

Episodio 3 - La bomba

Challenge

0 Solves

X

EPISODIO 3

300


Con todo el dinero robado, necesitamos escapar dando una distracción a la policía. Para ello, necesitamos encontrar la bomba programada en el firmware del sistema informático. Una vez resuelta, podremos acceder al servidor donde tras buscar bien, conseguiremos la flag final.

Info: La flag tiene el formato UAM{md5}

TOP 3: 1. 2. 3.

Unlock Hint for 20 points

Unlock Hint for 30 points

 firmware.zip

Flag

Submit

Estamos a punto de escapar con el dinero y solo falta conseguir la flag final. Para ello necesitamos encontrar la bomba oculta en el firmware.

Bajo firmware.zip y a descomprimir...

Aparece un fichero: backup.raw


Hago un file backup.raw para saber qué es:

```
$ file backup.raw
backup.raw: Linux rev 1.0 ext4 filesystem data, UUID=046b9ae6-97df-49fd-8785-2c68de053b05 (needs journal recovery) (ext
ents) (large files) (huge files)
```

Es la imagen de una partición ext4. Probaré a montarla...

```
mkdir /media/j0n3/ctf
sudo mount -t ext4 ../backup.raw /media/j0n3/ctf
```

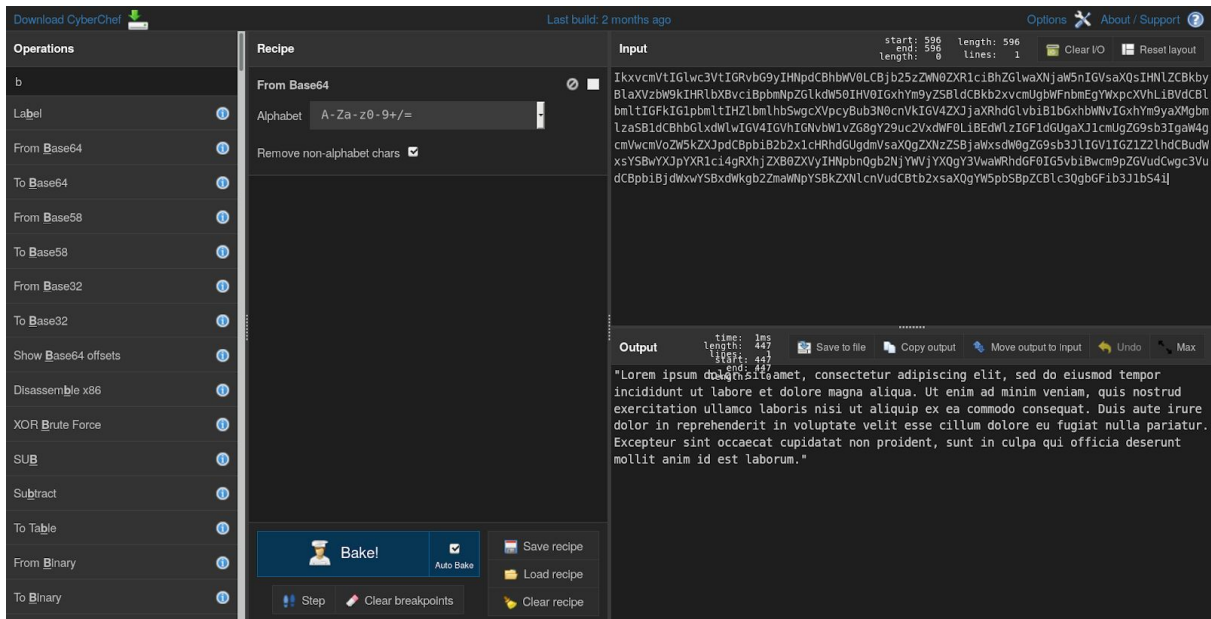
Buscando por los archivos veo cosas como esto y algunos directorios con nombre flag y otros txt similares...



```
lib
├── bomb.0
├── bomb.key
├── bomb.resolve
├── curllib64
├── flagnothere0.1.2.3
├── kill9.1
├── libcrypto-1-dev.dev
├── libcurl64
├── pushit1.6.7
├── resolve9.0.1.5
├── uan5.1
├── unalmesplatform6.0
└── varr_lib5.1
```

bomb.0! bomb.resolve! esto pinta bien!

Pero muchos de ellos son txt que no tienen nada. Otros son un base64 con *Lore ipsum* y diversos troleos infames con los nombres de directorios y el contenido. Flag, bomb... ¡Están jugando con nuestros sentimientos! Cuántas desilusiones... cuando crees haber encontrado algo... trolleo al canto.



