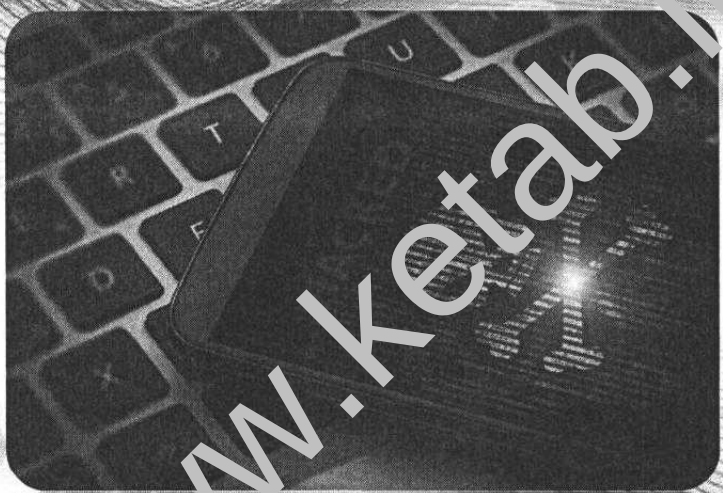
هک اندروید



نویسندگان:
Srinivasa Rao Kotipalli
Mohammed A. Imran

مترجم:
مهندس نیما نقدی روزبهانی

سرشناسه	: اسرینیواسا راو کاتیپالی
عنوان و نام پدیدآور	: هک اندروید، ترجمه نیما نقدی روزبهانی Nima Naghdi Ruzbehani
مشخصات نشر	: تهران: نبض دانش، ۱۳۹۷.
مشخصات ظاهری	: ۳۴۳ صفحه مصور
شابک	: ۹۷۸-۶۰۰-۸۸۷۱-۷۹-۸
وضعیت فهرست‌نویسی	: فیپا
یادداشت	: هک و امنیت
شناسه افزوده	نقدی روزبهانی، نیما - ۱۳۵۹
رده‌بندی کنگره	: ۱۳۹۷ ۹۳ ب ۹ ک / ۹ / ۷۶ QA
رده‌بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۵۴۵۳۴۴۹

نبض دانش

تهران – میدان انقلاب – خیابان منیری جاوید – نبش [illegible]ی‌نژاد و جمهوری – پلاک ۱۹ – واحد ۶ همراه: ۰۹۱۲۷۸۵۶۵۱۵

عنوان ..... **هک اندروید**

ترجمه ..... **نیما نقدی روزبهانی**

ناشر ..... نبض دانش

ناشر همکار ..... آبدوس

سال چاپ ۱۳۹۷

تیراژ ..... ۲۰۰ نسخه

قیمت ..... **۵۷۵۰۰ تومان**

پست الکترونیک: NabzeDanesh@gmail.com

فروشگاه اینترنتی: www.NabzeDanesh.ir

فهرست

Contents

مقدمه

امنیت تلفن‌های همراه یکی از داغ ترین موضوعات امروز است. اندروید که سیستم‌عامل تلفن‌های همراه بازار را رهبری می‌کند، دارای کاربران بسیار زیادی است که اطلاعات خود را بر روی تلفن‌های همراه ذخیره می‌نماید. تلفن‌های همراه اکنون منبع سرگرمی‌ها، کسب و کار، اطلاعات زندگی خصوصی می‌باشند و ریسک‌های جدیدی را در این زمینه به وجود آورده است.

حمله‌های هدفمند به تلفن‌های همراه و برنامه‌های مربوط به آن در حال افزایش است. پلتفرم اندروید به دلیل دارا بودن دامنه وسیعی از کاربران، اولین هدف بدیهی حمله‌کنندگان است. این کتاب دیدگاههایی را در مورد تکنیک‌های مختلف حمله به منظور کمک به توسعه‌دهندگان و متخصصین تست‌های نفوذ و همچنین کاربران نهایی جهت درک اساس امنیت در اندروید، ارائه می‌دهد.

این کتاب چه مباحثی را پوشش می‌دهد:

فصل اول به نام تجهیز آزمایشگاه است که یک بخش ضروری از کتاب است. این فصل شما را جهت تجهیز یک آزمایشگاه نرم‌افزاری با تمام ابزارهایی که در ادامه کتاب به آن‌ها نیاز خواهید داشت، راهنمایی می‌کند. این فصل همچنین یک بحث ضروری برای کسانی است که در زمینه امنیت اندروید تازه‌کار است. این فصل کمک می‌کند تا شما تمام ابزارهای موردنیاز برای امنیت اندروید را در یکجا داشته باشد.

فصل دوم به نام روت کردن اندروید(Android Rooting) است که مقدمه‌ای در مورد تکنیک‌های عمومی که جهت روت کردن دستگاه‌های اندروید استفاده می‌شود، را ارائه می‌دهد. در این فصل درباره مقدمات روت کردن و همچنین نظریات موافق و مخالف آن بحث می‌شود. سپس ما وارد مبحث تکنیک‌هایpartition layout، boot loader ها و شکستن قفل boot loaderها می‌شویم. این فصل برای راهنمایی کسانی که قصد دارند دستگاه اندروید خود را روت نمایند و می‌خواهند بدانند با روت کردن دستگاه چه چیزی را از دست داده و چه چیزی را به دست می‌آورند مفید است.

