Práctica 5: PGP y Protocolos

Ejercicio 2: Análisis del protocolo TELNET

El intercambio de mensajes (mostrando los del cliente y el servidor juntos) ha sido:

```
.......... ..!.."..'.....#..%..%.......... ..!.."."........P. ...."".....b........b.... B.
......................."......'.....#..&..&..$..&..&..$.. .....#.....'..........
.9600,9600....#.bam.zing.org:0.0....'..DISPLAY.bam.zing.org:0.0......xterm-color.............!
.............."............
OpenBSD/i386 (oof) (ttyp1)

login: .."........"ffaakkee
.
Password:user
.
Last login: Thu Dec  2 21:32:59 on ttyp1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ llss
.
$ llss  --aa
.
.         ..        .cshrc    .login    .mailrc   .profile  .rhosts
$ //ssbbiinn//ppiinngg  wwwwww..yyaahhoooo..ccoomm
.
PING www.yahoo.com (204.71.200.74): 56 data bytes
64 bytes from 204.71.200.74: icmp_seq=0 ttl=239 time=73.569 ms
64 bytes from 204.71.200.74: icmp_seq=1 ttl=239 time=71.099 ms
64 bytes from 204.71.200.74: icmp_seq=2 ttl=239 time=68.728 ms
64 bytes from 204.71.200.74: icmp_seq=3 ttl=239 time=73.122 ms
64 bytes from 204.71.200.74: icmp_seq=4 ttl=239 time=71.276 ms
64 bytes from 204.71.200.74: icmp_seq=5 ttl=239 time=75.831 ms
64 bytes from 204.71.200.74: icmp_seq=6 ttl=239 time=70.101 ms
64 bytes from 204.71.200.74: icmp_seq=7 ttl=239 time=74.528 ms
64 bytes from 204.71.200.74: icmp_seq=9 ttl=239 time=74.514 ms
64 bytes from 204.71.200.74: icmp_seq=10 ttl=239 time=75.188 ms
64 bytes from 204.71.200.74: icmp_seq=11 ttl=239 time=72.925 ms
...^C
.--- www.yahoo.com ping statistics ---
13 packets transmitted, 11 packets received, 15% packet loss
round-trip min/avg/max = 68.728/72.807/75.831 ms
$ eexxiitt
.
```

1. **¿Qué usuario y contraseña se ha aplicado para acceder al servidor de Telnet 192.168.0.1?**
   Usuario *fake* y contraseña *user*.

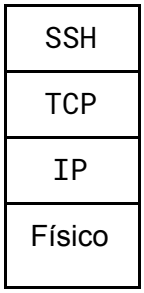
2. **¿Qué sistema operativo se está aplicando en el servidor?**
   OpenBSD.

3. **¿Qué comandos ha ejecutado el cliente en el servidor telnet?**
   `ls`, `ls -a`, `ping` (a yahoo) y `exit`.

Ejercicio 3: Análisis del protocolo SSH

1. **¿A partir de qué paquete comienza a cifrarse el tráfico de red?**
   A partir de la trama número 13, que ya posee contenido cifrado.

2. **¿A qué nivel se aplica el cifrado del protocolo SSH? Es decir, ¿se aplica el cifrado a los protocolos de red (IP, TCP, etc.), a las capas superiores, o a ambos?**
   Se aplica a nivel de aplicación:



Donde el orden de las cabeceras y datos es:
`Físico ( IP ( TCP ( SSH ( [datos] ) ) ) )`

Como el SSH es el que está cifrando, resulta:
`Físico ( IP ( TCP ( SSH ( [xxxxx] ) ) ) )`

Puede observarse que la capa de transporte no está cifrada.

3. **¿Es posible ver alguna información sobre credenciales de seguridad como puede ser el usuario y la contraseña?**
   No, pues la información ya ha sido cifrada. Los únicos datos que pueden observarse -abriendo las tramas SSH- son el paquete y su longitud (ambos valores cifrados).