

## PRÁCTICA 1 (almellonesfernandez-practica1)

### SSH. AUTENTICACIÓN. CONTROL DE ACCESO Y SEGURIDAD.

**CONEXIONES CIFRADAS USANDO CIFRADO ASIMÉTRICO, CONEXIÓN**

**CLIENTE-SERVIDOR. HERRAMIENTAS PARA CONTROLAR LAS CONEXIONES.**

1. Explique **con sus propias palabras** en relación al cifrado, poniendo ejemplos reales explicados en clase y algunas imágenes descriptivas, cuando lo crea oportuno:

a. ¿En qué consiste el cifrado asimétrico?

**El cifrado asimétrico es un método de seguridad que usa un par de claves distintas: una clave pública para cifrar el mensaje y una clave privada para descifrarlo. Esto permite que cualquier persona cifre información usando la clave pública, pero solo quien posee la clave privada puede descifrar y acceder al contenido. Este enfoque asegura que la información permanezca confidencial**

b. ¿En qué se basa la seguridad del cifrado asimétrico?

**La seguridad del cifrado asimétrico se basa en cifrar mensajes utilizando fórmulas matemáticas complejas que hacen que sea prácticamente imposible descifrarlos sin la clave privada correspondiente.**

c. ¿En qué se diferencia del cifrado simétrico?

**El cifrado simétrico usa una sola clave para cifrar y descifrar, esto lo hace más rápido, pero requiere compartir la clave de forma segura.**

d. ¿Para qué se usa en las conexiones con servidores SSH?

**Se usa para autenticar y establecer conexiones seguras. El servidor envía su clave pública al cliente, y el cliente la usa para cifrar los datos que solo el servidor puede descifrar**

2. Realice la instalación de servidor openssh-server en Servidor Ubuntu Server. (`#apt get install openssh-server`), y realice las siguientes evidencias: **(0,5 puntos cada uno)**

- a. Use comandos adecuados para comprobar que el servidor SSHD está funcionando y está escuchando en el puerto por defecto 22. (`#netstat -putan | grep 22 && systemctl status ssh`), y demuestre que ningún cliente está conectado. Posteriormente, realice la instalación de apache2, mysql-server y vsftpd y demuestre que esos servicios están escuchando (`netstat -putan | grep LISTEN`).

```
root@Ubuntu-server-bastionado:/home/almellonesfernandez$ netstat -putan | grep 22 && systemctl status ssh
tcp6      0      0 :::22                           ::::*                  LISTEN                1/init
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Sun 2024-10-20 10:09:48 UTC; 9min ago
TriggeredBy: ● ssh.socket
    Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 1878 (sshd)
    Tasks: 1 (limit: 2276)
   Memory: 1.2M (peak: 1.5M)
     CPU: 23ms
    CGroup: /system.slice/ssh.service
            └─1878 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 20 10:09:48 Ubuntu-server-bastionado systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 20 10:09:48 Ubuntu-server-bastionado sshd[1878]: Server listening on :: port 22.
Oct 20 10:09:48 Ubuntu-server-bastionado systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

al mellonesfernandez@Ubuntu-server-bastionado:~$ sudo netstat -putan | grep LISTEN
tcp      0      0 127.0.0.53:53          0.0.0.0:*          LISTEN        422/systemd-resolve
tcp      0      0 0.0.0.0:22           0.0.0.0:*          LISTEN        777/sshd: /usr/sbin
tcp      0      0 127.0.0.54:53          0.0.0.0:*          LISTEN        422/systemd-resolve
tcp      0      0 127.0.0.1:33060         0.0.0.0:*          LISTEN        980/mysqld
tcp      0      0 127.0.0.1:3306         0.0.0.0:*          LISTEN        980/mysqld
tcp6     0      0 ::::80              ::::*                  LISTEN        859/apache2
tcp6     0      0 ::::22              ::::*                  LISTEN        777/sshd: /usr/sbin
tcp6     0      0 ::::21              ::::*                  LISTEN        721/vsftpd
al mellonesfernandez@Ubuntu-server-bastionado:~$ _
```

- b. Conecte desde un cliente ssh GUI Windows anfitrión (putty, BitTunnelier, MobaTerm.) por primera vez usando el usuario XXxx (no es necesario en este caso introducir la contraseña para comprobar el ejercicio:

- Demuestre que hay un usuario conectado desde el cliente de Windows, con diferentes herramientas. (`ifconfig, netstat -putan | grep 22 | grep LISTEN` (en cliente y servidor), `tcpdump port 22, tcpdump port 22 and host XX, iptraf-ng`).

## Álvaro Almellones Fernández

```
3. almellonesfernandez@Ubuntu-server-bastionado:~$ echo "usamos el comando who para ver que ha entrado alguien desde otra ip:" && who && echo "salida de ifconfig: " && ifconfig && echo "salida del netstat del puerto 22 que estan escuchando: " && sudo netstat -putan | grep 22 | grep LISTEN
usamos el comando who para ver que ha entrado alguien desde otra ip:
almellonesfernandez tty1          2024-10-21 21:34
almellonesfernandez pts/0          2024-10-21 21:37 (192.168.1.106)
salida de ifconfig:
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.107  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe91:ca61  prefixlen 64  scopeid 0x20<link>
          ether 08:00:27:91:ca:61  txqueuelen 1000  (Ethernet)
            RX packets 1140  bytes 392037 (392.0 KB)
            RX errors 0  dropped 2  overruns 0  frame 0
            TX packets 975  bytes 95568 (95.5 KB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inetc6 ::1  prefixlen 128  scopeid 0x10<host>
          loop  txqueuelen 1000  (Local Loopback)
            RX packets 92  bytes 7904 (7.9 KB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 92  bytes 7904 (7.9 KB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

salida del netstat del puerto 22 que estan escuchando:
[sudo] password for almellonesfernandez:
tcp6       0      0  ::1:22                           ::*        LISTEN      1/init
almellonesfernandez@Ubuntu-server-bastionado:~$
```

```
3. root@Ubuntu-server-bastionado:~$ tcpdump port 22
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:38:45.754369 IP 192.168.1.106.54759 > Ubuntu-server-bastionado.ssh: Flags [P.], seq 953413540:953413576, ack 3
611882006, win 4100, length 36
21:38:45.754502 IP Ubuntu-server-bastionado.ssh > 192.168.1.106.54759: Flags [P.], seq 1:37, ack 36, win 488, length 36
21:38:45.764428 IP Ubuntu-server-bastionado.ssh > 192.168.1.106.54759: Flags [P.], seq 37:201, ack 36, win 488, length 164

3. root@Ubuntu-server-bastionado:~$ tcpdump port 22 and host 192.168.1.106
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:40:23.970633 IP Ubuntu-server-bastionado.ssh > 192.168.1.106.54759: Flags [P.], seq 3611903954:3611903990, ack 953434204, win 501, length 36
21:40:23.971175 IP 192.168.1.106.54759 > Ubuntu-server-bastionado.ssh: Flags [.], ack 36, win 4095, length 0
21:40:23.972383 IP 192.168.1.106.54759 > Ubuntu-server-bastionado.ssh: Flags [P.], seq 1:37, ack 36, win 4095, length 36
21:40:23.972473 IP Ubuntu-server-bastionado.ssh > 192.168.1.106.54759: Flags [P.], seq 36:72, ack 37, win 501, length 36

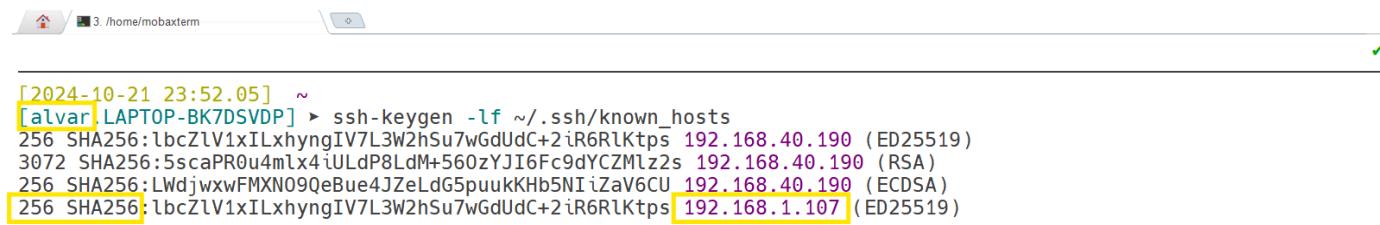
3. root@Ubuntu-server-bastionado:~$ iptraf-ng 1.2.1
iptraf-ng 1.2.1
TCP Connections (Source Host:Port) --> Packets --> Bytes --> Flag --> Iface --
[192.168.1.107:22] > 240 19764 -PA- enp0s3
[192.168.1.106:54759] > 194 12644 --A-- enp0s3
```

