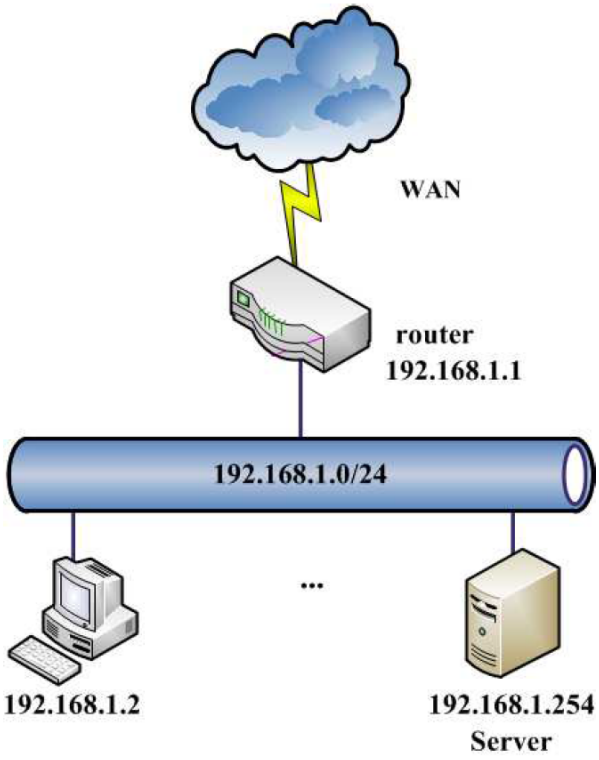
Práctica SSH

1.- Escenario A: OpenSSH Server

O principal obxectivo deste escenario é revisar e familiarizarse có funcionamento dun sistema SSH, tanto na parte servidor como no cliente. Instalaremos o servidor **openssh-server** nunha máquina **Debian Server 10** e faremos probas de conexión dende **clientes ssh** para probar os mecanismos de autenticación do *server* grazas ao uso da súa clave pública. Ademais, este escenario supón o comezo do estudo e revisión dos arquivos de configuración máis importantes tanto da parte servidor como da cliente; así como dos principais comandos *ssh*.

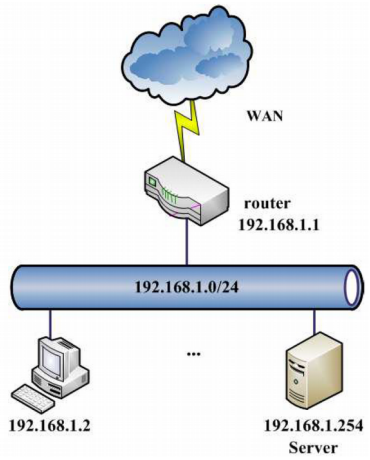


Ao longo do escenario realizaremos as seguintes accións:

- Actualizar a listaxe de paquetes no equipo correndo Debian Server 10 e instalar a última versión de openssh-server.
- Unha vez rematada a instalación, verificar que o servidor ssh está escoitando peticións no porto por defecto.
- Facer un listado dos arquivos de configuración do servidor ssh e localizar as claves públicas e privadas dos distintos algoritmos criptográficos.
- Explicar a misión do arquivo `known_hosts`.
- Conectarse dende o cliente Linux, verificando que se pide aceptar a clave pública e que unha vez aceptada, aparecerá no arquivo `known_hosts` do usuario.
- Conectarse novamente dende o cliente Linux, verificando que esta vez non se solicita aceptar a clave pública.
- Rexenerar as claves privada-pública que usa o servidor openssh-server.
- Comprobar que sucede cando o cliente detecta un erro na autenticación do *server* e como xestionar esta situación.
- Acceder usando o cliente *putty* nun sistema Microsoft Windows.

1.1. Configuración do escenario.

Esquema de rede do escenario A:



Configuración do *Server* para o escenario A:

Traballarase sobre Linux Debian Server 10 sen regras **netfilter/iptables** instaladas e configurado para saír a Internet ao través do *router* da figura. Importamos a máquina DS-10-00 e creamos, a partires dela, a máquina clonada DS-10-01 (cambiamos nome da máquina e contrasinais).
Características da máquina Linux Debian Server 10 DS-10-01:

- Sistema Operativo: Debian Server 10 (64 bits)
- Memoria RAM: 1024 MB
- Rede: Un único adaptador de rede configurado en modo "NAT Network" - ASO1 (192.168.1.0/24)

Configuración de rede:

