Verificació del funcionament d'SSH

Dr. Daniel Guasch Murillo
Dr. Rafael Vidal Ferré

Abril 2023

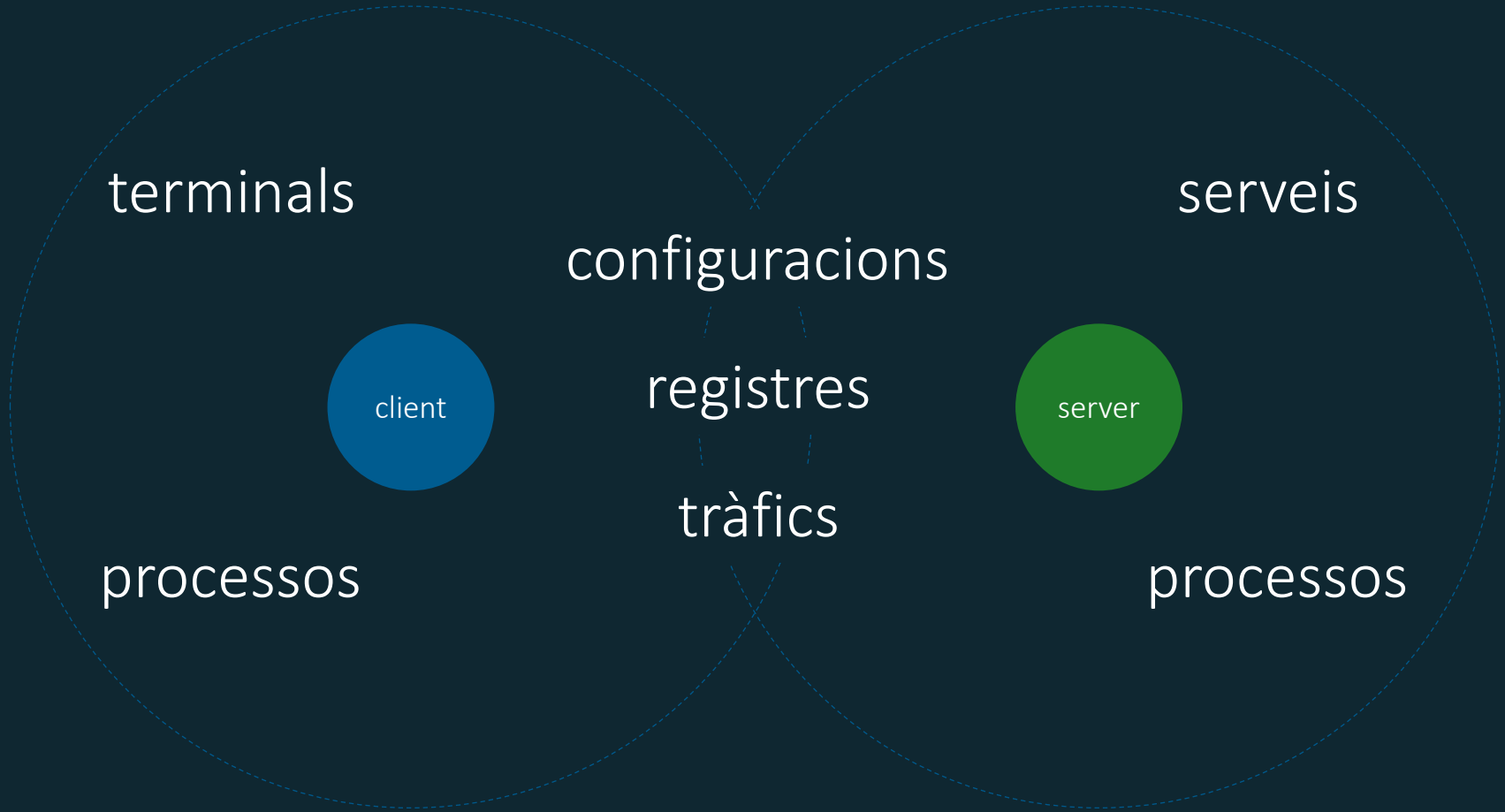
UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú

C

Cas pràctic

Cas pràctic

Com es verifica el funcionament de SSH?



