Challenge Forensic

Journées FedeRez 2011

Thomas Duboucher
thomas@duboucher.eu

19 Mars 2011

Obtenir l'archive

L'image est disponible sur

http ://journees.federez.net/media/forensic.enc

```
root@0:~# md5sum forensic.enc
4db8cbac0c0850379d9f6c2f0ade7108  forensic.enc
```

Obtenir l'archive

L'image est disponible sur

http ://journees.federez.net/media/forensic.enc

```
root@0:~# md5sum forensic.enc
4db8cbac0c0850379d9f6c2f0ade7108  forensic.enc
```

En cas de soucis

- si vous n'arrivez pas à accéder au réseau Wi-fi, l'image peut être transférée sur clef USB ;
- si vous n'arrivez pas à commencer, c'est que l'image est chiffrée, la clef sera donnée après.

Objectifs

Votre « *expertise* » est mise à contribution au cours d'une enquête

Un employé est soupçonné d'avoir transmis à plusieurs reprises des informations confidentielles à un concurrent via internet. Cependant, l'enquête n'a pas encore permis de montrer comment.
Une clef USB avait été saisie lors de la perquisition de son bureau et écartée par les enquêteurs car elle n'était pas « *lisible sous Windows* ».

Votre objectif est d'analyser le contenu de cette clef

Quatre *flags* sous la forme `FLG[1-4][0-9a-f]{8}` sont présent sur cette clef pour marquer votre avance dans l'analyse.

Ouvrir l’archive

Pour déchiffrer

```
root@0:~# openssl enc -d -aes-256-cbc -in forensic.enc -out forensic.img
enter aes-256-cbc decryption password:
```

Ouvrir l’archive

Pour déchiffrer

```
root@0:~# openssl enc -d -aes-256-cbc -in forensic.enc -out forensic.img
enter aes-256-cbc decryption password:
```

La clef

Yfbc1plF

Ouvrir l’archive

Pour déchiffrer

```
root@0:~# openssl enc -d -aes-256-cbc -in forensic.enc -out forensic.img
enter aes-256-cbc decryption password:
```

La clef

Yfbc1plF

En cas de soucis

- si vous n’arrivez pas à déchiffrer l’image, vous pouvez demander à votre voisin.

Bon jeu ! =)

Challenge Forensic

Journées FedeRez 2011

Thomas Duboucher
thomas@duboucher.eu

18 *mars* 2011

Décompression de l’archive

Explications

- L’image a été comprimée à l’aide de `gzip`...
- et était en fait une *tarball*.
- On obtient à la fin l’image de la clef USB.

Console

```
root@0:~# file forensic.img
forensic.img: gzip compressed data, from Unix
```

Décompression de l’archive

Explications

- L’image a été comprimée à l’aide de `gzip`…
- et était en fait une *tarball*.
- On obtient à la fin l’image de la clef USB.

Console

```
root@0:~# file forensic.img
forensic.img: gzip compressed data, from Unix
root@0:~# mv forensic.img forensic.gz && gzip -d forensic.gz
```

Décompression de l'archive

Explications

- L'image a été comprimée à l'aide de `gzip`…
- et était en fait une *tarball*.
- On obtient à la fin l'image de la clef USB.

Console

```
root@0:~# file forensic.img
forensic.img: gzip compressed data, from Unix
root@0:~# mv forensic.img forensic.gz && gzip -d forensic.gz
root@0:~# file forensic
forensic: POSIX tar archive (GNU)
```

Décompression de l’archive

Explications

- L’image a été comprimée à l’aide de `gzip`…
- et était en fait une *tarball*.
- On obtient à la fin l’image de la clef USB.

