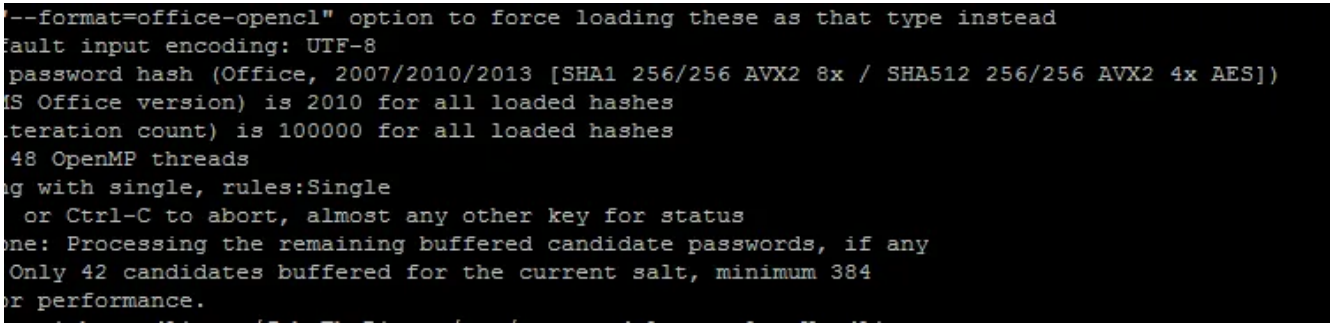
So Long, and Thanks for All the Fish

JUST SOME RANDOM THOUGHTS ABOUT THE MEANING OF LIFE, THE UNIVERSE, AND EVERYTHING

MENU



RECENT POSTS

How to upgrade BIOS on a Lenovo laptop running linux

October 8, 2019

My Weekly RoundUp #110

Cracking Microsoft Excel Documents using John The Ripper

Written by Andrea Fortuna • on March 20, 2019 • in Cybersecurity

Recently, during a forensic analysis on a laptop of an employee charged with corporate espionage, I've carved from disk a suspicious Excel file.

Obviously, the file was password protected, and I had to find a way to read it.

I did it,and now i'd like to share workflow for **XLSX** cracking.

What tools do i use?

The encryption algorithm of encrypted **Microsoft Excel** files is **40bit RC4**.
As it is encrypted nothing could be tweaked by opening the document with a hex editor.

The correct way is to extract the password hash from the file and then cracking it using **John The Ripper**.

October 7, 2019

Watch out! A new vulnerability in WhatsApp for Android allows attackers to perform remote commands on devices

October 4, 2019

Some thoughts about Windows 10 "Timeline" forensics artifacts

October 3, 2019

CATEGORIES

Select Category

For this purpose, you need to get a '**jumbo' build** of **John The Ripper**, that supports Office files cracking.

First, clone the git repository:

```
$ git clone https://github.com/magnumripper/JohnTheRipper.git
```

Then compile the sources:

```
$ cd JohnTheRipper/src

$ ./configure && make
```

If everything goes well, the executables for John and its related utilities will be created under "../run/".

Now, under "run" you can also find a python script, ***office2john.py***: you can use it for extract the hash from the encrypted XLSX file:

```
$ python office2john.py ./test.xlsx > hash.txt

$ cat hash.txt
test.xlsx:$office$2010100000128 16b1203fe2e498cec4d5452e1d0aea3775cd130baf73f5de29ec
```

Finally, you can start a bruteforce session with John The Ripper, maybe using a specific wordlist:

RECENT COMMENTS

Innocent Newton on PinMe: tracking a smartphone with localization services turned off

Tobiasz on A simple Windows code Injection example written in C#

What is the Point of a Virtual Machine? - Omghowto - Tutorials Related To Technology, Windows, Mac, iOS & Android on Commando VM: a full Windows-based penetration testing virtual machine distribution

Jake on How to mount an EWF image file (E01) on Linux

Stacey Atkinson on Some thoughts about Browser Fingerprinting

```
$ john --rules --wordlist=yourwordlist.txt hash.txt
```

Now, make a cup of coffee, sit back and wait for John to do its thing.

References

- John the Ripper password cracker
- magnumripper/JohnTheRipper

Related posts

TAGS

EXCEL JOHN THE RIPPER MICROSOFT

PRINT

Andrea Fortuna

My Weekly RoundUp #84

COMMENTS

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.