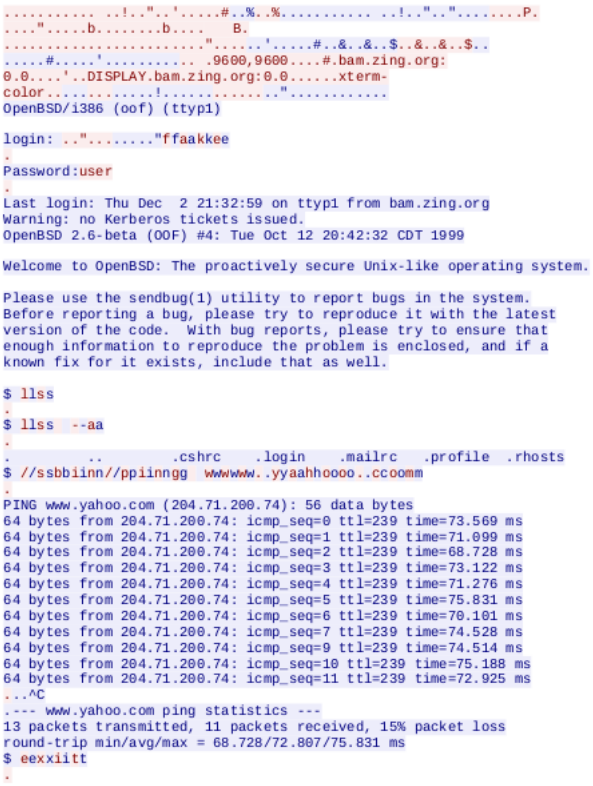
# Práctica 5: PGP y Protocolos

Cristina Díaz García

Enero 2019

# Índice

# 1. Análisis del protocolo TELNET



```
.......... ..!.."..'.....#..%..%.......... ..!.."."".....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
   **contraseña:** user

   ```
   login: .."........"ffaakkee
   .
   Password:user
   ```

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

   Linux.

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

3. ¿Qué comandos ha ejecutado el cliente en el servidor telnet?

   ls
   ls -a

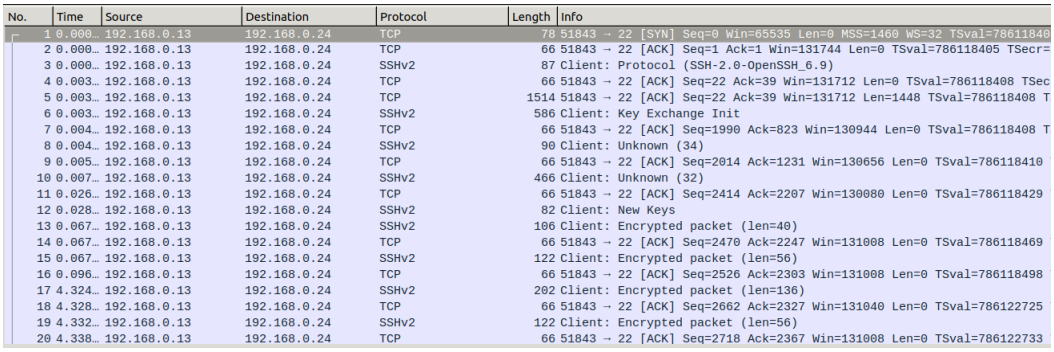
/sbin/ping www.yahoo.com
Ctrl+C
exit