Console

```
root@0:~# file forensic.img
forensic.img: gzip compressed data, from Unix
root@0:~# mv forensic.img forensic.gz && gzip -d forensic.gz
root@0:~# file forensic
forensic: POSIX tar archive (GNU)
root@0:~# tar xvf forensic
usb.img
```

Première analyse

Explications

- `file` montre la présence d'un secteur d'amorçage.
- `parted` confirme l'absence de la première partition.
- La seconde partition n'est pas identifiée par `parted`

Console

```
root@0:~# file usb.img
usb.img: x86 boot sector; partition 2: ID=0x83, starthead 24, startsector 387072, 137216
      ↪sectors, code offset 0x31
```

Première analyse

Explications

- file montre la présence d'un secteur d'amorçage.
- parted confirme l'absence de la première partition.
- La seconde partition n'est pas identifiée par parted

Console

```
root@0:~# parted usb.img print
Model:  (file)
Disk usb.img: 268MB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start   End     Size    Type     File system  Flags
 2      198MB   268MB   70.3MB  primary
```

Analyse du MBR

Explications

- L'analyse du premier secteur montre la présence d'un *bootloader*.
- La première partition a été proprement supprimée de la table.
- L'indicateur d'amorçage 55 AA est présent.

Console

```
root@0:~# dd if=usb.img of=/dev/stdout bs=512 count=1 |hexdump -C
1+0 records in
1+0 records out
512 bytes (512 B) copied, 0.000153162 s, 3.3 MB/s
```

Analyse du MBR

Explications

- L'analyse du premier secteur montre la présence d'un *bootloader*.
- La première partition a été proprement supprimée de la table.
- L'indicateur d'amorçage 55 AA est présent.

Console

```
00000000  fa 31 c0 8e d8 8e d0 bc  00 7c 89 e6 06 57 8e c0  |.1.......|...W..|
00000010  fb fc bf 00 06 b9 00 01  f3 a5 ea 1f 06 00 00 52  |...............R|
00000020  52 b4 41 bb aa 55 31 c9  30 f6 f9 cd 13 72 13 81  |R.A..U1.0....r..|
00000030  fb 55 aa 75 0d d1 e9 73  09 66 c7 06 8d 06 b4 42  |.U.u...s.f.....B|
00000040  eb 15 5a b4 08 cd 13 83  e1 3f 51 0f b6 c6 40 f7  |..Z......?Q...@.|
00000050  e1 52 50 66 31 c0 66 99  e8 66 00 e8 21 01 4d 69  |.RPf1.f..f..!.Mi|
00000060  73 73 69 6e 67 20 6f 70  65 72 61 74 69 6e 67 20  |ssing operating |
00000070  73 79 73 74 65 6d 2e 0d  0a 66 60 66 31 d2 bb 00  |system...f f1...|
```

Analyse du MBR

Explications

- L'analyse du premier secteur montre la présence d'un *bootloader*.
- La première partition a été proprement supprimée de la table.
- L'indicateur d'amorçage 55 AA est présent.

Console

```
00000180  ac b4 0e 8a 3e 62 04 b3  07 cd 10 3c 0a 75 f1 cd  |....>b.....<.u..|
00000190  18 f4 eb fd 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000001a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000001b0  00 00 00 00 00 00 00 00  a2 05 0b 00 00 00 00 00  |................|
000001c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 18  |................|
000001d0  01 18 83 a2 02 20 00 e8  05 00 00 18 02 00 00 00  |..... ..........|
000001e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000001f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 aa  |..............U.|
```

Analyse de l'image

Explications

- Une analyse avec `strings` nous permet de retrouver des traces...
- mais aussi les chaînes `lost+found`, `extlinux` et `finnix`.
- Le premier *flag* est là !

Console

```
root@0:~# strings -tx usb.img |head -n 20
     51 RPf1
     5e Missing operating system.
     79 f f1
     80 |fRfP
     dc Ht[y9Y[
    11d Multiple active partitions.
    161 Operating system load error.
```

Analyse de l'image

Explications

- Une analyse avec `strings` nous permet de retrouver des traces…
- mais aussi les chaînes `lost+found`, `extlinux` et `finnix`.
- Le premier *flag* est là !