- ¿En qué fichero y directorio se descarga esa llave pública/fingerprint?

```
[2024-10-21 23:45:57] ~
[alvar] LAPTOP-BK7DSVDP] > find ~ -name known_hosts
/home/mobaxterm/.ssh/known_hosts
```

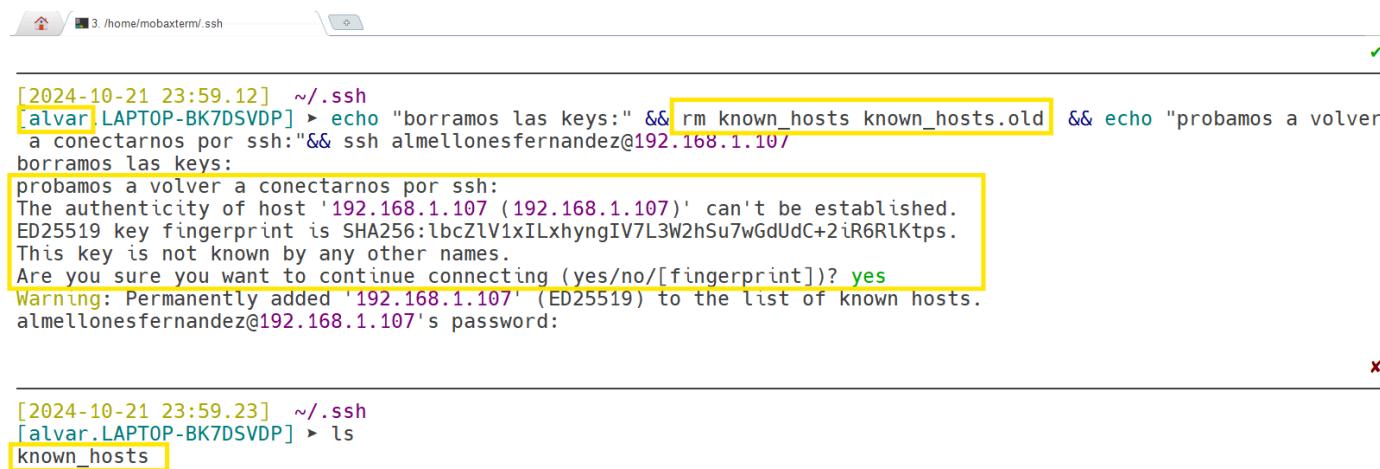
- ¿Qué características tiene esa llave pública/fingerprint (longitud de nº de bits y algoritmo)?

## Álvaro Almellones Fernández



```
[2024-10-21 23:52:05] ~
[alvar] LAPTOP-BK7DSVDP] > ssh-keygen -lf ~/.ssh/known_hosts
256 SHA256:lbCZlV1xILxhyngIV7L3W2hSu7wGdUdC+2iR6RlKtps 192.168.40.190 (ED25519)
3072 SHA256:5scaPR0u4mlx4iULdP8LdM+560zYJI6Fc9dYCZMLz2s 192.168.40.190 (RSA)
256 SHA256:LWdjwxwFMXN09QeBue4JZeLdG5puukKHb5NIiZaV6CU 192.168.40.190 (ECDSA)
256 SHA256:lbCZlV1xILxhyngIV7L3W2hSu7wGdUdC+2iR6RlKtps 192.168.1.107 (ED25519)
```

- ¿Qué pasa si borramos este fichero o borramos su contenido? Borre y comprueba que ocurre.



```
[2024-10-21 23:59:12] ~/.ssh
[alvar] LAPTOP-BK7DSVDP] > echo "borramos las keys:" && rm known_hosts known_hosts.old && echo "probamos a volver a conectarnos por ssh:&& ssh almellonesfernandez@192.168.1.107/borramos las keys:
probamos a volver a conectarnos por ssh:
The authenticity of host '192.168.1.107 (192.168.1.107)' can't be established.
ED25519 key fingerprint is SHA256:lbCZlV1xILxhyngIV7L3W2hSu7wGdUdC+2iR6RlKtps.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.107' (ED25519) to the list of known hosts.
almellonesfernandez@192.168.1.107's password:

[2024-10-21 23:59:23] ~/.ssh
[alvar] LAPTOP-BK7DSVDP] > ls
known_hosts
```

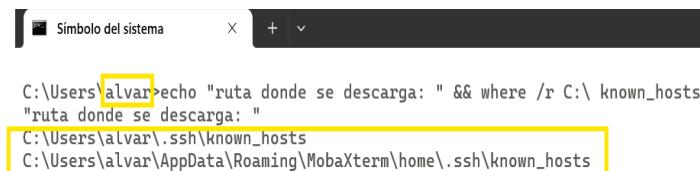
c. Responda a lo mismo que en el ejercicio anterior, pero ahora desde un equipo **cliente en modo comando (POWERSHELL o CMD)**. En este caso puede loguearse con el usuario XXXx:

- Muestre dicha conexión realizada con diferentes herramientas.



```
root@Ubuntu-server-bastionado:/home/almellonesfernandez] netstat -putan | grep 22 | grep ESTABLISHED && tcpdump port 22
tcp6          0      52 [192.168.1.107:22]           192.168.1.106 55458 [ESTABLISHED] 1418/sshd: almellon
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:14:16.223431 IP [Ubuntu-server-bastionado.ssh] > 192.168.1.106:55458: Flags [P.], seq 1166565554:1166565662, ack 3853410388, win 523, length 108
22:14:16.224177 IP 192.168.1.106:55458 > [Ubuntu-server-bastionado.ssh]: Flags [.], ack 108, win 4097, length 0
22:14:16.224435 IP [Ubuntu-server-bastionado.ssh] > 192.168.1.106:55458: Flags [P.], seq 108:224, ack 1, win 523, length 116
```

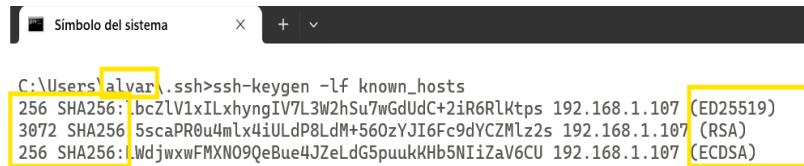
- ¿Dónde se descarga en nuestro equipo cliente?



```
C:\Users\alvar>echo "ruta donde se descarga: " && where /r C:\ known_hosts
"ruta donde se descarga: "
C:\Users\alvar\.ssh\known_hosts
C:\Users\alvar\AppData\Roaming\MobaXterm\home\.ssh\known_hosts
```

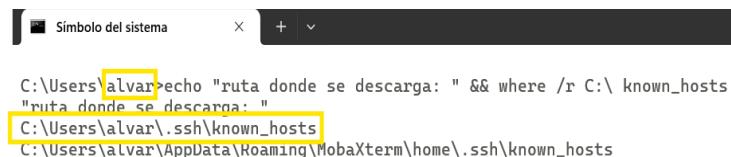
## Álvaro Almellones Fernández

- ¿Qué características tiene esa llave pública (longitud-nº de bits y algoritmo)?



