kit architectures, vulnerability exploitation chains, and exploit delivery mechanisms. Training Course on Understanding Exploit Kits and

Exploit Analysis is designed to equip participants with the expertise to detect, analyze, and mitigate risks associated with exploit kits across multiple environments.

With hands-on labs and real-world malware analysis scenarios, learners will dissect popular exploit kits like Rig, Magnitude, and Fallout, exploring their evolution, obfuscation techniques, and payload strategies. The training integrates the latest industry techniques in reverse engineering, sandboxing, dynamic analysis, and exploit lifecycle management—crucial skills for digital forensics investigators, SOC analysts, and penetration testers. Whether you're defending enterprise networks or conducting forensic investigations, this course will deepen your knowledge of how cybercriminals weaponize vulnerabilities for gain.

Course Objectives

1. Understand the evolution and purpose of exploit kits in modern cybercrime.
2. Analyze the components and inner workings of exploit kit frameworks.
3. Recognize obfuscation and evasion techniques used by modern kits.
4. Perform manual and automated exploit kit traffic analysis.
5. Apply threat hunting techniques to detect active exploit kit campaigns.
6. Conduct dynamic and static analysis on delivered malware payloads.
7. Reverse-engineer exploit kits to understand their exploit chains.
8. Analyze exploit delivery mechanisms via drive-by downloads.
9. Map exploit kits to MITRE ATT&CK techniques and tactics.
10. Identify common vulnerabilities exploited by top kits.
11. Use browser forensics to trace infection chains.
12. Integrate exploit kit IOCs into SIEM tools and EDR solutions.
13. Develop actionable mitigation strategies and hardening measures.

Target Audience

1. Security Operations Center (SOC) Analysts
2. Digital Forensics & Incident Response (DFIR) Professionals
3. Penetration Testers & Ethical Hackers
4. Malware Analysts & Threat Researchers
5. Cybersecurity Consultants
6. Security Architects & Risk Managers
7. Law Enforcement Cybercrime Units
8. IT Security Professionals in Government & Private Sector

Course Duration: 10 days

Course Modules

Module 1: Introduction to Exploit Kits

- Definition and purpose of exploit kits
- Historical evolution of popular kits
- Differences between exploit kits and malware droppers
- Role of exploit kits in cybercrime ecosystems
- Overview of recent global trends
- **Case Study:** Rig Exploit Kit in Malvertising Campaign

Module 2: Anatomy of an Exploit Kit

- Core components of exploit kits
- Landing pages and redirection techniques
- Exploit selection and matching engines

- Payload delivery and execution
- Hosting infrastructure and obfuscation
- **Case Study:** Magnitude EK's JavaScript Obfuscation

Module 3: Exploit Delivery Mechanisms

- Drive-by download process
- Malvertising and compromised websites
- Exploiting browser and plugin vulnerabilities
- Delivery via social engineering and phishing
- Fileless exploitation techniques
- **Case Study:** Fallout EK in Browser Exploitation

Module 4: Exploitation Techniques and Vulnerabilities

- Zero-day vs known vulnerabilities
- Common CVEs targeted by exploit kits
- Heap spraying and use-after-free vulnerabilities
- Browser-specific exploit chains
- Windows Kernel and ActiveX exploits
- **Case Study:** CVE-2021-26411 in Internet Explorer Exploit

Module 5: Obfuscation and Anti-Analysis Techniques

- JavaScript and shellcode obfuscation
- Encryption and polymorphism in exploit kits
- Evasion of sandboxes and VMs
- Traffic encryption with SSL/TLS
- Server-side payload hiding
- **Case Study:** Neutrino EK’s Anti-Sandbox Tactics

Module 6: Static and Dynamic Analysis of Exploit Kits

- Tools for static analysis (e.g., IDA Pro, Ghidra)
- Dynamic analysis environments (e.g., Cuckoo Sandbox)
- Memory forensics for dropped payloads
- String and network traffic analysis
- Using Wireshark and Fiddler for EK traffic
- **Case Study:** Sandbox Analysis of Angler EK

Module 7: Reverse Engineering Exploits

- Reverse engineering JavaScript and shellcode
- Deobfuscation techniques for landing pages
- Understanding return-oriented programming (ROP)
- Analyzing loader functions and shellcode execution
- Extracting exploit chains and payloads
- **Case Study:** Reverse Engineering Sundown EK Payload

Module 8: Exploit Kits and the MITRE ATT&CK Framework

- Mapping TTPs to MITRE ATT&CK
- Using ATT&CK for detection engineering
- Integrating ATT&CK into threat models
- Identifying persistence and lateral movement techniques
- Reporting and documentation best practices

- **Case Study:** Mapping Fallout EK to MITRE Framework

Module 9: Exploit Kit Detection and Threat Hunting

- Indicators of compromise (IOCs) for EK detection
- YARA rules and signature development
- Threat intelligence platforms and feeds
- Heuristics and behavioral detection
- Building hypothesis-driven threat hunts
- **Case Study:** EK Detection in a Financial Organization

Module 10: Incident Response to Exploit Kit Infections

- First response and isolation procedures
- Log collection and timeline analysis
- Post-exploitation detection
- Communication and containment strategies
- Reporting and lessons learned
- **Case Study:** Responding to an Angler EK Breach

Module 11: Exploit Kit Forensics

- Forensic imaging and browser artifact analysis
- Analyzing system memory and registry changes
- Network traffic correlation
- File system and persistence mechanism examination
- Artifact correlation with known EK behaviors
- **Case Study:** Digital Forensics on Magnitude EK Infection

Module 12: Malware Payloads in Exploit Kits

- Common malware delivered via EKs (e.g., ransomware, trojans)
- Payload encryption and unpacking
- Command and control (C2) behavior analysis
- Payload persistence strategies
- Real-world malware trends via EKs
- **Case Study:** GandCrab Ransomware via GrandSoft EK

Module 13: Exploit Kit Lifecycle and Infrastructure

- Stages of EK deployment and monetization
- Bulletproof hosting and criminal marketplaces
- Affiliate models and exploit-as-a-service (EaaS)
- Infrastructure takedowns and attribution
- EK-as-a-Service lifecycle analysis
- **Case Study:** Takedown of Blackhole EK

Module 14: Mitigation and Prevention Strategies

- Patch management and endpoint hardening
- Browser and plugin security controls
- Network segmentation and DNS filtering
- User education and awareness
- Exploit prevention tools (e.g., EMET, Defender Exploit Guard)
- **Case Study:** Organizational Defense Against Rig EK

Module 15: Future Trends and Threat Landscape

- Decline of EKs and rise of other vectors
- Exploit kits in mobile and IoT platforms
- Emerging exploit automation in AI
- Trends in vulnerability markets
- The role of threat intel in future EK detection
- **Case Study:** Emerging Exploit Kit in IoT Malware Campaign

Training Methodology

- Instructor-led interactive sessions
- Hands-on labs with real malware samples
- Group-based exploit chain analysis workshops
- Live demonstrations of tools and techniques
- Capstone project on analyzing an active exploit kit campaign

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	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

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

Register Online Now

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