

Cifrado asimétrico

Conexión Remota mediante SSH sen contrasinal

ESCENARIO

Máquinas virtuais ou físicas:

RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado

Rede: 192.168.120.0

BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

Máquina A:

Servidor SSH

IP/MS: 192.168.120.100/24

SO: Kali Live amd64

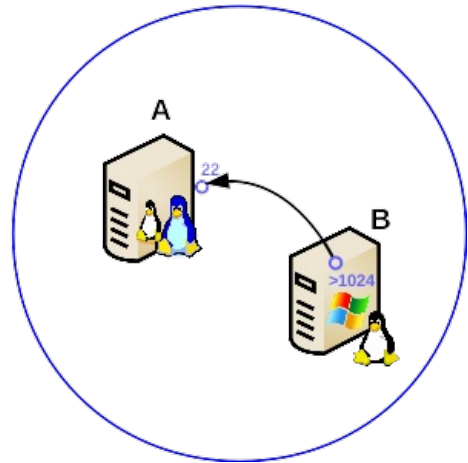
Máquina B:

Cliente SSH

IP/MS: 192.168.120.101/24

SO₁: Live GNU/Linux

SO₂: Microsoft Windows



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- Cliente ssh Microsoft Windows: **putty**
- Transferencia de arquivos mediante conexión cifrada ssh en Microsoft Windows: **pscp**
- Xeración/Carga/Conversión chaves pública/privada en Microsoft Windows: **puttygen**
- Documentación sobre **putty**

Práctica Cifrado asimétrico

Conexión Remota mediante SSH sen contrasinal dende Microsoft Windows

Arrancar coa máquina Microsoft Windows

1. Descargar pscp, puttygen e putty (Ver apartado NOTAS)
2. Configurar a rede: 192.168.120.101/24
3. pscp: Copiar a chave privada para poder acceder ao Servidor SSH:

cmd. Símbolo del sistema

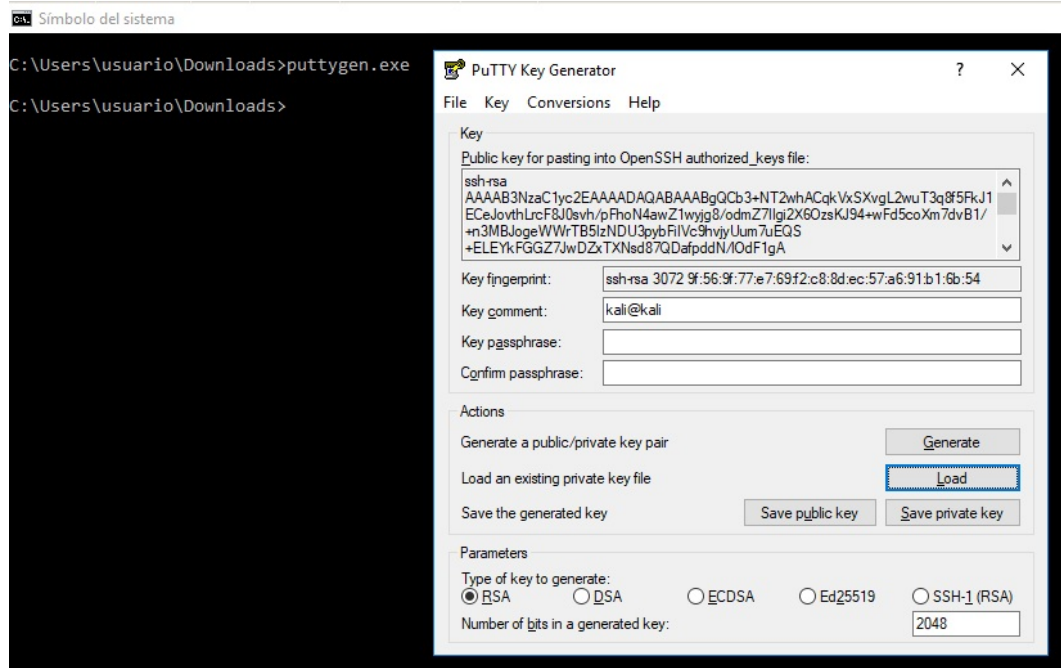
```
C:\Users\usuario\Downloads>pscp.exe -P 22 kali@192.168.120.100:.ssh/id_rsa .
kali@192.168.120.100's password:
id_rsa | 2 kB | 2.5 kB/s | ETA: 00:00:00 | 100%
C:\Users\usuario\Downloads>
```

