Training Course on Analyzing Rootkits and Bootkits

Professional Development Training Course Outline

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

Course Introduction

Rootkits and bootkits represent some of the most advanced and stealthiest forms of cyber threats targeting operating systems, firmware, and boot processes. These malware variants are designed to gain persistent, unauthorized access and control while evading detection by traditional security solutions. With the increasing sophistication of Advanced Persistent Threats (APTs), nation-state actors, and cybercriminals, understanding the internal workings of rootkits and bootkits is essential for cybersecurity professionals. Training Course on Analyzing Rootkits and Bootkits offers hands-on training in detecting, dissecting, and mitigating these threats using real-world tools and forensic techniques, aligning with today's cybersecurity trends and compliance requirements.

In this intensive training course, participants will engage in deep system analysis, kernel debugging, and reverse engineering techniques. The curriculum emphasizes memory forensics, BIOS/UEFI compromise detection, bootloader inspection, and live system incident response. The training aligns with cybersecurity frameworks such as NIST, MITRE ATT&CK, and ISO/IEC 27001, enabling participants to develop the expertise needed to defend enterprise infrastructure against rootkit and bootkit infections. Ideal for digital forensic analysts, incident responders, and SOC teams, the course bridges theoretical concepts with practical experience through case studies, labs, and real-world simulations.

Programme Curriculum

Training Course on Analyzing Rootkits and Bootkits

Introduction

Rootkits and bootkits represent some of the most advanced and stealthiest forms of cyber threats targeting operating systems, firmware, and boot processes. These malware variants are designed to gain persistent, unauthorized access and control while evading detection by traditional security solutions. With the increasing sophistication of Advanced Persistent Threats (APTs), nation-state actors, and cybercriminals, understanding the internal workings of rootkits and bootkits is

essential for cybersecurity professionals. Training Course on Analyzing Rootkits and Bootkits offers hands-on training in detecting, dissecting, and mitigating these threats using real-world tools and forensic techniques, aligning with today's cybersecurity trends and compliance requirements.

In this intensive training course, participants will engage in deep system analysis, kernel debugging, and reverse engineering techniques. The curriculum emphasizes memory forensics, BIOS/UEFI compromise detection, bootloader inspection, and live system incident response. The training aligns with cybersecurity frameworks such as NIST, MITRE ATT&CK, and ISO/IEC 27001, enabling participants to develop the expertise needed to defend enterprise infrastructure against rootkit and bootkit infections. Ideal for digital forensic analysts, incident responders, and SOC teams, the course bridges theoretical concepts with practical experience through case studies, labs, and real-world simulations.

Course Objectives

1. Understand the lifecycle and types of rootkits and bootkits.
2. Identify persistent threats and stealth malware signatures.
3. Perform memory forensics using Volatility and Rekall.
4. Analyze kernel-level hooks and driver manipulation techniques.
5. Detect UEFI/BIOS compromise and boot-level tampering.
6. Use reverse engineering tools for malware analysis.
7. Employ dynamic analysis and sandboxing methods.
8. Investigate user-mode and kernel-mode rootkits.
9. Map malware behavior to MITRE ATT&CK framework.
10. Simulate advanced persistent threat (APT) attacks.
11. Conduct forensic triage on compromised systems.
12. Apply threat hunting strategies for rootkit detection.
13. Develop incident response plans for malware persistence.

Target Audiences

1. Cybersecurity Analysts
2. Digital Forensic Experts
3. Malware Researchers
4. Incident Response Teams
5. SOC Analysts
6. System Administrators
7. Reverse Engineers
8. Penetration Testers

Course Duration: 5 days

Course Modules

Module 1: Introduction to Rootkits and Bootkits

- History and evolution of rootkits/bootkits
- Types: User-mode, Kernel-mode, Firmware-based
- Attack vectors and payload delivery
- Detection challenges and evasion tactics
- Overview of modern threats
- **Case Study:** Analysis of Stuxnet's stealth component

Module 2: Rootkit Installation and Persistence Mechanisms

- Process injection and DLL hijacking
- Registry modification techniques

- Scheduled tasks and service manipulation
- Bootkit persistence via MBR/VBR
- Rootkit behavior during system boot
- **Case Study:** ZeroAccess rootkit infection analysis

Module 3: Memory Forensics & Rootkit Detection

- RAM acquisition tools and techniques
- Using Volatility/Rekall for memory analysis
- Identifying hidden processes and hooks
- Signature vs heuristic detection
- Anomaly-based memory scanning
- **Case Study:** Detecting a hidden rootkit using Volatility

Module 4: Reverse Engineering Malware Components

- Intro to IDA Pro, Ghidra, and x64dbg
- Analyzing PE file structure
- Recognizing anti-analysis techniques
- Disassembly and static code analysis
- Decoding encrypted payloads
- **Case Study:** Reversing a polymorphic kernel rootkit

Module 5: Bootkits and Firmware-Level Threats

- Anatomy of a boot process
- BIOS/UEFI exploitation techniques
- Bootloader malware detection
- Secure Boot and measured boot bypass
- UEFI rootkits: detection and remediation
- **Case Study:** Analysis of the LoJax bootkit

Module 6: Kernel Debugging and Driver Analysis

- Setting up WinDbg and kernel debugging
- Analyzing suspicious drivers
- Hooking and rootkit behavior analysis
- Driver signing and verification
- API tracing and syscall monitoring
- **Case Study:** Uncovering kernel hooks in a rogue driver

Module 7: Threat Hunting and Advanced Detection Techniques

- Building YARA rules for rootkits
- Hunting using memory and disk artifacts
- Leveraging MITRE ATT&CK for detection mapping
- Behavior-based detection strategies
- SIEM and EDR integration
- **Case Study:** Threat hunting a custom rootkit in enterprise logs

Module 8: Incident Response and Mitigation Strategies

- Live incident handling procedures
- Rootkit removal tools and scripts
- Building a remediation playbook
- Chain of custody and forensic reporting

- Communication with stakeholders
- **Case Study:** Rootkit remediation in a compromised banking network

Training Methodology

- Hands-on labs using virtual machines and infected images
- Live demonstrations of malware analysis
- Group-based practical scenarios
- Real-world case studies and simulations
- Assessment quizzes and skill evaluations

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