Cas pràctic

Com es verifica el funcionament del client de SSH?

client

- Configuració (LogLevel INFO / VERBOSE / DEBUG)
  ```
  ~# cat /etc/ssh/ssh_config
  ```
- Terminal:
  ```
  ~# ssh entel@10.1.1.181 2>debug_client.log
  ```
- Procés
  ```
  ~# ps aux | grep -i ssh
  ```
- Registre
  ```
  ~# cat debug_client.log
  ```
- Tràfic
  - Captura
    ```
    ~# tcpdump -n -s 0 host 10.1.1.128 and 10.1.1.181 -w client_ssh.pcap
    ```
  - Visualització
    ```
    ~# tcpdump -r client_ssh.pcap
    ~# tshark -r client_ssh.pcap -j ssh
    ```

Cas pràctic

Com es verifica el funcionament del client de SSH?

server

- Configuració (LogLevel INFO / VERBOSE / DEBUG)
  ~# cat /etc/ssh/sshd_config

- Servei:
  ~# service ssh status

- Procés
  ~# ps aux | grep -i ssh

- Registre
  ~# cat /var/log/auth.log | grep -i ssh

- Tràfic
  - Captura
    ~# tcpdump -n -s 0 host 10.1.1.128 and 10.1.1.181 -w server_ssh.pcap

  - Visualització
    ~# tcpdump -r server_ssh.pcap
    ~# tshark -r server_sh.pcap -j ssh

El cas de l'accés SSH

server

El cas de l'accés SSH - servidor

És el dia 2 de maig de 2022...

L'equip amb IP 10.1.1.181 té el servei SSH actiu....

Té per PID el valor 391, registra en mode DEBUG

I el port 22 està en mode LISTEN...

```
~# service ssh status
● ssh.service - OpenBSD Secure Shell server
 Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e>
 Active: active (running) since Mon 2022-05-02 13:13:57 CEST; 3h 19min ago
...
Main PID: 391 (sshd)
...
~# ps aux | grep -i ssh
root         391  0.0  0.7  13292  7728 ?        Ss   13:13   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
...
~# ss -tlp
Netid  State    Recv-Q   Send-Q     Local Address:Port       Peer Address:Port  Process
tcp    LISTEN   0        128              0.0.0.0:ssh             0.0.0.0:*      users:(("sshd",pid=391,fd=3))
tcp    LISTEN   0        128                 [::]:ssh                [::]:*      users:(("sshd",pid=391,fd=4))
...
```

server

El cas de l'accés SSH - servidor

A les 16:24:33 arriba una connexió al port TCP 22 ...

Ve de la IP 10.1.1.128, des del port 54146...

El servei SSH [391] crea un nou procés per respondre...

El procés rep el PID 2294...

```
~# tcpdump -n -s 0 host 10.1.1.128 and 10.1.1.181 -w servidor_ssh.pcap
~# tcpdump -r servidor_ssh.pcap
reading from file servidor_ssh.pcap, link-type EN10MB (Ethernet), snapshot length 262144
16:24:33.170619 IP 10.1.1.128.54146 > 10.1.1.181.ssh: Flags [S], seq 3006517464, win 64240, options [mss 1460,sackOK,TS val
1776942468 ecr 0,nop,wscale 7], length 0
...
~# cat /var/log/auth.log | grep -i ssh
...
May  2 16:24:33 debian11 sshd[391]: debug1: Forked child 2294.
...
~# ps aux | grep -i ssh
root         391  0.0  0.7  13292  7728 ?        Ss   13:13   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        2294  0.0  0.8  14456  8832 ?        Ss   16:24   0:00 sshd: entel [priv]
...
```

server

El cas de l'accés SSH - servidor

El procés 2294 accepta la connexió SSH, inicia el handshake i valida l'usuari entel ...