- Interface de rede: enp0s3
- IP do server: 192.168.1.254/24
- *Default gateway*: 192.168.1.1
- Servidor DNS:
  - Instituto: 10.0.4.1
  - Casa: 8.8.8.8 e 8.8.4.4

Para configurar o *server* hai que:

- Instalar o paquete `resolvconf`

```
# apt update
# apt upgrade
# apt install resolvconf
```

- Editar o arquivo `/etc/network/interfaces`

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
      address 192.168.1.254
      netmask 255.255.255.0
      gateway 192.168.1.1
      #Instituto
      dns-nameserver 10.0.4.1
      #Casa
      #dns-nameserver 8.8.8.8
      #dns-nameserver 8.8.4.4
      #Casa e Instituto
      dns-search sanclemente.local
```

- Cambiamos de nome ao equipo: https://www.howtoforge.com/perfect-server-debian-10-buster-apache-bind-dovecot-ispconfig-3-1/#-configure-thenbsphostname

Unha vez modificados eses dous arquivos hai que reiniciar a rede có comando:

```
$ sudo /etc/init.d/networking restart
```

Se non está instalada a ferramenta `netstat` facelo instalando as ferramentas `net-tools`.

Pode verificarse que a nova configuración foi aplicada:

```
$ sudo ip a ; netstat -nr
eth0      Link encap:Ethernet  HWaddr 08:00:27:2c:c0:28
          inet addr:192.168.1.254  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2c:c028/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:159 errors:0 dropped:0 overruns:0 frame:0
          TX packets:190 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15122 (14.7 KiB)  TX bytes:26518 (25.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2843 (2.7 KiB)  TX bytes:2843 (2.7 KiB)
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

Configuración do *Cliente* para o escenario A:

Na primeira parte deste escenario traballaremos cun cliente ssh correndo nun equipo *Debian Desktop 10* e na segunda parte traballaremos có cliente *putty* sobre *Microsoft Windows*.

1.2. Autenticación do *server*

Instalación de OpenSSH Server

Aínda que existen diferentes implementacións tanto de clientes como de servidores ssh, a máis empregada é OpenSSH; de feito, a súa implementación do cliente ssh xa ben instalada na maioría das distribucións de Linux. Para instalar o servidor OpenSSH nunha máquina Linux Debian Server hai que executar os seguintes comandos:

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

Unha vez rematada a instalación, verifícase que o servizo ssh está correndo e se atopa preparado para aceptar conexións no porto por defecto tcp/22.

```
$ sudo netstat -putan | grep ssh
tcp     0    0 0.0.0.0:22            0.0.0.0:*               LISTEN      429/sshd
tcp     0   64 192.168.1.254:22      192.168.1.6:50797       ESTABLISHED 703/sshd: jefe [pri
tcp6    0    0 :::22                 :::*                    LISTEN      429/sshd
```

Arquivos de configuración do servidor openssh

Os arquivos de configuración e claves criptográficas do servidor openssh-server están ubicados en `/etc/ssh`

```
$ ls -lhF /etc/ssh
total 280K
-rw-r--r-- 1 root root 237K jul 22 19:45 moduli
-rw-r--r-- 1 root root 1,7K jul 22 19:45 ssh_config
-rw-r--r-- 1 root root 2,5K sep 12 11:40 sshd_config
-rw------- 1 root root  668 sep 12 11:40 ssh_host_dsa_key
-rw-r--r-- 1 root root  602 sep 12 11:40 ssh_host_dsa_key.pub
-rw------- 1 root root  227 sep 12 11:40 ssh_host_ecdsa_key
-rw-r--r-- 1 root root  174 sep 12 11:40 ssh_host_ecdsa_key.pub
-rw------- 1 root root  399 sep 12 11:40 ssh_host_ed25519_key
-rw-r--r-- 1 root root   94 sep 12 11:40 ssh_host_ed25519_key.pub
-rw------- 1 root root 1,7K sep 12 11:40 ssh_host_rsa_key
-rw-r--r-- 1 root root  394 sep 12 11:40 ssh_host_rsa_key.pub
```

Destacan os seguintes arquivos:

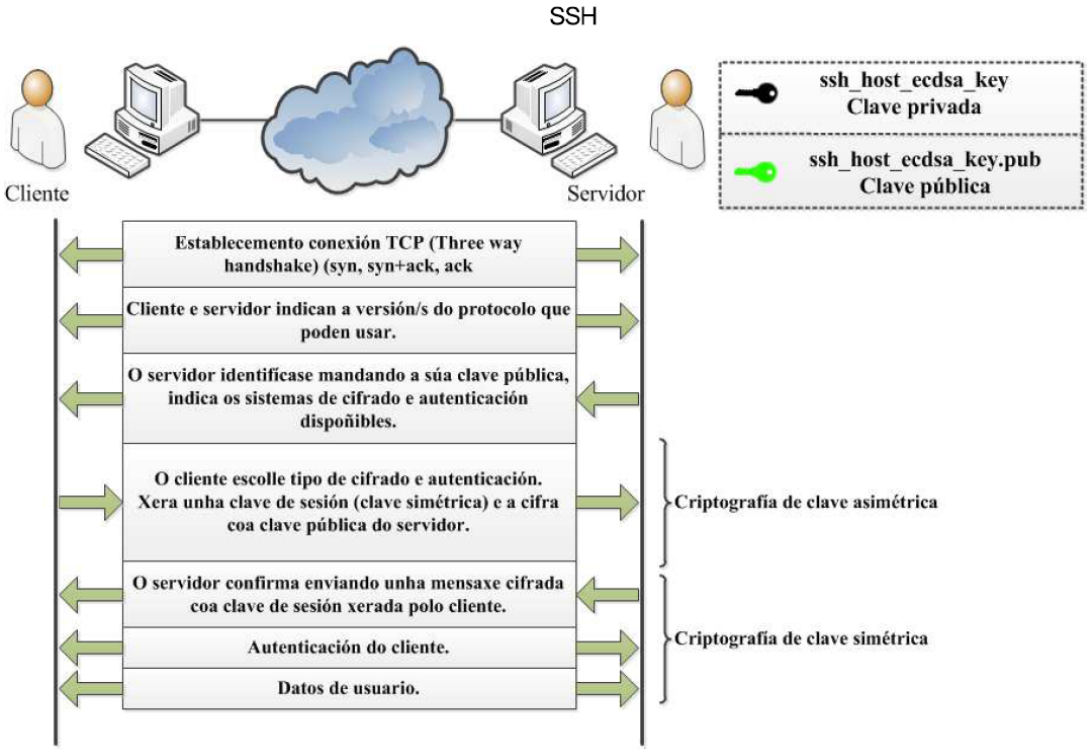
- **ssh_config:** é o arquivo onde están as directivas de configuración do cliente `openssh`. Aínda que teñen nomes parecidos aos arquivos de configuración, é importante non confundir o arquivo de configuración do cliente có do servidor.
- **sshd_config:** é o arquivo onde están as directivas de configuración do servidor `openssh-server` que controlan o seu funcionamento. Por exemplo, permiten configurar o/os porto/s onde se pon á espera de conexións o servidor ssh, se o usuario `root` pode iniciar ou non sesións por ssh, etc.
- **Arquivos de claves privada e pública:** do servidor para diferentes algoritmos de cifrado. Os seguintes arquivos son as parellas de claves privadas-pública:
  - Claves para DSA: `ssh_host_dsa_key` e `ssh_host_dsa_key.pub`.
  - Claves para ECDSA: `ssh_host_ecdsa_key` e `ssh_host_ecdsa_key.pub`.
  - Claves para ED25519: `ssh_host_ed25519_key` e `ssh_host_ed25519_key.pub`.
  - Claves para RSA: `ssh_host_rsa_key` e `ssh_host_rsa_key.pub`.

En relación ás claves fixarse en que:

- Todas as claves públicas dos diferentes algoritmos de cifrado rematan o seu nome en **.pub** e calquera usuario pode acceder a elas (permisos 644). Lembrar que as claves públicas están pensadas para distribuírse.
- Todas as claves privadas son accesibles unicamente polo propietario `root` (permisos 600). A razón destes permisos tan restritivos nas claves privadas é a necesidade de mantelas protexidas; xa que, se alguén puidese copialas podería suplantar a identidade do equipo.

Inicio de sesión e autenticación do servidor

SSH emprega un sistema criptográfico híbrido, onde a criptografía de clave asimétrica úsase para o intercambio seguro dunha clave simétrica de sesión, que permite un maior rendemento. Aínda que existen diferencias no funcionamento entre as versións 1 e 2 de ssh, o funcionamento xeral pode verse no seguinte esquema:



A primeira vez que dende un cliente ssh se establece unha conexión ao servidor aparece unha mensaxe indicando que non se recoñece a identidade do mesmo. O que sucede é que o servidor envía a súa

clave pública e o equipo cliente non tiña constancia dela. Unha vez aceptada esa clave pública a conexión segue o seu camiño e o usuario debe autenticarse.