فصل سوم به نام اساس بلوک‌های ساختمان برنامه اندروید است که خلاصه‌ای از محتویات درونی یک برنامه اندروید را ارائه می‌دهد. این فصل جهت درک چگونگی ساخته‌شدن برنامه های اندروید، چگونگی نمایش آن‌ها پس از نصب بر روی یک دستگاه، چگونگی اجراشدن و موارد مشابه دیگر مفید است.

فصل چهارم به نام خلاصه‌ای از حملات به اندروید است که خلاصه‌ای از حملاتی که به اندروید می‌شود را فراهم می‌کند. در این فصل درباره کلیه حملات ممکن به برنامه‌ها، دستگاه‌ها و دیگر اجزای ساختار برنامه به‌صورت گذرا بحث می‌شود. به‌صورت ضروری، این فصل به شما اجازه می‌دهد که یک مدل تهدید ساده جهت یک برنامه سنتی که برای ارتباط با پایگاه داده از شبکه استفاده می‌کند، را بسازید. این ضروری است که شما درک نمایید که تهدیدات از چه راه‌هایی امکان نفوذ دارند تا در زمان تست امنیتی بدانید

که چه قسمت‌هایی را باید تست نمایید. این فصل یک بخش سطح بالاست و شامل مقداری جزئیات تکنیکی است.

فصل پنجم به نام ذخیره‌سازی اطلاعات و امنیت آن‌ها در اندروید است که مروری بر تکنیک‌های عمومی که جهت ارزیابی امنیت ذخیره‌سازی اطلاعات در برنامه‌های اندروید استفاده می‌شوند، را ارائه می‌دهد. حافظه‌ها یکی از مهم‌ترین عناصر در توسعه برنامه‌های اندروید است. این فصل با بحث در مورد تکنیک‌های مختلف توسعه‌دهندگان جهت ذخیره‌سازی اطلاعات به‌صورت محلی و چگونگی تأثیر گذاشتن آن‌ها بر امنیت سیستم آغاز می‌شود. سپس ما باید نگاهی به مفاهیم امنیت حافظه‌هایی که توسط توسعه‌دهندگان انتخاب می‌شوند، بیندازیم.

فصل ششم به نام حملات سمت سرور (Server-Side Attacks) است که خلاصه‌ای درباره حملات به اندروید از سمت سرور را فراهم می‌کند. در این فصل درباره انواع حملات ممکن به برنامه‌های داخلی اندروید بحث می‌شود. این فصل یک بخش سطح بالاست و شامل مقداری جزئیات تکنیکی است. بیشتر آسیب‌پذیری‌های سمت سرور مربوط به حملات وب است که به‌صورت گسترده در تست‌های OWASP و راهنمایی‌های توسعه‌دهندگان پوشش داده می‌شود.

فصل هفتم به نام حملات سمت کاربر (Client-Side Attacks) – تکنیک‌های تجزیه‌وتحلیل استاتیک است که حملات مختلف سمت کاربر را از دیدگاه تست امنیتی استاتیک برنامه (SAST) پوشش می‌دهد. تجزیه‌وتحلیل استاتیک یک تکنیک ایج جهت شناسایی آسیب‌پذیری‌های برنامه‌های اندروید با استفاده از ابزارهای مهندسی معکوس برنامه‌های اندروید است. این فصل همچنین درباره استفاده از برخی ابزارهای خودکار در دسترس برای تجزیه‌وتحلیل استاتیک برنامه‌های اندروید بحث می‌کند.

فصل هشتم به نام حملات سمت کاربر (Client-Side Attacks) – تکنیک‌های تجزیه‌وتحلیل داینامیک است که برخی از تکنیک‌ها و ابزارهای مشترک برای دسترسی و بهره‌برداری از آسیب‌پذیری‌های سمت کاربر در برنامه اندروید با استفاده از تست امنیتی داینامیک برنامه (DAST)، را پوشش می‌دهد. در این فصل همچنین درباره ابزارهایی مانند Xposed و Frida که جهت دستکاری برنامهٔ در حال اجرا مورد استفاده قرار می‌گیرند، بحث می‌شود.

فصل نهم به نام بدافزارهای اندروید است که مروری بر تکنیک‌های عمومی استفاده‌شده در ساخت و تجزیه‌وتحلیل بدافزارهای اندروید است. این فصل با آشنایی با ویژگی‌های بدافزارهای سنتی اندروید آغاز می‌شود. در این فصل همچنین درباره چگونگی توسعه یک بدافزار ساده که باعث یک reverse shell بر روی تلفن همراه آلوده می‌شود، بحث می‌گردد.

فصل دهم به نام حمله به دستگاه‌های اندروید است که درباره چگونگی کمک به کاربران در جهت ایجاد امنیت برای گوشی همراهشان در مقابل حمله مهاجمان هنگامی‌که در حال انجام کارهای روزانه مانند اتصال گوشی هوشمند به Wi-Fi رایگان یک کافی شاپ و یا فرودگاه هستند، است. در این فصل همچنین در ارتباط با خطرات روت کردن گوشی اندروید و نصب برنامه‌های ناشناس بحث خواهد شد.

برای این کتاب شما به چه چیزی نیازمند هستید؟

به منظور تجربه عملی مثال‌ها در هنگام مطالعه این کتاب، شما نیاز به نرم‌افزارهای زیر دارید. لینک‌های دانلود و مراحل نصب آن‌ها در ادامه کتاب توضیح داده‌شده‌اند.

- Android Studio
- An Android emulator
- Burpsuite
- Apktool
- Dex2jar
- JD-GUI
- Drozer
- GoatDroid App
- QARK
- Cydia Substrate
- Introspy
- Xposed Framework
- Frida