OFFENSIVE ARM64 REVERSING AND EXPLOITATION

Expert-Led Cybersecurity Training · Beginner to Advanced

COURSE OVERVIEW

This course is designed for cybersecurity professionals and enthusiasts looking to master advanced techniques in ARM64 architecture. Starting with an in-depth exploration of ARM architecture, focusing on ARMv8/ARMv9 (64-bit) architecture and their historical evolution, participants will gain a solid understanding of the ARM Instruction set (includes updates from ARMv9), calling conventions, and architectural features. The course covers introduction to reverse engineering, providing essential concepts and methodologies for dissecting ARM binaries effectively. Participants will also receive hands-on training with Ghidra, a powerful reverse engineering tool, and learn how to leverage scripting to automate tasks and streamline analysis workflows.

Moving forward, the course covers various binary exploitation categories, such as Use-after-Free (UaF), Heap Overflow, and more. Participants will learn about exploit mitigations, including Address Space Layout Randomization (ASLR), Pointer Authentication Codes (PAC), PAuth, Scalable Vector Extension 2 (SVE2), Memory Tagging Extension (MTE), Realm Management Extension / Confidential Compute Architecture (RME/CCA), Stack Canaries, and other defenses commonly encountered in modern systems. Students will also learn the art of writing JOP and ROP chains tailored for ARM architecture.

8KSEC

This course will be a mix of lectures, practical labs, and projects designed to give students hands-on experience with ARM64 architecture. Students will gain the skills needed to reverse engineer, identify vulnerabilities and create exploits for ARM64 binaries.

This course prepares you for the **Offensive ARM Exploitation Expert (OAAE)** certification exam, a hands-on assessment specifically designed to test your grasp of advanced ARM64 reversing and exploitation knowledge.

KEY LEARNING OBJECTIVES

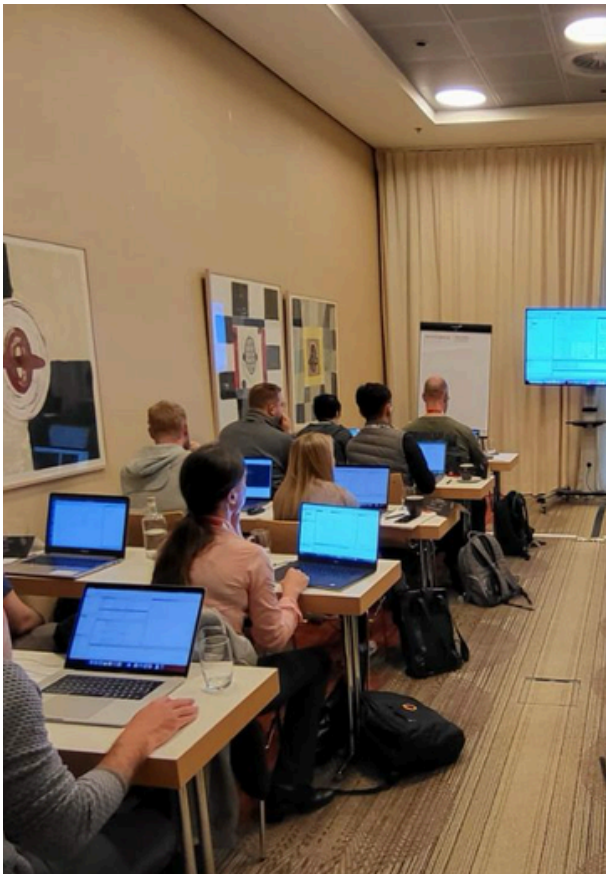
- ARM64 architecture fundamentals, including instruction set and conventions
- Introduction to Ghidra and scripting for reverse engineering
- Exploitation categories: UaF, Heap Overflow, and more
- Mitigations like ASLR, PAC, Stack Canaries, etc., explained
- Exploiting Info leaks to bypass ASLR
- Exploiting Uninitialized Stack Variables for privilege escalation
- Off-by-one byte overflow vulnerabilities and exploitation techniques
- Advanced exploitation tactics: ROP, JOP, and chaining strategies
- Constructing Jump-Oriented Programming (JOP) chains for ARM64
- Advanced Dynamic Instrumentation using Frida
- Firmware reversing for ARM64-based systems
- Exploiting IoT devices: firmware, protocol analysis, and exploitation
- Become a Offensive ARM Exploitation Expert (OAAE)

WHY SHOULD YOU TAKE THIS COURSE?

