Easy Exfil

Categoría “Forense”

Enunciado

Solución

El fichero que nos dan es una captura de tráfico de red que podemos abrir por ejemplo con Wireshark.

En esta captura vemos paquetes ping de una máquina a otra (192.168.56.102 → 192.168.56.101), vamos a analizar un paquete de ping normal.

```
08 00 27 7c 08 ed 08 00  27 47 10 a0 08 00 45 00   ··'|···· 'G····E·
00 54 cc a0 40 00 40 01  7b ec c0 a8 38 66 c0 a8   ·T··@·@· {···8f··
38 65 08 00 1b 8b 00 1a  01 9c 17 18 f7 61 00 00   8e······ ·····a··
00 00 0a 72 03 00 00 00  00 00 10 11 12 13 14 15   ···r···· ········
16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
36 37                                              67
```

La última parte del paquete es una parte opcional de un paquete “ICMP”, pero no parece tener datos muy interesantes... Sin embargo, hay otros paquetes más extraños.

```
08 00 27 7c 08 ed 08 00  27 47 10 a0 08 00 45 00   ··'|···· 'G····E·
00 54 cd ad 40 00 40 01  7a df c0 a8 38 66 c0 a8   ·T··@·@· z···8f··
38 65 08 00 9f 0b 00 27  00 01 18 18 f7 61 00 00   8e·····' ·····a··
00 00 3b 62 0d 00 00 00  00 00 53 47 46 6a 53 47   ··;b···· ··SGFjSG
46 6a 53 47 46 6a 53 47  46 6a 53 47 46 6a 53 47   FjSGFjSG FjSGFjSG
46 6a 53 47 46 6a 53 47  46 6a 53 47 46 6a 53 47   FjSGFjSG FjSGFjSG
46 6a                                              Fj
```

Estos paquetes contienen una cadena repetida varias veces “SGFj”, ¿que puede ser esto? Nos lo llevamos a cyberchef y vemos que se corresponde con la cadena “Hac” encodeada en base64... Si seguimos el mismo proceso y vamos paquete a paquete mirando las cadenas extrañas, sacamos la flag que un intruso ha sacado de nuestra máquina a través de ping.

```
SGFja09uezN4ZjFsdHJBdDEwbl8xc19uMHRfZlVufQo=
HackOn{3xf1ltrAt10n_1s_n0t_fUn}
```