

۲۰۱۰۹۴۴

هک اندروید



نویسندگان:

Srinivasa Rao Kotipalli

Mohammed A. Imran

مترجم:

مهندس نیما نقدی روزبهانی

سرشناسه : اسرینواسا 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

شماره افزوده : نقدی روزبهانی، نیما - ۱۳۵۹

هبنای کنگره : ۱۳۹۷ ۹۳ ب ۹ ک ۹ / ۶ / ۷۶ QA

رده‌بندی دی‌سی : ۰۰۵/۸

شماره کتابشناسی ملی : ۵۴۵۳۴۴۹

این اثر مشمول قانون حمایت مورفان، مصنفان و هنرمندان مصوب ۱۳۴۸ است هرکس تمام یا قسمتی از این اثر را بدون اجازه ناشر، نشر یا پخش کند مورد پیگیری قانونی قرار خواهد گرفت.



نبض دانش

تهران - میدان انقلاب - خیابان منیری جاوید - پیرا انی نژاد 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

Contents

۱.....	هک اندروید و راه‌های مقابله با آن.....
۱۴.....	مقدمه.....
۱۴.....	این کتاب چه مباحثی را پوشش می‌دهد:.....
۱۶.....	برای این کتاب شما به چه چیزی نیازمند هستید؟.....
۱۷.....	فصل اول: تجهیز آزمایشگاه.....
۱۷.....	نصب ابزارهای موردنیاز.....
۱۷.....	جاوا.....
۲۰.....	اندروید استودیو.....
۳۰.....	ساخت AVD در اندروید استودیو و شبیه‌سازی برنامه در آن.....
۳۵.....	شبیه‌سازی برنامه در گوشی واقعی.....
۳۹.....	ابزار Apktool.....
۴۰.....	ابزار Dex2jar/JD-GUI.....
۴۱.....	ابزار Burp Suite.....
۴۴.....	ابزار ADB Primer.....
۴۵.....	بررسی دستگاه‌های متصل.....
۴۵.....	دریافت یک shell.....
۴۶.....	لیست کردن پکیج‌ها.....
۴۷.....	انتقال فایل به دستگاه.....
۴۸.....	نصب برنامه‌های اندرویدی با استفاده از adb.....
۴۹.....	عیب‌یابی اتصالات adb.....
۴۹.....	ابزار Drozer.....
۵۴.....	ابزار QARK (توسط ویندوز پشتیبانی نمی‌شود).....

۵۴	نصب و تنظیمات QARK
۵۶	ابزار Droid Explorer
۵۷	ابزارهای Cydia Substrate و Introspsy
۶۰	ابزار Frida
۶۱	تنظیمات Frida server
۶۲	تنظیمات frida-client
۶۳	تست نصب:
۶۴	برنامه‌های آسیب‌پذیر
۶۴	ابزار Kali Linux
۶۵	خلاصه فصل
۶۶	فصل دوم: روت کردن اندروید (Android Rooting)
۶۶	روت کردن چیست؟
۶۷	چرا باید یک دستگاه را روت کنیم؟
۶۸	مزایای روت کردن دستگاه
۶۸	کنترل نامحدود بر روی دستگاه
۶۸	نصب برنامه‌های اضافی
۶۸	امکانات بیشتر و سفارشی کردن
۶۹	معایب روت کردن
۷۰	روت کردن ممکن است دستگاه شما را غیرقابل استفاده کند
۷۱	خارج شدن از گارانتی
۷۱	قفل کردن و باز کردن boot loader ها
۷۱	تعیین وضعیت boot loader در دستگاه‌های سونی
۷۴	باز کردن قفل boot loader دستگاه‌های سونی توسط روش خاص سازنده
۷۶	روت کردن boot loader های قفل‌گشایی شده در یک دستگاه سامسونگ
۷۷	بازیابی معمول و بازیابی سفارشی

