

# Amogus

Categoría "Forense"

## Descripción

Hay un traidor entre nosotros.

Nos dan un fichero zip con el reto

## Solución

Al descomprimir el fichero zip, vemos un montón de ficheros numerados del 1 al 10000.

```
~/Downloads/files ls
1      1427  1857  2286  2715  3144  3574  4002
10     1428  1858  2287  2716  3145  3575  4003
100    1429  1859  2288  2717  3146  3576  4004
1000   143   186   2289  2718  3147  3577  4005
10000  1430  1860  229   2719  3148  3578  4006
1001   1431  1861  2290  272   3149  3579  4007
1002   1432  1862  2291  2720  315   358   4008
1003   1433  1863  2292  2721  3150  3580  4009
1004   1434  1864  2293  2722  3151  3581  401
1005   1435  1865  2294  2723  3152  3582  4010
```

Dichos ficheros contienen aparentemente basura, si intentamos leer uno cualquiera vamos a recibir un output parecido al siguiente.

```
~/Downloads/files cat 1567
U??VFSp W5??#?4?T?.Z0??n| ?"??=F?"?w?"Vx
3?K??M?????L?BY.
'Z?}?
DEL<?K^[?1W?bl?j?V?
?%?NDEL*?v?dM????
?|c????][?d*???.??#?
J?vrs?Ja)??gk?5"?t?K3??\?o????}? ?? ô.??$??ux>?P`@9
/D?X?o/?????k?
???D?`t<E?
?R5,?-???}?H??"s???f?df?[~?PU@#4?)????I???B?
```

Parece que el output de todos los ficheros es ilegible. Pero... ¿de absolutamente todos los ficheros?

```
2,0K  9 feb 00:04 9981
2,0K  9 feb 00:04 9982
2,0K  9 feb 00:04 9983
2,0K  9 feb 00:04 9984
2,0K  9 feb 00:04 9985
2,0K  9 feb 00:04 9986
2,0K  9 feb 00:04 9987
2,0K  9 feb 00:04 9988
```

Observamos también que todos los ficheros tienen una fecha de modificación parecida, y un tamaño idéntico.

## Entropía

Para resolver este reto tenemos que hablar de un término llamado “entropía”, la podemos definir como “la medida de el desorden de un sistema”. Utilizando distintas técnicas, se pretende detectar aquello que parece aleatorio pero no lo es.

```
~/Downloads/files ent 1
Entropy = 7.893446 bits per byte.
```

Por ejemplo, si analizamos la entropía del fichero “1” nos sale muy cercana a 8.

Contra más cercano a “8”, más aleatorio es el contenido, normalmente los ficheros con contenido ascii están entre 2 y 5 de entropía. Si nos picamos un script, llegamos al fichero “6969”.

```
~/Downloads/files  ent 6969
Entropy = 0.190213 bits per byte.
```

Este fichero tiene una entropía muy baja comparado con todo el resto, vamos a ver sus contenido.

[illegible]

Como vemos, hay muchísimas "A"s pero hay un string raro ahí dentro. Miramos a ver que es ese string.

Lo metemos a cyberchef y voilà! Tenemos la flag

HackOn{3ntr0p1ado\_xD}