Llavors crea el procés 2300 que inicia la sessió interactiva SSH de l'usuari entel en el terminal pts/2 ...

```
~# cat /var/log/auth.log | grep -i ssh
...
May  2 16:24:33 debian11 sshd[2294]: Connection from 10.1.1.128 port 54146 on 10.1.1.181 port 22 rdomain ""  ...
May  2 16:24:40 debian11 sshd[2294]: Accepted password for entel from 10.1.1.128 port 54146 ssh2             ...
May  2 16:24:40 debian11 sshd[2294]: User child is on pid 2300                                               ...
May  2 16:24:40 debian11 sshd[2300]: Starting session: shell on pts/2 for entel from 10.1.1.128 port 54146 id 0
...
~# ps aux | grep -i ssh
root         391  0.0  0.7  13292  7728 ?        Ss   13:13   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        2294  0.0  0.8  14456  8832 ?        Ss   16:24   0:00 sshd: entel [priv]
entel       2300  0.0  0.6  14668  6012 ?        S    16:24   0:00 sshd: entel@pts/2
...
~# ss -tp
State    Recv-Q    Send-Q       Local Address:Port       Peer Address:Port    Process
ESTAB    0         80              10.1.1.181:ssh         10.1.1.128:54146    users:(("sshd",pid=2300,fd=4),("sshd",pid=2294,fd=4))
...
```

server

El cas de l'accés SSH - servidor

L'anàlisi del handshake des del registre de SSH i les captures de tràfic són coherents ...

```
~# cat /var/log/auth.log | grep -i ssh
...
May  2 16:24:33 debian11 sshd[2294]: debug1: Local version string SSH-2.0-OpenSSH_8.4p1 Debian-5                    ...
May  2 16:24:33 debian11 sshd[2294]: debug1: Remote protocol version 2.0, remote software version OpenSSH_8.4p1 Debian-5  ...
May  2 16:24:33 debian11 sshd[2294]: debug1: kex: algorithm: curve25519-sha256 [preauth]                             ...
May  2 16:24:33 debian11 sshd[2294]: debug1: kex: host key algorithm: ecdsa-sha2-nistp256 [preauth]                  ...
May  2 16:24:33 debian11 sshd[2294]: debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit>  ...
May  2 16:24:33 debian11 sshd[2294]: debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit>  ...
May  2 16:24:40 debian11 sshd[2300]: debug1: Entering interactive session for SSH2.                                  ...
...

~# tshark -r servidor_ssh.pcap -j ssh
...
4   0.000579   10.1.1.128 → 10.1.1.181   SSH     98 Client: Protocol (SSH-2.0-OpenSSH_8.4p1 Debian-5)        ...
6   0.011571   10.1.1.181 → 10.1.1.128   SSHv2   98 Server: Protocol (SSH-2.0-OpenSSH_8.4p1 Debian-5)        ...
8   0.012165   10.1.1.128 → 10.1.1.181   SSHv2 1578 Client: Key Exchange Init                                 ...
10  0.012815   10.1.1.181 → 10.1.1.128   SSHv2 1122 Server: Key Exchange Init                                 ...
16  2.877060   10.1.1.128 → 10.1.1.181   SSHv2   82 Client: New Keys                                          ...
18  2.877622   10.1.1.128 → 10.1.1.181   SSHv2  110 Client: Encrypted packet (len=44)                         ...
20  2.878569   10.1.1.181 → 10.1.1.128   SSHv2  110 Server: Encrypted packet (len=44)                         ...
...
```

server

El cas de l'accés SSH - servidor

Minuts més tard, l'usuari entel tanca la sessió a les 16:26:02...

Els processos 2300 i 2294 són eliminats del sistema...

