دورة إختبار إختراق نظام الأندرويد

Android Penetration Testing Course

By Anwar Mohamed

مقدمة

مقدمة

- الأندرويد هو نظام تشغيل للهواتف الذكيه قائم علي نواة لينكس (لكي يستمد منها الأمان والثبات) ومؤخراً صدرت منه عدة إصدارات تعمل علي الأجهزه اللوحيه.

- أندرويد هو نظام مفتوح المصدر حيث يتم السماح للمطورين بكتابة وإضافة مكتباتهم المبينه علي لغة جافا (حيث أن لغة الجافا هي اللغة الرسمية المستخدمه للتطوير لأندرويد) كما يمكنك كتابة وإضافة مكتباتك المبنيه علي لغة سي.

مقدمة

- مع تزايد انتشار الأجهزة التى تعمل على نظام الأندرويد انتشرت بل و اصبحت البرامج الخبيثة فى تطور مستمر بالرغم من جهود جوجل للقضاء على البرمجيات والتطبيقات الخبيثة قبل أن تصيب أجهزة الأندرويد.

- من هذا المنطلق أقيمت عدة دراسات فى انظمة الحماية المتعلقة بنظام الأندرويد و هذا ما سنتناوله فى هذه الدورة من اختبار اختراق هذا النظام بجانب الكشف و تحليل البرمجيات الخبيثة و اكتشاف الثغرات فى نظام الأندرويد ان شاء الله.

فهرس الدورة

- **أساسيات نظام الأندرويد**
  - مقدمة نظام الأندرويد
  - معمارية نظام الأندرويد
- **نموذج نظام الحماية بنظام الأندرويد**
  - معمارية نظام الحماية بنظام الأندرويد
  - نموذج الصلاحيات بنظام الأندرويد
- **HelloWorld نظام ألاندرويد :**
  - مكونات التطبيقات بنظام الأندرويد
  - إنشاء تطبيقك الأول بنظام الأندرويد
- **إعداد بيئة التطوير و الفحص**
  - إعداد ال Emulator
  - إنشاء بيئة الاختبار و إعداد الجوال
- **اختبار اختراق التطبيقات**
  - تحليل التطبيقات
  - الهندسة العكسية
  - اعتراض حزم بيانات التطبيقات
- **مقدمة عن نظام ملفات Dalvik**
- **البحث الجنائى الرقمى بنظام الأندرويد**

متطلبات الدورة

- من المتوقع من المشاركين أن يكون لديهم معرفة بأنظمة تشغيل الجوال.
- من لديه المعرفة بلغات البرمجة (Java و C، وبيثون لعمل ال scripts) فهى ميزة إضافية لفهم الأشياء بسرعة.

- **متطلبات الأجهزة**
  - Android (preferably Rooted) >= 2.3
  - Minimum 2GB RAM and 20 GB free Hard Disk space
- **متطلبات النظام**
  - أى توزيعة لنظام لينكس
  - Android SDK installed

أساسيات نظام الأندرويد

مقدمة نظام الأندرويد

مقدمة نظام الأندرويد

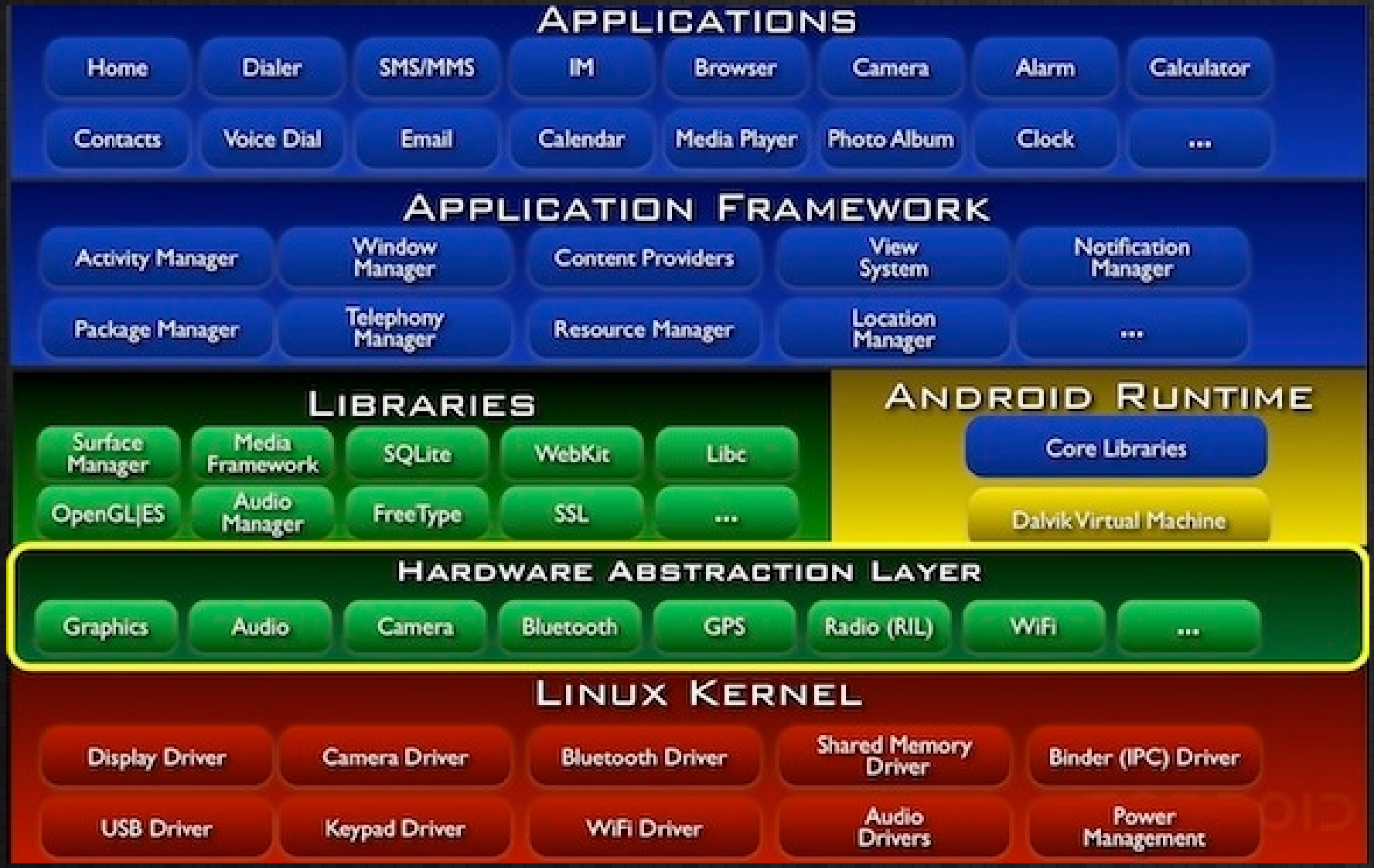
- الأندرويد هو نظام تشغيل للهاتف الجوال.
- نظام مجاني ومفتوح المصدر مبني على نواة لينكس.
- صُمّم أساسًا للأجهزة ذات شاشات اللمس كالهواتف الذكية والحواسب اللوحية.
- يتم تطوير الأندرويد من قبل التحالف المفتوح للهواتف (Open Handset Alliance) الذي تديره شركة جوجل.