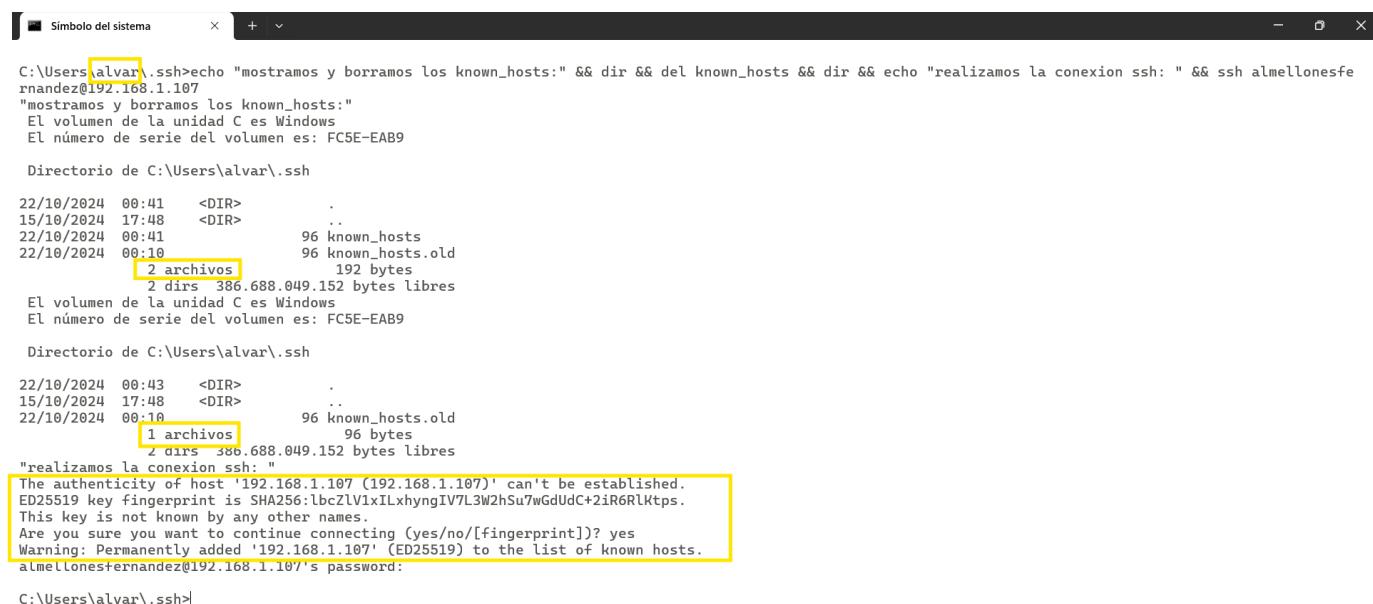
```
C:\Users\alvar\.ssh>ssh-keygen -lf known_hosts
256 SHA256:bczLvlV1xILxhyngIV7L3W2hSu7wGdUdC+2iR6Rlktps 192.168.1.107 (ED25519)
3072 SHA256:5scsPR0u4mlx4iULdP8LdM+560zYJ16Fc9dYCZMlz2s 192.168.1.107 (RSA)
256 SHA256:LwdjwxwFMXN09QeBue4JZeLdG5puukKHb5NIiZaV6CU 192.168.1.107 (ECDSA)
```

- ¿Dónde se ha guardado esa key/llave pública en el cliente?



```
C:\Users\alvar>echo "ruta donde se descarga: " && where /r C:\ known_hosts
"ruta donde se descarga: "
C:\Users\alvar\.ssh\known_hosts
C:\Users\alvar\AppData\Roaming\MobaXterm\home\.ssh\known_hosts
```

- ¿Qué pasa si borramos este fichero o borramos su contenido? Borra y comprueba que ocurre.



```
C:\Users\alvar>echo "mostramos y borramos los known_hosts: " && dir && del known_hosts && dir && echo "realizamos la conexion ssh: " && ssh almellonesfernandez@192.168.1.107
"mostramos y borramos los known_hosts: "
El volumen de la unidad C es Windows
El n mero de serie del volumen es: FC5E-EAB9

Directorio de C:\Users\alvar\.ssh

22/10/2024 00:41    <DIR>      .
15/10/2024 17:48    <DIR>      ..
22/10/2024 00:41            96 known_hosts
22/10/2024 00:10            96 known_hosts.old
[2 archivos]           192 bytes
2 dirs 386.688.049.152 bytes libres
El volumen de la unidad C es Windows
El n mero de serie del volumen es: FC5E-EAB9

Directorio de C:\Users\alvar\ssh

22/10/2024 00:43    <DIR>      .
15/10/2024 17:48    <DIR>      ..
22/10/2024 00:10            96 known_hosts.old
[1 archivos]           96 bytes
2 dirs 386.688.049.152 bytes libres
"realizamos la conexion ssh: "
The authenticity of host '192.168.1.107 (192.168.1.107)' can't be established.
ED25519 key fingerprint is SHA256:bczLvlV1xILxhyngIV7L3W2hSu7wGdUdC+2iR6Rlktps.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.107' (ED25519) to the list of known hosts.
almellonesfernandez@192.168.1.107's password:
```

- d. Realice una conexión desde el cliente en modo comando desde Ubuntu Desktop y demuestre que se ha producido la conexión.

## Álvaro Almellones Fernández

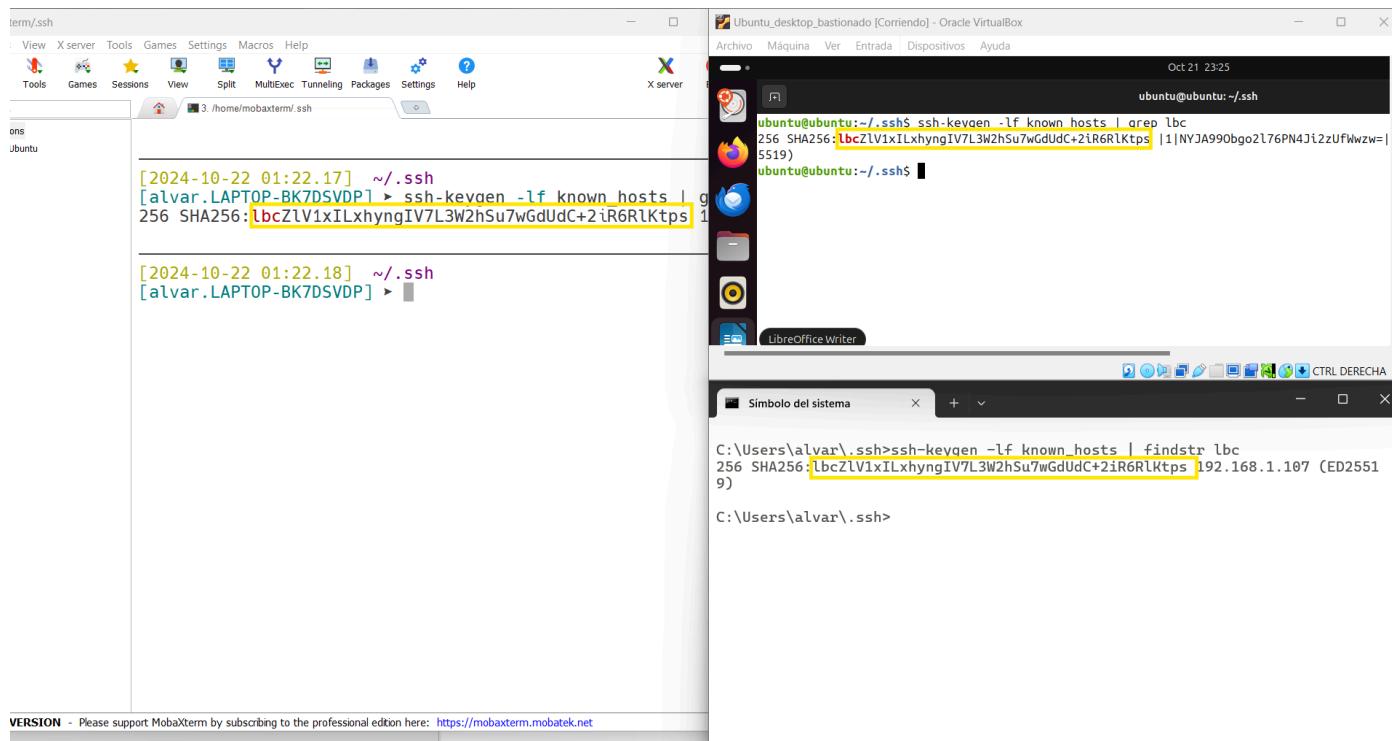
```
root@Ubuntu-server-bastionado:/home/almellonesfernandez
root@Ubuntu-server-bastionado:/home/almellonesfernandez: who && netstat -putan | grep ESTABLISHED && tcpdump p
ort 22
almellonesfernandez tty1      2024-10-21 21:34
almellonesfernandez pts/0      2024-10-21 23:09 (192.168.1.108)
almellonesfernandez pts/1      2024-10-21 23:10 (192.168.1.108)
tcp6      0      [REDACTED] 192.168.1.107:22 192.168.1.108:44742 ESTABLISHED 1839/sshd: almellon
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:10:49.296078 IP Ubuntu-server-bastionado.ssh > 192.168.1.108.44742: Flags [P.], seq 4105126265:4105126373, ack 367557
7530, win 480, options [nop,nop,TS val 1117980561 ecr 1713193384], length 108
23:10:49.297259 IP 192.168.1.108.44742 > Ubuntu-server-bastionado.ssh: Flags [.], ack 108, win 1135, options [nop,nop,TS
val 1713193401 ecr 1117980547], length 0
23:10:49.298030 IP Ubuntu-server-bastionado.ssh > 192.168.1.108.44742: Flags [P.], seq 108:224, ack 1, win 480, options
[nop,nop,TS val 1117980563 ecr 1713193401], length 116
23:10:49.303344 IP 192.168.1.108.44742 > Ubuntu-server-bastionado.ssh: Flags [P.], seq 1:37, ack 224, win 1135, options
[nop,nop,TS val 1713193401 ecr 1117980563], length 36
23:10:49.303617 IP Ubuntu-server-bastionado.ssh > 192.168.1.108.44742: Flags [P.], seq 224:260, ack 37, win 480, options
[nop,nop,TS val 1117980568 ecr 1713193407], length 36
23:10:49.327380 IP 192.168.1.108.44742 > Ubuntu-server-bastionado.ssh: Flags [P.], seq 37:73, ack 260, win 1135, options
```