Console

```
100132 +fRfP
10015b 2}+f f
1001cc Boot error
100469 &eH><B
180020 lost+found
180034 extlinux
180044 finnix
180054 FLG1e98300fc
```

Récupération de la partition #1

Explications

- Il est possible de reconstruire la partition avec `parted`.
- Utiliser un disque d'une machine virtuelle est une solution pratique.
- Un outil plus avancé comme `testdisk` apporte beaucoup plus d'informations.

Console

```
root@0:~# cat usb.img >/dev/sdX
```

Récupération de la partition #1

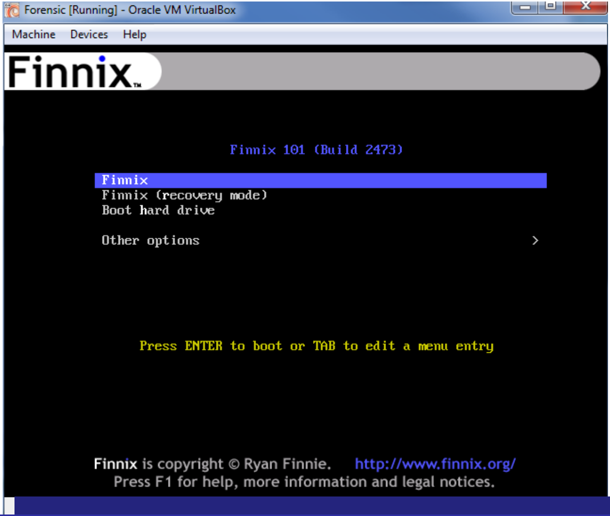
Explications

- Il est possible de reconstruire la partition avec `parted`.
- Utiliser un disque d'une machine virtuelle est une solution pratique.
- Un outil plus avancé comme `testdisk` apporte beaucoup plus d'informations.

Console

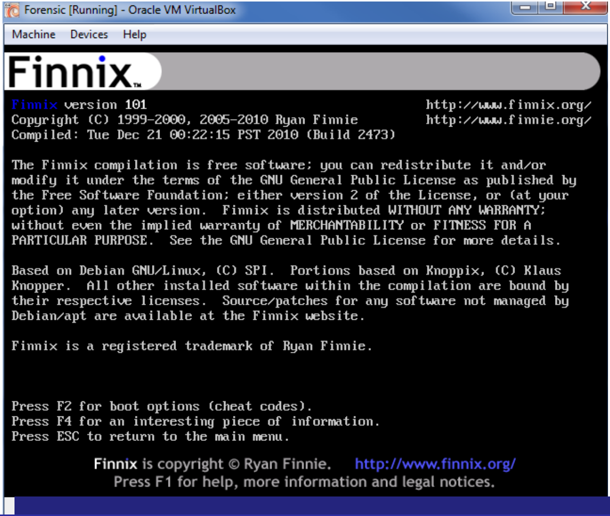
```
root@0:~# cat usb.img >/dev/sdX
root@0:~# parted /dev/sdX mkpart primary 1 198M
Information: You may need to update /etc/fstab.
root@0:~# parted /dev/sdX set 1 boot on
Information: You may need to update /etc/fstab.
```

Démarrons cette clef !



```
Finnix 101 (Build 2473)

Finnix
Finnix (recovery mode)
Boot hard drive

Other options                                   >

Press ENTER to boot or TAB to edit a menu entry

Finnix is copyright © Ryan Finnie.     http://www.finnix.org/
Press F1 for help, more information and legal notices.
```

