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

GMOB
Mobile Device Security Analyst
giac.org/gmob

GIAC Mobile Device Security Analyst

The GIAC Mobile Device Security Analyst (GMOB) certification ensures that people charged with protecting systems and networks know how to properly secure mobile devices that are accessing vital information. GMOB certification holders have demonstrated knowledge about assessing and managing mobile device and application security, as well as mitigating against malware and stolen devices.

- Analyzing application network activity and static applications, assessing mobile application security
- Attacking mobile & wireless infrastructure and web applications, unlocking and rooting mobile devices
- Managing android and iOS devices, manipulating mobile application behavior and network traffic
- Mitigating against mobile malware & stolen mobile devices, penetration testing against mobile devices

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 Now Covers Android 11 and iOS 14

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.

Learn How to Pen Test the Biggest Attack Surface in Your Entire Organization

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.

Take a Deep Dive into Evaluating Mobile Apps and Operating Systems and Their Associated Infrastructures

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.

Your Mobile Devices are Going to Come Under Attack – Help Your Organization Prepare for the Onslaught

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.

Section Descriptions

SECTION 1: Device Architecture and Application Interaction

The first section of SEC575 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 10) and Apple iOS 13. 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. Finally, we will examine how applications interact with each other, as application interaction creates an interesting attack surface for mobile penetration tests.

TOPICS: Mobile Problems and Opportunities; Mobile Device Platform Analysis; Mobile Application Interaction; Mobile Device Lab Analysis Tools

SECTION 2: The Stolen Device Threat and Mobile Malware

A very important threat for mobile devices is the stolen or lost device, as this can cause a major disclosure of sensitive information. In this course section we first examine how a device can be properly protected, and how someone might be able to circumvent those protections. Once access to the device has been obtained, we examine which information is available and how we can access it. On the other hand, gaining privileged access to a device is often needed to perform a security assessment, so we will take a look at the steps required to root an Android phone and jailbreak an iOS device. At the end of the section, we will take a look at how mobile malware (ab)uses the ecosystem to steal money or data or brick the device.

TOPICS: Unlocking, Rooting, and Jailbreaking Mobile Devices; Mobile Phone Data Storage and File System Architecture; Mobile Device Malware Threats

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: Static Application Analysis

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. The lectures and hands-on exercises presented in this course section will enable you to use your analysis skills to evaluate critical mobile applications to determine the type of access threats and information disclosure threats they represent. We will use automated and manual application assessment tools to statically evaluate iOS and Android apps. Initially, the applications will be easy to understand, but towards the end of the section we will dig into obfuscated applications that are far more difficult to dissect. Finally, we will examine different kinds of application frameworks and how they can be analyzed with specialized tools.

TOPICS: Reverse Engineering Obfuscated Applications; Static Application Analysis; Third-Party Application Frameworks

SECTION 4: Dynamic Mobile Application Analysis and Manipulation

After having performed static analysis on applications in Section 3, we now move on to dynamic analysis. A skilled analyst combines both static and dynamic analysis to evaluate the security posture of an application. Using dynamic instrumentation frameworks, we see how applications can be modified at runtime, how method calls can be intercepted and modified, and how we can have direct access to the native memory of the device. We will learn about Frida, Objection, Needle, Drozer, and method swizzling to fully instrument and examine both Android and iOS applications. The section ends with a look at a consistent system for evaluating and grading the security of mobile applications using the Application Report Card Project. 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 you and your organization identify and resolve vulnerabilities before they become incidents.

TOPICS: Manipulating and Analyzing iOS Applications; Manipulating and Analyzing Android Applications; Application Report Cards

SECTION 5: Penetration Testing Mobile Devices

After having analyzed the applications both statically and dynamically, one component is still left untouched: the back-end server. In this course section we will examine how you can perform ARP spoofing attacks on a network in order to obtain a man-in-the-middle position, and how Android and iOS try to protect users from having their sensitive information intercepted. Next, we'll examine how you can set up a test device to purposely intercept the traffic in order to find vulnerabilities on the back-end server. We end the section by creating a RAT application that can be used during a red team assessment in order to target users and gain access to internal networks.

TOPICS: Network Manipulation Attacks; SSL/TLS Attacks; Web Framework Attacks; Using Mobile Device Remote Access Trojans

SECTION 6: Hands-On 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.