### Bastionaje de Redes y Sistemas Francisco Javier López 3 de 45

Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información

e. ¿Es la misma key/llave pública la que se ha descargado con los tres clientes diferentes?

Responda con palabra: ¿Por qué ocurre eso? ¿en qué equipo y en qué lugar se queda siempre la key/clave/llave privada?



La key pública que se descarga en los tres clientes es la misma , debido a que el servidor genera un par de keys , cada vez que un cliente quiere realizar una conexión con el servidor por primera vez , este hace una copia de la key pública y se la da al cliente. Mientras que la key privada siempre se queda en el servidor

**REFORZANDO CONOCIMIENTO COMUNICACIONES CIFRADAS USANDO CIFRADO ASIMÉTRICO CON HTTPS**

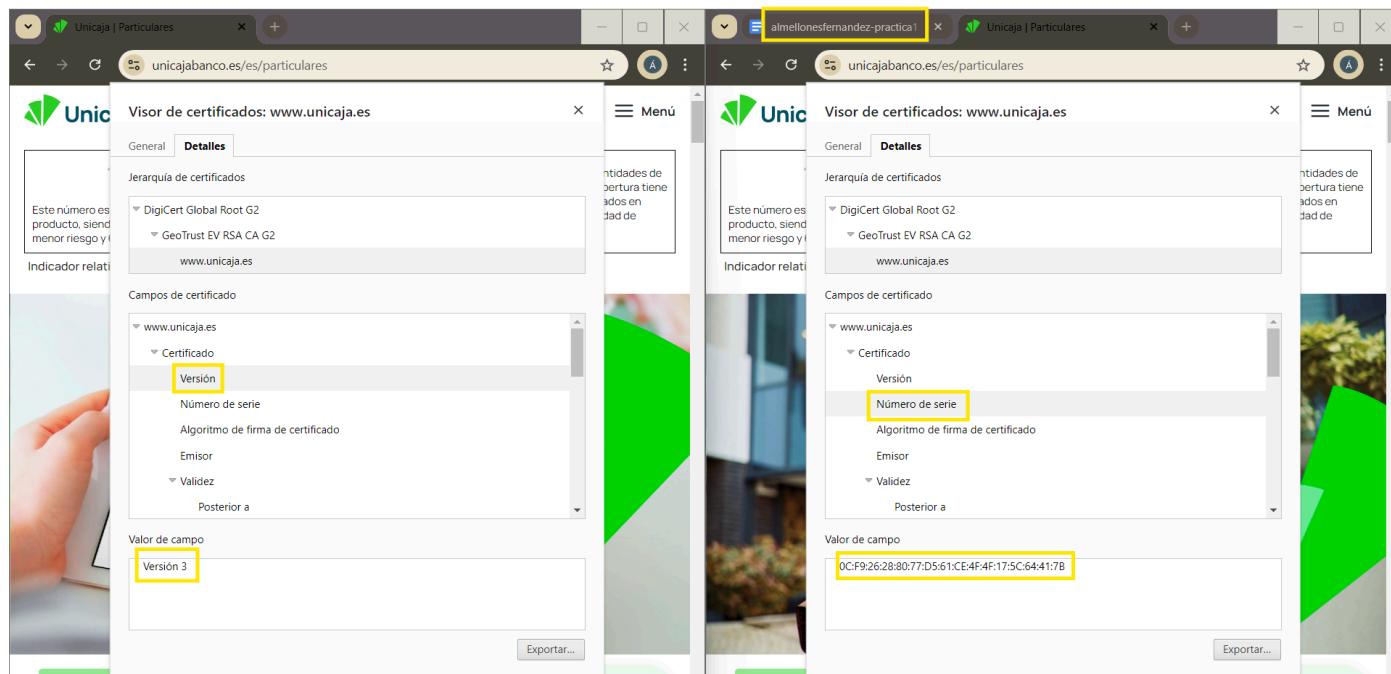
**Bastionaje de Redes y Sistemas Francisco Javier López 3 de 41**

*Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información*

3. En relación a los servidores webs en Internet y su protocolo https, realice una conexión al servidor <https://www.unicajabanco.es/>, desde un navegador web predeterminado y responda (mediante capturas) a las siguientes preguntas relacionadas con la llave pública usada en la conexión:

**▪ RELACIONADO CON LA CONEXIÓN A SERVIDOR <https://www.unicajabanco.es/>**

a. ¿Versión y número de serie del certificado?



b. ¿Qué autoridad certificada internacional certifica esta llave pública? Busque alguna información relevante en relación a esta empresa.

## Álvaro Almellones Fernández

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

Indicador relativo a la Cuenta

Bizum

**Volando promoción 150€ con Bizum**

Sorteamos 10 tarjetas de 150€\*\*\* entre los primeros 100.000 usuarios de Bizum. Descarga nuestra app y consigue una tarjeta de 150€ para volar hacia ti.

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

Indicador relativo a la Cuenta

Bizum

**Volando promoción 150€ con Bizum**

Sorteamos 10 tarjetas de 150€\*\*\* entre los primeros 100.000 usuarios de Bizum. Descarga nuestra app y consigue una tarjeta de 150€ para volar hacia ti.

DigiCert es una empresa que ofrece certificados digitales para asegurar sitios web y proteger datos en línea. Se especializa en soluciones de seguridad para empresas, ayudando a que las comunicaciones sean más seguras.

c. ¿Con qué algoritmo y número de bytes se ha firmado el certificado?

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

Indicador relativo a la Cuenta

Bizum

**Volando promoción 150€ con Bizum**

Sorteamos 10 tarjetas de 150€\*\*\* entre los primeros 100.000 usuarios de Bizum. Descarga nuestra app y consigue una tarjeta de 150€ para volar hacia ti.