NOTA ACLARATORIA#1: Para que apareza a mensaxe indicando que non se recoñece a identidade do mesmo, ten que ser a primeira vez que se envía esta clave pública. Para borrar nun cliente Linux o arquivo known_hosts executarase o comando:

```
$ rm .ssh/known_hosts
```

NOTA ACLARATORIA#2: Se os intentos de conexión por ssh se demoran moito (sobre uns 20 segundos), pode probarse a editar o arquivo `/etc/ssh/sshd_config` e configurar o parámetro `UseDNS` como `no`. Logo hai que reiniciar o servidor:

```
$ /etc/init.d/ssh restart
```

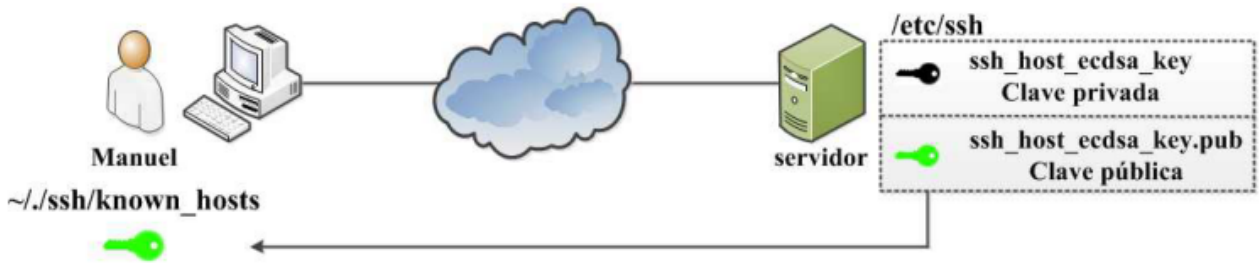
Efectuamos unha primeira conexión ao servidor ssh dende o cliente e aparece o aviso para aceptar a clave pública do servidor:

```
$ ssh jefe@192.168.1.254
The authenticity of host '192.168.1.254 (192.168.1.254)' can't be established.
ECDSA key fingerprint is 4c:bf:6d:15:43:bd:0d:f3:bd:6f:a9:fe:91:2f:72:38.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.254' (ECDSA) to the list of known hosts.
jefe@192.168.1.254's password:

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 Sep 19 12:52:02 2016 from 192.168.1.4
```

O equipo cliente garda as claves públicas dos servidores aos que se conecta no arquivo `.ssh/known_hosts` dentro do directorio home do usuario que lanzou a conexión:



Ao revisar o contido do arquivo `known_hosts` atopámonos con:

```
$ cat .ssh/known_hosts
|1|hDKOFknFqGpQFjrHnFrACpW/668=|TpWkVXhW23j3dW8dryJpQDyDEjw=
ecdsa-sha2-nistp256AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCZNxdyzSlCs2gtcvTtcBY
I8hVRzRDDO3f2riuf5IkUWFSDLqNWq5MT4nXGIjQDas4WXFLiV1U5XhfVxb6ceZrQ=
```

Pódese comparar a clave pública gardada no arquivo `known_hosts` do cliente coa clave pública ECDSA do servidor e ver que se trata da mesma clave pública:

```
$ cat /etc/ssh/ssh_host_ecdsa_key.pub
ecdsa-sha2-nistp256AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCZNxdyzSlCs2gtcvTtcBY
I8hVRzRDDO3f2riuf5IkUWFSDLqNWq5MT4nXGIjQDas4WXFLiV1U5XhfVxb6ceZrQ=
```

Gardar as claves públicas permite que en conexións posteriores:

- Se a clave enviada polo equipo remoto coincide coa clave pública gardada en `known_hosts` non aparecerá a mensaxe de advertencia e o usuario verá que debe autenticarse para poder iniciar a sesión no equipo remoto. É dicir, o servidor autenticouse correctamente fronte ao cliente e continúa o proceso de establecemento da sesión ssh.

- Se a clave enviada polo equipo remoto é diferente á clave pública gardada en `known_hosts` aparecerá unha mensaxe de erro e abortarase a conexión. Hai un erro de autenticación e o cliente non confía no equipo remoto.

