Acceso SSH

03/10/2023

Guillermo Bellettini
Seguridad
Creado por: Nicolas Pavel Ballesteros Barrado

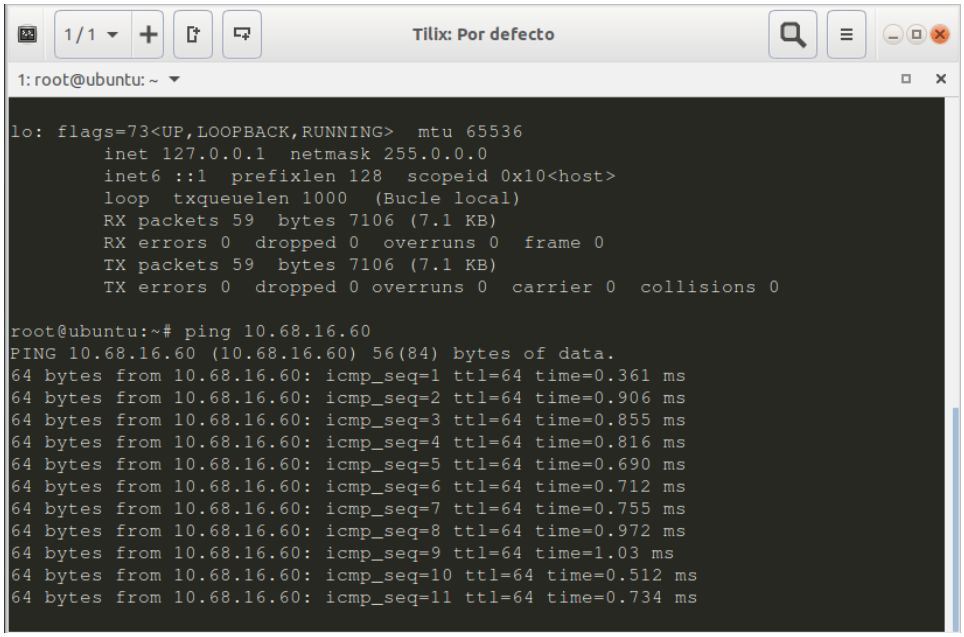
Contenido

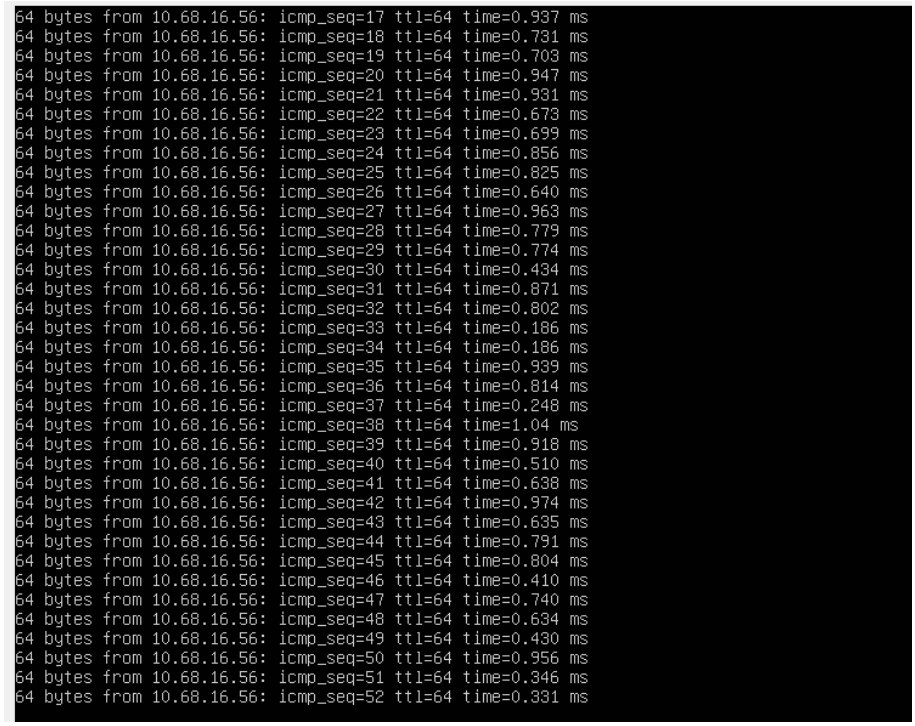
Arrancamos las dos maquinas

LUBUNTU_Guillermo
Corriendo

LUBUNTU_Seguridad
Corriendo

Las maquinas se hacen ping entre ellas





Nos vamos a la carpeta .ssh

```
root@npa:~# cd .ssh
root@npa:~/.ssh# _
```

Esta carpeta si existe ya que estamos en un Ubuntu server

Ponemos el comando ll

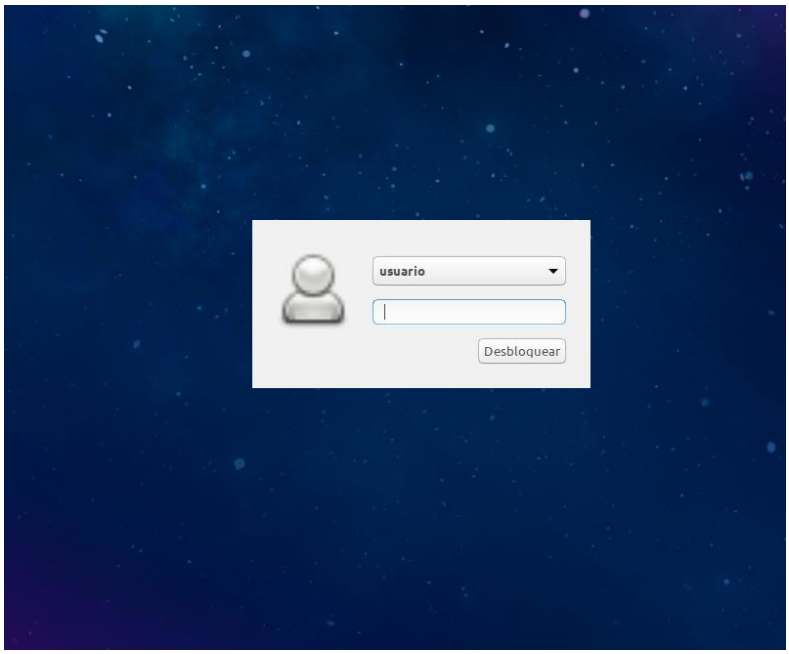
```
root@npa:~# ll
total 24
drwx------  4 root root 4096 sep 29 18:49 ./
drwxr-xr-x 19 root root 4096 sep 29 18:35 ../
-rw-r--r--  1 root root 3106 oct 15  2021 .bashrc
-rw-r--r--  1 root root  161 jul  9  2019 .profile
drwx------  3 root root 4096 sep 29 18:49 snap/
drwx------  2 root root 4096 sep 29 18:49 .ssh/
root@npa:~# _
```

Comando more known_host

```
root@npa:~# more known_host
more: cannot open known_host: No such file or directory
root@npa:~# more known_hosts
more: cannot open known_hosts: No such file or directory
root@npa:~#
```

Se genera este fichero cuando te conectas con control remoto al servidor, en este caso no existe ya que no estoy conectado y nadie ha sido conectado por control remoto

Nos conectamos remotamente al usuario



Ponemos su IP para podernos conectar

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.68.16.56  netmask 255.255.252.0  broadcast 10.68.19.255
        inet6 fe80::a00:27ff:febb:2dbc  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bb:2d:bc  txqueuelen 1000  (Ethernet)
        RX packets 36951  bytes 3807414 (3.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 673  bytes 58355 (58.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ponemos el comando ssh usuario@10.68.16.56

```
root@npa:~# ssh usuario@10.68.16.56
The authenticity of host '10.68.16.56 (10.68.16.56)' can't be established.
ED25519 key fingerprint is SHA256:oKB5uZFXTE/KDQSpAKoEOngN2c56un7S3P8b5CjAKLA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.68.16.56' (ED25519) to the list of known hosts.
usuario@10.68.16.56's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 399 paquetes.
326 actualizaciones son de seguridad.


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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

usuario@ubuntu:~$ _
```

Ya estamos conectado

Ponemos el comando pwd

```
usuario@ubuntu:~$ pwd
/home/usuario
usuario@ubuntu:~$ _