This is a completely hands-on course designed for beginners and intermediate students. Instead of just slides, attendees will get a chance to exploit all of the vulnerabilities taught by the instructors. For the Onsite and Virtual sessions, the attendees will be provided with Cloud-based labs for performing the hands-on exercises without the need to carry physical ARM64 devices. Slack channel is created before the course for the students so that they can be adequately prepared in terms of hardware and software before the class.

PREREQUISITE KNOWLEDGE

- Working knowledge of cybersecurity and pentesting fundamentals
- Basic Linux skills and command-line proficiency
- Understanding of fundamental programming concepts and looping structures in at least one higher-level language (Java, Kotlin, Objective-C, Swift, C, C++, or similar)
- Basic ARM/AARCH64 binary assembly and exploitation knowledge is recommended, but not required
- Basic working knowledge of iOS and Android platforms is recommended, but not required



WHO SHOULD ATTEND?

This course is specifically designed with the needs of modern exploit development and reverse engineering. This course will also be applicable for vulnerability researchers, penetration testers, mobile developers, or anyone keen to learn more about the ARM64 ecosystem.

WHAT WILL THE STUDENTS GET?

- An attempt to Offensive ARM Exploitation Expert (OAAE) certification exam
- Certificate of completion for the Training program
- Source code for vulnerable binaries used during the class
- Source code for Exploit PoCs' that can be used for Bug Bounties
- All Python Scripts used during the course
- Students will be provided with access to Corellium for for the duration of the course (Live On-site & Virtual Training only)
- Students will be provided access to cloud instances for the duration of the course (Live On-site & Virtual Training only)
- Slack access for the class and after for regular mobile security discussions (Live On-site & Virtual Training only)

HARDWARE/SOFTWARE REQUIREMENT

- Laptop with 8+ GB RAM and 40 GB hard disk space
- Students will be provided with access to Linux cloud instances
- Students will be provided with access to Corellium for iOS hands-on and as such do not need to carry iOS devices
- Administrative access on the system

Detailed Course Setup instructions and Slack access will be sent a few weeks prior to the class (Live On-site & Virtual Training only)

COURSE SYLLABUS

Module 1: Fundamentals of ARM64 Exploitation

- Overview of ARM64 architecture and instruction set
- Introduction to ARM64 security mitigations
- Understanding ARM64 calling convention
- System specific Proprietary registers
- Setting up a testing environment for ARM64 research
- Overview of the different Binary Formats (Mach-O, ELF)
- Segments and Sections in different Binary formats
- ARM64 virtual memory management in mobile devices

Module 2: Reverse Engineering Essentials for ARM64

- Key concepts and terminologies in reverse engineering
- Introduction to reverse engineering tools like Hopper and Ghidra for ARM64
- Exploring the ARM Instruction set in depth (includes updates from ARMv9)
- Analyzing and bypassing ARM64 security mitigations
- Deep dive into ARM64 calling convention
- Reversing sample binaries on ARM64 architecture
- Disassembling methods and analyzing assembly instructions
- Modifying assembly instructions for ARM64 exploitation
- Deciphering Mangled Symbols in ARM64 binaries

Module 3: Advanced Exploitation Techniques for ARM64

- Exploiting Heap Overflow in ARM64 binaries
- Exploiting uninitialized stack variables in ARM64 binaries
- Leveraging off-by-one byte overflow vulnerabilities for ARM64 exploitation
- Constructing Jump-Oriented Programming (JOP) chains for ARM64
- Crafting Return-Oriented Programming (ROP) chains for ARM64 binaries
- Understanding and exploiting Uninitialized Memory vulnerabilities in ARM64 code
- Analyzing and exploiting JOP (Jump-Oriented Programming) chains in ARM64 binaries
- Exploiting ARM64-specific vulnerabilities and attack vectors

Module 4: Real-World Application and IoT Device Exploitation

- Applying ARM64 exploitation techniques to real-world applications and systems
- Exploiting IoT devices powered by ARM64 architecture
- Firmware reversing and exploitation on ARM64-based devices
- Analyzing protocols and performing exploitation on ARM64 IoT devices
- Hands-on labs and practical exercises simulating real-world ARM64 exploitation scenarios
- Capstone Lab: Capture the Flag (CTF)

8KSEC

About the company

8kSec is a foremost cyber security research company offering exceptional training and consulting services to aid clients in enhancing their security stance. Our experts possess extensive experience in delivering specialised cybersecurity training and consulting to several commercial and defence organisations across the United States, Europe, and the Middle East and North Africa region.

Get in touch

8kSec.io
trainings@8ksec.io