Laboratorio 3.2

Estudiante: Jorge Isaac Vásquez Valenciano

Cédula: 1-1711-0637

Se listan los documentos con clave que se trabajarán

```
┌──(kali㉿kali)-[/media/…/pen-testing/Especializacion UFIDELITAS/Modulo 3/Semana 3]
└─$ ls -d Clave*
Claves.docx  Claves.xlsx
```

Se genera el diccionario:

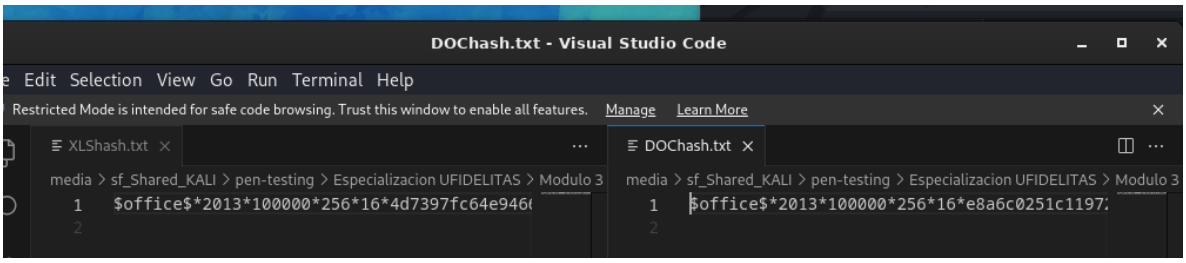
```
┌──(kali㉿kali)-[/media/…/pen-testing/Especializacion UFIDELITAS/Modulo 3/Semana 3]
└─$ crunch 6 6 87654321! -o ./diccionario.txt
Crunch will now generate the following amount of data: 3720087 bytes
3 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 531441

crunch: 100% completed generating output
```

Se ven los archivos necesarios según el laboratorio, utilizo grep para filtrar, ya que tengo todo el material de Semana 3 del módulo 3, en esa carpeta:

```
┌──(kali㉿kali)-[/media/…/pen-testing/Especializacion UFIDELITAS/Modulo 3/Semana 3]
└─$ ls | grep "Clave*\|.txt"
Claves.docx
Claves.xlsx
diccionario.txt
DOChash.txt
XLShash.txt
```

Se eliminan los encabezados de ambos archivos txt:



Inicializamos el hashcat

```
┌──(kali㉿kali)-[/media/…/pen-testing/Especializacion UFIDELITAS/Modulo 3/Semana 3]
└─$ hashcat -m 9600 -o ./DOCXCracked.txt DOChash.txt diccionario.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG)
 - Platform #1 [The pocl project]
==================================================================================================================
* Device #1: pthread-penryn-Intel(R) Core(TM) i9-10900KF CPU @ 3.70GHz, 5145/10354 MB (2048 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP
* Uses-64-Bit

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: diccionario.txt
* Passwords.: 531441
* Bytes.....: 3720087
* Keyspace..: 531441
```

Vemos que poco a poco el va realizando su scaneo, en esta etapa lleva 5.40%, es bastante tardado, hay que tener paciencia.