۸۱	فرآیند روت کردن و نصب ROM سفارشی
۸۱	نصب نرم افزارهای بازیابی
۸۱	استفاده از Odin
۸۳	استفاده از Heimdall
۸۶	روت کردن تلفن همراه سامسونگ Note 2
۸۸	نصب ROM سفارشی در یک تلفن همراه
۹۶	خلاصه فصل
۹۷	فصل سوم: بلوک های بنیادین ساختمان برنامه های اندروید
۹۷	بنیان برنامه های اندروید
۹۷	ساختار برنامه اندروید
۹۹	چگونگی دریافت یک فایل APK
۹۹	مکان ذخیره سازی فایل های APK
۱۰۵	کامپوننت های برنامه های اندروید
۱۰۵	Activity
۱۰۶	Service
۱۰۶	Broadcast receiver
۱۰۶	Content provider
۱۰۷	فرآیند ساخت شدن برنامه اندروید
۱۱۰	ساخت فایل های DEX از خط دستورات DEX
۱۱۳	چه اتفاقی می افتد زمانی که یک برنامه اجرا می شود؟
۱۱۴	ART - Runtime جدید اندروید
۱۱۴	درک sandbox نمودن برنامه
۱۱۴	UID هر برنامه
۱۱۸	Sandbox برنامه
۱۲۰	آیا راهی برای شکستن sandbox وجود دارد؟

۱۲۰	 خلاصه فصل
۱۲۱	 فصل چهارم: مروری بر حملات برنامه‌های اندروید
۱۲۱	 مقدمه‌ای بر برنامه‌های اندروید
۱۲۱	 برنامه‌هایی بر پایه وب (Web-based apps)
۱۲۲	 برنامه‌های بومی (Native apps)
۱۲۲	 برنامه‌های ترکیبی (Hybrid apps)
۱۲۲	 درک نقاط حمله به برنامه
۱۲۲	 معماری برنامه تان همراه
۱۲۴	 تهدیدات سمت کاربر
۱۲۶	 تهدیدات سمت سرور
۱۲۸	 دستور العمل تست کردن اپلیکیشن‌های موبایل
۱۲۸	 ۱۰ ریسک برتر موبایل از دیدگاه OWASP
۱۲۹	 M1: کنترل‌های ضعیف سمت سرور
۱۲۹	 M2: ذخیره‌سازی‌های ناایمن
۱۲۹	 M3: حفاظت ناکافی لایه Transport
۱۳۰	 M4: نشست‌های غیرعمدی اطلاعات
۱۳۱	 M5: مجوزات و احراز هویت‌های ضعیف
۱۳۱	 M6: رمزنگاری‌های شکننده
۱۳۱	 M7: Injection‌های سمت کاربر
۱۳۲	 M8: تصمیمات امنیتی از طریق ورودی‌های نامعتبر
۱۳۲	 M9: مدیریت نادرست Session ها
۱۳۲	 M10: عدم محافظت از کدهای باینری
۱۳۳	 ابزارهای خودکار
۱۳۳	 Drozer
۱۳۴	 انجام ارزیابی‌های امنیتی اندروید توسط Drozer

۱۳۴	 نصب برنامه testapp.apk
۱۳۵	 لیست کردن تمام ماژول ها
۱۳۵	 بازیابی اطلاعات پکیج
۱۳۶	 شناسایی سطوح حمله
۱۳۷	 شناسایی و بهره‌برداری از آسیب‌پذیری‌های برنامه اندروید با استفاده از Drozer
۱۳۷	 حمله به Activity های export شده
۱۳۸	 چه مشکلی اینجا وجود دارد؟
۱۳۹	 OARK (کیت بررسی سریع اندروید)
۱۳۹	 اجرای OARK در مد تعاملی
۱۴۶	 گزارش دهی
۱۴۷	 اجرای OARK در یکبارچه
۱۵۰	 خلاصه فصل
۱۵۱	 فصل پنجم: ذخیره‌سازی اطلاعات و امنیت آن‌ها در اندروید
۱۵۱	 ذخیره‌ساز اطلاعات چیست؟
۱۵۴	 Shared preferences
۱۵۴	 پایگاه‌های داده SQLite
۱۵۴	 حافظه داخلی
۱۵۴	 حافظه خارجی
۱۵۶	 Shared preferences
۱۵۷	 استفاده از یک برنامه واقعی
۱۵۹	 پایگاه داده SQLite
۱۶۲	 حافظه داخلی
۱۶۴	 حافظه خارجی
۱۶۶	 حافظه موقت دیکشنری کاربر
۱۶۷	 ذخیره‌سازی نا امن - پایگاه داده NoSQL

