iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
حلول امنية متكاملة

دورة اختبار اختراق نظام أندرويد

مركز تدريبات
iSECUR1TY

01 - المقدمة:

1.1 - نبذة عن نظام الأندرويد.

1.2 - معمارية نظام أندرويد.

1.3 - نموذج الحماية.

1.4 - عملية الإقلاع.

02 - صنع مختبر اختراق:

2.1 - التعرف على توزيعة Santoku.

2.2 - ما هو محاكي الأندرويد وما الذي يميزه عن محاكي الـiOS؟

2.3 - ما هو الروت وفائدته وخطورته؟

03 - التفاعل مع نظام الأندرويد:

3.1 - Android Debug Bridge.

3.2 - DDMS File Explorer.

3.3 - SSH.

3.4 - VNC.

3.5 - BusyBox.

04 - الهندسة العكسية لتطبيقات الأندرويد:

4.1 - مقدمة عن الهندسة العكسية.

4.2 - التعرف على مكونات ملف الـAPK.

4.3 - التعرف على مكونات تطبيق الأندرويد.

4.4 - معمارية ملفات الـDEX.

4.5 - الفرق بين الـDalvik Bytecode والـJava Bytecode.

4.6 - ما هو الـSmali والـBaksmali؟

4.7 - Decompiling DEX to Java.

4.8 - عملية التوثيق في تطبيقات الأندرويد.

05 - تحليل حزم البيانات:

5.1 - مقدمة عن تحليل الحزم.

5.2 - التحليل الغير نشط.

5.3 - التحليل النشط.

5.4 - اعتراض حزم الـHTTPs.

06 - اختبار اختراق تطبيقات الأندرويد:

6.1 - مقدمة عن اختبار اختراق تطبيقات الأندرويد.

6.2 - منهجية اختبار اختراق تطبيقات الأندرويد.

6.3 - تثبيت تطبيقات المختبر.

6.4 - جمع المعلومات عن التطبيق.

6.5 - ما يجب أن تعرفه قبل عملية اختبار الاختراق!

6.7 - التعرف على Drozer.

6.8 - OWASP Top 10 Mobile Risks.

6.8.1 - استغلال ثغرة من نوع Weak Server Side Controls.

6.8.2 - استغلال ثغرة من نوع Insecure Data Storage.

6.8.3 - استغلال ثغرة من نوع Insufficient Transport Layer Protection.

6.8.4 - استغلال ثغرة من نوع Unintended Data Leakage.

6.8.5 - استغلال ثغرة من نوع Poor Authorization and Authentication.

6.8.6 - استغلال ثغرة من نوع Broken Cryptography.

6.8.7 - استغلال ثغرة من نوع Client Side Injection.

6.8.8 - استغلال ثغرة من نوع Security Decisions Via Untrusted Inputs.

6.8.9 - استغلال ثغرة من نوع Improper Session Handling.

6.8.10 - استغلال ثغرة من نوع Lack of Binary Protections.

6.9 - ما يجب أن تعرفه أيضًا!

07 - التحقيق الجنائي لأنظمة الأندرويد:

7.1 - أنواع التحقيق الجنائي.

7.2 - معمارية الـFileSystem في نظام الأندرويد.

7.3 - استخدام أداة dd من أجل استخراج البيانات.

7.4 - استخدام AFLogical لاستخراج جهات الاتصال، الاتصالات، الرسائل النصية.

7.5 - استخدام أداة Logcat.

7.6 - استخدام Backup لاستخراج بيانات التطبيقات.

7.7 - تخطي الـAndroid Locks.

7.7.1 - تخطي الـPattern.

7.7.2 - تخطي الـPassword/Pin.

08 - التقرير:

8.1 - كتابة تقرير اختبار اختراق.

8.2 - مكونات التقرير.