+33 (0)1 48 10 09 46
formation@ambient-it.net 140 Avenue Jean Lolive 93500 Pantin - France

Updated on 12/17/2024

Sign up

OSMR™ Training: Certification (EXP-312)

ALL-IN-ONE: EXAM INCLUDED IN PRICE: COURSE EXP-312

4 days (28 hours)

PRESENTATION

OSMR™ certification (EXP-312) offers an invaluable opportunity to validate your macOS security skills, allowing you to demonstrate your expertise in a constantly evolving field.

This OSMR™ training course offers a deep dive into the macOS security landscape, focusing on:

- Advanced systems analysis
- Identifying security vulnerabilities
- Operating techniques

Our OSMR™ training (EXP-312) provides comprehensive exam preparation, offering quality didactic content and practical exercises to reinforce your understanding and skills in securing Apple systems.

We regularly update our program to reflect the latest trends and developments in macOS security, ensuring the most up-to-date and relevant information.

OSMR™ training is constantly updated to reflect the latest trends and developments in OffSec IT security.

OBJECTIVES

- Understand macOS architecture and security mechanisms
- Acquire advanced binary analysis and debugging skills on macOS
- Master code injection and system service exploitation techniques

- Learn how to bypass security mechanisms such as TCC, GateKeeper and the macOS sandbox
- Develop advanced attack and defense strategies on macOS systems

TARGET AUDIENCE

- Pentesters
- Safety researchers
- Developers
- MacOS application developers
- Analysts SOC

Prerequisites

- Knowledge of C programming
- A normal user experience with macOS
- Basic knowledge of 64-bit assembly and debugging
- Understanding of basic operating concepts

Note: Ambient IT does not own OSMR™, this certification belongs to OffSec ® Services LLC.

OSMR™ CERTIFICATION TRAINING PROGRAM

Introduction

- OSMR™ course overview (EXP-312)
- General strategies for approaching the course
- Introducing EXP-312 VPN labs
- About OSMR
- Installing virtual machines on Apple Silicon
- Configuring Xcode and Homebrew
- Conclusion of the introduction

Binary analysis on macOS

- macOS system overview
- Static and dynamic analysis of binaries
- Using command line tools
- Using Hopper for static analysis
- Debugging with LLDB
- Dynamic debugging and tracing with DTrace
- Case studies and practical examples
- Conclusion on binary analysis

Crafting Shellcodes and Dylib Injection

- Writing shellcodes in ASM and C
- Creating custom shellcodes
- Injection of Dylib and DYLD_INSERT_LIBRARIES
- Bypassing security mechanisms with Dylib
- Mach micro-core for injection moulding
- Function interception and hooking on macOS
- Examples of use cases and recommended practices
- Conclusion on shellcodes crafting and Dylib injection

Bypassing security mechanisms

- Understanding macOS Sandbox profiles
- Bypassing TCC, GateKeeper and File Quarantine
- Symlink and hardlink attacks
- Get kernel code execution
- Examples of successful bypasses
- Case study analysis
- Best practices for securing macOS
- Conclusion on bypassing security mechanisms

Mach IPC and Chaining Exploits

- Exploiting Mach inter-process communications
- Use case CVE-2022-22639
- Exploit chaining on macOS Ventura
- Mitigations on macOS Ventura
- Case studies and practical examples
- Best practices for detection and prevention
- Recommended defense strategies
- Conclusion on Mach IPC exploitation and exploit chaining

Security vulnerability analysis

- Understanding vulnerabilities and their impact
- Searching for and identifying bugs on macOS
- Analysis of known security vulnerabilities
- Research and reporting methodologies
- Disclosure coordination practices
- Practical exercises in vulnerability analysis
- Feedback and lessons learned
- Conclusion on security vulnerability analysis

Advanced attack strategies

- Exploring sophisticated attack vectors
- Development of advanced operating techniques
- Bypassing detection mechanisms
- Analysis of targeted attacks
- Defense against advanced threats
- Use of specialized safety tools
- Simulation of attacks in controlled environments
- Conclusion on advanced attack strategies

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.

approval.