... pero al buscar ficheros ocultos encuentro en la raíz del sistema de ficheros un ejecutable llamado .bomb

Al ejecutarlo aparece un contador y cuando acaba pide una clave. Si no es la correcta... **booom!**

Al hacer un `strings` no veo nada de nada :(si lo miro con `hexdump` .bomb veo `UPX!`.

```

00000000  45 4C 46 02 01 01 03 00 00 00 00 00 00 00 02 00 3E 00 01 00 00 00  .ELF.....>.....
00000018  C0 0C 40 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00  .@.....@.....
00000030  00 00 00 00 40 00 38 00 02 00 40 00 00 00 00 00 01 00 00 00 05 00 00 00  ...@.8...@.....
00000048  00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 40 00 00 00  .....@.....@.....
00000060  AC 14 00 00 00 00 00 00 AC 14 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00  .....@#.....@#`.....
00000078  01 00 00 00 06 00 00 00 40 23 00 00 00 00 00 00 40 23 60 00 00 00 00 00  .....@#.....@#`.....
00000090  40 23 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  @#.....@#`.....
000000A8  00 00 20 00 00 00 00 00 BF 97 62 F7 55 50 58 21 F4 07 0D 16 00 00 00 00  .b.UPX!.....
000000C0  B0 3B 00 00 00 3B 00 00 38 02 00 00 CF 00 00 00 02 00 00 00 FB FB 21 FF  ;.....8.....!.....
000000D8  7F 45 4C 46 02 01 01 00 02 00 3E 00 0D 60 0F 40 0F 96 E4 6D 16 05 00 B0  .ELF.....>...@...m...
000000F0  33 00 13 03 D6 7D F7 38 00 09 05 20 00 1D 00 06 0F 05 27 40 36 21 4F D8  3.....}.8.....@6!0..
00000108  00 40 07 F8 01 00 08 27 DB 6C D3 0D 03 03 04 38 02 0F 07 40 C8 84 3C 21  .@.....'.l.....8...@.<!.
00000120  1C 00 00 01 27 EC C0 0E 05 00 00 40 07 E3 19 7E C9 9E 90 00 00 00 20 37  .....@.....@.....7
00000138  AB E8 1D C5 12 B2 CD 15 07 60 90 76 90 0B DB 00 58 05 37 02 08 1E BF 09  .....v...X.7.....
00000150  79 C2 0E 1E 60 07 F0 01 00 0F 36 D8 61 DF 04 03 54 DF 54 02 40 C8 84 3C  y...'.6.a...T.T.@.<.
00000168  61 07 44 00 00 04 64 9B FD 3E 50 E5 74 64 0B 4C 17 0F 07 40 1C 96 90 27  a.D...d...>P.td.L...'.
00000180  5C 00 00 37 51 9D BC 02 DB 06 00 00 10 00 52 B0 8F 10 82 6F 17 18 02 00  \..7Q.....R...o...
00000198  07 00 00 86 90 87 09 00 00 00 FF AB 17 00 00 07 0A 00 00 02 49 00 00 DB  ....I.....
000001B0  7F BB FD 2F 6C 69 62 36 34 05 64 2D 08 6E 75 78 2D 78 38 36 2D 0F 2E F7  .../lib64.d..nux-x86-...
000001C8  A6 DB FE 73 6F 2E 32 00 04 00 00 10 03 01 47 4E 55 00 00 BA CF 34 DD 02  ...so.2.....GNU...4..
000001E0  03 06 20 1F 14 03 03 F7 FF FF C1 1F C0 C0 29 97 54 08 66 77 21 55 1F 99  .....).T.fw!U...

```

Eso nos dice que es un ejecutable comprimido y para descomprimirlo usamos `upx -d .bomb`

```

Ultimate Packer for eXecutables
Copyright (C) 1996 - 2017
UPX 3.94      Markus Oberhumer, Laszlo Molnar & John Reiser   May 12th 2017

File size      Ratio      Format      Name
-----
15280 <-      7548      49.40%     linux/amd64  .bomb

Unpacked 1 file.

```

y ahora, después de hacer un `strings` al fichero, tenemos cosas interesantes.

```
strings .bomb
```

```

AUATL
[]A\A]A^A_
_dbf7c981d7e_fe8
_c462eab3c39
_f2b06_fd
Tienes 1 minuto
clear
|-----|
|-----|
|-----|
Insert Code:
italy
B000M
;*3$"
zPLR

```

probemos con **italy**

```

|-----|
|-----|
|-----|0:0|-----|
|-----|
|-----|
Insert Code: italy
_dbf7c981d7e_fe8_c462eab3c39_f2b06_fd

```

No nos explota! y nos da este código: `_dbf7c981d7e_fe8_c462eab3c39_f2b06_fd`

si quitamos los guiones bajos nos queda un string de 32 caracteres...

`dbf7c981d7efe8c462eab3c39f2b06fd` y parece un md5.

Lo busco en crackmanworld y no aparece, pero sí en

<https://www.md5online.es/descifrar-md5.html>

Encontrado : <http://95.216.138.194/>
(hash = dbf7c981d7efe8c462eab3c39f2b06fd)

Si accedemos a la url <http://95.216.138.194>



como curiosidad, al acceder por https al puerto 80...



...de la vaca :|

Analicemos el certificado autofirmado que nos entregan:

Visor de certificados: "lacasadepapel.cloud"

General

Detalles

No se pudo verificar este certificado porque el emisor es desconocido.

Emitido para

Nombre común (CN)

lacasadepapel.cloud

Organización (O)

La Casa de Papel SL

Unidad organizativa (OU)

Films and Fun!