۱۶۸	برنامه کاربردی آزمایشی NoSQL
۱۷۱	تکنیک‌های Backup
۱۷۱	Backup گرفتن از اطلاعات برنامه با استفاده از دستور adb backup
۱۷۳	تبدیل فرمت ab به tar با استفاده از backup extractor اندروید
۱۷۵	خارج نمودن فایل TAR از حالت فشرده با استفاده از pax یا star utility
۱۷۶	بررسی محتویات خارج‌شده از فشرده‌سازی جهت شناسایی مشکلات امنیتی
۱۷۹	امن باشید
۱۸۰	خلاصه فصل
۱۶۹	فصل ششم: عملیات سمت سرور
۱۷۰	انواع برنامه‌های وب‌بیل و مدل‌های تهدید آنها
۱۷۰	برنامه‌هایی بر پایه وب (Web-based apps)
۱۷۰	برنامه‌های بومی (Native apps)
۱۷۱	برنامه‌های ترکیبی (Hybrid apps)
۱۷۱	نقاط حمله سمت سرور برنامه‌های موبایل
۱۷۱	معماری برنامه‌های موبایل
۱۷۲	استراتژی‌های تست backend موبایل
۱۷۲	تنظیمات برنامه Burp Suite Proxy جهت تست
۱۷۳	تنظیمات Proxy جهت استفاده از طریق APN
۱۷۵	تنظیمات Proxy جهت استفاده از طریق Wi-Fi
۱۷۶	عبور از اخطار certificate و HSTS
۱۸۳	HSTS – امنیت قوی در تبادلات HTTP
۱۸۳	دور زدن certificate pinning
۱۸۴	دور زدن SSL pinning با استفاده از AndroidSSLTrustKiller
۱۸۵	رأماندازی یک برنامه آزمایشی
۱۸۵	نصب برنامه GoatDroid

- ۱۸۷.....تهدیدات مربوط به backend
- ۱۸۷.....ارتباط ۱۰ ریسک برتر موبایل از دیدگاه OWASP و برنامه‌های تحت وب
- ۱۸۸.....مشکلات مجوز و احراز هویت
- ۱۸۸.....آسیب‌پذیری‌های احراز هویت
- ۱۹۰.....آسیب‌پذیری مجوزات
- ۱۹۲.....مدیریت Session
- ۱۹۳.....حفاظت نا کافی لایه Transport
- ۱۹۳.....۱۰ ریسک برتر موبایل: شماره M1 و M5
- ۱۹۳.....مشکلات مرتبط با اعتبار سنجی ورودی
- ۱۹۳.....۱۰ ریسک برتر موبایل: شماره M1، M5 و M8
- ۱۹۳.....مدیریت نادرست خطا
- ۱۹۳.....۱۰ ریسک برتر موبایل: شماره M1
- ۱۹۳.....ذخیره‌سازی ناامن اطلاعات
- ۱۹۴.....۱۰ ریسک برتر موبایل: شماره M1 و M2
- ۱۹۴.....حمله به پایگاه‌های داده
- ۱۹۴.....۱۰ ریسک برتر موبایل: شماره M1
- ۱۹۵.....خلاصه فصل
- ۱۹۶.....فصل هفتم: حملات سمت کاربر- تکنیک‌های تجزیه و تحلیل استاتیک
- ۱۹۷.....حمله به اجزای برنامه
- ۱۹۷.....حملات به Activity ها
- ۱۹۷.....رفتار یک Activity که export شده است، چگونه است؟
- ۲۰۳.....Intent filter
- ۲۰۴.....حملات به سرویس ها
- ۲۰۵.....ارث‌بری از کلاس Binder
- ۲۰۵.....استفاده از یک Messenger

