UNPSJB

LICENCIATURA EN SISTEMAS OPGCPI

ADMINISTRACIÓN DE REDES Y SEGURIDAD

Trabajo Práctico 4

SSH y túneles

Cátedra
Lic. Bruno Damián Zappellini

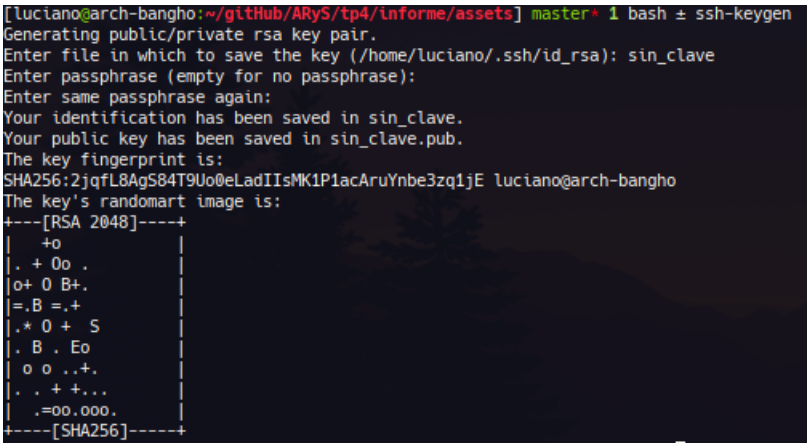
Integrantes:
Luciano Serruya Aloisi

28 de noviembre de 2018

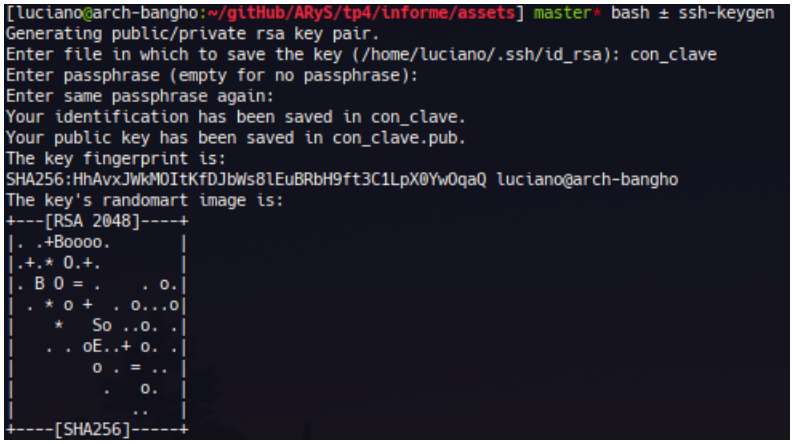
Índice

1. Sistema de autenticación de SSH

Según las páginas `man`, el comando `ssh-keygen` *genera, gestiona, convierte, y autoriza claves para ssh. ssh-keygen puede generar claves para que las use SSH protocolo versión 2*



Creación de una llave SSH sin contraseña



Creación de una llave SSH con contraseña “unaClave”

1.1. Archivos de autorización

Para gestionar el ingreso con *clave pública* y para llevar registro de los sitios confiables a los cuales ya se ingresó, SSH mantiene dos archivos, respectivamente:

- *authorized_keys*: lleva registro de las claves públicas aceptadas para conectarse vía SSH al sistema

- *known_hosts*: indica a los sitios que se conectó el usuario y son seguros (antes de establecer la conexión SSH con un sitio nuevo, el sistema pregunta si desea confiar en el sitio)

1.2. Ingresando a un servidor remoto con clave pública

Luego de registrar la clave pública personal en el servidor remoto y de haber configurado este último para que sólo permita ingresar (por SSH) mediante clave pública, se puede ingresar al servidor sin problemas.

Gracias al *log* que imprime SSH al ejecutarlo con la bandera `-vvv`, se puede ver la siguiente sección con respecto al ingreso con clave pública

```
1  .
2  .
3  .
4  debug1: Authentications that can continue: publickey
5  debug3: start over, passed a different list publickey
6  debug3: preferred publickey,keyboard-interactive,password
7  debug3: authmethod_lookup publickey
8  debug3: remaining preferred: keyboard-interactive,
     password
9  debug3: authmethod_is_enabled publickey
10 debug1: Next authentication method: publickey
11 .
12 .
13 .
```