C:\Users\usuario\Downloads> pscp.exe -P 22 kali@192.168.120.100:.ssh/id_rsa . #Copiar mediante conexión cifrada ssh (pscp.exe) o arquivo id_rsa (chave privada do usuario kali)

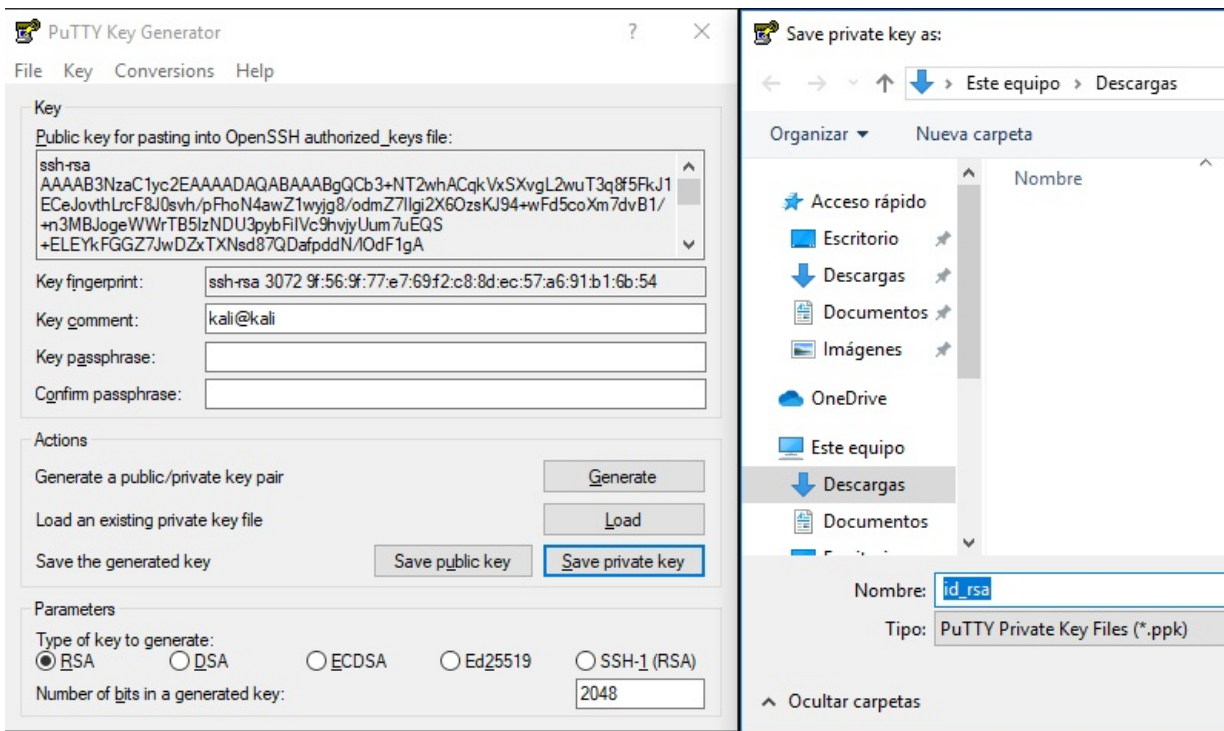
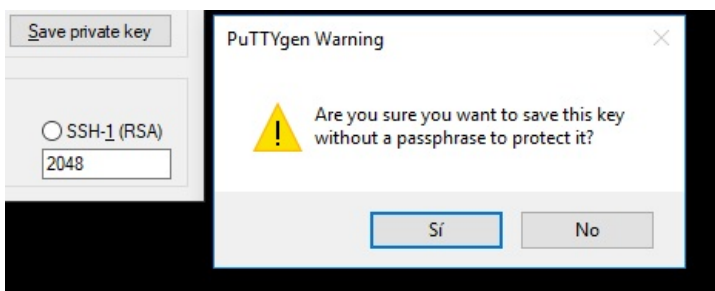
4. puttygen: Convertir a chave privada a formato ppk (formato entendible por putty):

a. Executar puttygen.exe:

C:\Users\usuario\Downloads> puttygen.exe #Executar o aplicativo puttygen.exe e unha vez executado cargar a chave privada id_rsa

