Amogus

Categoría “Forense”

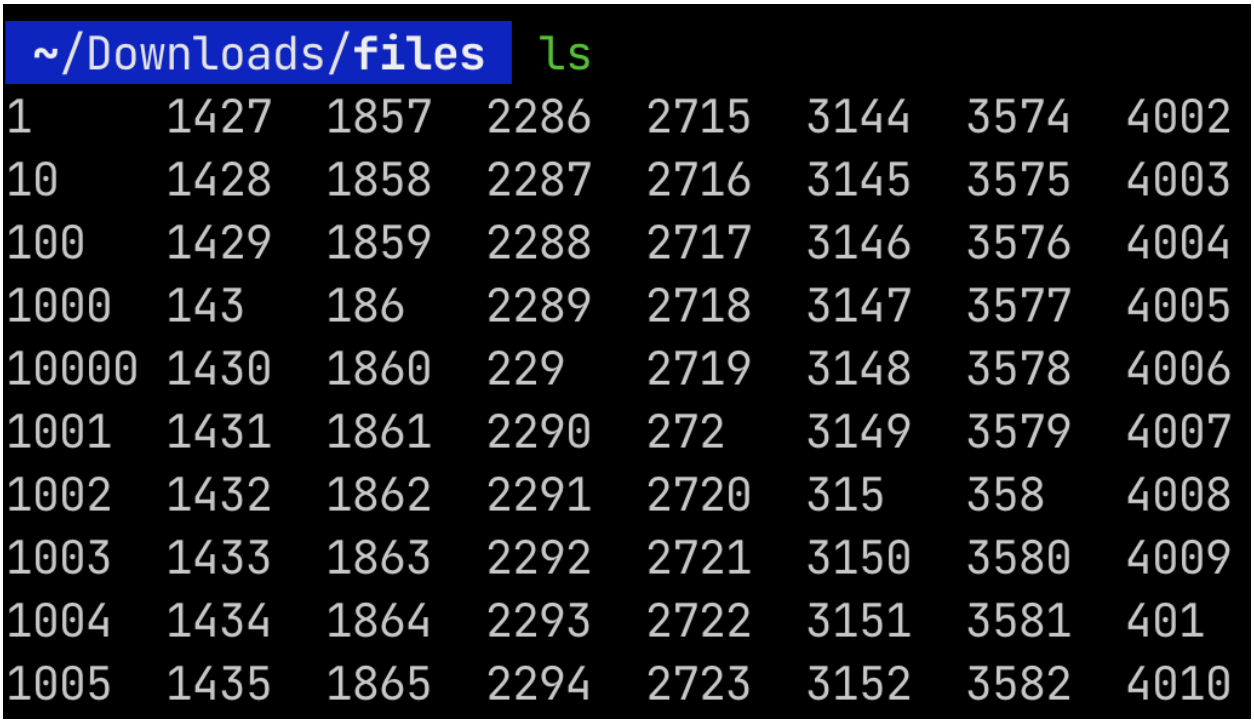
Descripción

```
Hay un traidor entre nosotros.
```