I la connexió TCP finalitza a les 16:26:02...

```
~# cat /var/log/auth.log | grep -i ssh
...
May  2 16:26:02 debian11 sshd[2300]: Received disconnect from 10.1.1.128 port 54146:11: disconnected by user ···
May  2 16:26:02 debian11 sshd[2300]: Disconnected from user entel 10.1.1.128 port 54146                       ···
May  2 16:26:02 debian11 sshd[2294]: pam_unix(sshd:session): session closed for user entel                    ···
May  2 May  2 16:26:02 debian11 sshd[391]: debug1: main_sigchld_handler: Child exited                         ···
..”
~# ps aux | grep -i ssh
root         391  0.0  0.7  13292  7728 ?        Ss   13:13   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
...
~# tshark -r servidor_ssh.pcap -j ssh
...
130  89.021758  10.1.1.128 → 10.1.1.181   SSHv2 126 Client: Encrypted packet (len=60)
131  89.021793  10.1.1.181 → 10.1.1.128   TCP 66 22 → 54146 [ACK] Seq=5865 Ack=2741 Win=64128 Len=0 TSval=3058335243 TSecr=...
132  89.022008  10.1.1.128 → 10.1.1.181   TCP 66 54146 → 22 [FIN, ACK] Seq=2741 Ack=5865 Win=64128 Len=0 TSval=1777031490 TSecr=...
133  89.025138  10.1.1.181 → 10.1.1.128   TCP 66 22 → 54146 [FIN, ACK] Seq=5865 Ack=2742 Win=64128 Len=0 TSval=3058335246 TSecr=…
134  89.025476  10.1.1.128 → 10.1.1.181   TCP 66 54146 → 22 [ACK] Seq=2742 Ack=5866 Win=64128 Len=0 TSval=1777031493 TSecr=...
```

server

El cas de l'accés SSH - servidor

És el dia 2 de maig de 2022 a les 16:26:03...

El servei SSH amb PID 391 té el port 22 en mode LISTEN ...

Què ha fet l'usuari mentre ha estat connectat?...

Tot ha tornat a la normalitat?...

```
~# service ssh status
● ssh.service - OpenBSD Secure Shell server
 Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e>
 Active: active (running) since Mon 2022-05-02 13:13:57 CEST; 3h 19min ago
...
Main PID: 391 (sshd)
...
~# ps aux | grep -i ssh
root         391  0.0  0.7  13292  7728 ?        Ss   13:13   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
...
~# ss -tlp
Netid  State    Recv-Q   Send-Q     Local Address:Port       Peer Address:Port  Process
tcp    LISTEN   0        128              0.0.0.0:ssh             0.0.0.0:*      users:(("sshd",pid=391,fd=3))
tcp    LISTEN   0        128                 [::]:ssh                [::]:*      users:(("sshd",pid=391,fd=4))
...
```

client

El cas de l'accés SSH - client

A la mateixa xarxa, un equip té la IP 10.1.1.128 ...

A les 16:24:33 inicia una sessió SSH des del port TCP 54146 cap al port TCP 22 del servidor 10.1.1.181 ...

L'usuari amb que es vol connectar és entel ...

```
~# ssh entel@10.1.1.181 2>debug_client.log
...
~# tcpdump -n -s 0 host 10.1.1.128 and 10.1.1.181 -w client_ssh.pcap; tcpdump -r client_ssh.pcap
reading from file client_ssh.pcap, link-type EN10MB (Ethernet), snapshot length 262144
16:24:33.163402 IP 10.1.1.128.54146 > 10.1.1.181.ssh: Flags [S], seq 3006517464, win 64240, options [mss 1460,sackOK,TS val
1776942468 ecr 0,nop,wscale 7], length 0
16:24:33.163751 IP 10.1.1.181.ssh > 10.1.1.128.54146: Flags [S.], seq 2950651346, ack 3006517465, win 65160, options [mss
1460,sackOK,TS val 3058246221 ecr 1776942468,nop,wscale 7], length 0
...
~# tshark -r client_ssh.pcap -j ssh
Running as user "root" and group "root". This could be dangerous.
1   0.000000   10.1.1.128 → 10.1.1.181   TCP 74 54146 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1776942468
TSecr=0 WS=128
2   0.000349   10.1.1.181 → 10.1.1.128   TCP 74 22 → 54146 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1
TSval=3058246221 TSecr=1776942468 WS=128
3   0.000366   10.1.1.128 → 10.1.1.181   TCP 66 54146 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1776942468 TSecr=3058246221
4   0.000683   10.1.1.128 → 10.1.1.181   SSH 98 Client: Protocol (SSH-2.0-OpenSSH_8.4p1 Debian-5)
```

client

El cas de l'accés SSH - client

El procés client SSH (amb PID 1285) no reconeix l'empremta digital del servidor i demana autorització a l'usuari ....

