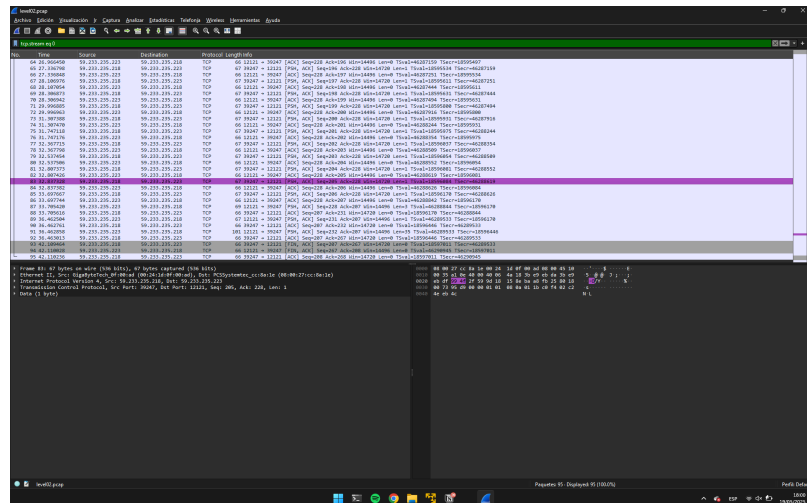


2

Level02

Para este nivel nos dan un archivo con extensión `.pcap`, este tipo de archivos es un archivo de capturas de paquetes por lo que se me ocurre abrirlo con wireshark.



Viendo las peticiones, busco alguna que tenga algo interesante y aquí encuentro la palabra password.

Usando `ctrl + shift + alt + t` puedo ver directamente todo lo que se ha enviado y obtengo lo siguiente:

```
..%
..%
..&...#...'$
..&...#...'$
..#...
..38400,38400...#..SodaCan:0....'.DISPLAY.SodaCan:0.....xterm..
!
".....b....B.
.....1.....!
"
!....."
"
"
Linux 2.6.38-8-generic-pae (::ffff:10.1.1.2) (pts/10)
..wwwbugs login:
l
.l
e
.e
v
.v
e
.e
l
.l
x
.x
..
Password:
ft_wandr...NDRe1.L0L
..
Login incorrect
wwwbugs login:
```

Viendo esto, observamos que la contraseña tiene unos caracteres no imprimibles en medio, mirando esos puntos observamos que en hexadecimal esos puntos significan `DEL` por lo que da a pensar que quizás tengamos que eliminar los caracteres que se han enviado antes como si el usuario se hubiera equivocado y hubiera escrito las cosas en minúscula cuando eran en mayúscula. Por lo que probamos a escribir la siguiente contraseña para acceder a la flag02:

`ft_waNDReL0L`

Finalmente con esta contraseña accedemos a flag02 y por ende al token del siguiente nivel.