INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2021-2022 – 1st Period

Digital Forensics Report

Fátima Napoleão - 91605

Miguel Henriques - 102148

Ielga Oliveira - 92479

1 Do you find any traces of the Football Leaks files on Mr. Daniels' computers?

Sim, começamos por analisar o **charlied_disk.img** com o comando **mmls charlied_disk.img** que devolve uma tabela com as partições existentes, a partição começa **no setor 1052672 (número 006 slot 001:00).**

```
┌──(fan㉿kali)-[~/Área de Trabalho/Lab2]
└─$ mmls charlied_disk.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  ------    0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0001050623   0001048576   Win95 FAT32 (0x0b)
003:  ------    0001050624   0001052671   0000002048   Unallocated
004:  Meta      0001052670   0020969471   0019916802   DOS Extended (0x05)
005:  Meta      0001052670   0001052670   0000000001   Extended Table (#1)
006:  001:000   0001052672   0020969471   0019916800   Linux (0x83)
```

Figura 1

Para acedermos a partição usamos o comando **fls -o 1052672 charlied_disk.img** que devolve uma lista com todas as diretorias e ficheiros existentes.

```
┌──(fan㉿kali)-[~/Área de Trabalho/Lab2]
└─$ fls -o 1052672 charlied_disk.img
d/d 393218:     home
d/d 11: lost+found
d/d 131073:     boot
r/r 12: swapfile
d/d 262145:     etc
d/d 393217:     media
l/l 13: bin
d/d 262147:     dev
l/l 14: lib
l/l 15: lib32
l/l 16: lib64
l/l 17: libx32
d/d 131075:     mnt
d/d 262148:     opt
d/d 393219:     proc
d/d 262149:     root
d/d 393220:     run
l/l 18: sbin
d/d 131076:     snap
d/d 393221:     srv
d/d 131077:     sys
d/d 262150:     tmp
d/d 131078:     usr
d/d 262151:     var
d/d 397985:     cdrom
V/V 622593:     $OrphanFiles
```

Figura 2

Em seguida utilizamos o comando **fls -o 1052672 charlied_disk.img -Frd charlied_disk.img** para identificar que ficheiros foram removidos.

```
r/r * 404856:   home/charlied/rhfc/drqoid.xsd
r/r * 397778:   home/charlied/rhfc/extract_instructions.txt
r/r * 397780:   home/charlied/rhfc/extract_tool.py
r/r * 398254:   home/charlied/rhfc/hawks_fc.zip
r/r * 398255:   home/charlied/rhfc/chants.zip
r/r * 399244:   home/charlied/rhfc/daft_punk.gif
r/r * 404851:   home/charlied/rhfc/discovery.jpg
r/r * 404852:   home/charlied/rhfc/hbfs.wav
r/r * 404853:   home/charlied/rhfc/homework.jpg
r/r * 404854:   home/charlied/rhfc/ram.jpg
r/r * 404855:   home/charlied/rhfc/SNA_Football_Lyrics.mp4
r/r * 404856:   home/charlied/rhfc/ticket.jpg
r/r * 397777:   home/charlied/rhfc/mydxwzfivvvaloc.zv
r/r * 404860:   home/charlied/rhfc/club_statement.pdf
r/r * 404861:   home/charlied/rhfc/data.zip
r/r * 404862:   home/charlied/rhfc/James_Santos_profile.pdf
r/r * 419418:   home/charlied/rhfc/chant2
r/r * 419448:   home/charlied/rhfc/chant1.wav
r/r * 419456:   home/charlied/rhfc/supporters_statement.pdf
r/r * 419418:   home/charlied/rhfc/club_memo.pdf
r/r * 404857:   home/charlied/rhfc/ozgivkdthslzms.nbv
r/r * 422938:   home/charlied/rhfc/secure_delete_commands.txt
```

Figura 3

Como se pode observar na **Figura 3** os ficheiros relativos ao footbal leaks foram removidos. Redirecionamos a nossa atenção para o **backup_disk.img** com o propósito de extrair estes ficheiros para comprovar a veracidade dos mesmos. Com o comando **mmls backup_disk.img** identificamos que a partição começa no setor 2048 (número 002, slot 000:000). Com o comando **fls -o backup_disk.img 2048,** começamos por analisar a home:

- **fls -o 2048 backup_disk.img 12**
    - **fls -o 2048 backup_disk.img 168820**

```
┌──(fan㉿kali)-[~/Área de Trabalho/Lab2]
└─$ fls -o 2048 backup_disk.img 12
d/d 168820:     charlied

┌──(fan㉿kali)-[~/Área de Trabalho/Lab2]
└─$ fls -o 2048 backup_disk.img  168820
r/r 168821:     .bashrc
r/r 168822:     .bash_logout
r/r 168824:     .profile
r/r 142948:     .Xauthority
r/r 136726:     .xsession-errors
d/d 143005:     Desktop
d/d 143006:     Downloads
d/d 143007:     Templates
d/d 143008:     Public
d/d 143009:     Documents
d/d 143010:     Music
d/d 143011:     Pictures
d/d 143012:     Videos
d/d 143013:     .config
d/d 143853:     .dbus
d/d 144007:     .cache
r/r 144085:     .xscreensaver
d/d 144281:     .local
r/r 136657:     .bash_history
r/r 143004:     .xsession-errors.old
r/r 144586:     .sudo_as_admin_successful
d/d 144372:     .ssh
r/r 168635:     backup_1634405485.zip
r/r 168617:     francesinha.html
r/r 168638:     .dmrc
r/r * 168650(realloc):  .backup_1634414401.zip.sF7OoH
r/r 168646:     backup_1634412601.zip
r/r 168650:     backup_1634414401.zip
```

Identicamos estes três backups (zip) que tentamos extrair, mas não conseguimos pois requerem uma password.

Figura 4

Retrocedemos um passo e voltamos a analisar o **charlied_disk.img.** Começamos por explorar a home, fls **-o 1052672 charlied_disk.img 393218 (ver fig1),** em seguida a diretoria **charlied (434942)**. Dentro desta, analisámos todas as diretorias, destacando-se as diretorias **password_gen, crown_manager e irclogs.**

- **Password_gen (420001):** encontramos estes dois ficheiros (seeds.txt e obfuscator) em que o obfuscator é um ficheiro - python3 que o descompilamos usando a tool – https://www.decompiler.com/

  Para extrair os ficheiros usamos o comando **icat -o 1052672 charlied_disk.img** 557188 **>** seeds.txt.tgz. 557188. Numa primeira abordagem descartamos estes dois ficheiros e prosseguimos para o **Cron_manager.**

- **Cron_manager (419601):** encontramos três ficheiros removidos e um script (backup.sh). O backup.sh tem indicações de como é gerada a palavra-passe de cada backup, utilizando assim como recursos o obfuscator, o time-stamp de cada backup e por último o seed.txt que é um ficheiro com caracteres ASCII.

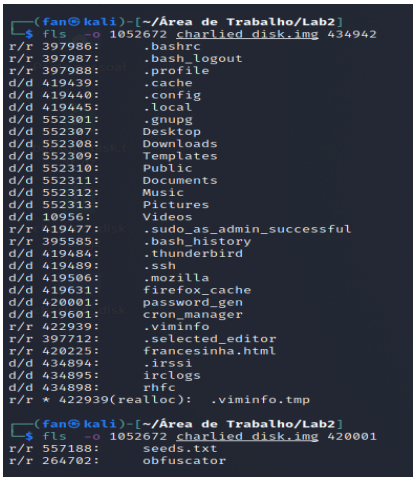

Figura 5

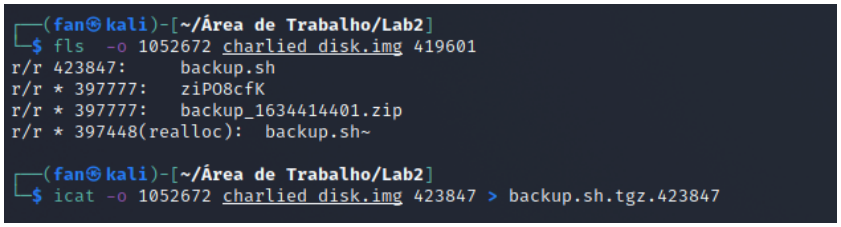

Figura 5 1

Passamos então a analisar o funcionamento do obfuscator, concluímos que a medida que corríamos o seeds.txt, ele alterava-se passando sempre a primeira linha para última. Assim o último backup corresponde a última linha do seeds.txt. Para descobrir a palavra-passe do último backup:

1. convertemos os Unix TimeStamp para o tempo real para identificar o último backup **(backup_1634414401.zip)** usando a tool https://www.unixtimestamp.com/index.php
2. passamos a última linha do seed.txt para primeira
3. corremos o obfuscator **python obfuscator.py 1634414401** e este gerou a palavra-passe e64b1b6ba974f1b1097d767175ff7adaad0cb17caff3f71683cfa7362764ebe4

Seguimos a mesma lógica para os outros dois backups tendo como palavra-passe:

- **(backup_1634412601.zip)** - 0b70142bc4d6bb1a78a0466c4986d18b5e2383f69d0a017f280a5d16c1177a9b
- **(backup_1634405385.zip)** - 8c34a71b8ae5c67a2ee309622f4ae28bdcc838f76cf924c994b8b9d719d684ae

Analisámos a **pasta rhfc** nos três backups e encontrámos no backup das 20:30h (backup_1634412601) todos os artefactos que estavam na pen-drive. Comparámos os md5sum destes artefactos com os originais e, concluímos que a maioria dos md5sum são os mesmos exceto os de ficheiro de áudio. Esta diferença é devido a maneira como extraímos estes no primeiro laboratório. O que comprova que estes são os ficheiros que encontramos no primeiro lab.

2 If so, can you track the source of these files and how they have been manipulated over time? Establish a timeline of relevant events.

Ao analisarmos os ficheiros do backup_1634412601, encontrámos no irclogs , um ficheiro (chapman13.10-16.log) aberto **num sábado,** precisamente no dia **16 de Outubro às 18:13:51,** que revela uma conversa entre Daniels e uma outra pessoa que trabalha no departamento de IT da Red Hawks, ao longo da conversa esta pessoa afirmou ter tirado todos os artefactos do computador do presidente da Red Hawks, Velluci, e que encontraria com Daniels para lhe entregar uma pen drive onde provavelmente estariam os documentos extraídos do computador de Velluci. **As 18:19, no dia e mês em questão** Daniels, fez o downloa de uma tool, que lhe ia permitir aceder aos ficheiros da Red Hawks sem que ninguém suspeitasse. **Às 18:29:45**, Daniels fez o primeiro backup (backup_1634405385), onde se encontravam as instruções de como obter os artefactos. Constatou-se ainda que foi feito plug-in desta mesma pen drive no computador de Daniels ainda no dia **16 de Outubro, às 19:07:30,** facto este identificado por nós, após compararmos o serial number da pen com o histórico de log do sistema (syslog). Após isto, **às 20:30:01** Daniels faz o segundo seu backup (backup_1634412601), backup este que já possuía os ficheiros em causa. **No dia 16, às 21:00:01**, Daniels fez o último backup (backup_1634414401), e neste os artefactos já haviam sido todos removidos.

Analisamos também a cache do Daniels e de facto confirma-se que fez o download da tool que o "Chapman13" o enviou, confirma-se o post que fez no wordpress bem como a pesquisa no Google sobre como apagar ficheiros. Para tal recorremos ao comando **icat -o 1052672 charlied_disk.img 422576 > filesearch.txt** (**Filesearch** que consta no histórico de pesquisas que foi apagado), para obtermos o ficheiro correspondente a pesquisa que Daniels efetuou de como apagar ficheiros de forma segura. Esta pesquisa foi feita **sábado 16 de outubro às 20:11:38.**

3 Do you find any evidence of anti-forensic activity?

Sim. Tal como se verificou, no último backup de Daniels não havia mais ficheiro algum, uma vez que já havia removido os zips, usando o comando **rm $ZIPFILE**, presente no script (backup.sh) que o mesmo utilizou para gerar as passwords de seus backups.

Na conversa do ficheiro (chapman13.10-16.log), também foi dito a Daniels que escondesse todos os ficheiros dentro de outros. Entretanto, no histórico do firefox, verificou-se também que Daniels procurou por formas de apagar ficheiros permanentemente (**filesearch**).

Foram ainda encontradas três imagens AF, AF2, AF3, na pasta **entries da cahe do firefox** de Daniels, vinculadas a remoção.

4 What can you tell about the identity of the person(s) involved in the leakage of the files?

Analisando a conversa (chapman13.10-16.log) entre Daniels e o responsável pela fuga dos ficheiros, verificamos alguns pontos que nos podem levar a uma identidade deste. Primeiro, o responsável pela fuga trabalhou no departamento de IT da Red Hawks, o que nos leva a perceber que era um indivíduo com algum conhecimento na área. Segundo, o seu posicionamento é o de um indivíduo que reprova qualquer tipo de enriquecimento ilícito e que faria o necessário para que pessoas com este histórico fossem expostas, como é o caso de Velluci. E ainda por intermédio desta conversa, o responsável da fuga também identificado como "abby" por Daniels, menciona ser uma pessoa que tem o prazer em aceder a sistemas alheios. Após todos estes factos, pareceu-nos credível suspeitar que o responsável se tratasse de um hacker, ou um whistleblower, um indivíduo movido por ideais válidos.