Actividad - Configuración de SSH con autenticación por certificados

Introducción

SSH (Secure Shell) es un protocolo de red que permite el acceso remoto seguro a sistemas. La autenticación mediante claves (pública/privada) ofrece mayor seguridad que las contraseñas tradicionales, eliminando el riesgo de ataques de fuerza bruta.

En esta práctica configuraremos un servidor SSH en Ubuntu Server, estableceremos conexión desde un cliente Kali Linux utilizando autenticación por clave pública, y posteriormente verificaremos la conexión desde Windows con los mismos certificados.

Escenario de la práctica

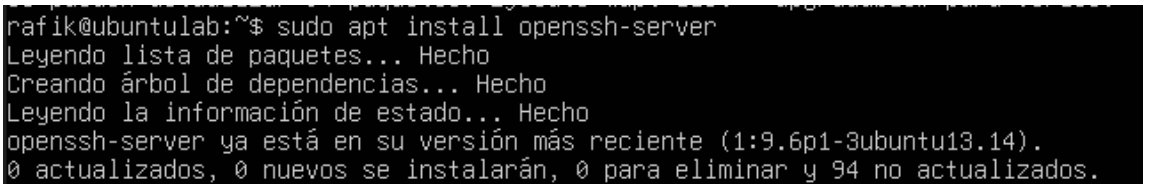
Rol	Sistema	IP
Servidor SSH	Ubuntu Server	192.168.10.40
Cliente SSH	Kali Linux	192.168.10.99
Cliente SSH	Windows	-

Parte 1: Configuración del servidor SSH en Ubuntu

1.1 Instalación del servidor OpenSSH

En la máquina que actuará como servidor, instalamos el paquete del servidor SSH:

```
sudo apt update
sudo apt install openssh-server
```



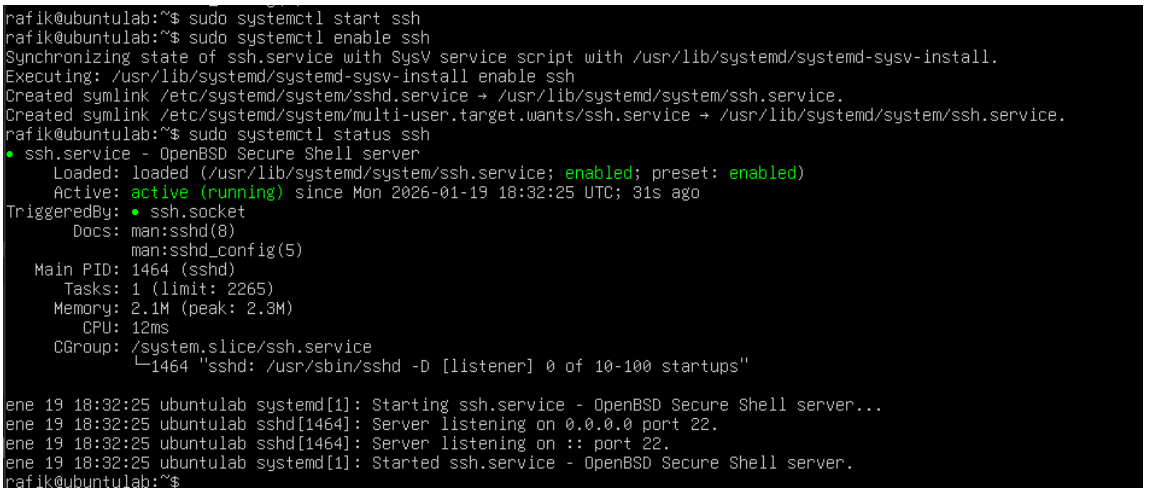
1.2 Verificar el estado del servicio

Comprobamos que el servicio SSH está activo:

```
sudo systemctl status ssh
```

Si no está activo, lo iniciamos y habilitamos:

```
sudo systemctl start ssh
sudo systemctl enable ssh
```



Parte 2: Generación de claves SSH en el cliente Kali Linux

2.1 Crear el par de claves

En la máquina **cliente Kali Linux**, generamos el par de claves:

```
ssh-keygen
```

Durante la ejecución nos preguntará:

1. **Ubicación del archivo**: Podemos aceptar la ruta por defecto o especificar un nombre personalizado (ej: `~/.ssh/id_rsa_actividad`)
2. **Passphrase**: Podemos dejarla vacía o introducir una contraseña adicional para proteger la clave

Este comando genera dos archivos en `~/.ssh/` :

- `id_rsa_actividad` → Clave privada (nunca debe compartirse)
- `id_rsa_actividad.pub` → Clave pública (se copia al servidor)

```
┌──(ron㉿Klab)-[~]
└─$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/ron/.ssh/id_ed25519): /home/ron/.ssh/id_rsa_actividad
Enter passphrase for "/home/ron/.ssh/id_rsa_actividad" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ron/.ssh/id_rsa_actividad
Your public key has been saved in /home/ron/.ssh/id_rsa_actividad.pub
The key fingerprint is:
SHA256:a8dsO1e6KnMThrVjplpGiALMoCycO1m/sSEZa9/fLI4 ron@Klab
The key's randomart image is:
+--[ED25519 256]--+
|.                |
|B .              |
|+* o             |
|..+ =. .  .      |
| +.=.+. So .     |
|  o.o *..+B   .  |
|     + .═══o o   |
|       +***.o    |
|      .E.*+B..   |
+────[SHA256]─────+
```

