

Cómo dumpear las claves SSH desde el firmware de un router

Publicado por Vicente Motos on jueves, 19 de febrero de 2015 Etiquetas: [ingeniería inversa](#), [redes](#), [shodan](#), [técnicas](#), [tutoriales](#), [vulnerabilidades](#)

Algunos me preguntáis como sacar las claves ssh de los routers en referencia a la [entrada](#) de anoche. Os veo venir... pero bueno, veremos rápidamente como hacerlo extrayendo la imagen del firmware de un router ;)



En esta ocasión sin embargo vamos a dejar al *pobre* Comtrend VG-8050 y vamos a ir a por el **D-Link Dsl-2750u** (*la belleza de la derecha*). En concreto vamos a echar un vistazo a una de las versiones de firmware que también viene con un demonio [Dropbear 0.46](#) con "premio": la **ME_1.11** de octubre de 2013:

http://www.dlinkmea.com/partner/media/product_item_downloadables/1351-DSL2750U-U1_FW1.11.rar

Después de descargar los menos de 7mb que ocupa el rar, lo descomprimimos y analizamos la imagen con [Binwalk](#), el estándar de facto para el análisis de firmwares:

```
root@kali:~/firmwares# file GAN9.9T113A-B-DL-DSL2750U-R5B0024-
Dubai.EN_2T2R_text_for_lan_update.img
GAN9.9T113A-B-DL-DSL2750U-R5B0024-
Dubai.EN_2T2R_text_for_lan_update.img: data

root@kali:~/firmwares# binwalk GAN9.9T113A-B-DL-DSL2750U-R5B0024-
Dubai.EN_2T2R_text_for_lan_update.img

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          LZMA compressed data, properties: 0x5D, dictionary
size: 8388608 bytes, uncompressed size: 5402908 bytes
1722624      0x1A4900     Squashfs filesystem, little endian, version 4.0,
compression:lzma, size: 5080877 bytes, 1142 inodes, blocksize: 262144 bytes,
created: Thu Oct 24 07:46:30 2013
```

Como veis el filesystem es [SquashFS](#), uno de los más ampliamente utilizados en sistemas con Linux embebido, y está comprimido con LZMA en lugar del estandar zlib (algo que también suelen hacer):

```
root@kali:~# binwalk --dd='squashfs:squashfs' GAN9.9T113A-B-DL-DSL2750U-R5B0024-Dubai.EN_2T2R_text_for_lan_update.img
```

| DECIMAL | HEXADECIMAL | DESCRIPTION |
|---------|-------------|-------------|
|---------|-------------|-------------|

| | | |
|---------|----------|---|
| 0 | 0x0 | LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 5402908 bytes |
| 1722624 | 0x1A4900 | Squashfs filesystem, little endian, version 4.0, compression:lzma, size: 5080877 bytes, 1142 inodes, blocksize: 262144 bytes, created: Thu Oct 24 07:46:30 2013 |

```
root@kali:~/_GAN9.9T113A-B-DL-DSL2750U-R5B0024-Dubai.EN_2T2R_text_for_lan_update.img.extracted# file 1A4900.squashfs
1A4900.squashfs: Squashfs filesystem, little endian, version 4.0, 5080877 bytes, 1142 inodes, blocksize: 262144 bytes, created: Thu Oct 24 07:46:30 2013
```

El siguiente paso es extraer la imagen y, para ello, vamos a instalar y utilizar la utilidad [unsquashfs-2.1](#) de Jeremy Collake:

```
apt-get install liblzo2-dev
git clone https://github.com/devttyS0/sasquatch
make

root@kali:~/_GAN9.9T113A-B-DL-DSL2750U-R5B0024-Dubai.EN_2T2R_text_for_lan_update.img.extracted# ./sasquatch/sasquatch
1A4900.squashfs
SquashFS version [4.0] / inode count [1142] suggests a SquashFS image of the same endianness
Parallel unsquashfs: Using 1 processor
Trying to decompress using default lzma decompressor...
Successfully decompressed with default lzma decompressor
1083 inodes (1113 blocks) to write

[=====
=====] 1113/1113 100%

created 679 files
created 59 directories
created 123 symlinks
```

```
created 281 devices
created 0 fifos
```

Ahora veremos el filesystem colgando del directorio squashfs-root, por lo que sólo tenemos que ir a pescar nuestras claves...

```
root@kali:~/firmwares/_GAN9.9T113A-B-DL-DSL2750U-R5B0024-
Dubai.EN_2T2R_text_for_lan_update.img.extracted# cd squashfs-
root/etc/dropbear/
root@kali:~/firmwares/_GAN9.9T113A-B-DL-DSL2750U-R5B0024-
Dubai.EN_2T2R_text_for_lan_update.img.extracted/squashfs-
root/etc/dropbear# ls -las
total 16
4 drwxr-xr-x  2 594 594 4096 Oct 24  2013 .
4 drwxr-xr-x 10 594 594 4096 Oct 24  2013 ..
4 -rwxr-xr-x  1 594 594  459 Oct 24  2013 dropbear_dss_host_key
4 -rwxr-xr-x  1 594 594  427 Oct 24  2013 dropbear_rsa_host_key
```