Número de serie

00:FF:BC:AD:1C:5D:D8:B2:4F

Emitido por

Nombre común (CN)

lacasadepapel.cloud

Organización (O)

La Casa de Papel SL

Unidad organizativa (OU)

Films and Fun!

Periodo de validez

Comienza el

11 de julio de 2018

Caduca el

11 de julio de 2019

Huellas digitales

Huella digital SHA-256

8A:76:E8:11:45:BC:A5:37:D7:03:1E:91:F9:34:C2:B7:03:3C:98:78:9B:AE:C6:B7:2B:99:D7:31:03:0E:F6:5E

Huella digital SHA1

6B:FE:7C:51:F2:B9:EC:12:9E:7B:DB:12:71:9C:6F:41:B5:02:F3:82

CN=lacasadepapel.cloud?

Voy a añadir la ip del server a /etc/hosts para ver si responde con otra cosa... es probable que el virtualhost responda a peticiones de ese dominio y accedo a <https://lacasadepapel.cloud>



bingo!

Si vemos el código fuente podemos ver un jpg, un wav y un mp3 comentado.

```
view-source:https://lacasadepapel.clou  
1 <html>  
2 <head>  
3   <title>La casa de papel</title>  
4 </head>  
5 <body bgcolor="black">  
6 <!-- <audio src="audio/Bella_Ciao.mp3"></audio> -->  
7 <center>  
8   <audio controls>  
9     <source src="audio/Bella_Cia0.wav" type="audio/mp4">  
10  </audio>  
11 </center>  
12 <br />  
13 <center>  
14     
15 </center>  
16 </body>  
17 </html>  
18
```


Los bajo todos:

```
wget https://lacasadepapel.cloud/audio/Bella_Cia0.wav --no-check-certificate
wget https://lacasadepapel.cloud/audio/Bella_Ciao.mp3 --no-check-certificate
wget https://lacasadepapel.cloud/images/back.jpg --no-check-certificate
```

pruebo con stego, veo los metadatos y poco más. No consigo nada.

Después de escuchar varias veces el audio percibo cierto sonido de fondo.... es morse!

Como los pulsos son en un mismo tono puedo abrir el audio en audacity y ver su espectrograma, de esta manera veré la intensidad de cada frecuencia de forma visual. Si encontrara algún patrón para un rango estrecho de frecuencias seguramente sea el morse que busco.

Descubro que los tonos están en torno a 550hz. Ajusto un poco las opciones de audacity para el visualizar mejor los tonos y veo esto.



Apenas consigo entender todo el código morse, pero no sé darle “más resolución” y la canción mete algo de ruido en esas frecuencias, tapando parte del código.

Con una herramienta online cualquiera para decodificar morse y una tabla al lado para buscar las letras que más se parecen en caso de duda, transcribo lo que parece que pone:

laflagesb??la??oremoenmd5

Hasta llegar a eso probé unas cuantas palabras para intentar sacar la flag confiando un poco en la suerte... intentos fallidos, claro.

Después de un rato caigo en que podría ser como el nombre de archivo del audio que me bajé...

`Bella_Cia0.wav` !!!!!

bellacio con dos eles! lo probé con una ele alguna vez antes... estaba cerca y no me fijé bien!

pero encaja!

unit-conversion.info Converters Line tools Special Hash & Encryption More

HOME / TEXT TOOLS / CONVERTERS / CONVERT MORSE CODE

freshdesk Work together. Resolve Faster. TRY FRESHDESK

Convert morse code to text

Input data

Convert

morse_code to text

Output:

flagesbellaciaoremoenmd5

Probamos el md5(bellaciaoremo) = f3b2c8d7436ccb3eaebc832c447f9051

la flag sería UAM{f3b2c8d7436ccb3eaebc832c447f9051}

Lo meto en la plataforma y... ¡sí! ¡acabamos la prueba! 4º puesto esta vez argghhg..., por poco :D

Ha sido muy divertido y se nota la subida de nivel. Enhorabuena a los remeros mayores dpua y mario por hacer unos retos divertidos y originales, con los que siempre aprendemos cosas nuevas, que es de lo que se trata. Enhorabuena también al ganador, DarkEagle, quien estuve comentando cómo lo habíamos logrado cada uno y entendí el porqué del mp3. Como aficionado a la producción musical y tratamiento de audio debí darme cuenta de *aquel detalle* pues era bastante fácil lograr el morse completamente limpio, como lo veréis en su writeup, que entiendo era lo que pretendían que hiciéramos ;)

Tras haber realizado varios retos de UAM puedo decir que aquí tenéis un incondicional. Habéis ayudado a despertar mi interés por la seguridad y el hacking en general. Aprendo y mucho, me divierto en extremo con los retos y en Telegram, consigo herramientas nuevas, conozco gente estupenda...

Son retos muy bien pensados y se nota que cada vez están más pulidos (nueva plataforma, temática, variedad de técnicas, el canal de Telegram...). ¡Seguid así, cracks!

¿Cuánto queda para el siguiente? :D

José Ángel Sánchez (j0n3)