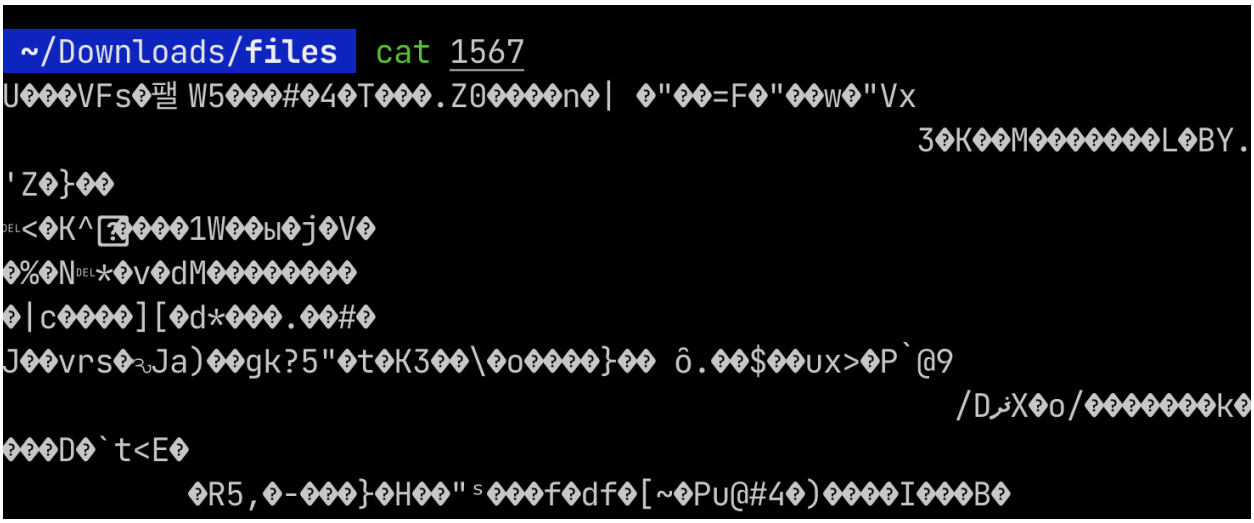
Nos dan un fichero zip con el reto

Solución

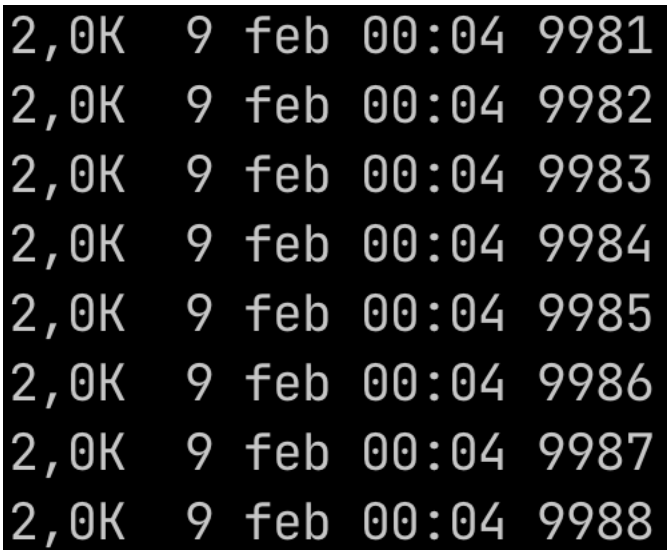
Al descomprimir el fichero zip, vemos un montón de ficheros numerados del 1 al 10000.



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



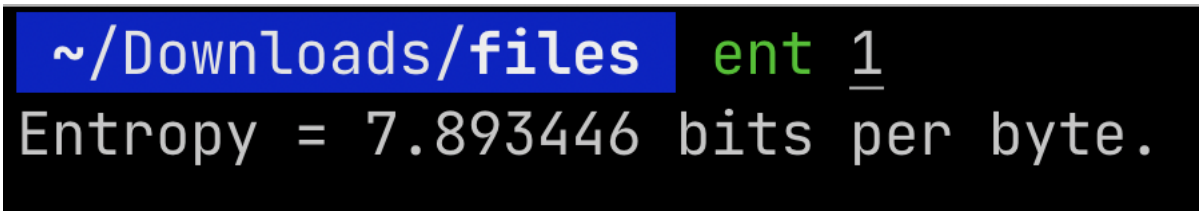
Parece que el output de todos los ficheros es ilegible. Pero... ¿de absolutamente todos los ficheros?



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 pretente detectar aquello que parece aleatorio pero no lo es.



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.

```
AAAAAAAAAAAA
AAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
5T9SYQ1bbRKV6XBcCaxFZBTmNXFVn
A
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
A
```

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 voilá! Tenemos la flag

```
HackOn{3ntr0p1ado_xD}
```