مقدمة نظام الأندرويد

- **الخصائص الرئيسية**
  - ماكينة إفتراضية للجافا (Dalvik Java Virtual Machine) مخصصة لأجهزة الجوال ذات الذاكرة المحدودة.
  - متصفح الانترنت مبنى على Webkit Engine.
  - مكتبة جرافيكس ثنائية الأبعاد (2D Graphics Library)
  - مكتبة جرافيكس ثلثي البعاد مبنية على أساس OpenGL ES 3.0.
  - SQLite لقواعد البيانات

معمارية نظام الأندرويد

معمارية نظام الأندرويد



معمارية نظام الأندرويد

- نظام التشغيل أندرويد هو مجموعة من البرامج المكملة التي تنقسم إلى خمسة أقسام وأربعة طبقات رئيسية كما هو موضح في الرسم البياني السابق.

معمارية نظام الأندرويد

- **نواة لينكس**
  - في الجزء السفلي من الطبقات هى نواة لينكس – نواة لينكس اصدار 2.6 مع ما يقرب من 115 ترقيع. هذا يوفر وظائف النظام الأساسية مثل إدارة العمليات process management ، إدارة الذاكرة memory management ، إدارة الجهاز device management مثل الكاميرا، لوحة المفاتيح، وشاشة العرض وما إلى ذلك أيضا، النواة تعالج كل الأشياء التي معروف أن لينكس هو جيد حقا في معالجتها مثل الشبكات ومجموعة واسعة من برامج تشغيل الجهاز، والتي تتواصل مع الأجهزة الطرفية.

معمارية نظام الأندرويد

- **المكتبات**
  - على قمة نواة لينكس هناك مجموعة من المكتبات بما في ذلك محرك مستعرض الويب المفتوح المصدر Webkit, المكتبة المعروفة LIBC ، قاعدة بيانات SQLite و هى مستودع مفيد لتخزين وتبادل بيانات التطبيقات والمكتبات للعب وتسجيل الصوت والفيديو، مكتبات SSL المسؤولة عن أمن الإنترنت الخ.

معمارية نظام الأندرويد

- **أندرويد Runtime**
  - هذا هو الجزء الثالث من المعمارية ومتاحة على الطبقة الثانية من القاع. يوفر هذا القسم مكون رئيسي يسمى Dalvik Virtual Machine و هى نوع من Java Virtual Machine المصممة خصيصا والأمثل لأندرويد.
  - Dalvik Virtual Machine تجعل من استخدام الميزات الأساسية للينكس مثل إدارة الذاكرة وتعدد خيوط المعالجة، والتي هي جوهرية في لغة الجافا
  - Dalvik Virtual Machine تمكن كل تطبيق أندرويد للتشغيل في العملية الخاصة بها، مع المثيل الخاص به من Dalvik Virtual Machine
  - يوفر أندرويد Runtime أيضا مجموعة من المكتبات الأساسية التي تمكن مطوري التطبيقات من كتابة تطبيقات الأندرويد باستخدام لغة البرمجة جافا.

معمارية نظام الأندرويد

- **Application Framework**
  - توفر العديد من الخدمات ذات المستوى الأعلى للتطبيقات في شكل Java Classes. وتسمح لمطوري التطبيقات الاستفادة من هذه الخدمات في تطبيقاتهم.

معمارية نظام الأندرويد

- **التطبيقات**
  - سوف تجد كل تطبيقات الأندرويد في الطبقة العليا. سوف تبرمج تطبيقك ليتم تثبيتها على هذه الطبقة فقط. من أمثلة هذه التطبيقات هي Contacts Books, Browser, Games الخ