۲۰۵	 استفاده از AIDL
۲۰۶	 حمله کردن به سرویس‌های AIDL
۲۰۶	 حملات به broadcast receiver ها
۲۰۹	 حملات به content provider ها
۲۱۰	 کوثری گرفتن از content provider ها
۲۱۲	 بهره‌برداری از SQL Injection از content provider ها با استفاده از adb
۲۱۳	 کوثری گرفتن از content provider ها
۲۱۳	 نوشتن یک شرط where
۲۱۴	 بررسی‌های اولیه جهت انجام حمله Injection
۲۱۵	 پیدا کردن شماره ستون‌ها برای استخراج بیشتر
۲۱۶	 این دستور چگونه کار می‌کند؟
۲۱۶	 اجرای توابع پایگاه داده
۲۱۷	 پیدا کردن نسخه SQLite
۲۱۸	 پیدا کردن نام جدول
۲۱۹	 تجزیه و تحلیل ایستا با استفاده از QARK
۲۲۲	 خلاصه فصل
۲۲۳	 فصل هشتم: حملات سمت کاربر- تکنیک‌های تجزیه و تحلیل داینامیک
۲۲۳	 ارزیابی خودکار برنامه‌های اندروید با استفاده از Drozer
۲۲۴	 لیست کردن تمام ماژول‌ها
۲۲۵	 بازیابی اطلاعات کل پکیج‌ها
۲۲۶	 پیدا کردن نام پکیج برنامه هدف
۲۲۶	 گرفتن اطلاعات در مورد یک بسته
۲۲۷	 استخراج فایل AndroidManifest.xml
۲۳۰	 حمله به Activity ها
۲۳۳	 حمله به سرویس‌ها

۲۳۴	حمله به Broadcast receiver ها
۲۳۵	نشت اطلاعاتی از Content provider و حمله SQL Injection
۲۳۵	با استفاده از Drozer
۲۳۸	حمله SQL Injection با استفاده از Drozer
۲۴۲	حمله Path traversal به content provider ها
۲۴۴	خواندن /etc/hosts
۲۴۵	خواندن نسخه هسته (kernel)
۲۴۵	بهره‌بردار از برنامه‌های debuggable
۲۴۷	مقدمه‌ای بر ابزار Cydia Substrate
۲۴۹	نظارت و تجزیه و تحلیل حین اجرا بوسیله Introspsy
۲۵۴	نفوذ با استفاده از فریم‌ورک Xposed
۲۶۳	تست داینامیک با استفاده از Frida
۲۶۳	Firda چیست؟
۲۶۵	مراحل عملکرد داینامیک نفوذ با Firda
۲۶۷	آسیب‌پذیری‌هایی بر پایه Logging
۲۶۹	حمله‌های WebView
۲۷۰	دسترسی به اطلاعات حساس منابع داخلی از طریق file scheme
۲۷۴	مشکلات دیگر WebView
۲۷۵	خلاصه فصل
۲۷۶	فصل نهم: بدافزارهای اندروید
۲۷۶	بدافزارهای اندروید چه کاری انجام می‌دهند؟
۲۷۷	نوشتن یک بدافزار اندروید
۲۷۷	نوشتن یک تروجان reverse shell ساده با socket programming
۲۸۵	ثبت مجوز ها
۲۸۸	نوشتن یک برنامه دزد SMS ساده