Podemos probar a conectarnos novamente ao servidor e veremos que xa non aparece a mensaxe; xa que, a identidade do server é coñecida ao estar a súa clave pública no `known_host`:

```
$ ssh jefe@192.168.1.254
jefe@192.168.1.254's password:

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 Sep 19 13:13:44 2016 from 192.168.1.2
```

A continuación imos provocar un erro de autenticación do servidor, facendo que a clave pública enviada polo servidor non coincida coa clave pública anteriormente aceptada e gardada en `known_hosts`. Unha forma sinxela de facelo e rexenerar as claves do server; polo que, en primeiro lugar borramos as claves en uso:

```
$ sudo rm /etc/ssh/ssh_host*
$ sudo ls -lhF /etc/ssh
total 248K
-rw-r--r--  1 root root 237K jul 22 19:45 moduli
-rw-r--r--  1 root root 1,7K jul 22 19:45 ssh_config
-rw-r--r--  1 root root 2,5K sep 12 11:40 sshd_config
```

E despois xeramos outras novas coa utilidade **ssh-keygen**:

```
$ man ssh-keygen
-A      For each of the key types (rsa1, rsa, dsa, ecdsa and ed25519) for which host keys do
not exist, generate the host keys with the default key file path, an empty passphrase,
default bits for the key type, and default comment.  This is used by system administration
scripts to generate new host keys.
$ sudo ssh-keygen -A
ssh-keygen: generating new host keys: RSA1 RSA DSA ECDSA ED25519
$ sudo ls -lhF /etc/ssh
total 280K
-rw-r--r-- 1 root root 237K jul 22 19:45 moduli
-rw-r--r-- 1 root root 1,7K jul 22 19:45 ssh_config
-rw-r--r-- 1 root root 2,5K sep 12 11:40 sshd_config
-rw------- 1 root root  668 sep 24 17:33 ssh_host_dsa_key
-rw-r--r-- 1 root root  602 sep 24 17:33 ssh_host_dsa_key.pub
-rw------- 1 root root  227 sep 24 17:33 ssh_host_ecdsa_key
-rw-r--r-- 1 root root  174 sep 24 17:33 ssh_host_ecdsa_key.pub
-rw------- 1 root root  399 sep 24 17:33 ssh_host_ed25519_key
-rw-r--r-- 1 root root   94 sep 24 17:33 ssh_host_ed25519_key.pub
-rw------- 1 root root 1,7K sep 24 17:33 ssh_host_rsa_key
```

Ao rexenerar as claves, hai unha discrepancia entre a clave pública que emprega o servidor para autenticarse fronte ao cliente e a clave que o identifica gardada no arquivo `known_hosts` do cliente:

```
$ cat /etc/ssh/ssh_host_ecdsa_key.pub
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMZfirRkyoSQ4w3z...
$ cat .ssh/known_hosts
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCZNxdyzSlCs2gtcvT...
```

Isto tradúcese nun erro ao tratar de establecer a conexión:

```
$ ssh jefe@192.168.1.254
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
28:39:b0:98:a1:08:ae:78:c4:50:bd:e1:aa:c4:b5:37.
Please contact your system administrator.
Add correct host key in /home/jefe/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /home/jefe/.ssh/known_hosts:1
  remove with: ssh-keygen -f "/home/jefe/.ssh/known_hosts" -R 192.168.1.254
ECDSA host key for 192.168.1.254 has changed and you have requested strict checking.
Host key verification failed.
```

Na mensaxe de erro indícase que pode ser que alguén estea a suplantar a identidade do server ou que a clave cambiou. Tamén nos indica como facer para eliminar a clave vella do arquivo *known_hosts*, executando no cliente a utilidade `ssh-keygen` coa opción `-R` para eliminar as claves almacenadas no *known_hosts* asociadas a un equipo:

```
$ ssh-keygen -f "/home/jefe/.ssh/known_hosts" -R 192.168.1.254
# Host 192.168.1.254 found: line 1 type ECDSA
/home/jefe/.ssh/known_hosts updated.
Original contents retained as /home/jefe/.ssh/known_hosts.old
```

Unha vez eliminada a clave vella, o cliente pode conectarse ao servidor como se fose a primeira vez:

```
$ ssh jefe@192.168.1.254
The authenticity of host '192.168.1.254 (192.168.1.254)' can't be established.
ECDSA key fingerprint is 28:39:b0:98:a1:08:ae:78:c4:50:bd:e1:aa:c4:b5:37.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.254' (ECDSA) to the list of known hosts.
jefe@192.168.1.254's password:

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: Sat Sep 24 17:25:37 2016
```