2.2 Copiar la clave pública al servidor

Utilizamos `ssh-copy-id` para transferir la clave pública. Si usamos un nombre personalizado, especificamos el archivo con `-i`:

```
ssh-copy-id -i ~/.ssh/id_rsa_actividad.pub usuario@IP_SERVIDOR
```

Nos pedirá la contraseña del usuario en el servidor. Este comando añade nuestra clave pública al archivo `~/.ssh/authorized_keys` del servidor.

```
┌──(ron㉿Klab)-[~]
└─$ ssh-copy-id rafik@192.168.10.40
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/ron/.ssh/id_rsa_actividad.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
rafik@192.168.10.40's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'rafik@192.168.10.40'"
and check to make sure that only the key(s) you wanted were added.
```

Método alternativo (manual):

Si `ssh-copy-id` no está disponible:

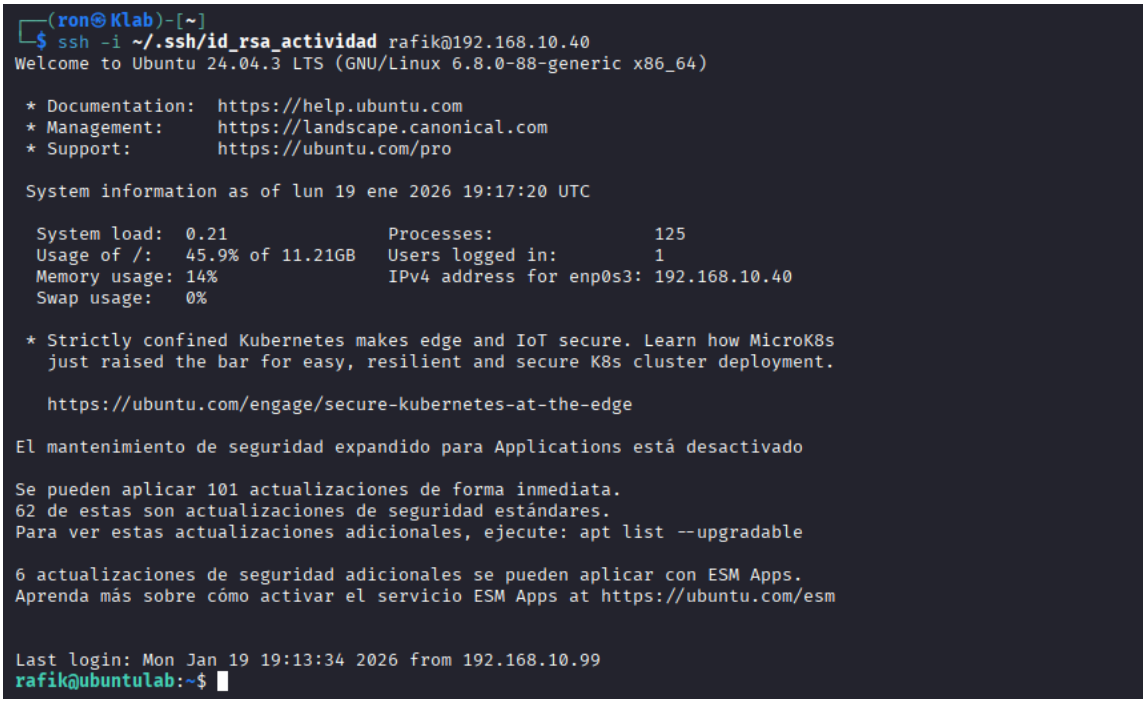
```
cat ~/.ssh/id_rsa_actividad.pub | ssh usuario@IP_SERVIDOR "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

2.3 Conectar al servidor con la clave

Probamos la conexión especificando la clave privada:

```
ssh -i ~/.ssh/id_rsa_actividad usuario@IP_SERVIDOR
```

Si la configuración es correcta, accederemos **sin que nos pida contraseña** (solo passphrase si la configuramos).



Parte 3: Deshabilitar autenticación por contraseña (opcional)

Una vez verificada la autenticación por clave, podemos deshabilitar el acceso por contraseña en el **servidor** para mayor seguridad.

3.1 Editar la configuración de SSH

```
sudo nano /etc/ssh/sshd_config
```

Buscamos y modificamos estas líneas:

```
PasswordAuthentication no
```

3.2 Reiniciar el servicio SSH

```
sudo systemctl restart ssh
```

Parte 4: Conexión desde Windows

4.1 Copiar las claves al cliente Windows

Transferimos los archivos de claves desde el cliente Kali Linux a Windows. Las claves están en `~/.ssh/`:

- `id_rsa_actividad` (clave privada)
- `id_rsa_actividad.pub` (clave pública)

Métodos de transferencia:

- USB
- Carpeta compartida de red
- SCP/SFTP

4.2 Ubicar las claves en Windows

En Windows, copiamos las claves a:

```
C:\Users\TU_USUARIO\.ssh\
```

Creamos la carpeta `.ssh` si no existe.

