

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

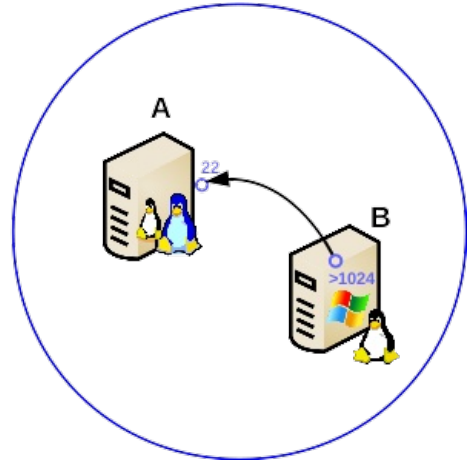
Máquina B:

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.

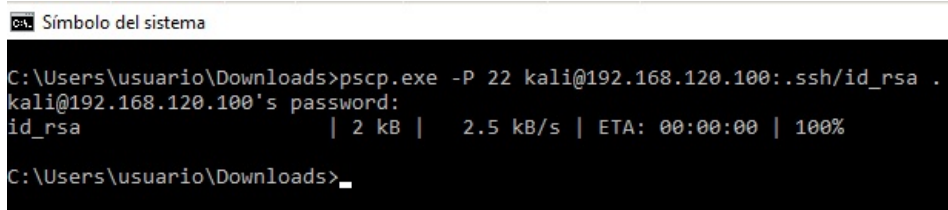
NOTAS:

- **IMPORTANTE:** Ter realizada a práctica **Practica BRS Cifrado asimetrico Conexion SSH sen contrasinal**
- Cliente ssh Microsoft Windows: **putty**
- Transferencia de arquivos mediante conexión cifrada ssh en Microsoft Windows: **pscp**
- Xeración/Carga/Conversión claves pública/privada en Microsoft Windows: **puttygen**
- Documentación sobre **putty**
- Descarga versión avaliación: **Windows 10 Enterprise**
- Descarga versión avaliación: **Windows 11 Enterprise**

Práctica Cifrado asimétrico Conexión Remota mediante SSH sen contrasinal dende Microsoft Windows

Arrancar coa máquina Microsoft Windows

1. Descargar na sección **Alternative binary files**: 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:



```
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%

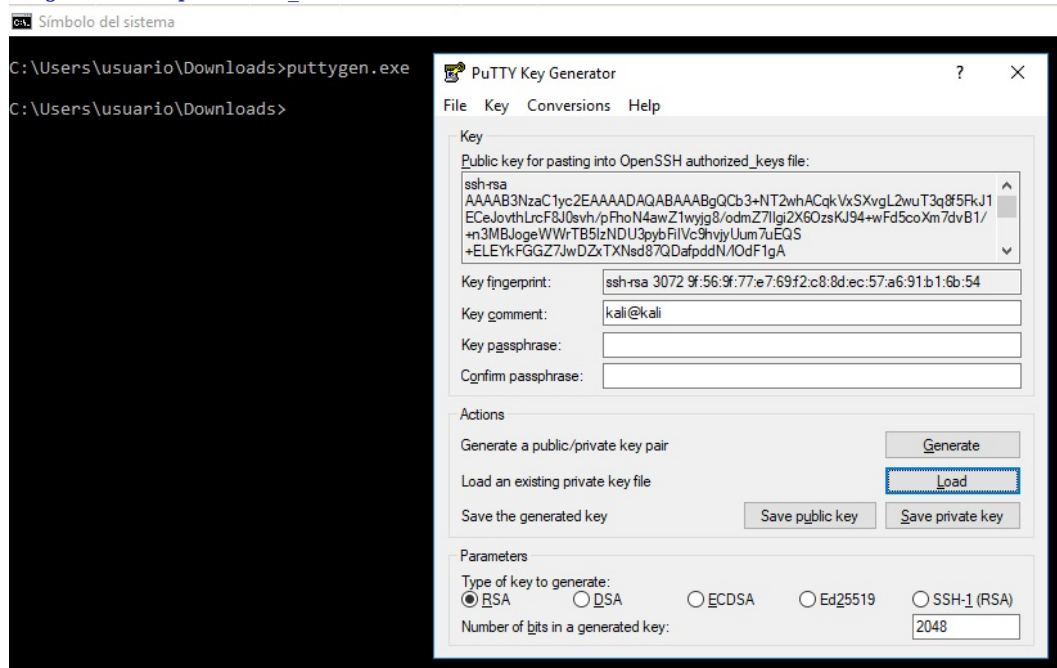
C:\Users\usuario\Downloads>
```

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)