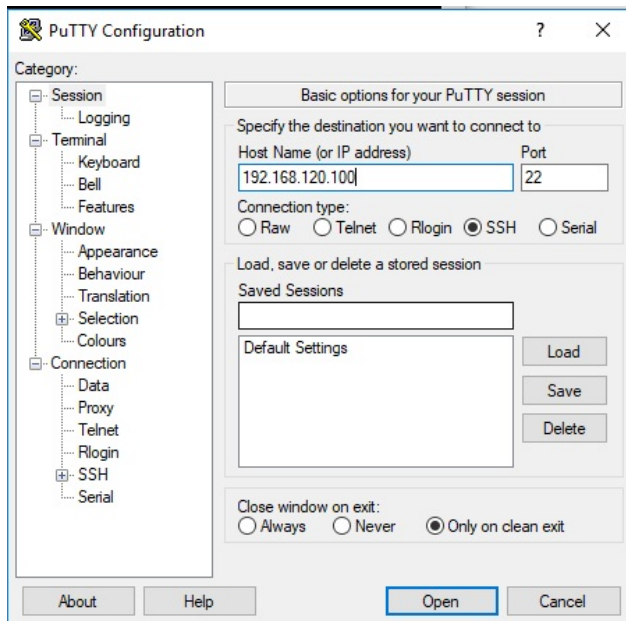


b. Convertir esa chave privada ao formato entendible polo aplicativo putty gardándoa en formato PPK

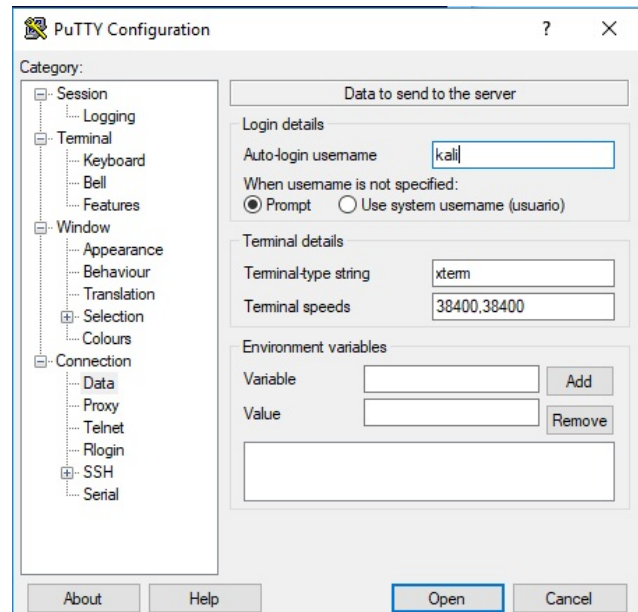


5. putty: Acceder mediante conexión cifrada sen contrasinal ao Servidor SSH:

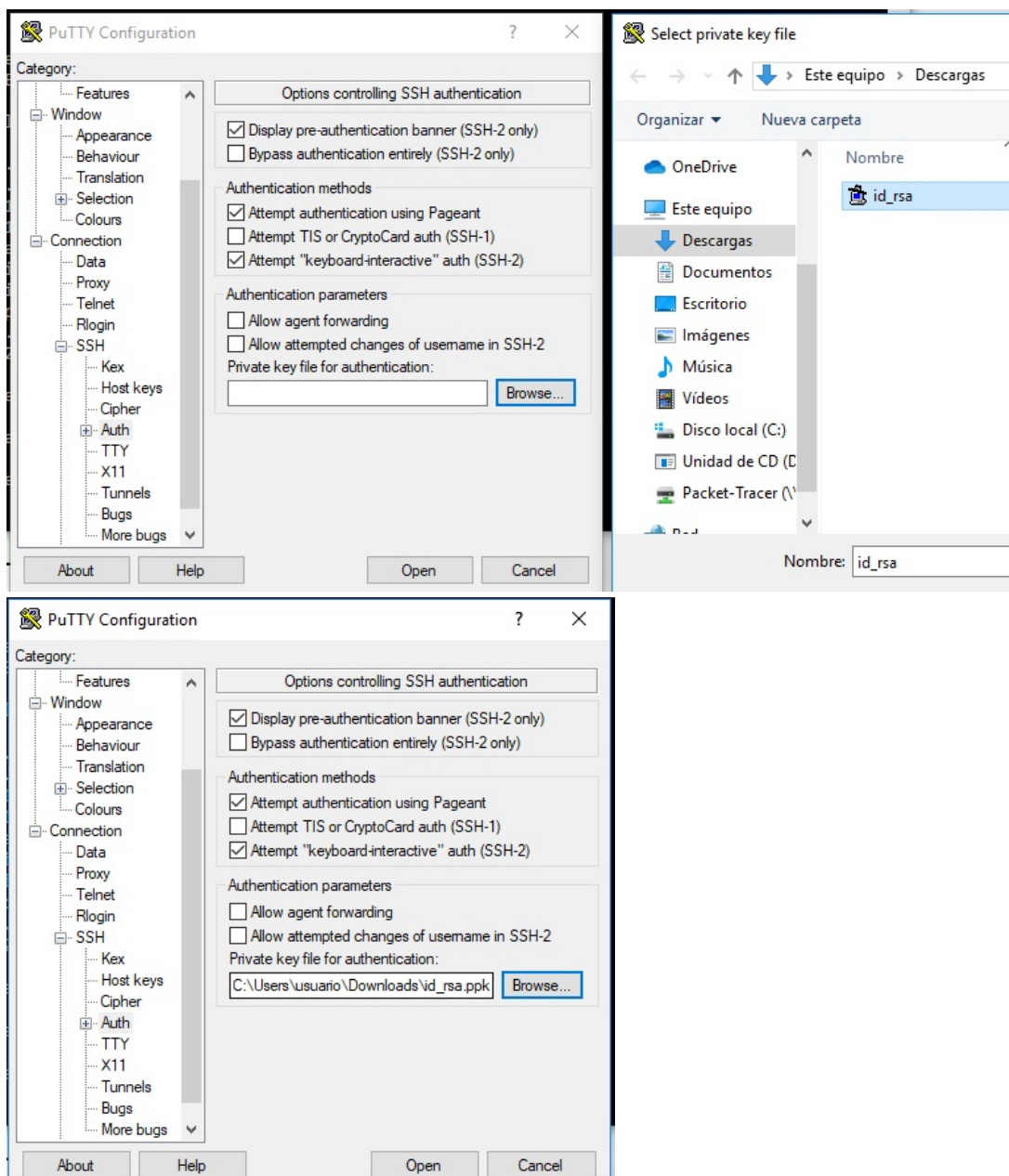
a. Pór a IP.



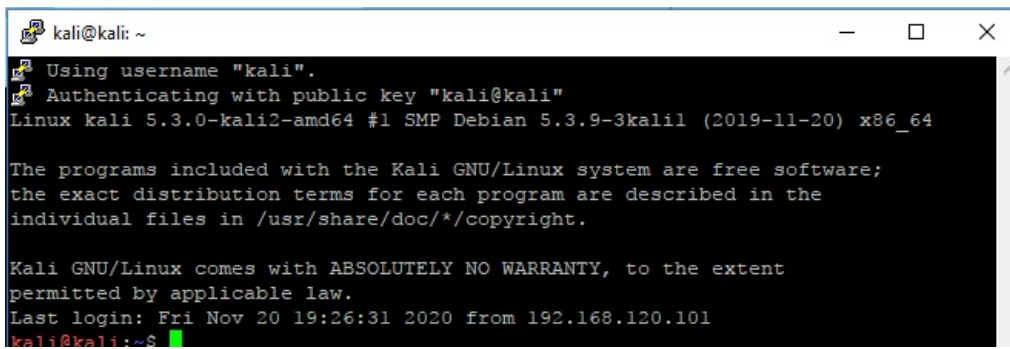
b. Pór o usuario a empregar na conexión: kali



c. Cargar a chave privada (formato PPK).



- d. Conectar: Pícar no botón Open para acceder sen contrasinal mediante conexión cifrada co usuario kali.

A terminal window titled 'kali@kali: ~' with standard window controls. The terminal output shows the login process for the 'kali' user. It starts with 'Using username "kali".', followed by 'Authenticating with public key "kali@kali"'. Then it displays system information: 'Linux kali 5.3.0-kali2-amd64 #1 SMP Debian 5.3.9-3kali1 (2019-11-20) x86_64'. A message follows: 'The programs included with the Kali GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.' Another message states: 'Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.' The login time is shown as 'Last login: Fri Nov 20 19:26:31 2020 from 192.168.120.101'. Finally, the prompt 'kali@kali:~\$' is displayed with a green cursor.

```
kali@kali: ~  
Using username "kali".  
Authenticating with public key "kali@kali"  
Linux kali 5.3.0-kali2-amd64 #1 SMP Debian 5.3.9-3kali1 (2019-11-20) x86_64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Fri Nov 20 19:26:31 2020 from 192.168.120.101  
kali@kali:~$
```

Ricardo Feijoo Costa



This work is licensed under a **Creative Commons Attribution-ShareAlike 4.0 International License**