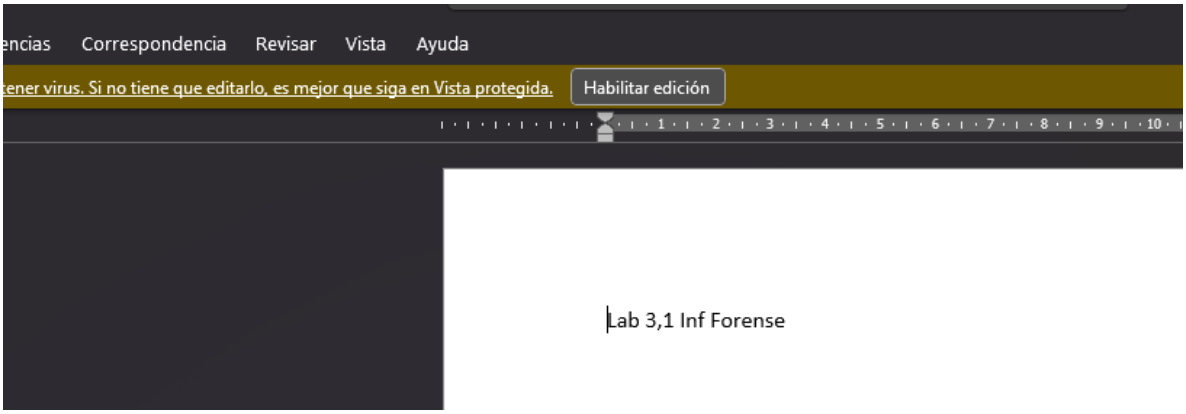
```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 9600 (MS Office 2013)
Hash.Target......: $office$*2013*100000*256*16*e8a6c0251c11972260e0c56...3221b6
Time.Started.....: Wed Jun 14 17:01:55 2023 (1 min, 57 secs)
Time.Estimated...: Wed Jun 14 17:37:30 2023 (33 mins, 38 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (diccionario.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      249 H/s (8.65ms) @ Accel:1024 Loops:256 Thr:1 Vec:2
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 28672/531441 (5.40%)
Rejected.........: 0/28672 (0.00%)
Restore.Point....: 28672/531441 (5.40%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:37632-37888
Candidate.Engine.: Device Generator
Candidates.#1....: 8456!1 -> 844234
Hardware.Mon.#1..: Util: 55%

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
```

Aquí ya terminó y podemos ver que da la contraseña

```
estricted Mode is intended for safe code browsing. Trust this window to enable all features.  Manage  Learn More
DOCXCracked.txt ×
media > sf_Shared_KALI > pen-testing > Especializacion UFIDELITAS > Modulo 3 > Semana 3 > DOCXCracked.txt
1   :c44b72bb80b0a17e0d*86935c27820f052f0ee934ee93019bd4584b937beb757055777a0acce73221 6:78542!
2
```

Podemos ver el interior del documento:



Ahora empezamos con el Archivo Excel

```
┌──(kali㉿kali)-[/media/…/pen-testing/Especializacion UFIDELITAS/Modulo 3/Semana 3]
└─$ hashcat -m 9600 -o ./XLSXCracked.txt XLShash.txt diccionario.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBU
 - Platform #1 [The pocl project]
=================================================================================================================
================================
* Device #1: pthread-penryn-Intel(R) Core(TM) i9-10900KF CPU @ 3.70GHz, 5145/10354 MB (2048 MB allocatable), 8M

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP
* Uses-64-Bit

Watchdog: Temperature abort trigger set to 90c
```

En el laboratorio utilizaba el modo 9800, pero no funciona así que volví a 9600 según la documentación:

```
 9500 | MS Office 2010                                          | Document
 9600 | MS Office 2013                                          | Document
25300 | MS Office 2016 - SheetProtection                        | Document
 9700 | MS Office <= 2003 $0/$1, MD5 + RC4                      | Document
 9710 | MS Office <= 2003 $0/$1, MD5 + RC4, collider #1         | Document
 9720 | MS Office <= 2003 $0/$1, MD5 + RC4, collider #2         | Document
 9810 | MS Office <= 2003 $3, SHA1 + RC4, collider #1           | Document
 9820 | MS Office <= 2003 $3, SHA1 + RC4, collider #2           | Document
 9800 | MS Office <= 2003 $3/$4, SHA1 + RC4                     | Document
18400 | Open Document Format (ODF) 1.2 (SHA-256, AES)           | Document
18600 | Open Document Format (ODF) 1.1 (SHA-1, Blowfish)        | Document
16200 | Apple Secure Notes                                      | Document
```

Y Aquí ya nos da la clave

```
XLSXCracked.txt - Visual Studio Code
File  Edit  Selection  View  Go  Run  Terminal  Help
XLXhash.txt   XLShash.txt   XLSXCracked.txt ×   Workspace Trust
media > sf_Shared_KALI > pen-testing > Especializacion UFIDELITAS > Modulo 3 > Semana 3 > XLSXCracked.txt
1  ı792753ee6bc422c3f7*be95a155cf660848fe91b733249f31de65b8a15611ab700c734d85fe4cd38b4::78542!
2
```

Archivo Inicio Insertar Disposición de página Fórmulas Da

VISTA PROTEGIDA Tenga cuidado: los archivos de Internet pueden con

D15 fx

	A	B	C	D
1				
2		Lab 3.2	Informatica Forense	
3				