Training Course on Firmware and Embedded Malware Analysis

Professional Development Training Course Outline

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

Course Introduction

Training Course on Firmware and Embedded Malware Analysis is designed to empower cybersecurity professionals, reverse engineers, and security analysts with the skills required to dissect, analyze, and defend against malicious firmware threats targeting embedded systems and IoT devices. With the exponential growth of embedded technology in critical infrastructure, automotive systems, medical devices, and smart homes, firmware has become a prime target for persistent malware and sophisticated cyberattacks. This hands-on course blends theoretical concepts with practical labs to expose participants to real-world scenarios, reverse engineering techniques, and vulnerability detection in firmware binaries.

As threat actors increasingly leverage firmware-level exploits to evade traditional security mechanisms, organizations need professionals equipped to detect and counter these hidden dangers. This training will cover firmware extraction, unpacking, code analysis, file system inspection, hardware interfaces, and behavioral analysis of embedded malware. By mastering this domain, learners will gain the ability to protect high-value systems and reduce risk exposure in the face of advanced persistent threats (APTs) and supply chain attacks. This course ensures proficiency in firmware forensic techniques aligned with cybersecurity best practices, MITRE ATT&CK for ICS, and IoT security frameworks.

Programme Curriculum

Training Course on Firmware and Embedded Malware Analysis

Introduction

Training Course on Firmware and Embedded Malware Analysis is designed to empower cybersecurity professionals, reverse engineers, and security analysts with the skills required to dissect, analyze, and defend against malicious firmware threats targeting embedded systems and IoT devices. With the exponential growth of embedded technology in critical infrastructure, automotive systems, medical devices, and smart homes, firmware has become a prime target for persistent

malware and sophisticated cyberattacks. This hands-on course blends theoretical concepts with practical labs to expose participants to real-world scenarios, reverse engineering techniques, and vulnerability detection in firmware binaries.

As threat actors increasingly leverage firmware-level exploits to evade traditional security mechanisms, organizations need professionals equipped to detect and counter these hidden dangers. This training will cover firmware extraction, unpacking, code analysis, file system inspection, hardware interfaces, and behavioral analysis of embedded malware. By mastering this domain, learners will gain the ability to protect high-value systems and reduce risk exposure in the face of advanced persistent threats (APTs) and supply chain attacks. This course ensures proficiency in firmware forensic techniques aligned with cybersecurity best practices, MITRE ATT&CK for ICS, and IoT security frameworks.

Course Objectives

1. Understand the structure and components of firmware in embedded systems.
2. Perform firmware extraction using hardware and software methods.
3. Analyze firmware file systems for hidden threats and backdoors.
4. Utilize reverse engineering tools like Ghidra and Binwalk.
5. Detect and analyze embedded malware persistence mechanisms.
6. Conduct static and dynamic analysis of firmware binaries.
7. Identify and patch firmware vulnerabilities.
8. Utilize virtualization and emulation techniques for behavioral analysis.
9. Leverage YARA rules and indicators of compromise (IoCs) in analysis.
10. Understand supply chain threats and how malware is implanted in firmware.
11. Map findings to MITRE ATT&CK for ICS and Enterprise.
12. Apply incident response strategies for firmware-based compromises.
13. Create professional malware analysis reports with actionable intelligence.

Target Audiences

1. Cybersecurity Analysts
2. Incident Response Teams
3. Reverse Engineers
4. IoT Security Specialists
5. Firmware Developers
6. Red/Blue Team Members
7. Embedded System Engineers
8. Threat Intelligence Professionals

Course Duration: 5 days

Course Modules

Module 1: Introduction to Firmware and Embedded Malware

- Types of embedded systems and firmware formats
- Firmware update mechanisms and vectors for exploitation
- Introduction to firmware structure and architecture
- Overview of common embedded operating systems (e.g., VxWorks, RTOS)
- Understanding bootloaders and initialization code
- **Case Study**: Analysis of a Mirai-infected IoT device

Module 2: Firmware Extraction and Acquisition

- Firmware dumping via UART, JTAG, SPI interfaces
- Software-based firmware acquisition (e.g., firmware update packages)
- Use of tools: Binwalk, Firmware Mod Kit, dd

- Handling encrypted or compressed firmware blobs
- Validating and preserving extracted images
- **Case Study**: Extracting and analyzing router firmware from a live device

Module 3: File System and Code Analysis

- Identifying and unpacking firmware file systems (SquashFS, CramFS, etc.)
- Static analysis of embedded binaries and config files
- Locating embedded credentials and hardcoded keys
- Detection of init scripts, startup behavior, and backdoors
- Forensic recovery of deleted or hidden files
- **Case Study**: Discovery of malicious startup script in a camera firmware

Module 4: Reverse Engineering Firmware Binaries

- Use of Ghidra, IDA Pro, and Radare2 in firmware RE
- Analyzing control flow and function calls
- Identifying suspicious binaries and shellcode
- Understanding memory mapping in embedded systems
- Automating analysis with Python and firmware RE plugins
- **Case Study**: Reverse engineering a modified U-Boot binary

Module 5: Malware Detection and Behavior Analysis

- Introduction to behavioral analysis and sandboxing
- Identifying malware indicators within firmware
- Emulating firmware in QEMU for dynamic analysis
- Using YARA rules to detect known patterns
- Isolating malware C2 communications in firmware
- **Case Study**: Emulating firmware to detect stealthy backdoor behavior

Module 6: Firmware Vulnerabilities and Exploits

- Common vulnerabilities in firmware (e.g., buffer overflows, command injection)
- CVE analysis and NVD mapping
- Exploiting firmware flaws in lab environments
- Writing basic proof-of-concept firmware exploits
- Patching firmware vulnerabilities securely
- **Case Study**: Exploiting command injection in a smart light controller

Module 7: Advanced Threats and Supply Chain Attacks

- Overview of firmware-level APTs and nation-state malware
- Techniques for implanting malware in legitimate firmware
- Detection of malicious firmware updates and bootkits
- Supply chain compromise case studies
- Implementing trust verification and digital signing
- **Case Study**: The SolarWinds-style firmware attack scenario

Module 8: Reporting, Documentation, and Defense

- Writing technical and executive-level analysis reports
- Mapping malware behavior to MITRE ATT&CK
- Creating IoCs and YARA rules from findings
- Firmware hardening and secure development principles
- Collaboration with SOC and DevSecOps teams

- **Case Study**: Real-world incident response using firmware analysis report

Training Methodology

- Hands-on labs and real-world firmware samples
- Use of open-source tools like Binwalk, Ghidra, QEMU
- Case-based learning for practical understanding
- Group activities and reverse engineering challenges
- Access to virtual embedded device environments
- Post-training assessment and certification

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	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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