Training Course on Anti-Reverse Engineering Techniques and Countermeasures

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 an era where cyber threats evolve daily, protecting software applications and systems against reverse engineering has become a top priority. Training Course on Anti-Reverse Engineering Techniques and Countermeasures is meticulously designed to equip cybersecurity professionals, developers, and digital defenders with cutting-edge knowledge and hands-on skills. This course empowers participants to detect, prevent, and mitigate reverse engineering attempts that expose critical intellectual property, sensitive data, and proprietary algorithms. With real-world case studies and trending threat intelligence, this course ensures learners are always a step ahead in fortifying their digital assets.

Combining both theoretical foundations and practical countermeasure implementations, this course emphasizes modern obfuscation methods, software hardening, anti-debugging strategies, code virtualization, and cryptographic protection techniques. Participants will gain a comprehensive understanding of attacker tactics and how to deploy robust defenses using automation, AI-assisted detection tools, and advanced runtime protection. The course concludes with a capstone project involving a real-world simulation of reverse engineering prevention, ensuring participants walk away industry-ready.

Programme Curriculum

Training Course on Anti-Reverse Engineering Techniques and Countermeasures

Introduction

In an era where cyber threats evolve daily, protecting software applications and systems against reverse engineering has become a top priority. Training Course on Anti-Reverse Engineering Techniques and Countermeasures is meticulously designed to equip cybersecurity professionals, developers, and digital defenders with cutting-edge knowledge and hands-on skills. This course empowers participants to detect, prevent, and mitigate reverse engineering attempts that expose critical intellectual property, sensitive data, and proprietary algorithms. With real-world case studies and trending threat

intelligence, this course ensures learners are always a step ahead in fortifying their digital assets.

Combining both theoretical foundations and practical countermeasure implementations, this course emphasizes modern obfuscation methods, software hardening, anti-debugging strategies, code virtualization, and cryptographic protection techniques. Participants will gain a comprehensive understanding of attacker tactics and how to deploy robust defenses using automation, AI-assisted detection tools, and advanced runtime protection. The course concludes with a capstone project involving a real-world simulation of reverse engineering prevention, ensuring participants walk away industry-ready.

Course Objectives

1. Understand the fundamentals of reverse engineering and its impact on cybersecurity.
2. Analyze common tools and techniques used by reverse engineers.
3. Apply binary obfuscation and code encryption to deter reverse engineering.
4. Implement dynamic and static anti-debugging mechanisms.
5. Utilize anti-tamper methods to safeguard application integrity.
6. Learn software watermarking for intellectual property protection.
7. Deploy software virtualization techniques to complicate code analysis.
8. Identify vulnerabilities exploitable through disassemblers and debuggers.
9. Secure mobile and embedded applications against reverse engineering.
10. Leverage AI and ML in reverse engineering detection and defense.
11. Conduct penetration testing focusing on reverse engineering scenarios.
12. Build customized countermeasure workflows using DevSecOps pipelines.
13. Develop incident response strategies for reverse engineering breaches.

Target Audience

1. Cybersecurity Professionals
2. Malware Analysts
3. Software Developers
4. DevSecOps Engineers
5. Threat Intelligence Analysts
6. Security Researchers
7. Mobile App Developers
8. Government and Defense Cyber Units

Course Duration: 10 days

Course Modules

Module 1: Introduction to Reverse Engineering

- Definition and scope of reverse engineering
- Legal and ethical implications
- Overview of common RE tools (IDA Pro, Ghidra)
- Case: Sony DRM vs. RE community
- Static vs. dynamic analysis
- **Case Study**: Fallout of WinRAR vulnerability exploitation

Module 2: Threat Landscape and Attack Vectors

- Common entry points for reverse engineers
- Nation-state vs. cybercriminal tactics
- RE in the software piracy ecosystem
- Anti-analysis environment detection

- Role of AI in modern reverse engineering
- **Case Study**: Pegasus spyware dissection

Module 3: Binary Obfuscation Techniques

- Control flow flattening
- Instruction substitution
- String encryption and decoding
- Dummy code injection
- Polymorphic and metamorphic code
- **Case Study**: ConfuserEx .NET obfuscator in practice

Module 4: Anti-Debugging Mechanisms

- API-based detection (IsDebuggerPresent, NtQueryInformationProcess)
- Timing checks and breakpoints
- Exception-based anti-debugging
- Anti-VM techniques
- Environment fingerprinting
- **Case Study**: TrickBot malware's anti-debug methods

Module 5: Code Virtualization and Obfuscation

- What is code virtualization
- Using VMProtect and Themida
- Creating virtual machines for opcode interpretation
- Limits and strengths of virtualization
- Performance and compatibility considerations
- **Case Study**: Software license protection using VMProtect

Module 6: Anti-Tampering Technologies

- Checksum and hash validation
- Anti-patching mechanisms
- Dynamic checks at runtime
- Secure boot sequences
- Encrypted storage of logic
- **Case Study**: Anti-tamper methods in banking apps

Module 7: Software Watermarking

- Types of software watermarks
- Watermark resilience and stealth
- Fingerprinting vs. watermarking
- Embedding copyright notices
- Watermark detection and validation tools
- **Case Study**: Legal case involving proprietary game engine

Module 8: Runtime Application Self-Protection (RASP)

- What is RASP and how it works
- Deployment architectures
- Runtime monitoring vs. prevention
- Integration with existing apps
- RASP vs. WAF
- **Case Study**: RASP defending a financial transaction app

Module 9: Secure Coding Practices for Anti-RE

- Writing non-linear logic
- Removing debugging metadata
- Using compiler-level obfuscation flags
- Minimizing reflection and dynamic code
- Building resilience against decompilers
- **Case Study**: Android app decompilation and prevention

Module 10: AI and Machine Learning in RE Defense

- Behavior-based analysis for detection
- AI-powered anti-debugging
- Predictive threat modeling
- Reinforcement learning for defense evolution
- Toolsets: DeepRE, MalConv
- **Case Study**: Machine learning model used to detect RE in real time

Module 11: Mobile Application Protection

- Challenges in Android/iOS environments
- Code obfuscation in APKs
- Root/jailbreak detection
- Code integrity checks
- Encryption of mobile resources
- **Case Study**: Securing fintech app against RE

Module 12: Embedded Systems and IoT Security

- Reverse engineering firmware
- Secure bootloaders
- Hardware obfuscation
- Code signing for embedded systems
- Attack surface minimization
- **Case Study**: IoT camera firmware hijacking

Module 13: Penetration Testing for RE Scenarios

- Reverse engineering from the attacker’s perspective
- Tools used in pentesting (Radare2, Binary Ninja)
- Developing RE-resistant test apps
- Evaluating existing defenses
- Reporting and remediation
- **Case Study**: Pen-testing DRM-protected application

Module 14: DevSecOps and Reverse Engineering Protection

- Integration of anti-RE in CI/CD pipelines
- Static and dynamic security scanning
- Securing build artifacts
- Using code signing at deployment
- Automation of countermeasures
- **Case Study**: DevSecOps pipeline integrating anti-RE tools

Module 15: Incident Response and Post-RE Attack Strategy

- Identifying signs of reverse engineering

- Forensics collection and analysis
- Containment and code regeneration
- Legal and compliance response
- Building a long-term protection plan
- **Case Study**: Company response to RE breach of IP

Training Methodology

- Instructor-led sessions with real-time demos
- Hands-on labs using reverse engineering tools
- Scenario-based learning using case studies
- Group discussions and collaborative problem solving
- Capstone project focused on designing anti-RE systems

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
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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