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

Indicador relativo a la Cuenta

Bizum

**Volando promoción 150€ con Bizum**

Sorteamos 10 tarjetas de 150€\*\*\* entre los primeros 100.000 usuarios de Bizum. Descarga nuestra app y consigue una tarjeta de 150€ para volar hacia ti.

## Álvaro Almellones Fernández

En relación a la clave/key/llave pública:

a. Algoritmo usado.

Visor de certificados: www.unicaja.es

General Detalles

Jerarquía de certificados

» DigiCert Global Root G2  
» GeoTrust EV RSA CA G2  
www.unicaja.es

Campos de certificado

Emisor  
» Validez  
Tema  
» Información de clave pública de la entidad receptor  
Algoritmo de clave pública de la entidad receptor  
Clave pública de la entidad receptor  
» Extensiones  
ID de clave de la entidad emisora de certificados

Valor de campo

PKCS #1 con cifrado RSA

Exportar...

b. Tamaño en número de bytes.

www.unicaja.es

Campos de certificado

Emisor  
» Validez  
Tema  
» Información de clave pública de la entidad receptor  
Algoritmo de clave pública de la entidad receptor  
Clave pública de la entidad receptor  
» Extensiones  
ID de clave de la entidad emisora de certificados

Valor de campo

Módulo (2048 bits)  
E7 AC B5 43 79 CA 6A B7 84 10 A6 C1 D5 F1 71 B8  
DA B4 EE D9 92 D0 63 A3 60 39 6F A1 F2 22 A2 8E  
69 98 64 0C 37 41 C0 11 3E 2E 9A 5B 1D 38 7D 27  
20 35 B9 B7 CF FF 8C 0A D3 38 72 90 A7 51 AE E1

Exportar...

## Álvaro Almellones Fernández

e. ¿Cuándo fue emitido y cuando caduca? ¿Está en vigor?

The image displays two side-by-side screenshots of the Unicaja website's certificate viewer. Both screenshots show the certificate for the domain [www.unicaja.es](http://www.unicaja.es). The left screenshot has the 'Anterior a' button highlighted with a yellow box, while the right screenshot has the 'Posterior a' button highlighted with a yellow box. Both screenshots also highlight the issuance date '23/2/25, 0:59:59 CET' and the expiration date '17/6/24, 2:00:00 CEST'.

a. La Llave pública. Demuestre que el número de bytes es correcto.

The image shows a detailed view of the certificate's public key section. It highlights the 'Clave pública de la entidad receptor' field with a yellow box. Below this, the 'Valor de campo' section displays the modulus as 'Módulo (2048 bits)' followed by a long string of hex digits: E7 AC B5 43 79 CA 6A B7 84 10 A6 C1 D5 F1 71 B8 DA B4 EE D9 92 D0 63 A3 60 39 6F A1 F2 22 A2 8E 69 98 64 0C 37 41 C0 11 3E 2E 9A 5B 1D 38 7D 27 20 35 B9 B7 CF FF 8C 0A D3 38 72 90 A7 51 AE E1.

## Álvaro Almellones Fernández

En relación a la huella digital o fingerprint:

- a. Algoritmo
- b. Tamaño en número de bytes. Demuestre que el número de bytes es correcto.
- c. Fingerprint

Visor de certificados: www.unicaja.es

General Detalles

Jerarquía de certificados

- ▼ DigiCert Global Root G2
- ▼ GeoTrust EV RSA CA G2
- www.unicaja.es

Campos de certificado

Tema

- Información de clave pública de la entidad receptora
- Extensiones
- Algoritmo de firma de certificado
- Valor de firma de certificados
- ▼ Huellas digitales: SHA-256

