SEC575: Mobile Device Security and Ethical Hacking

GMOB
Mobile Device Security Analyst
giac.org/gmob

6 Day Program	36 CPEs	Laptop Required

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

"SEC575 provides an incredible amount of information, and the hands-on labs are awesome. It is a must-have for mobile penetration testers."

— Richard Takacs, **Integrity360**

Course Preview
available at: **sans.org/demo**

Imagine an attack surface that is spread across 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. Such a surface 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.

SEC575 is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS and Android devices. 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. The SEC575 course examines the full gamut of these devices.

With the skills you learn in SEC575, you will be able to evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption and how to manipulate apps to circumvent client-side security 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, and you'll bypass lock screen to exploit lost or stolen devices.

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 ways to effectively communicate threats to key stakeholders. You'll leverage tools, including Mobile App Report Cards, to characterize threats for managers and decision-makers, while also identifying sample code and libraries that developers can use to address risks for in-house applications.

In employing your newly learned skills, you'll apply a step-by-step mobile device deployment penetration test. 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 of the 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, or better informed on 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 to attackers of enterprise secrets, intellectual property, and personally identifiable information assets. 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 having 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.

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

Section Descriptions

SECTION 1: Device Architecture and Common Mobile Threats

The first module of SEC575 quickly looks at the significant threats affecting mobile device deployments, highlighted by 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 between Android (including Android Pie), Apple iOS 12, 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. We'll examine the tools used to evaluate mobile devices as part of establishing a lab environment for mobile device assessments, including the analysis of mobile malware affecting Android and non-jailbroken iOS devices. Finally, we will address the threats of lost and stolen devices (and opportunities for a pen tester), including techniques to bypass mobile device lock screens.

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

SECTION 2: 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 on the evaluation of mobile applications. This module 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. We will also start to evaluate the security of mobile applications, using network capture analysis tools to identify weak network protocol use and sensitive data disclosure over the network. Finally, we'll wrap up the module with an introduction to reverse engineering of iOS and Android applications using decompilers, disassemblers, and by manual analysis techniques.

TOPICS: Unlocking, Rooting, and Jailbreaking Mobile Devices; Mobile Phone Data Storage and File System Architecture; Network Activity Monitoring; Static Application Analysis

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

SECTION 3: Mobile Application Reverse Engineering

One of the core skills you need as a mobile security analyst is the ability to evaluate the risks and threats a mobile app introduces to your organization. Through lecture and hands-on exercises in this module, with some analysis skills, you will be able to evaluate critical mobile applications to determine the type of access threats and information disclosure threats they represent. In this module 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 Module 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, such as method swizzling on iOS, and disassembly, modification, and reassembly of Android apps. The module ends with a look at a consistent system for evaluating and grading the security of mobile applications using the Application Report Card Project.

TOPICS: Automated Application Analysis Systems; Reverse Engineering Obfuscated Applications; Application Report Cards

SECTION 4: Penetration Testing Mobile Devices – Part 1

An essential component of developing a secure mobile device deployment is to perform or outsource a penetration test. Through ethical hacking and 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. By identifying these flaws we can evaluate the mobile phone deployment risk to the organization with practical and useful risk metrics. Whether your role is to implement the penetration test, or to source and evaluate the penetration tests of others, understanding these techniques will help your organization identify and resolve vulnerabilities before they become incidents.

TOPICS: Manipulating Application Behavior; Using Mobile Device Remote Access Trojans; Wireless Network Probe Mapping; Weak Wireless Attacks; Enterprise Wireless Security Attacks

SECTION 5: 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. Hands-on exercises are used throughout the module to practice these attacks, exploiting both vulnerable mobile applications and the supporting back-end servers.

TOPICS: Network Manipulation Attacks; Sidejacking Attacks; SSL/TLS Attacks; Client-Side Injection Attacks; Web Framework Attacks; Back-end Application Support Attacks

SECTION 6: Capture-the-Flag Event

In the final module of SEC575 we will pull together all the concepts and technology covered during the week in a comprehensive Capture-the-Flag event. In this hands-on exercise, you will have the option to participate in multiple roles, including 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. During this mobile security event you will put into practice the skills you have learned in order to evaluate systems and defend against attackers, simulating the realistic environment you will be prepared to protect when you get back to the office.