

DESCIFRAR CONTENIDO OCULTO EN UN FICHERO IMAGEN

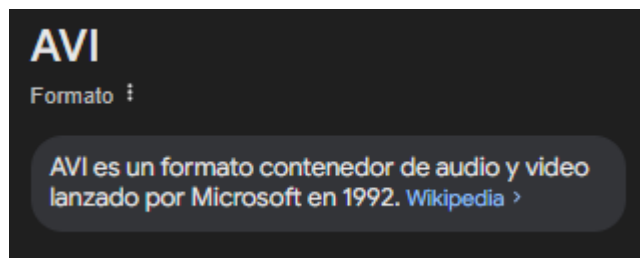
SANTIAGO PEÑARANDA MEJIA

EN ESTE INFORME LO QUE VAMOS HACER ES UNA TÉCNICA MUY CONOCIDA QUE SE LLAMA ESTEGANOGRAFÍA, ESTA PRÁCTICA TRATA DE OCULTAR INFORMACIÓN DENTRO DE OTRO MENSAJE, ARCHIVO U OBJETO FÍSICO PARA EVITAR SU DETECCIÓN. AUNQUE CABE RECALCAR QUE LAS TÉCNICAS DE ESTEGANOGRAFÍA LO QUE HACEN ES OCULTAR, NO PROTEGER, CIERTA INFORMACIÓN SENSIBLE DELANTE DE LA VISTA.

LO PRIMERO QUE VAMOS HACER ES ANALIZAR EL ARCHIVO QUE TENEMOS, PARA ELLOS ESCRIBIMOS EL SIGUIENTE COMANDO

```
➤ /home/s/Descargas > file 350911.avi root@parrot
350911.avi: RIFF (little-endian) data, AVI, 1280 x 720, >30 fps, video:, audio: (stereo, 44100 Hz)
➤ /home/santo/Descargas > █
```

Y COMO PODEMOS OBSERVAR ES UN FICHERO CON FORMATO “.AVI” ESTO QUIERE DECIR QUE ES UN FORMATO DE AUDIO Y VIDEO, COMO PODEMOS VER AQUÍ EN LA BUSCA QUE HICIMOS EN INTERNET.



AHORA VAMOS A EXTRAER DATOS DEL ARCHIVO, PARA ELLO VAMOS A USAR LA HERRAMIENTA BINWALK QUE ES UNA HERRAMIENTA DESTINADA A LA EXTRACCIÓN DE DATOS DE IMÁGENES, ESTO LO HACEMOS CON EL SIGUIENTE COMANDO.

```
/home/santo/Descargas > binwalk 350911.avi

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
26013116     0x18CEDBC   Zip archive data, at least v2.0 to extract, compressed size: 613, uncompressed size: 811, name: bandera64.txt
26013883     0x18CF0BB   End of Zip archive, footer length: 22

/home/santo/Descargas >
```

Y ASÍ ES COMO NOS PODEMOS DAR CUENTA DE QUE ESTE “SUPUESTO VIDEO CONTIENE UN FICHERO ZIP EL CUAL ADENTRO TIENE UN ARCHIVO LLAMADO “BANDERA64.TXT”.

```
as > binwalk 350911.avi

DESCRIPTION
-----
Zip archive data, at least v2.0 to extract, compressed size: 613, uncompressed size: 811, name: bandera64.txt
End of Zip archive, footer length: 22

as >
```

COMO YA SABEMOS QUE EL “SUPUESTO VIDEO” CONTIENE UN FICHERO ZIP VAMOS A PROCEDER A EXTRAERLO, ESTO LO HACEMOS CON EL SIGUIENTE COMANDO.

```
/home/santo/Descargas > binwalk -e 350911.avi
```