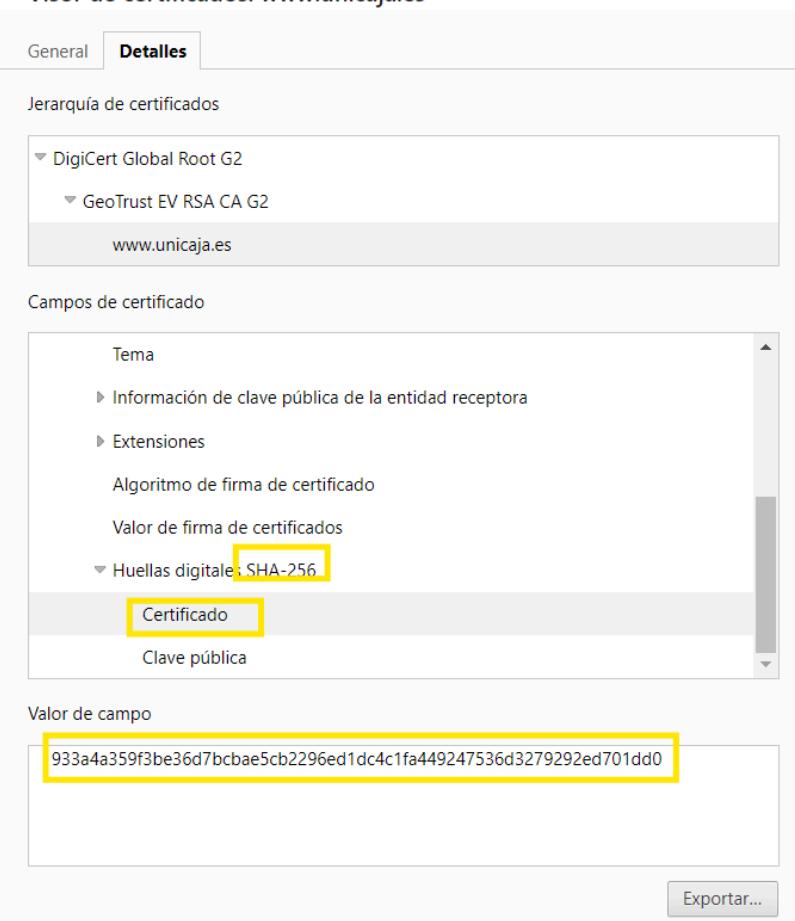
Certificado

Clave pública

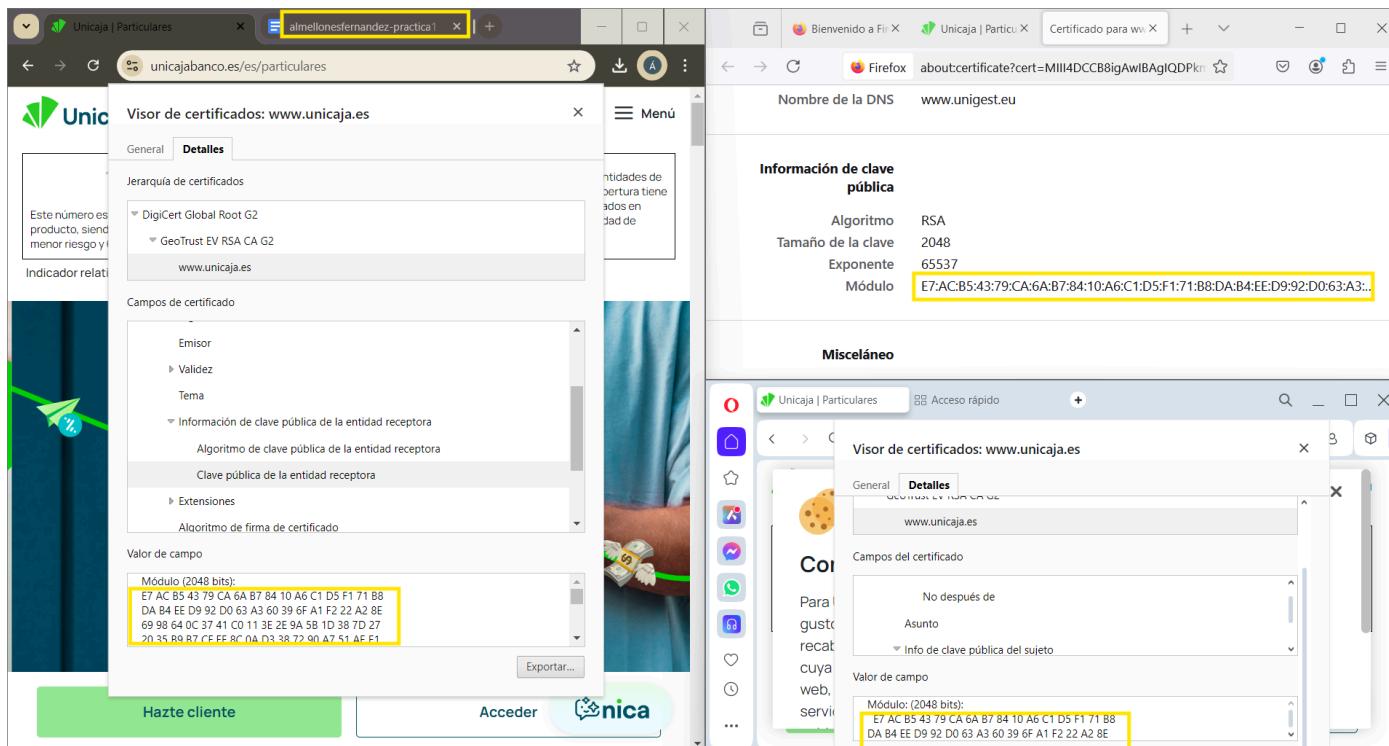
Valor de campo

933a4a359f3be36d7bcbae5cb2296ed1dc4c1fa449247536d3279292ed701dd0

Exportar...



- g. A continuación, realice la conexión desde otros dos navegadores distinto al anterior (Opera, Firefox Chrome, etc.), y demuestre mediante una única captura, que todas las llaves públicas que aparece son iguales en cada navegador. ¿Por qué cree que ocurre esto (*palabras*)? ¿Le recuerda esto algo a lo que ha ocurrido con el cifrado en comunicaciones SSH (*con sus palabras*)?



**Las llaves públicas son iguales en todos los navegadores porque el servidor (Unicaja Banco) presenta el mismo certificado digital a cada cliente. Este certificado contiene la llave pública utilizada para establecer conexiones seguras (HTTPS)**

**En las conexiones SSH, ocurre algo similar: se presenta un certificado con una llave pública que también se verifica de la misma manera. Tanto en HTTPS como en SSH, la seguridad se fundamenta en el uso de llaves públicas para cifrar y autenticar la comunicación**

h. ¿Qué diferencias hay entre la “la descarga de la llave pública del servidor ssh, y la de “servidor https”?

**La descarga de la llave pública en SSH es manual y se utiliza para la administración remota de servidores, usando llaves en formato OpenSSH. La validación depende de la confianza del usuario. En HTTPS, la llave pública se incluye en certificados digitales, obteniéndose automáticamente al establecer una conexión segura, con validación a través de autoridades certificadoras preinstaladas. SSH es manual y enfocado en la administración, mientras que HTTPS es automático y orientado a la navegación segura.**

**REDUCIENDO LAS PROBABILIDADES DE EXPOSICIÓN ATAQUES. CONEXIÓN CLIENTE SERVIDOR**

4. Sobre el fichero de configuración del servidor Ubuntu Server ([/etc/ssh/sshd\\_config](#)) modifique las siguientes opciones y realice diferentes conexiones variadas (cliente Windows (CMD/Powershell), GUI de Windows) para demostrar lo que realiza cada una de las opciones. Los cambios a realizar son (0,5 puntos cada opción):

a. Active el banner (Banner [/etc/issue.net](#)) para que muestre información cada vez que se conecte y escriba en dicho fichero el siguiente contenido (Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno XXXX. Está prohibida la conexión si no es Administrador de este sistema informático).

**Bastionaje de Redes y Sistemas** Francisco Javier López 4 de 45  
Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información

```
C:\Users\alvar>ssh almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
almellonesfernandez@192.168.1.107 s password:
```

b. Pruebe a conectarse desde cualquier cliente con el usuario root. Haga todo lo necesario para que pueda conectarse con el usuario root. ([PermitRootLogin](#)) ([iptraf-ng](#), # [tcpdump port 22](#))

```
almellonesfernandez@Ubuntu-server-bastionado:~$ sudo cat /etc/ssh/sshd_config |grep PermitRootLogin |grep yes
PermitRootLogin yes
```

```
C:\Users\alvar>ssh root@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
root@192.168.1.107 s password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)
```

```
root@Ubuntu-server-bastionado:~# tcpdump port 22
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
01:04:38.721692 IP Ubuntu-server-bastionado.ssh > 192.168.1.106.59042: Flags [P.], seq 3413666824:3413667020, ack 63721032, win 501, length 36
01:04:38.728468 IP 192.168.1.106.59042 > Ubuntu-server-bastionado.ssh: Flags [P.], seq 1:37, ack 196, win 509, length 36
01:04:38.728592 IP Ubuntu-server-bastionado.ssh > 192.168.1.106.59042: Flags [P.], seq 196:232, ack 37, win 501, length 36
```

```
iptraf-ng 1.2.1
          (Press Ctrl+C to stop)
          (Press Ctrl+D to close Host:Port)
          (Press Ctrl+L to clear screen)
          (Press Ctrl+T to toggle table mode)
          (Press Ctrl+R to refresh)
          (Press Ctrl+M to show menu)
          (Press Ctrl+H to show help)
          (Press Ctrl+Q to quit)

          Host:Port          Source          Destination      Packets      Bytes   Flag    Iface
          192.168.1.107:22  192.168.1.106.59042      >           208       32896  -PA-   enp0s3
          192.168.1.106.59042  192.168.1.107:22      >           168       10644  --A-- enp0s3
```

## Álvaro Almellones Fernández

c. Sólo se permite dos intentos para loguearse (*MaxAuthTries 2*). Pruebe a realizar tres intentos (fallando la contraseña 3 veces).

```
almellonesfernandez@Ubuntu-server-bastionado:~$ sudo cat /etc/ssh/sshd_config |grep MaxAuthTries
MaxAuthTries 2

C:\Users\alvar>ssh almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
almellonesfernandez@192.168.1.107's password:
Permission denied, please try again.
almellonesfernandez@192.168.1.107's password:
Received disconnect from 192.168.1.107 port 22:2: Too many authentication failures
Disconnected from 192.168.1.107 port 22
```

d. Demuestre para que vale la opción. (*LoginGraceTime 60*)

```
almellonesfernandez@Ubuntu-server-bastionado:~$ sudo cat /etc/ssh/sshd_config |grep LoginGraceTime
LoginGraceTime 60

C:\Users\alvar>ssh almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
almellonesfernandez@192.168.1.107's password:
Connection closed by 192.168.1.107 port 22
```

SI TARDAS MÁS DE UN MINUTO EN PONER LA CONTRASEÑA NO TE CONECTA

e. Sólo se permiten **dos** bash abiertas a la vez. (*MaxStartups 2*). Cuidado con algunos programas GUI que abren varias sesiones a la vez. (*netstat -an | grep 22 | grep ESTABLISHED,iptraf-ng*)

```
almellonesfernandez@Ubuntu-server-bastionado:~$ sudo cat /etc/ssh/sshd_config |grep MaxStartups
MaxStartups 2

C:\Users\alvar>ssh almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
(almellonesfernandez@192.168.1.107) Password:
```

C:\Users\alvar>ssh almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
(almellonesfernandez@192.168.1.107) Password:

```
C:\Users\alvar>ssh almellonesfernandez@192.168.1.107
Connection closed by 192.168.1.107 port 22

C:\Users\alvar>
```

**REDUCIENDO LAS PROBABILIDADES DE EXPOSICIÓN DE ATAQUES. SEGURIDAD DEL**

**SERVICIO DIRECTAMENTE.**

Siguiendo con las opciones de configuración del servidor SSHD de Ubuntu Server: (1 punto cada opción)

5. Demuestra que permite conectarse desde una determinada IP (por ejemplo, equipo IP anfitrión), pero no desde otra IP (Ubuntu Desktop), y al revés, jugando además con diferentes usuarios (XXxx, root, pXXxx, etc.). (AllowUsers y DenyUser) (GroupUsers y Denygroups). Se deja al alumno que elija la configuración que deseé de IP/red/usuario, adaptada a las IPs de su casa/trabajo.

