SEC575

GMOB Certification
Mobile Device Security Analyst
www.giac.org/gmob

Mobile Device Security and Ethical Hacking

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

You Will Be Able To

- Use jailbreak tools for Apple iOS and Android systems
- Conduct an analysis of iOS and Android filesystem data to plunder compromised devices and extract sensitive mobile device use information
- Analyze Apple iOS and Android applications with reverse-engineering tools
- Change the functionality of Android and iOS apps to defeat anti-jailbreaking or circumvent in-app purchase requirements
- Conduct an automated security assessment of mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks used by mobile devices
- Intercept and manipulate mobile device network activity
- Leverage mobile-device-specific exploit frameworks to gain unauthorized access to target devices
- Manipulate the behavior of mobile applications to bypass security restrictions

> "Outstanding course material and instructor presentation. It truly drills in the analytic process, while remaining technical. I highly recommend this course to anyone performing any level of intelligence support to defensive cyber operations."
>
> -Thomas L, U.S. Air Force

Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. You don't need to imagine any further because this already exists today: **mobile devices**. These devices are the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

Mobile devices are no longer a convenience technology: they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll exploit lost or stolen devices to harvest sensitive mobile application data.

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review the ways in which we can effectively communicate threats to key stakeholders. You'll leverage tools including Mobile App Report Cards to characterize threats for management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications as well.

You'll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you'll examine each step in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you'll return to work prepared to conduct your own test, and you'll be better informed about what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as being prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

SANS
www.sans.org/SEC575

SANS Technology Institute
www.sans.edu

▶II Bundle OnDemand
with this course
www.sans.org/ondemand

575.1 HANDS ON: Device Architecture and Common Mobile Threats

The first section of the course quickly looks at the significant threats affecting mobile device deployments, highlighted with a hands-on exercise evaluating network traffic from a vulnerable mobile banking application. As a critical component of a secure deployment, we will examine the architectural and implementation differences and similarities in Android (including Android Marshmallow), Apple iOS 10, and the Apple Watch and Google Wear platforms. We will also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification, and more. Hands-on exercises will be used to interact with mobile devices running in a virtualized environment, including low-level access to installed application services and application data.

Topics: Mobile Problems and Opportunities; Mobile Device Platform Analysis; Wearable Platforms: Mobile Device Lab Analysis Tools; Mobile Device Malware Threats

575.2 HANDS ON: Mobile Platform Access and Application Analysis

With an understanding of the threats, architectural components and desired security methods, we dig deeper into iOS and Android mobile platforms focusing on sandboxing and data isolation models, and the evaluation of mobile applications. This section is designed to help build skills in analyzing mobile device data and applications through rooting and jailbreaking Android and iOS devices and using that access to evaluate file system artifacts.

Topics: Static Application Analysis; Unlocking, Rooting, Jailbreaking Mobile Devices; Mobile Phone Data Storage and Filesystem Architecture; Network Activity Monitoring

575.3 HANDS ON: Mobile Application Reverse Engineering

One of the critical decisions you will need to make in supporting a mobile device deployment is to approve or disapprove of unique application requests from end-users in a corporate device deployment. With some analysis skills, we can evaluate applications to determine the type of access and information disclosure threats they represent. In this section we will use automated and manual application assessment tools to evaluate iOS and Android apps. We'll build upon the static application analysis skills covered in day 2 to manipulate application components including Android intents and iOS URL extensions. We'll also learn and practice techniques for manipulating iOS and Android applications: method swizzling on iOS, and disassembly, modification, and reassembly of iOS apps. The day ends with a look at a standard system for evaluating and grading the security of mobile applications in a consistent method through the application report card project.

Topics: Application Report Cards; Automated Application Analysis Systems; Manipulating App Behavior

575.4 HANDS ON: Penetration Testing Mobile Devices – PART 1

An essential component of developing a secure mobile phone deployment is to perform an ethical hacking assessment. Through ethical hacking or penetration testing, we examine the mobile devices and infrastructure from the perspective of an attacker, identifying and exploiting flaws that deliver unauthorized access to data or supporting networks. Through the identification of these flaws we can evaluate the mobile phone deployment risk to the organization with practical, useful risk metrics.

Topics: Fingerprinting Mobile Devices; Wireless Network Probe Mapping; Weak Wireless Attacks; Enterprise Wireless Security Attacks; Network Manipulation Attacks; Sidejacking Attacks

575.5 HANDS ON: Penetration Testing Mobile Devices – PART 2

Continuing our look at ethical hacking and penetration testing, we turn our focus to exploiting weaknesses on iOS and Android devices. We will also examine platform-specific application weaknesses and look at the growing use of web framework attacks in mobile application exploitation.

Topics: SSL/TLS Attacks; Client Side Injection (CSI) Attacks; Web Framework Attacks; Back-end Application Support Attacks

575.6 HANDS ON: Capture the Flag

On the last day of class we'll pull in all the concepts and technology we've covered in the week for a comprehensive Capture-the-Flag (CTF) challenge. During the CTF event, you'll have the option to participate in multiple roles, designing a secure infrastructure for the deployment of mobile phones, monitoring network activity to identify attacks against mobile devices, extracting sensitive data from a compromised iPad, and attacking a variety of mobile phones and related network infrastructure components. In the CTF, you'll use the skills you've built to practically evaluate systems and defend against attackers, simulating the realistic environment you'll be prepared to protect when you get back to the office.

SANS

SEC575 Training Formats

(subject to change)

Live Training
www.sans.org/security-training/by-location/all

Summit Events
www.sans.org/summit

Mentor Training
www.sans.org/mentor

Private Training
www.sans.org/onsite

vLive
www.sans.org/vlive

Simulcast
www.sans.org/simulcast

OnDemand
www.sans.org/ondemand

SelfStudy
www.sans.org/selfstudy