Un cop introduïda la contrasenya, entel accedeix al servidor ...

```
~# ps aux | grep -i ssh
tcpdump     1281  0.0  0.6  14652  6900 pts/1    S+   16:23   0:00 tcpdump -n -s 0 host 10.1.1.128 and 10.1.1.181 -w
client_ssh.pcap
root        1285  0.0  0.6  11984  6436 pts/0    S+   16:24   0:00 ssh entel@10.1.1.181
...
~# ssh entel@10.1.1.181 2>debug_client.log
The authenticity of host '10.1.1.181 (10.1.1.181)' can't be established.
ECDSA key fingerprint is SHA256:JO1Lip8qdvCotXmLgth2mCCokzIV+CM/B42jfU6PXg4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
entel@10.1.1.181's password:
Linux debian11 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon May  2 15:49:41 2022 from 10.1.1.128
entel@debian11:~$
```

client

El cas de l'accés SSH - client

L'usuari entel finalitza la sessió a la terminal, s'allibera la connexió TCP i s'elimina el procés 1285...

Què ha fet l'usuari mentre ha estat connectat?...

```
~# ssh entel@10.1.1.181 2>debug_client.log
...
entel@debian11:~$ exit
~#

~# cat debug_client.log
...
debug1: channel 0: free: client-session, nchannels 1
debug1: fd 2 clearing O_NONBLOCK
Connection to 10.1.1.181 closed.
Transferred: sent 2436, received 4904 bytes, in 82.0 seconds
Bytes per second: sent 29.7, received 59.8
debug1: Exit status 0

~# tcpdump -r client_ssh.pcap
...
16:26:02.185545 IP 10.1.1.128.54146 > 10.1.1.181.ssh: Flags [F.], seq 2741, ack 5865, win 501, options [nop,nop,TS val …
16:26:02.188941 IP 10.1.1.181.ssh > 10.1.1.128.54146: Flags [F.], seq 5865, ack 2742, win 501, options [nop,nop,TS val …
16:26:02.188967 IP 10.1.1.128.54146 > 10.1.1.181.ssh: Flags [.], ack 5866, win 501, options [nop,nop,TS val 1777031493 ecr …

~# ps aux | grep -i ssh
```

El cas de l'accés SSH – client-servidor

L'anàlisi comparatiu d'ambdues configuracions SSH és coherent

Els paràmetres de treball són compatibles i els registres estan habilitats en mode DEBUG ...

Client

```
~# cat /etc/ssh/ssh_config

# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.
...
LogLevel DEBUG
```

Servidor

```
~# cat /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.
...
SyslogFacility AUTH
LogLevel DEBUG
```

El cas de l'accés SSH – client-servidor

L'anàlisi comparatiu d'ambdós registres SSH és coherent ...

El registre del client té singularitats, com l'actualització dels known hosts ...

Client

```
~# cat debug_client.log
debug1: Connecting to 10.1.1.181 [10.1.1.181] port 22.                    ...
debug1: Connection established.                                           ...
debug1: Local version string SSH-2.0-OpenSSH_8.4p1 Debian-5               ...
debug1: Remote protocol version 2.0, remote software version OpenSSH_8.4p1 Debian-5 ...
debug1: kex: algorithm: curve25519-sha256                                 ...
debug1: kex: host key algorithm: ecdsa-sha2-nistp256                      ...
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none ...
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none ...
Warning: Permanently added '10.1.1.181' (ECDSA) to the list of known hosts. ...
Authenticated to 10.1.1.181 ([10.1.1.181]:22).                            ...
debug1: Entering interactive session.                                     ...
```