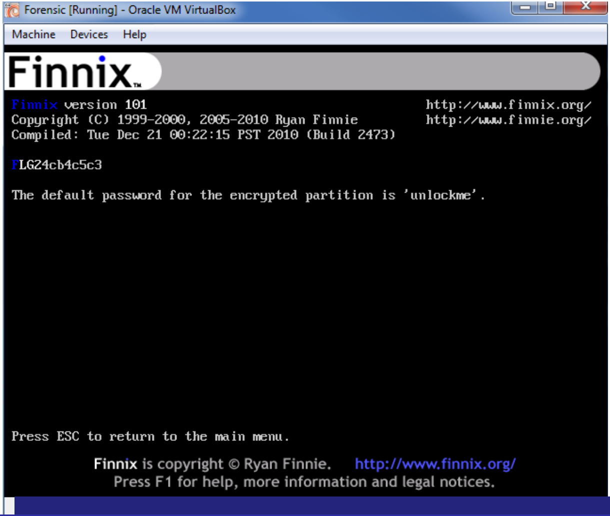
Démarrons cette clef !



```
Finnix version 101                                   http://www.finnix.org/
Copyright (C) 1999-2000, 2005-2010 Ryan Finnie       http://www.finnie.org/
Compiled: Tue Dec 21 00:22:15 PST 2010 (Build 2473)

The Finnix compilation is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or (at your
option) any later version.  Finnix is distributed WITHOUT ANY WARRANTY;
without even the implied warranty of MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.  See the GNU General Public License for more details.

Based on Debian GNU/Linux, (C) SPI.  Portions based on Knoppix, (C) Klaus
Knopper.  All other installed software within the compilation are bound by
their respective licenses.  Source/patches for any software not managed by
Debian/apt are available at the Finnix website.

Finnix is a registered trademark of Ryan Finnie.



Press F2 for boot options (cheat codes).
Press F4 for an interesting piece of information.
Press ESC to return to the main menu.
```

Finnix is copyright © Ryan Finnie. http://www.finnix.org/
Press F1 for help, more information and legal notices.

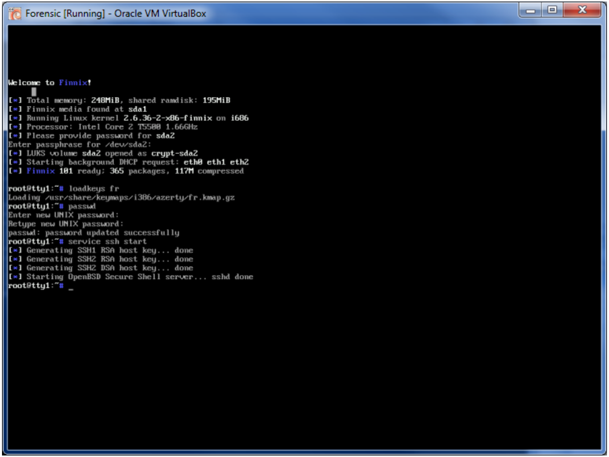
Démarrons cette clef !



```
Finnix version 101                                  http://www.finnix.org/
Copyright (C) 1999-2000, 2005-2010 Ryan Finnie      http://www.finnie.org/
Compiled: Tue Dec 21 00:22:15 PST 2010 (Build 2473)

FLG24cb4c5c3

The default password for the encrypted partition is 'unlockme'.







Press ESC to return to the main menu.
```

Finnix is copyright © Ryan Finnie. http://www.finnix.org/
Press F1 for help, more information and legal notices.

Et ouvrons cette partition !



```
Welcome to Finnix!

[*] Total memory: 248MiB, shared ramdisk: 195MiB
[*] Finnix media found at sda1
[*] Running Linux kernel 2.6.36-2-x86-finnix on i686
[*] Processor: Intel Core 2 T5500 1.66GHz
[*] Please provide password for sda2
Enter passphrase for /dev/sda2:
[*] LUKS volume sda2 opened as crypt-sda2
[*] Starting background DHCP request: eth0 eth1 eth2
[*] Finnix 101 ready; 365 packages, 117M compressed

root@tty1:~# loadkeys fr
Loading /usr/share/keymaps/i386/azerty/fr.kmap.gz
root@tty1:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@tty1:~# service ssh start
[*] Generating SSH1 RSA host key... done
[*] Generating SSH2 RSA host key... done
[*] Generating SSH2 DSA host key... done
[*] Starting OpenBSD Secure Shell server... sshd done
root@tty1:~# _
```