```
move C:\ruta\carpeta\compartida\id_rsa_actividad C:\Users\TU_USUARIO\.ssh\
```

```
PS C:\Users\rafik> move C:\Users\rafik\Desktop\kali\drop\id_rsa_actividad C:\Users\rafik\.ssh\
PS C:\Users\rafik> ssh -i C:\Users\rafik\.ssh\id_rsa_actividad rafik@192.168.10.40
The authenticity of host '192.168.10.40 (192.168.10.40)' can't be established.
ED25519 key fingerprint is SHA256:xfMvk4f1SPGCkEWBWligiuO+wThfbdE1mpdOF9nR8/E.
This host key is known by the following other names/addresses:
    C:\Users\rafik/.ssh/known_hosts:4: 192.168.1.40
    C:\Users\rafik/.ssh/known_hosts:7: 192.168.10.64
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.10.40' (ED25519) to the list of known hosts.
```

4.3 Ajustar permisos de la clave privada

En PowerShell (como Administrador), restringimos los permisos del archivo:

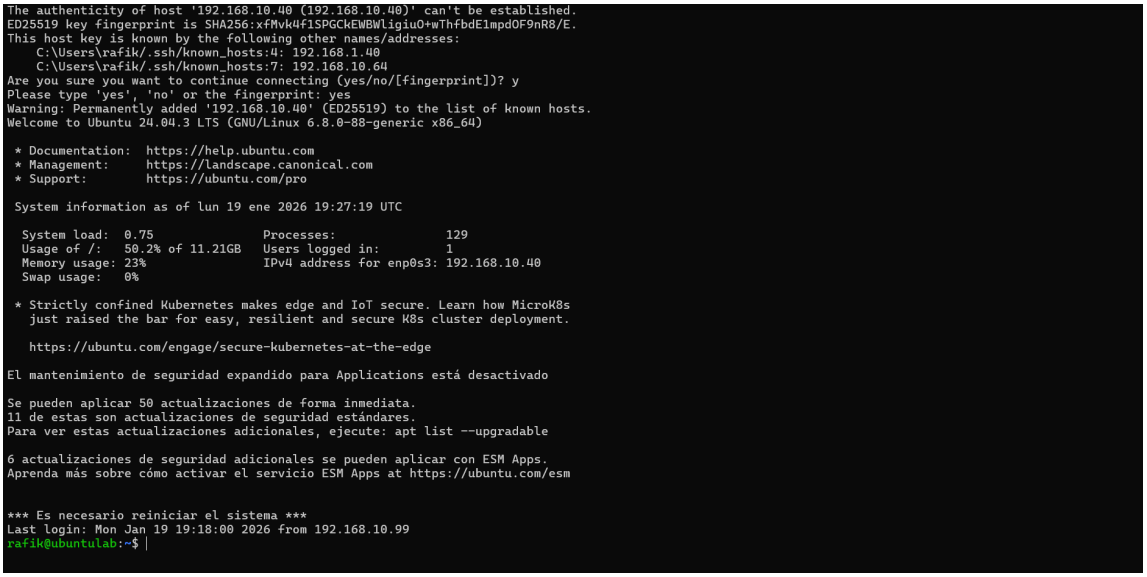
```
icacls "C:\Users\TU_USUARIO\.ssh\id_rsa_actividad" /inheritance:r
icacls "C:\Users\TU_USUARIO\.ssh\id_rsa_actividad" /grant:r "%USERNAME%:R"
```

```
PS C:\Users\rafik> icacls "C:\Users\rafik\.ssh\id_rsa_actividad" /inheritance:r
archivo procesado: C:\Users\rafik\.ssh\id_rsa_actividad
Se procesaron correctamente 1 archivos; error al procesar 0 archivos
PS C:\Users\rafik>   icacls "C:\Users\rafik\.ssh\id_rsa_actividad" /grant:r "rafik:R"
archivo procesado: C:\Users\rafik\.ssh\id_rsa_actividad
Se procesaron correctamente 1 archivos; error al procesar 0 archivos
PS C:\Users\rafik>
```

4.4 Conectar desde Windows

Windows 10/11 incluye cliente SSH nativo. Abrimos CMD o PowerShell, especificando la clave:

```
ssh -i C:\Users\TU_USUARIO\.ssh\id_rsa_actividad usuario@IP_SERVIDOR
```



Verificación

Prueba	Comando	Resultado esperado
Estado del servidor	`sudo systemctl status ssh`	active (running)
Conexión desde Kali	`ssh usuario@IP_SERVIDOR`	Acceso sin contraseña
Conexión desde Windows	`ssh usuario@IP_SERVIDOR`	Acceso sin contraseña

Conclusión

Hemos configurado un servidor SSH con autenticación por certificados y verificado el acceso tanto desde un cliente Kali Linux como desde Windows utilizando el mismo par de claves. Este método es más seguro que la autenticación por contraseña.