```
$ ls
$ ls -a
.         ..        .cshrc    .login    .mailrc   .profile  .rhosts
$ /sbin/ping www.yahoo.com
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
$ exit
```

## 2. Análisis del protocolo SSH

1. ¿A partir de qué paquete comienza a cifrarse el tráfico de red?

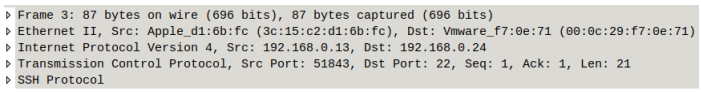
   A partir del 13º paquete.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000… | 192.168.0.13 | 192.168.0.24 | TCP | 78 | 51843 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=78611840 |
| 2 | 0.000… | 192.168.0.13 | 192.168.0.24 | TCP | 66 | 51843 → 22 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=786118405 TSecr= |
| 3 | 0.000… | 192.168.0.13 | 192.168.0.24 | SSHv2 | 87 | Client: Protocol (SSH-2.0-OpenSSH_6.9) |
| 4 | 0.003… | 192.168.0.13 | 192.168.0.24 | TCP | 66 | 51843 → 22 [ACK] Seq=22 Ack=39 Win=131712 Len=0 TSval=786118408 TSec |
| 5 | 0.003… | 192.168.0.13 | 192.168.0.24 | TCP | 1514 | 51843 → 22 [ACK] Seq=22 Ack=39 Win=131712 Len=1448 TSval=786118408 T |
| 6 | 0.003… | 192.168.0.13 | 192.168.0.24 | SSHv2 | 586 | Client: Key Exchange Init |
| 7 | 0.004… | 192.168.0.13 | 192.168.0.24 | TCP | 66 | 51843 → 22 [ACK] Seq=1990 Ack=823 Win=130944 Len=0 TSval=786118408 T |
| 8 | 0.004… | 192.168.0.13 | 192.168.0.24 | SSHv2 | 90 | Client: Unknown (34) |
| 9 | 0.005… | 192.168.0.13 | 192.168.0.24 | TCP | 66 | 51843 → 22 [ACK] Seq=2014 Ack=1231 Win=130656 Len=0 TSval=786118410 |
| 10 | 0.007… | 192.168.0.13 | 192.168.0.24 | SSHv2 | 466 | Client: Unknown (32) |
| 11 | 0.026… | 192.168.0.13 | 192.168.0.24 | TCP | 66 | 51843 → 22 [ACK] Seq=2414 Ack=2207 Win=130080 Len=0 TSval=786118429 |
| 12 | 0.028… | 192.168.0.13 | 192.168.0.24 | SSHv2 | 82 | Client: New Keys |
| 13 | 0.067… | 192.168.0.13 | 192.168.0.24 | SSHv2 | 106 | Client: Encrypted packet (len=40) |
| 14 | 0.067… | 192.168.0.13 | 192.168.0.24 | TCP | 66 | 51843 → 22 [ACK] Seq=2470 Ack=2247 Win=131008 Len=0 TSval=786118469 |
| 15 | 0.067… | 192.168.0.13 | 192.168.0.24 | SSHv2 | 122 | Client: Encrypted packet (len=56) |
| 16 | 0.096… | 192.168.0.13 | 192.168.0.24 | TCP | 66 | 51843 → 22 [ACK] Seq=2526 Ack=2303 Win=131008 Len=0 TSval=786118498 |
| 17 | 4.324… | 192.168.0.13 | 192.168.0.24 | SSHv2 | 202 | Client: Encrypted packet (len=136) |
| 18 | 4.328… | 192.168.0.13 | 192.168.0.24 | TCP | 66 | 51843 → 22 [ACK] Seq=2662 Ack=2327 Win=131040 Len=0 TSval=786122725 |
| 19 | 4.332… | 192.168.0.13 | 192.168.0.24 | SSHv2 | 122 | Client: Encrypted packet (len=56) |
| 20 | 4.338… | 192.168.0.13 | 192.168.0.24 | TCP | 66 | 51843 → 22 [ACK] Seq=2718 Ack=2367 Win=131008 Len=0 TSval=786122733 |

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?

   A la capa de aplicación.



```
▸ Frame 3: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
▸ Ethernet II, Src: Apple_d1:6b:fc (3c:15:c2:d1:6b:fc), Dst: Vmware_f7:0e:71 (00:0c:29:f7:0e:71)
▸ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 192.168.0.24
▸ Transmission Control Protocol, Src Port: 51843, Dst Port: 22, Seq: 1, Ack: 1, Len: 21
▸ SSH Protocol
```

3. ¿Es posible ver alguna información sobre credenciales de seguridad como puede ser el usuario y la contraseña?

   No, ya que está cifrado.