حل تحدي OPCDE CTF Challenge

مازن احمد - mazin@mazinahmed.net

السلام عليكم

هذا المقال يتحدث عن حل تحدي OPCDE CTF challenge.
في البدأ, اود ان اشكر استاذ محمد الدوب على اقامة التحدي الجميل.

لنبدأ

https://twitter.com/Voulnet/status/973226280031318018

في بداية التحدي, قمت بتحميل الملف. الملف عبارة عن برنامج اندرويد بصيغة apk.

اول خطوة استخدمتها هي فك الملف. ملف apk هو عبارة عن ملف zip archive.

unzip ctf.apk

وجدت ملف مثير للاهتمام, يدعى ctf.png

نوعية الملف لا تبدو انها صورة, استعملت

```
$ file ctf.png
ctf.png: data
```

و في نفس الوقت, استعملت احد ادواتي المفضلة في اختبار برامج الأندرويد. البرنامج يدعى Mara Framework الاداة تقوم بعمل عدد من العمليات التي تستعمل للهندسة العكسية في برامج الاندرويد.

قمت بتحليل المعطيات و لم اجد شيّ.

فتأكدت من استاذ محمد اذا كنت في الطريق الصحيح, و في نفس الوقت نشر استاذ محمد تلميح

https://twitter.com/Voulnet/status/973334597965680641

XOR and BaseXX?

جميل جدا!

بمراجعة الملف hex بأستخدام ghex

ثم جربت ان فك ترميز الملف باستخدام base64 and base32

```
base64 -d ctf.png
base32 -d ctf.png
```

لكن لم تنجح المحاولة. ثم ركزت في تجربة طرق مختلفة لفك ترميز/تشفير الملف عن طريق xor

لم تكن لي تجربة وافرة مع xor, تعلمت مبادئها.

ثم عرفت ما احتاج وفقا للتحدي. احتاج الى اداة تقوم بقراءة الملف و تقوم بعملية تخمين للمفتاح.

جربت عدة ادوات و قارنت نتائجها للبحث عن الاداة التي تقوم باسترجاع الملف المقصود.

اداة xorbruteforcer قامت بعملية تخمين المفتاح و استرجاع الملف المقصود

http://eternal-todo.com/category/bruteforce

بعد تأكيد النتيجة, قمت باستعمال foremost لأستخراج محتويات الملف

```
foremost xor-output
```

وجدت ملف zip, قمت بفكه.

كان من احدى الملفات التي وجدتها ملف dalvik executable.

قمت بعمل هندسة عكسية بسيطة لاسترجاع الكود البرمجي, و اخدت اقرأ الملفات.

```
        public static final String qx = "ZmFsc2VmbGFnIDtQ";
```

```
$ echo -n 'ZmFsc2VmbGFnIDtQ' | base64 -d  ; echo
falseflag ;P
```

```
        public static final String f3b = "MFXG65DIMVZCAZTBNRZWKIDGNRQWO";
```

ترميز base32

“another false flag”

```
echo -n
'GRDDKMBUGM2DINBVGQZDIMRVGE2EMNCEGQ3TKRRUHE2UMNJXGRDDIRI=' |
base32 -d; echo
4F504344454242514F4D475F495F574F4E
```

و هي قيمة ascii hex, تساوي

OPCDEBBQOMG_I_WON

شكرا للقراءة :)
مازن احمد