Analyse de la partition chifrée

Explications

- Maintenant nous avons même accès à la seconde partition.
- Des fichiers, des fichiers, et des paquets…
- Regardons ça de plus près…

Console

```
root@0:/media# mount /dev/mapper/crypt-sda2 /media/sda2/
root@0:/media# cd /media/sda2/
root@0:/media/sda2# ls
data  lost+found  vpn
root@0:/media/sda2# cd vpn/
root@0:/media/sda2/vpn# ls
FLG3179ed03e                       openvpn-blacklist_0.4_all.deb
openssl-blacklist_0.5-2_all.deb   openvpn_2.1.3-2_i386.deb
```

Analyse de la partition chifrée

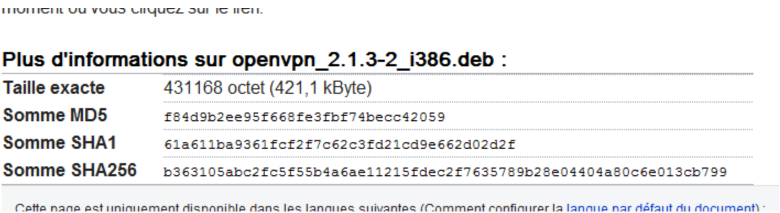
Explications

- Maintenant nous avons même accès à la seconde partition.
- Des fichiers, des fichiers, et des paquets…
- Regardons ça de plus près…

Console

```
root@0:/media/sda2# cd vpn/
root@0:/media/sda2/vpn# ls
FLG3179ed03e                 openvpn-blacklist_0.4_all.deb
openssl-blacklist_0.5-2_all.deb  openvpn_2.1.3-2_i386.deb
root@0:/media/sda2/vpn# md5sum *.deb
c633e29fdb1ad514c4d7cced506229b1  openssl-blacklist_0.5-2_all.deb
e51868662dee74f31faae0bffb795892  openvpn-blacklist_0.4_all.deb
5c8c53eb10c4cb7446c824e4372b111c  openvpn_2.1.3-2_i386.deb
```

Wut ! ?



moment où vous cliquez sur le lien.

Plus d'informations sur openvpn_2.1.3-2_i386.deb :

Taille exacte	431168 octet (421,1 kByte)
Somme MD5	`f84d9b2ee95f668fe3fbf74becc42059`
Somme SHA1	`61a611ba9361fcf2f7c62c3fd21cd9e662d02d2f`
Somme SHA256	`b363105abc2fc5f55b4a6ae11215fdec2f7635789b28e04404a80c6e013cb799`

Cette page est uniquement disponible dans les langues suivantes (Comment configurer la langue par défaut du document) :

Analyse du paquet modifié

Explications

- Regardons en détails ce paquet.
- Quelques fichiers sont de trop.
- Et voila notre dernier *flag*.

Console

```
root@0:/media/sda2/vpn# ar x openvpn_2.1.3-2_i386.deb
root@0:/media/sda2/vpn# tar xzvf data.tar.gz
...
./etc/init.d/openvpn
./etc/openvpn/
./etc/openvpn/vpn.conf
./etc/openvpn/update-resolv-conf
./etc/openvpn/FLG40475d41b
```

Analyse du paquet modifié

Explications

- Regardons en détails ce paquet.
- Quelques fichiers sont de trop.
- Et voila notre dernier *flag*.

./etc/openvpn/vpn.conf

```
remote 160.228.159.254 9000
proto udp
dev tun0
ifconfig 192.168.254.2 192.168.254.1
cipher BF-CBC
comp-lzo
secret /etc/openvpn/FLG40475d41b
```

Questions

?