The screenshot shows three terminal windows. The top window is a terminal session on the server (Ubuntu Server - bastionado) displaying the configuration of the SSH daemon. It shows two lines of configuration: `AllowUsers *@192.168.1.106 almellonesfernandez@192.168.1.108` and `DenyUsers root@192.168.1.108`. The middle window is a desktop session (Ubuntu\_desktop\_bastionado [Corriendo] - Oracle VirtualBox) showing a failed attempt to log in as root from the server's IP (192.168.1.107). The bottom window is another terminal session on the server showing a successful login as root from the desktop's IP (192.168.1.107).

```
al mellonesfernandez@Ubuntu-server-bastionado:~$ cat /etc/ssh/sshd_config |grep AllowUsers && cat /etc/ssh/sshd_config |grep DenyUsers
AllowUsers *@192.168.1.106 almellonesfernandez@192.168.1.108
DenyUsers root@192.168.1.108
al mellonesfernandez@Ubuntu-server-bastionado:~$
```

```
ubuntu@ubuntu:~$ ssh root@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez
da la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
(root@192.168.1.107) Password:
(root@192.168.1.107) Password:
(root@192.168.1.107) Password:
(root@192.168.1.107's password:
Permission denied, please try again.
root@192.168.1.107's password:|||
```

```
ubuntu@ubuntu:~$ ssh almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez
da la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
(al mellonesfernandez@192.168.1.107) Password:
(al mellonesfernandez@192.168.1.107) Verification code:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

System information as of Tue Oct 22 10:53:22 AM UTC 2024

System load: 0.08          Processes: 107
107
Usage of /: 12.9% of 24.44GB  Users logged in: 1
1
Memory usage: 28%          IPv4 address for enp0s3: 192.168.1.107
192.168.1.107
Swap usage: 0%              Swap usage: 0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.
```

## Álvaro Almellones Fernández

6. Cambie el puerto de escucha del servidor SSHD a 2222 para conexiones vía localhost y 22 para conexiones externas (**ListenAddress**) (tarjeta de red) (#netstat -putan | grep 22 | grep LISTEN , tcpdump -i lo port 222, iptraf-ng, etc.). Realice las evidencias suficientes para demostrar este hecho.

```
al mellonesfernandez@Ubuntu-server-bastionado:~$ sudo netstat -putan | grep 22 && sudo tcpdump -i lo port 2222
tcp6      0      0 ::::22          ::::*                      LISTEN      1/init
tcp6      0      36 192.168.1.107:22    192.168.1.106:59367 ESTABLISHED 3519/sshd: almellon
udp      0      0 192.168.1.107:68    0.0.0.0:*                  422/systemd-network
udp6      0      0 fe80::a00:27ff:fe91:546 ::::*                  422/systemd-network
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

```
al mellonesfernandez@Ubuntu-server-bastionado:~$ sudo netstat -putan | grep LISTEN && sudo tcpdump -i lo port 2222
tcp      0      0 127.0.0.53:53    0.0.0.0:*                  LISTEN      391/systemd-resolve
tcp      0      0 127.0.0.1:33060   0.0.0.0:*                  LISTEN      904/mysqld
tcp      0      0 0.0.0.0:22       0.0.0.0:*                  LISTEN      4546/sshd  /usr/sbi
tcp      0      0 127.0.0.1:2222   0.0.0.0:*                  LISTEN      4546/sshd  /usr/sbi
tcp      0      0 127.0.0.1:3306   0.0.0.0:*                  LISTEN      904/mysqld
tcp      0      0 127.0.0.54:53    0.0.0.0:*                  LISTEN      391/systemd-resolve
tcp6     0      0 ::::80          ::::*                      LISTEN      784/apache2
tcp6     0      0 ::::21          ::::*                      LISTEN      680/vsftpd
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Álvaro Almellones Fernández

7. Configure /etc/hosts.deny (ALL:ALL), y realice algunas actuaciones usando acl de [TCP-Wrappers](#) ([/etc/hosts.allow](#), [/etc/hosts.deny](#)), para permitir algunos equipos (se deja libertad al alumno desde el número de hosts clientes desde donde probar). Las actuaciones tienen que mostrar que se “juega” con:

- a. Comprobar que esta activada TCP-Wrappers para los servicios SSHD y vsftfp, pero no para mysql-server y apache2).

```
[almellonesfernandez@Ubuntu ~]$ echo "comprobacion de que sshd y vsftpd usa tcp-Wrapper:" && ldd $(which sshd) | grep libwrap && ldd $(which vsftpd) | grep libwrap && echo "comprobacion de que mysql y apache2 no usa tcp-Wrapper:" && ldd $(which mysql) | grep libwrap && ldd $(which apache2) | grep libwrap
comprobacion de que sshd v vsftpd usa tcp-Wrapper:
    libwrap.so.0 => /lib/x86_64-linux-gnu/libwrap.so.0 (0x00007df15bac7000)
    libwrap.so.0 => /lib/x86_64-linux-gnu/libwrap.so.0 (0x000070dafbff000)
comprobacion de que mysql y apache2 no usa tcp-Wrapper:
[almellonesfernandez@Ubuntu-server-bastionado ~]$
```

b. Servicio SSHD con hosts individuales, subredes, localhost.

```
almellonesfernandez@Ubuntu-server-bastionado:~$ echo "salida deny: " && cat /etc/hosts.deny |grep ALL && echo "salida allow:  
" && cat /etc/hosts.allow |grep sshd  
salida deny:  
# Example:    ALL: some.host.name, .some.domain  
#                  ALL EXCEPT in.fingerd: other.host.name, .other.domain  
ALL: ALL  
salida allow:  
sshd: 192.168.1.106  
sshd: 192.168.1.107  
almellonesfernandez@Ubuntu-server-bastionado:~$
```

```
al mellonesfernandez@Ubuntu ~$ exit
logout
Connection to 192.168.1.107 closed.

C:\Users\alvar>ipconfig |find str
FIND: formato de parámetros incorrecto

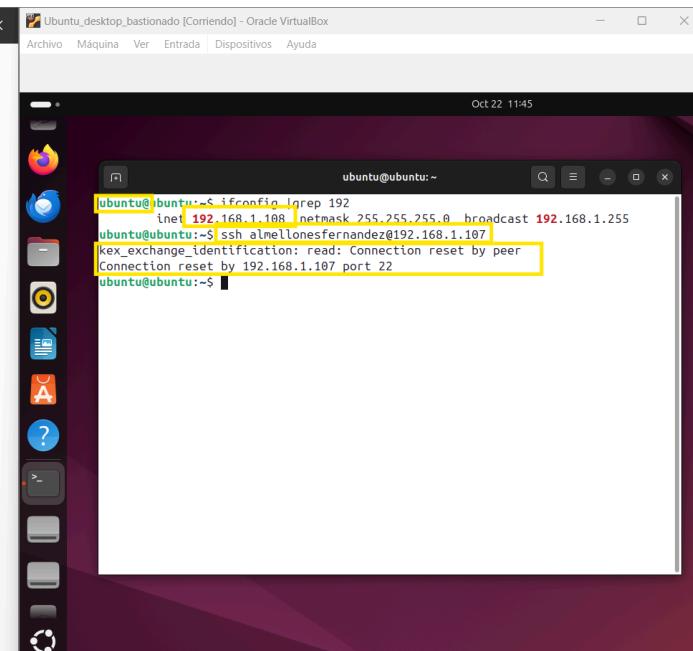
C:\Users\alvar>ipconfig |findstr 192
    Dirección IPv4. . . . . : 192.168.56.1
    Dirección IPv4. . . . . : 192.168.1.106
    Puerta de enlace predeterminada . . . . : 192.168.1.1

C:\Users\alvar>ssh almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje
de redes, del alumno almellonesfernandez. Está prohibida la
conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
(almellonesfernandez@192.168.1.107) Password:
(almellonesfernandez@192.168.1.107) Verification code:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86
_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Tue Oct 22 11:44:30 AM UTC 2024

      System load:  0.12          Processes:               1
      05
      Usage of /:   12.9% of 24.44GB  Users logged in:  1
      Memory usage: 28%            IPv4 address for enp0s3: 1
```



c. Servicio vsftpd con hosts individuales, subredes, localhost.