۲۸۸	رابط کاربری برنامه
۲۸۹	MainActivity.java فایل محتویات
۲۹۰	SMS خواندن
۲۹۳	uploadData() متد کدهای
۲۹۴	MainActivity.java کد کامل
۲۹۵	ثبت مجوزها
۲۹۶	کد مربوط به وب سرور
۲۹۷	مروری بر برنامه‌های قانونی آلوده شده
۲۹۸	تجزیه و تحلیل بدافزار
۲۹۸	تجزیه و تحلیل اباتیک
۲۹۸	خارج کردن برنامه از حالت فشرده با استفاده از Apktool
۲۹۹	جستجو در میان محتویات فایل AndroidManifest.xml
۳۰۱	جستجوی فایل‌های پوشه smali
۳۰۳	بازیابی سورس کد اصلی جاوای برنامه اندروید با استفاده از dex2jar و JD-GUI
۳۰۵	تجزیه و تحلیل داینامیک
۳۰۵	تجزیه و تحلیل HTTP/HTTPS با استفاده از Burp
۳۰۷	تجزیه و تحلیل ترافیک شبکه با استفاده از tcpdump و Wireshark
۳۱۱	ابزارهایی برای تجزیه و تحلیل خودکار
۳۱۱	چگونه از بدافزارهای اندروید در امان بمانیم؟
۳۱۱	خلاصه فصل
۳۱۲	فصل دهم: حملات به دستگاه‌های اندروید
۳۱۲	حملات MITM
۳۱۵	مخاطرات برنامه‌های مهیا کننده دسترسی به شبکه
۳۱۹	استفاده از آسیب‌پذیری‌های موجود
۳۲۴	دور زدن قفل‌های صفحه‌نمایش (screen locks)

۳۲۵.....	adb با استفاده از pattern قفل
۳۲۶.....	gesture.key فایل پاک کردن
۳۲۶.....	gesture.key file در فایل hash شده SHA1 به دست آوردن
۳۲۷.....	adb با استفاده از password/PIN دور زدن
۳۳۰.....	CVE-2013-6271 با استفاده از دور زدن قفل صفحه نمایش
۳۳۰.....	sdcard از انتقال اطلاعات
۳۳۱.....	خلاصه فصل

www.ketab.ir

امنیت تلفن‌های همراه یکی از داغ‌ترین 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 می‌نمایند. 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، بهایی جهت درک اساس امنیت در اندروید، ارائه می‌دهد.

این کتاب چه مباحث را پوشش می‌دهد:

فصل اول به نام تجریش آتشگاه است که یک بخش ضروری از کتاب است. این فصل شما را جهت تجهیز یک آزمایشگاه نرم‌افزاری تا تمام ابزارهایی که در ادامه کتاب به آن‌ها نیاز خواهید داشت، راهنمایی می‌کند. این فصل همچنین یک قسمت 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 باشید.

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 بحث تکنیک‌های boot loader، partition layout و شکستن boot loader 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 محتوای درونی یک برنامه اندروید را ارائه می‌دهد. این فصل جهت درک چگونگی ساخته شدن برنامه‌های اندروید، چگونگی نمایش آن‌ها پس از نصب بر روی یک دستگاه، چگونگی اجرا شدن 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 به صورت گذرا بحث می‌شود. به صورت 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 تجزیه و تحلیل استاتیک است که حملات مختلف سمت کاربر را از دیدگاه تست امنیتی استاتیک برنامه (SAST) پوشش می‌دهد. تجزیه و تحلیل استاتیک یک تکنیک رایج جهت شناسایی آسیب‌پذیری‌های برنامه‌های اندروید با استفاده از ابزارهای مهندسی معکوس است. این فصل همچنین درباره استفاده از برخی ابزارهای خودکار در دسترس برای تجزیه و تحلیل استاتیک برنامه‌های اندروید بحث می‌کند.

فصل هشتم به نام حملات سمت کاربر (Client-Side Attacks) - تکنیک‌های تجزیه و تحلیل دینامیک است که برخی از تکنیک‌ها و ابزارها را برای دسترسی و بهره‌برداری از آسیب‌پذیری‌های سمت کاربر در برنامه اندروید با استفاده از حملات دینامیک برنامه (DAST)، را پوشش می‌دهد. در این فصل همچنین درباره ابزارهایی مانند Xposed و Frida که جهت دستکاری برنامه در حال اجرا مورد استفاده قرار می‌گیرند، بحث می‌کند.

فصل نهم به نام بدافزارهای اندروید است که مروری بر تکنیک‌های عمومی استفاده‌شده در ساخت و تجزیه و تحلیل 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 هنگامی که 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 داده شده‌اند.

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