دوره مقدماتی تحلیل بدافزار اندرویدی

تحلیل بدافزار اندروید

مدت(ساعت): ۱۵

اهداف دوره :

اندروید یک سیستم عامل متن باز (Open Source) است که هسته آن لینوکس می باشد و برای گوشیهای هوشمند (smart phone) و تبلت ها ایجاد شده است. این سیستم عامل همانند سایر سیستم عامل ها، مورد تهدیدات جدی در زمینه بدافزارها قرار گرفته و برای حفظ امنیت سیستم عامل و برنامه های کاربردی آن باید تلاش کرد. بنابراین باید راهکارهایی در زمینه شناسایی و پاک کردن بدافزارهای اندرویدی را به کار گرفت.

در پایان این دوره کارآموز با مفاهیم سیستم عامل اندروید و مفاهیم کلیدی و پایه مرتبط با تحلیل در اندروید آشنا می شود. همچنین کارآموز دانش خوبی درباره ی مهندسی معکوس، روال disassemble کردن فایل ها و تحلیل فایل های اندرویدی پیدا کرده و قادر خواهد بود بدافزارها را به‌صورت ایستا و پویا تحلیل نموده و بخش قابل توجهی از آلودگی های بدافزار را شناسایی کند.

پیش نیاز دوره :

- آشنایی با مفاهیم کلی برنامه نویسی
- مهندس کامپیوتر و فناوری اطلاعات
- درک مفهوم Vmware و تجربه کار با آن ضروری نیست ولی میتواند مفید باشد

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی

Accredited by CARRIER DIGIT Computer Software LLC

EC-Council

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس :۸۸۰۶۵۲۲۲

محتوای دوره :

۱. مقدمه ای بر مفاهیم اندروید
۱.۱. اندروید چیست
۱.۲ تصویر کلی از معماری اندروید
۱.۳ تاریخچه اندروید و ویرایشهای مختلف آن
۱.۴ مقایسه ورژنهای قبل و بعد از اندروید ۵
۲. مفاهیم مربوط به فایل apk
۲.۱. آشنایی با ساختار فایل apk
۲.۲. آشنایی با ساختار فایل dex
۲.۳. روال نصب برنامه های اندرویدی
۳. آشنایی با ابزارهای تحلیل فایل اندرویدی
۳.۱ Apktool
۳.۲ Dex2jar
۳.۳ Jd-gui
۳.۴ aapt.exe
۳.۵ DDMS
۳.۶ Androguard.
۴. مولفه های برنامه های اندرویدی(Application Component)
۴.۱ Activities
۴.۲ Services
۴.۳ Content Providers
۴.۴ Broadcast Receivers
۵. شیوه اجرایی کامپوننت ها

Course Outline :

۶. متدهای اجرایی کامپوننت ها
۷. آشنایی با ساختار فایل AndroidManifest.xml
۷.۱ Permissions
۷.۲ Components
۸. مبانی و مفاهیم بدافزارها
۸.۱. تعریف بدافزارها
۸.۲. انواع بدافزارها
۹. روشهای تحلیل بدافزار
۹.۱. استاتیک
۹.۲. داینامیک
۱۰. تکنیک های بدافزارهای اندرویدی
۱۰.۱. روش بقا
۱۰.۲. روش انتشار
۱۰.۳. روش مخفی شدن
۱۰.۴. روش تخریب
۱۱. مبانی شبکه
۱۱.۱. اصول پایه شبکه
۱۱.۱.۱. آشنایی با مفاهیم زیر
۱۱.۱.۱.۱. مدل OSI
۱۱.۱.۱.۲. مدل TCP/IP
۱۱.۱.۱.۳. مفهوم NAT/Port Forward/Bridge/Route/ Firewall
۱۱.۱.۱.۴. پروتکل DNS/ARP
۱۱.۲. آشنایی با Wireshark

Accredited by CARRIER DIGIT Computer Software LLC
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس :۸۸۰۶۵۲۲۲