ارزنگ
مؤسسه آموزش عالی آزاد

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

دوره حرفه ای تست نفوذ موبایل SANS SEC ۵۷۵

مروری بر دوره

مروری بر دوره

این دوره یکی از از دوره های حرفه ایی تست نفوذ شرکت SANS در زمینه موبایل می باشد که شما را با آخرین آسیب پذیری های تحت سیستم عامل های اندروید و IOS آشنا خواهد کرد این دوره بر اساس آخرین سیلابس شرکت SANS می باشد یکی از مزایای این دوره جزوه و فیلم دوره به صورت فارسی می باشد که در آموزشگاههای دیگر ارائه نمی شود.

آنچه در این دوره خواهید آموخت

آنچه خواهید آموخت

- آشنایی با مفاهیم و ساختار معماری اندروید و IOS
- آشنایی با روش های مهندسی معکوس برروی موبایل
- آشنایی با روش های تست نفوذ برروی سیستم عامل های اندروید
- IOSآشنایی با روش های تست نفوذ برروی سیستم عامل های

سرفصل ها (حضوری)

سرفصل ها

SEC۵۷۵.۱: Device Architecture and Common Mobile Threats

Mobile Problems and Opportunities

- Challenges and opportunities for secure mobile phone deployments
- Weaknesses in mobile devices
- Exploiting weaknesses in mobile apps: Bank account hijacking exercise

Mobile Device Platform Analysis

- iOS and Android permission management models
- Code signing weaknesses on Android
- Inter-app communication channels on iOS
- Android app execution: Android Runtime vs. Android Dalvik virtual machine
- Android Nougat security benefits

Wearable Platforms

- Application isolation and data sharing for Apple Watch
- Network connectivity and Android Wear apps
- Data exfiltration in WatchOS
- Weaknesses in wearable device authentication controls
- Deficiencies in Android Wear and storage encryption

Mobile Device Lab Analysis Tools

- Using iOS and Android emulators
- Android mobile application analysis with Android Debug Bridge (ADB) tools
- Uploading, downloading, and installing applications with ADB
- Application testing with the iOS Simulator

Mobile Device Malware Threats

- Trends and popularity of mobile device malware
- Mobile malware command and control architecture
- Efficiency of Android ransomware malware threats
- Analysis of iOS malware targeting non-jailbroken devices
- Hands-on analysis of Android malware
- Mobile malware defenses: What works and what doesn't

SEC۵۷۵.۲: Mobile Platform Access and Application Analysis

Unlocking, Rooting, and Jailbreaking Mobile Devices

- Legal issues with rooting and jailbreaking
- Jailbreaking iOS
- Android root access through unlocked bootloaders
- Root exploits for Android
- Debugging and rooting Android Wear devices
- Using a rooted or jailbroken device effectively: Tools you must have!

Mobile Phone Data Storage and File System Architecture

- Data stored on mobile devices
- Mobile device file system structure
- Decoding sensitive data from database files on iOS and Android
- Extracting data from Android backups
- Using file system artifacts for location disclosure attacks beyond GPS coordinates

- Hands-on attacks against password management apps

Network Activity Monitoring

- Mobile application network capture and data extraction
- Capturing iOS cellular/۴G network traffic
- Transparent network proxying for data capture
- Encrypted data capture manipulation
- Extracting files and sensitive content from network captures
- Recovering sensitive data from popular cloud storage providers

Static Application Analysis

- Retrieving iOS and Android apps for reverse engineering analysis
- Decompiling Android applications including Android Wear
- Circumventing iOS app encryption with Dumpdecrypted and Rasticrac
- Header analysis and Objective-C disassembly
- Accelerating iOS disassembly: Hopper and IDA Pro
- Swift iOS apps and reverse engineering tools

SEC۵۷۵.۳: Mobile Application Reverse Engineering

Automated Application Analysis Systems

- iOS application vulnerability analysis with Needle
- Structured iOS application header analysis
- Tracing iOS application behavior and API use

- Effective Android application analysis with Androwarn
- Android application interaction and Intent manipulation with Drozer
- Extracting secrets with KeychainDumper

Reverse Engineering Obfuscated Applications

- Identifying obfuscation techniques
- Decompiling obfuscated applications
- Effective reconstructed code annotation with Android Studio
- Decrypting obfuscated content with Simplify

Application Report Cards

- Step-by-step recommendations for application analysis
- Tools and techniques for mobile platform vulnerability identification and evaluation
- Recommended libraries and code examples for developers
- Detailed recommendations for jailbreak detection, certificate pinning, and application integrity verification
- Android and iOS critical data storage: Keychain and key store recommendations

SEC۵۷۵.۴: Penetration Testing Mobile Devices, Part ۱

Manipulating Application Behavior

- Runtime iOS application manipulation with Cycript
- iOS method swizzling
- Android application manipulation with Apktool
- Reading and modifying Dalvik bytecode
- Adding Android application functionality, from Java to Dalvik bytecode

Using Mobile Device Remote Access Trojans

- Building RAT tools for mobile device attacks
- Hiding RATs in legitimate Android apps
- Customizing RATs to evade anti-virus tools
- Integrating the Metasploit Framework into your mobile pen test
- Effective deployment tactics for mobile device Phishing attacks

Wireless Network Probe Mapping

- Monitoring network probing activity
- Visualizing network discovery and search
- Wireless anonymity attacks
- Exploiting iOS and Android wireless network scanning characteristics

Weak Wireless Attacks

- Wireless network scanning and assessment
- Exploiting weak wireless infrastructure
- Monitoring mobile device network scanning
- Exploiting "Google WiFi" and iPad or iPhone captive portal detection
- Secure network impersonation

Enterprise Wireless Security Attacks

- Exploiting WPA۲ Enterprise networks with certificate impersonation
- Manipulating enterprise wireless authentication protocols
- RADIUS server impersonation attacks

SEC۵۷۵.۵: Penetration Testing Mobile Devices, Part ۲

Network Manipulation Attacks

- Using man-in-the-middle tools against mobile devices
- Sniffing, modifying, and dropping packets as man-in-the-middle
- Mobile application data injection attacks

Sidejacking Attacks

- Identifying mobile applications vulnerable to sidejacking
- Using sidejacking effectively in a penetration test
- Hands-on exploitation of popular mobile applications

SSL/TLS Attacks

- Exploiting HTTPS transactions with man-in-the-middle attacks
- Core pen test technique: TLS impersonation against iOS Mail.app for password harvesting

- Integrating man-in-the-middle tools with Burp Suite for effective HTTP manipulation attacks

Client-Side Injection Attacks

- Android WebView and JavaScript injection for remote code execution
- Harvesting session cookies through Android browser vulnerabilities with Metasploit
- Using the Spec.js library for mobile browser vulnerability detection and exploit delivery

Web Framework Attacks

- Site impersonation attacks
- Application cross-site scripting exploits
- Remote browser manipulation and control
- Data leakage detection and analysis
- Hands-on attacks: Mobile banking app transaction manipulation

Back-end Application Support Attacks

Exploiting SQL injection in mobile application frameworks
Leveraging client-side injection attacks
Getting end-to-end control of mobile application server resources

مخاطبان دوره

مخاطبان دوره

- کارشناسان امنیت و تست نفوذ و برنامه نویسان موبایل

پیش نیاز ها

پیش نیازها

- آشنایی با برنامه نویسی موبایل