## Álvaro Almellones Fernández

The image shows three terminal windows. The top-left window (Ubuntu terminal) displays a command to filter hosts.allow and hosts.deny for the vsftpd service. The output shows 'vsftpd' is denied (ALL) and allowed (192.168.1.106). The bottom-left window (Windows terminal) shows an attempt to connect via FTP to 192.168.1.107, which fails with 'Service not available'. The right window (Ubuntu desktop terminal) shows a successful connection attempt via SSH to the same IP.

```
almellonesfernandez@Ubuntu-server-bastionado:~$ echo "salida deny: " && cat /etc/hosts.deny |grep vsftpd && echo "salida allow: "
W: "&& cat /etc/hosts.allow |grep vsftpd
salida deny:
vsftpd: ALL
salida allow:
vsftpd: 192.168.1.106
vsftpd: 192.168.1.107
almellonesfernandez@Ubuntu-server-bastionado:~$"

Símbolo del sistema - ftp 192  +  ×
C:\Users\alvar>ftp 192.168.1.107
Conectado a 192.168.1.107.
220 (vsFTPd 3.0.5)
200 Always in UTF8 mode.
Usuario (192.168.1.107:(none)):

Ubuntu_desktop_bastionado [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Oct 22 12:08
ubuntu@ubuntu:~$ buntu@ubuntu:~$ ftp 192.168.1.107
Connected to 192.168.1.107.
421 Service not available.
ftp>
```

d. Retoque el fichero /etc/hosts.deny, para Denegar alguna conexión pero loguear el acceso de un intento de “ataque” (poner mensaje personalizado). (*tail -f ficheroXXXX.log*).

The image shows four terminal windows. The top-left window (Ubuntu terminal) shows the 'tail -f' command running on a log file ('ficheroalvaroalmellones.log') capturing multiple failed connection attempts from 192.168.1.106. The top-right window (Ubuntu terminal) shows a command to edit /etc/hosts.deny to log failed connections to a specific log file. The bottom-left window (Windows terminal) shows two failed FTP connection attempts to 192.168.1.107, both failing with 'Service not available' and closing the connection. The bottom-right window (Ubuntu desktop terminal) shows a third failed connection attempt via SSH to 192.168.1.107.

```
almellonesfernandez@Ubuntu-server-bastionado:~$ tail -f /var/log/ficheroalvaroalmellones.log
::::ffff:192.168.1.106 que es sospechoso ,intento acceder al servicio vsftpd
::::ffff:192.168.1.106 que es sospechoso ,intento acceder al servicio vsftpd
::::ffff:192.168.1.106 que es sospechoso ,intento acceder al servicio vsftpd
::::ffff:192.168.1.106 que es sospechoso ,intento acceder al servicio vsftpd
almellonesfernandez@Ubuntu-server-bastionado:~$ sudo tail -n 3 /etc/hosts.deny
# versions of Debian this has been the default.
vsftpd: ALL : spawn \
(/bin/echo % que es sospechoso ,intento acceder al servicio %>> /var/log/ficheroalvaroalmellones.log )
almellonesfernandez@Ubuntu-server-bastionado:~$"

Símbolo del sistema  +  ×
C:\Users\alvar>ftp 192.168.1.107
Conectado a 192.168.1.107.
421 Service not available.
Conexión cerrada por el host remoto.

C:\Users\alvar>ftp 192.168.1.107
Conectado a 192.168.1.107.
421 Service not available.
Conexión cerrada por el host remoto.

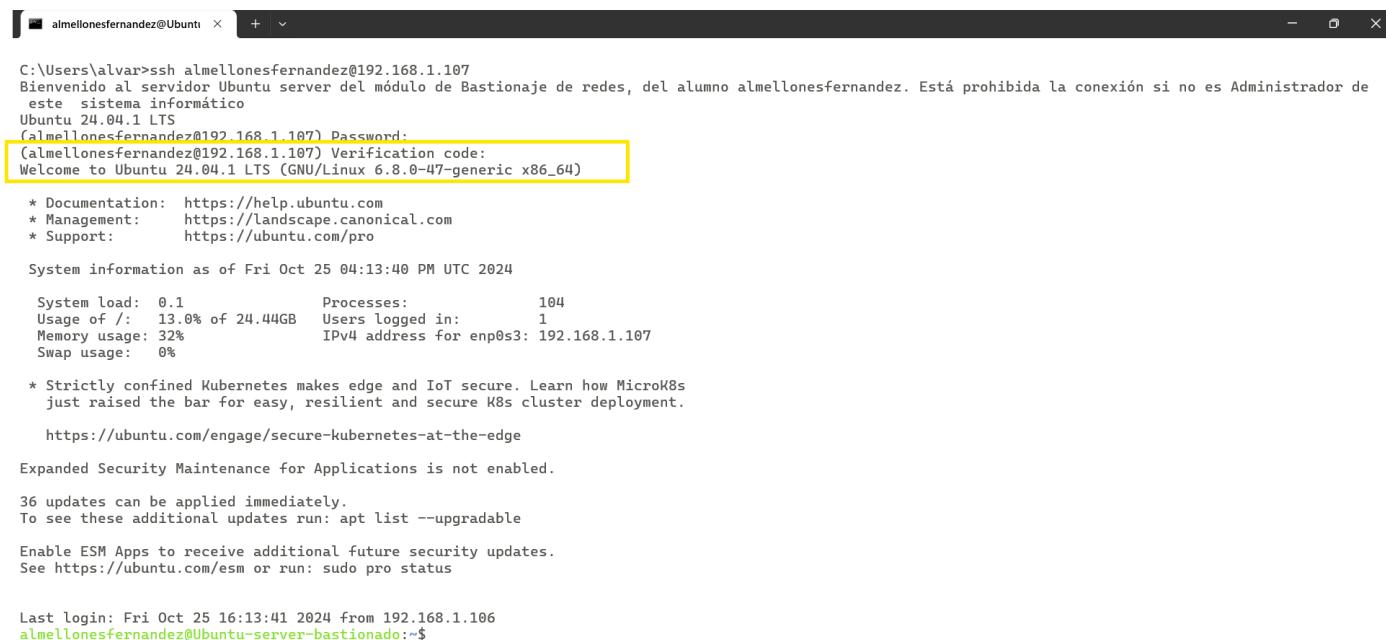
C:\Users\alvar>ftp 192.168.1.107
Conectado a 192.168.1.107.
421 Service not available.
Conexión cerrada por el host remoto.

C:\Users\alvar>
```

## Álvaro Almellones Fernández

### **DOBLE FACTOR DE AUTENTIFICACIÓN (2FA) USANDO TOTP (Time-based one-time Password)**

8. Realice todo lo necesario para que se pueda entrar al servidor SSHD de Ubuntu Server mediante usuario/contraseña doble [Autenticación](#) (TOTP, contraseña de un sólo uso por tiempo), usando para ello la herramienta Google Authenticator. **(0,5 puntos)**. Se deja al alumno que realice las capturas de evidencias que desee (no realizar manual, sólo demostrar que os funciona).



```
C:\Users\alvar>ssh almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
(almellonesfernandez@192.168.1.107) Password:
[almellonesfernandez@192.168.1.107] Verification code:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:      https://ubuntu.com/pro

System information as of Fri Oct 25 04:13:40 PM UTC 2024

System load: 0.1          Processes:           104
Usage of /: 13.0% of 24.44GB  Users logged in:    1
Memory usage: 32%          IPv4 address for enp0s3: 192.168.1.107
Swap usage:  0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

36 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Fri Oct 25 16:13:41 2024 from 192.168.1.106
almellonesfernandez@Ubuntu-server-bastionado:~$
```