... y con la herramienta [dropbearkey](#) mostrar la clave pública:

```
root@kali:~/firmwares/_GAN9.9T113A-B-DL-DSL2750U-R5B0024-
Dubai.EN_2T2R_text_for_lan_update.img.extracted/squashfs-
root/etc/dropbear# dropbearkey -y -f dropbear_rsa_host_key
Public key portion is:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQgWCAmPVBs6DX2/2G6NcLwFI6jP055kbQzx
GNNaYngPhR3TT9MMiGnR2waCQYrZq0n7D+RKu9tEiYU05tPiaMqm5z4qHq2OePK
IL4jFhcTJk8p0yz1IpPp9FJjvZ6Daw4Mvr+r+RNNnSTn7Iq7bIxWyNgXnQc7Lx7IPm
m8JDqskFEtOC7 root@kali
Fingerprint: md5 63:05:01:4f:cd:09:6d:ad:ed:95:ae:89:19:2c:b8:bc
```

Finalmente sólo nos queda buscar el fingerprint correspondiente:

[Link shodan](#)

Shodan Scanhub Developers View All...

SHODAN 63:05:01:4f:cd:09:6d:ad:ed:95:ae:09:19:2c:b8:bc Q Explore Contact Us Blog New to Shodan

Exploits Maps

TOP COUNTRIES

Showing results 1 - 10 of 42,904

218

Colombia Telecomunicaciones S.A. Esp

Added on 2015-02-18 02:20:28 GMT

Colombia

Details

SSH-2.0-dropbear_0.51

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQCAmPVbs6DX2/2G6NclwF16jP055kbQzxGNlaYngPhR3TT9

MW1GrR2waCQYrZq0nTD+RKu9tE1YU05tPiaMqm5z4qHq20ePKIL4jfhcTJk8p0yz1IpPp9F3jvZ6

Daw4Mvr+r+RNWnSTn7Iq7bIXWlyNgXnQc7Lx7IPmm8JDqskFEt0C7

Fingerprint: 63:05:01:4f:cd:09:6d:ad:ed:95:ae...

Thailand 15,238

Colombia 7,531

Argentina 6,516

India 3,584

Iran, Islamic Republic of 3,135

TOP SERVICES

SSH 42,880

2222 24

TOP ORGANIZATIONS

55

TOT Public Company Limited 11,591

Telefonica de Argentina 6,312

Telecomunicaciones S.A. Esp 5,066

TOT 3,320

Colombia Telecomunicaciones ... 1,330

SSH-2.0-dropbear_0.51

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQCAmPVbs6DX2/2G6NclwF16jP055kbQzxGNlaYngPhR3TT9

MW1GrR2waCQYrZq0nTD+RKu9tE1YU05tPiaMqm5z4qHq20ePKIL4jfhcTJk8p0yz1IpPp9F3jvZ6

Daw4Mvr+r+RNWnSTn7Iq7bIXWlyNgXnQc7Lx7IPmm8JDqskFEt0C7

Fingerprint: 63:05:01:4f:cd:09:6d:ad:ed:95:ae...

y tenemos otros 40.000 equipos cuyas comunicaciones podremos descifrar :)



5 comentarios :

1.

[Anónimo19 de febrero de 2015, 18:57](#)

Muy bueno :-O y gracias por el ejemplo

[Responder](#)



2.

[Emilio Nahuel20 de febrero de 2015, 8:56](#)

Qué hay de las claves privadas(si hay alguna)? También están duplicadas?

[Responder](#)

[Respuestas](#)



[Vicente Motos](#)20 de febrero de 2015, 11:31

Estoy hablando en alto, pero si no me equivoco, el par de claves RSA está en dropbear_rsa_host_key... y sí, estan también duplicadas...

[Responder](#)

3.

[Anónimo](#)20 de febrero de 2015, 10:30

Si tienes la clave pública pero no la privada, ¿Cómo puedes conectarte por ssh? ¿No necesitarías la privada?

[Responder](#)

[Respuestas](#)



[Vicente Motos](#)20 de febrero de 2015, 11:32

hasta donde yo sé Dropbear no está configurado por defecto para acceder con claves asimétricas por lo que tener las claves duplicadas te permitirá "sólo" descifrar el tráfico al vuelo.