Servidor

```
~# cat /var/log/auth.log | grep -i ssh
...
May  2 16:24:33 debian11 sshd[2294]: debug1: Local version string SSH-2.0-OpenSSH_8.4p1 Debian-5 ...
May  2 16:24:33 debian11 sshd[2294]: debug1: Remote protocol version 2.0, remote software version OpenSSH_8.4p1 Debian-5 ...
May  2 16:24:33 debian11 sshd[2294]: debug1: kex: algorithm: curve25519-sha256 [preauth]  ...
May  2 16:24:33 debian11 sshd[2294]: debug1: kex: host key algorithm: ecdsa-sha2-nistp256 [preauth] ...
May  2 16:24:33 debian11 sshd[2294]: debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> ...
May  2 16:24:33 debian11 sshd[2294]: debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> ...
May  2 16:24:40 debian11 sshd[2300]: debug1: Entering interactive session for SSH2. ...
```

El cas de l'accés SSH – client-servidor

L'anàlisi comparatiu d'ambdós tràfics SSH és coherent ...

S'han enviat 134 missatges, amb RTT_{mig} ≈ 0,665 ms i una diferència de rellotges dins la tolerància (Δrellotges ≈ 6ms).

Client

```
~# ping -c 10 10.1.1.181
...
--- 10.1.1.181 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9145ms
rtt min/avg/max/mdev = 0.388/0.665/1.045/0.228 ms

~# tcpdump -r client_ssh.pcap
16:24:33.163402 IP 10.1.1.128.54146 > 10.1.1.181.ssh: Flags [S], seq 3006517464, win 64240, options [mss 1460,sackOK,TS val
1776942468 ecr 0,nop,wscale 7], length 0
...
16:26:02.188967 IP 10.1.1.128.54146 > 10.1.1.181.ssh: Flags [.], ack 5866, win 501, options [nop,nop,TS val 1777031493 ecr
3058335246], length 0
```

Servidor

```
~# tcpdump -r servidor_ssh.pcap
16:24:33.170619 IP 10.1.1.128.54146 > 10.1.1.181.ssh: Flags [S], seq 3006517464, win 64240, options [mss 1460,sackOK,TS val
1776942468 ecr 0,nop,wscale 7], length 0
...
16:26:02.196095 IP 10.1.1.128.54146 > 10.1.1.181.ssh: Flags [.], ack 5866, win 501, options [nop,nop,TS val 1777031493 ecr
3058335246], length 0
```

El cas de l'accés SSH – client-servidor

Què ha fet l'usuari mentre ha estat connectat?...

```
~# ssh entel@10.1.1.181 2>debug_client.log
The authenticity of host '10.1.1.181 (10.1.1.181)' can't be established.
ECDSA key fingerprint is SHA256:JO1Lip8qdvCotXmLgth2mCCokzIV+CM/B42jfU6PXg4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
entel@10.1.1.181's password:
Linux debian11 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon May  2 15:49:41 2022 from 10.1.1.128
entel@debian11:~$ ps aux | grep -i ssh
root         391  0.0  0.7  13292  7728 ?        Ss   13:13   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root         529  0.0  0.8  14456  8472 ?        Ss   13:14   0:00 sshd: entel [priv]
entel        555  0.0  0.6  14664  6172 ?        S    13:14   0:01 sshd: entel@pts/0
root        2121  0.0  0.8  14456  8796 ?        Ss   15:41   0:00 sshd: entel [priv]
entel       2127  0.0  0.6  14664  6072 ?        S    15:41   0:00 sshd: entel@pts/1
tcpdump     2290  0.0  0.7  14652  7056 pts/1    S+   16:23   0:00 tcpdump -n -s 0 host 10.1.1.128 and 10.1.1.181 -w servidor_ssh.pcap
root        2294  0.0  0.8  14456  8832 ?        Ss   16:24   0:00 sshd: entel [priv]
entel       2300  0.0  0.6  14668  6012 ?        S    16:24   0:00 sshd: entel@pts/2
entel       2305  0.0  0.0   6320   644 pts/2    R+   16:25   0:00 grep -i ssh
entel@debian11:~$ exit
cerrar sesión
```

"Posem llum a la foscor..."

El cas de l'accés SSH