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

Updated 05/17/2024

Sign up

Training for GIAC GMOB® Certification

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

4 days (28 hours)

Presentation

GIAC GMOB® certification is much more than just an accreditation; it's a validation of your skills in mobile device security. By obtaining this certification, you prove your expertise in a crucial area of cybersecurity, thus reinforcing your professional credibility.

The GIAC GMOB® exam is designed to assess your in-depth knowledge of various aspects of mobile device security. With modules covering everything from mobile application analysis to network traffic manipulation, the GIAC GMOB exam tests your understanding and ability to meet today's security challenges.

Our GIAC GMOB® training course offers a complete pathway to prepare you to successfully pass the exam. You'll acquire the skills you need to detect vulnerabilities, secure applications and protect data on mobile devices.

Training is constantly updated to reflect the latest advances and best practices in mobile security.

Objectives

- Master mobile application evaluation techniques
- Understand the potential weaknesses of encrypted channels and develop techniques for protecting mobile network traffic
- Gain an in-depth understanding of Android and iOS security models
- Learn to detect, prevent and mitigate Man-in-the-Middle (MitM) attacks on mobile communications

- Reverse-engineer mobile applications and implement tampering protection measures

Target audience

- **Network administrators**
- Security Consultants
- Pentesters
- IT security engineers
- Security Analysts

Prerequisites

No specific prerequisites, but professional experience in security is a plus.

Note: Ambient IT is not the owner of GIAC GMOB®, this certification belongs to GIAC®, Inc.

OUR GIAC GMOB TRAINING PROGRAM

INTRODUCTION TO MOBILE DEVICE SECURITY

- Overview of mobile device security
- Common threats to mobile platforms
- Legal framework and compliance standards
- Overview of mobile security analysis tools
- The importance of a corporate mobile security policy

MOBILE APPLICATION ANALYSIS

- Evaluation techniques for mobile application binaries
- Understanding and analyzing application permissions
- Detecting potentially harmful behavior
- Use of static and dynamic analysis tools
- Case studies of common vulnerabilities

MOBILE APPLICATION SECURITY ASSESSMENT

- Introduction to the Mobile Application Security Verification Standard (MASVS)
- Auditing mobile application security with MASVS
- Good coding and secure development practices
- Study of session security and data storage

- Penetration testing for mobile applications

ATTACKING ENCRYPTED TRAFFIC

- Understanding SSL/TLS and potential weaknesses
- Tools and techniques for exploiting encrypted channels
- Setting up a test environment for traffic interception
- Analysis of intercepted data and detection of information leaks
- Encryption protection and enhancement techniques

MANAGING ANDROID DEVICES AND APPLICATIONS

- Android data configuration and structure
- Android application security and management
- Android security models and implications for security posture
- Rooting, bootloader unlocking and their security implications
- Business management tools for Android devices

MANAGING IOS DEVICES AND APPLICATIONS

- iOS data configuration and structure
- Security and management of iOS applications
- iOS security models and implications for the security posture
- Jailbreaking and its security implications
- Business management tools for iOS devices

MANIPULATING THE BEHAVIOR OF MOBILE APPLICATIONS

- Security evasion techniques for testing applications
- Modification of configuration files and application parameters
- Using test frameworks to simulate application behavior
- Hijacking application logic to reveal vulnerabilities
- Automating security testing of mobile applications

NETWORK TRAFFIC HANDLING

- Techniques for capturing and manipulating mobile network traffic
- Using proxies and network analyzers for penetration testing
- Simulation of attacks on wireless and cellular networks
- Detection and prevention of Man-in-the-Middle (MitM) attacks
- Secure communications between application and server

MITIGATION AGAINST MALWARE AND MOBILE DEVICE THEFT

- Protection strategies against mobile malware
- Mobile data backup and recovery solutions
- Encryption and data protection technologies at rest and in transit
- Managing the risks of lost or stolen mobile devices
- Use of integrated security features and MDM/EMM solutions

REVERSE ENGINEERING AND SECURING MOBILE APPLICATIONS

- Basic concepts of mobile application reverse engineering
- Tools and environments for reverse engineering
- Application protection against reverse engineering
- Tampering detection and defense techniques
- Risk assessment and security measures for distributed applications

SUMMARY AND PRACTICAL APPLICATION

- Review of key concepts and preparation for the GIAC GMOB exam
- Practical workshops and case studies
- Mobile application security audit simulation
- Strategies for maintaining competence in mobile safety
- Discussion on emerging trends and the future of mobile security

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.