```

Ponemos el comando ssh-keygen

```
root@npa:~/.ssh# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:xs5QvuAgFV2A9jrJ3zX8irmPWatNvhFYSsheFIkrTWQ root@npa
The key's randomart image is:
+---[RSA 3072]----+
|     .+E++o      |
|     o++o.       |
|    ..+o.+ .     |
|    ...+* +      |
|   ...++ S..     |
|    .=o * .+.    |
|      o..+.+o    |
|       . .X o.   |
|         B+Bo    |
+----[SHA256]-----+
root@npa:~/.ssh#
```

Ponemos otra vez el comando ll

```
root@npa:~/.ssh# ll
total 24
drwx------ 2 root root 4096 oct  3 16:50 ./
drwx------ 4 root root 4096 oct  3 16:49 ../
-rw------- 1 root root    0 sep 29 18:49 authorized_keys
-rw------- 1 root root 2590 oct  3 16:50 id_rsa
-rw-r--r-- 1 root root  562 oct  3 16:50 id_rsa.pub
-rw------- 1 root root  364 oct  3 16:32 known_hosts
-rw-r--r-- 1 root root  142 oct  3 16:32 known_hosts.old
root@npa:~/.ssh#
```

Ponemos comando ssh-copy-id -i

```
pavel@npa:~/.ssh$ ssh-copy-id -i  /home/pavel/.ssh/id_rsa.pub usuario@10.68.16.56
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/pavel/.ssh/id_rsa.pub"
The authenticity of host '10.68.16.56 (10.68.16.56)' can't be established.
ED25519 key fingerprint is SHA256:oKB5uZFXTE/KDQSpAKoEOngN2c56un7S3P8b5CjAKLA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
usuario@10.68.16.56's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'usuario@10.68.16.56'"
and check to make sure that only the key(s) you wanted were added.

pavel@npa:~/.ssh$
```

Ya nos dicen que ya se ha añadido en el servidor remoto

Nos conectamos ahora sin que nos pida contraseña

```
pavel@npa:~/.ssh$ ssh usuario@10.68.16.56
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 399 paquetes.
326 actualizaciones son de seguridad.

Last login: Tue Oct  3 18:34:44 2023 from 10.68.16.60
usuario@ubuntu:~$ _
```

Nos deja acceder porque hemos copiado la clave publica al servidor destino

Nos vamos conectados a la carpeta .ssh y ejecutamos el comando ll nos sale una carperta llamada llaves autorizadas y que tienen las claves permitidas para conectarnos al servidor

```
usuario@ubuntu:~/.ssh$ ll
total 12
drwx------  2 usuario usuario 4096 oct  3 19:06 ./
drwxr-xr-x 18 usuario usuario 4096 oct  3 19:06 ../
-rw-------  1 usuario usuario  563 oct  3 19:06 authorized_keys
usuario@ubuntu:~/.ssh$
```

Comando More authorized_keys

Nos sale la clave encriptada y si leemos al final nos pone el nombre del usuario pavel@npa, es el que genero las claves.