السلام عليكم ورحمة الله وبركاته.....

بداية عند تحميل الملف الخاص بالتحدي نجد انه ملف ينتهي بامتداد apk. الخاص بتطبيق اندرويد. طبعا لا نحتاج في البداية الى محاكاة لمعرفة ما بداخل الملف.

حيث ان ملفات apk. هي عبارة عن ارشيف او حزمة ملفات تحتوي على الملفات المطلوبة لتشغيل التطبيق على انظمة اندرويد.

وهي عبارة عن ملف zip مضغوط

بإمكاننا استخدام اي برنامج فتح ضغط لمعرفة المحتويات .

عند فك الضغط عن حزمة ملفات التطبيق نحصل على عدة ملفات ومجلدات.

قمت باستخدام الاداة file و strings الموجودة على نظام لينكس للتركيز على ملف معين.

شد اهتمام ملف باسم ctf.png داخل مجلدassets

حيث عند استخدام الامر file على هذا الملف بدلا من يظهر لي ان الملف من نوع صورة يظهر ان الملف من نوع data اي ان محتوى الملف غير معروف.

من خلال النظر لمحتوى الملف. يبدو انه مرمز (او مشفر).

باستخدام اداة cyberchef وخاصية xor وجدت ان محتوى الملف مشفر ب XORبمفتاح 0) 12xعدد ستعشري(Hexidecimal

ولكن لم تنتهي القصة بعد.....

محتوى الملف بعد فك التشفير هو محتوى ملف صورة بتنسيق png فعلا ولكن محتوى الملف مازال غريب.

من خلال النظر لمحتي الملف داخل برنامج Hex Editor يتضح لي ان الملف يحتوى على ملف مضغوط . تعرفة على ذلك من خلال Magic Byte الخاص بملفات الضغط PK او B504

ملاحظة اخرى اكتشفتها اثناء القراء عن تنسيق png ان الصور بتنسيق png تحتوي على مقاطع او اجزاء تسمىchunks

ويتم قراءة كل جزء او مقطع من النهاية الى البداية from end to beginning ويتم تحديد حجم المقطع اولا ثم اسم المقطع وبعد ذلك محتوى المقطع.

بينما تنسيق الملفات المضغوطة ZIP فيتم التعامل معها بالعكس تماما. وهنا اتضحت الصورة. ان ملف الصورة png يحتوي على ملف مضغوط ايضا وبسبب طريقة تصميم صيغة png و zip بإمكان ان

يتم دمج ملفين من النوعين داخل ملف واحد.

بدأت في تطبيق ما قرأت عن كلا هذين التنسيقين.

واستخدمت الاداة binwalk مع الخيار e- لكي على الصورة التي سبق فك تشفيرها لكي استخرج ملفات pngوzip

من خلال استخدام محرر Hex للنظر في الملفات التي تم استخراجها وجدت على ما يبدو انه ترميز من نوع base64 وهو المستخدم في تحويل البيانات من binary الى صيغة يستخدم فيها الاحرف والرموز المطبوعة) printable characters في القدم تم استخدامها في نقل البريد الالكتروني وصفحات الويب لأن بعض

تطبيقات الشبكة القديمة كانت غير قادرة مع بعض الحروف او الرموز الغير المطبوعة.

خلال بحثي في الملفات المستخرجة اكتشفت عبارة:

8GRDDKMBUGM2DINBVGQZDIMRVGE2EMNCEGQ3TKRRUHE2UMNJXGRDDIRI=

طبعا لم تكون بتنيق base64 ولكن كانت بتنسيق base32 بعد محاولة فك الترميز في cyberchef ظهرت لي النتيجة النهائية.

"OPCDEBBQOMG_I_WON"