EN DEFINITIVA ESTE SERIA EL COMANDO, PERO COMO PODEMOS VER ME DA ERROR, PORQUE LA HERRAMIENTA USA HERRAMIENTAS DE TERCEROS Y PODRÍAN NO SER SEGURAS.

```
/home/santo/Descargas > binwalk -e 350911.avi

Extractor Exception: Binwalk extraction uses many third party utilities, which may not be secure. If you wish to have extraction utilities executed as the current user, use '--run-as=root'.
binwalk itself must be run as root).

Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/binwalk/core/module.py", line 258, in __init__
    self.load()
  File "/usr/lib/python3/dist-packages/binwalk/modules/extractor.py", line 147, in load
    raise ModuleException("Binwalk extraction uses many third party utilities, which may not be secure. If you wish to have extraction utilities executed as the current user, use '--run-as=root'. (binwalk itself must be run as root).") % user_info.pw_name)
binwalk.core.exceptions.ModuleException: Binwalk extraction uses many third party utilities, which may not be secure. If you wish to have extraction utilities executed as the current user, use '--run-as=root'. (binwalk itself must be run as root).
```

POR ENDE TENEMOS QUE ESCRIBIR EL SIGUIENTE COMANDO A POSTERIOR PARA PODER EJECUTARLA.

```
> sudo binwalk -e --run-as=root 350911.avi
```

ESTO NOS GENERA UN FICHERO

```
/home/santo/Descargas > ls
350911.avi  _350911.avi.extracted  rockyou.txt  salida.raw  z  zap_root_ca.cer
```

Y ASÍ ES COMO HEMOS EXTRAÍDO LA INFORMACIÓN QUE CONTENÍA EL ARCHIVO QUE
“APARENTEMENTE SÓLO ERA UN VIDEO”

```
/home/santo/Descargas/_350911.avi.extracted > ls
18CEDBC.zip  bandera64.txt
```

AL ABRIR EL ARCHIVO .TXT PODEMOS VER QUE HAY CREDENCIALES CIFRADAS, PERO NO SABEMOS
EN QUÉ FORMATO DE CIFRADO ESTÁ CIFRADA LAS CREDENCIALES

```
/home/santo/Descargas/_350911.avi.extracted > cat bandera64.txt
UESDBAoACQBjALpE5UyE1fPolAEAAHgBAAALAAAsAYmFuZGVyYS5wbmcBmQcAAQBRRQMAAPKu8K6x
c7GJh/VmKva+f8JqD7Pe3X95ttenp+LwVVKiTrs1N450IIK7cjKsIYwqYBWiSwcClH2S51vh+L6/
xnICJFdIYuqD+sB282j0guUmoXbdIwU3dMtkYeUs/t0m7yd4TxHMFQ2wM+i64R/iuhx9xvvh5PV
jnyPiKnjKPTQf9tH1xfIKezQ8IHDAFPeEWZSMIRBa0wVwLywkiopyEYSuJGzJchCoRtiMX3fmfJX
8bD3SozBFIOPMjje/3/Xn6tVdmaaAVpAt8+iXu05VwXmmg8Ub7isi2KJBljiGMTQ+knFndW3gCEr
V3pk10fNOGWAIO915QXe6I+UKJZ5p9bpLi0fBbTHJCFcFuSy/IJHr9Vr5rzi6vpPU7p0ZtNJyYoK
EUB18DsmONTxc+xuqloJtzhrUQ5ZHRWumnfMk9Cw1tYT/KHa4gWh/GOVHLEAkizskRobAfanZ00Y
TfmYtjl/60UaL/sFkDYH4+uNt9MKLLiLR4WomoTq2Qi4o+EyzLD00drgZXjsd1aN9s3EYkNY+Ug6
UESHCITV8+iUAQAAeAEAAFBLAQIFAAoACQBjALpE5UyE1fPolAEAAHgBAAALAC8AAAAAAAAAIAAA
AAAAABiYW5kZXJhLnBuZwoIAAAAAAAAAQAYAAByYR+FNQBD0sSrJY51AHbTw9ChznUAQGZBwAB
AEFFAwAAUESFBgAAAAABAAEAaAAAAAngBAAAAA==
/home/santo/Descargas/_350911.avi.extracted >
```

PERO AL LLAMARSE BANDERA**64**.TXT PODEMOS INTUIR QUE ESTÉ CIFRADA EN EL FORMATO **BASE 64**, ASÍ QUE PODRÍAMOS HACER UN ATAQUE DE DICCIONARIO EN BASE **64** Y ASÍ PODER OBTENER LAS CONTRASEÑAS EN TEXTO CLARO.

ESTO SERÍA TODO, **CHAO Y GRACIAS**.