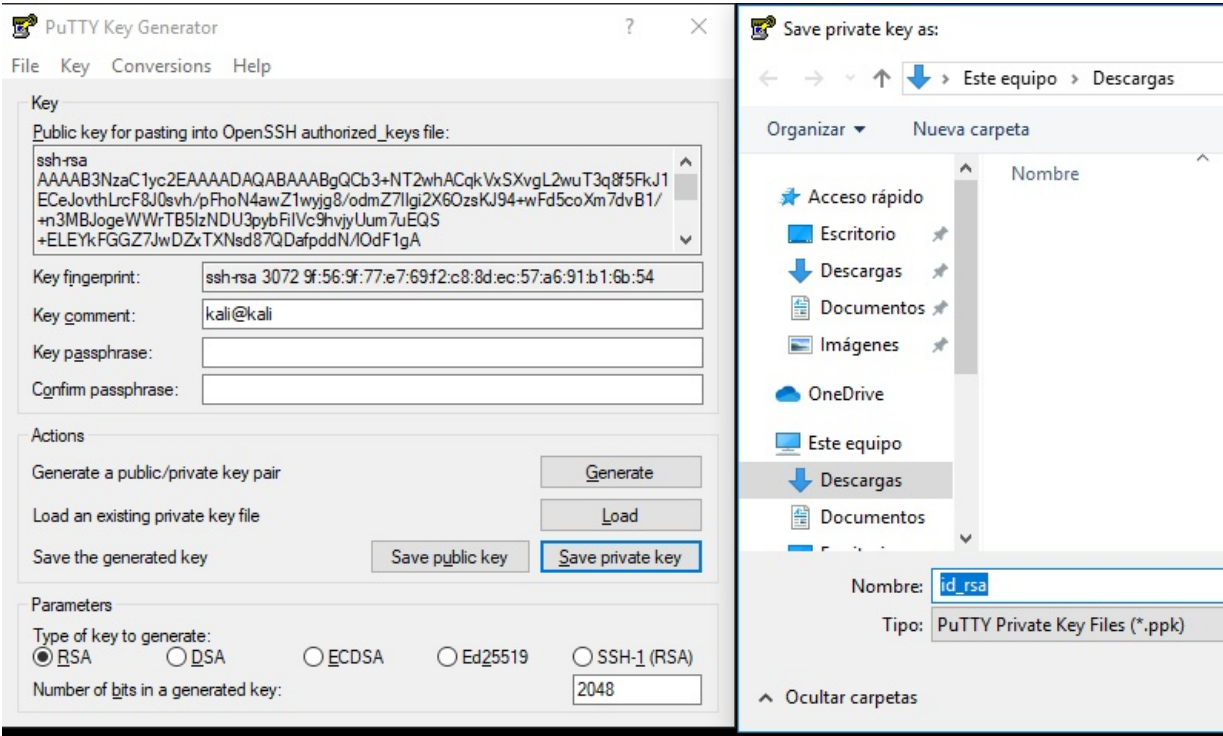
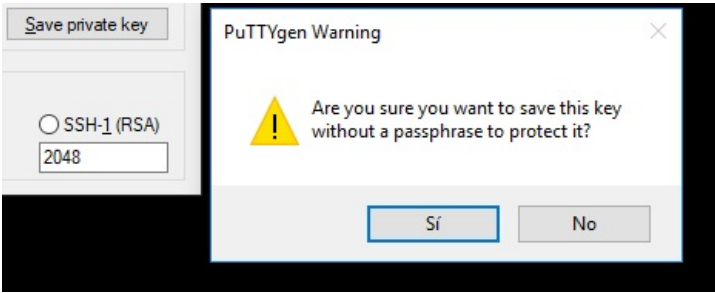
4. puttygen: Convertir a chave privada a formato ppk (formato entendible por putty):

- a. Executar puttygen.exe:

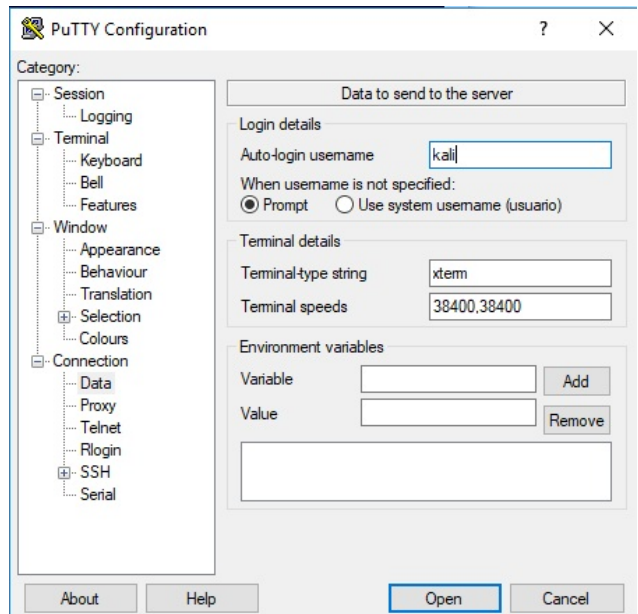
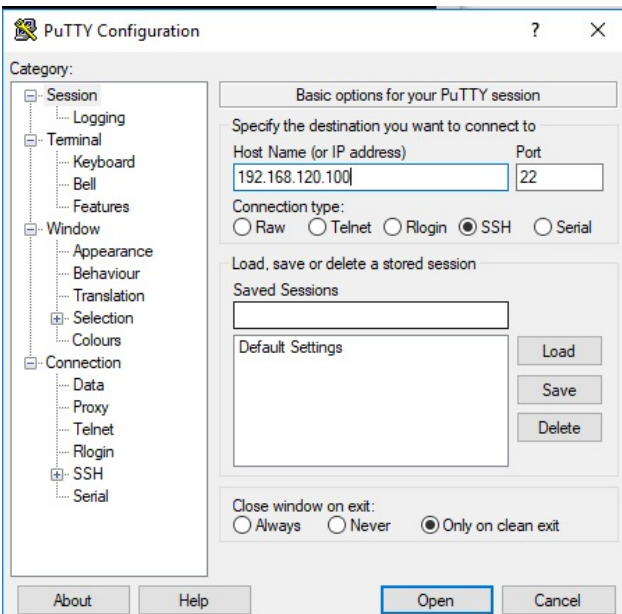
C:\Users\usuario\Downloads> puttygen.exe #Executar o aplicativo puttygen.exe e unha vez executado cargar a chave privada id_rsa



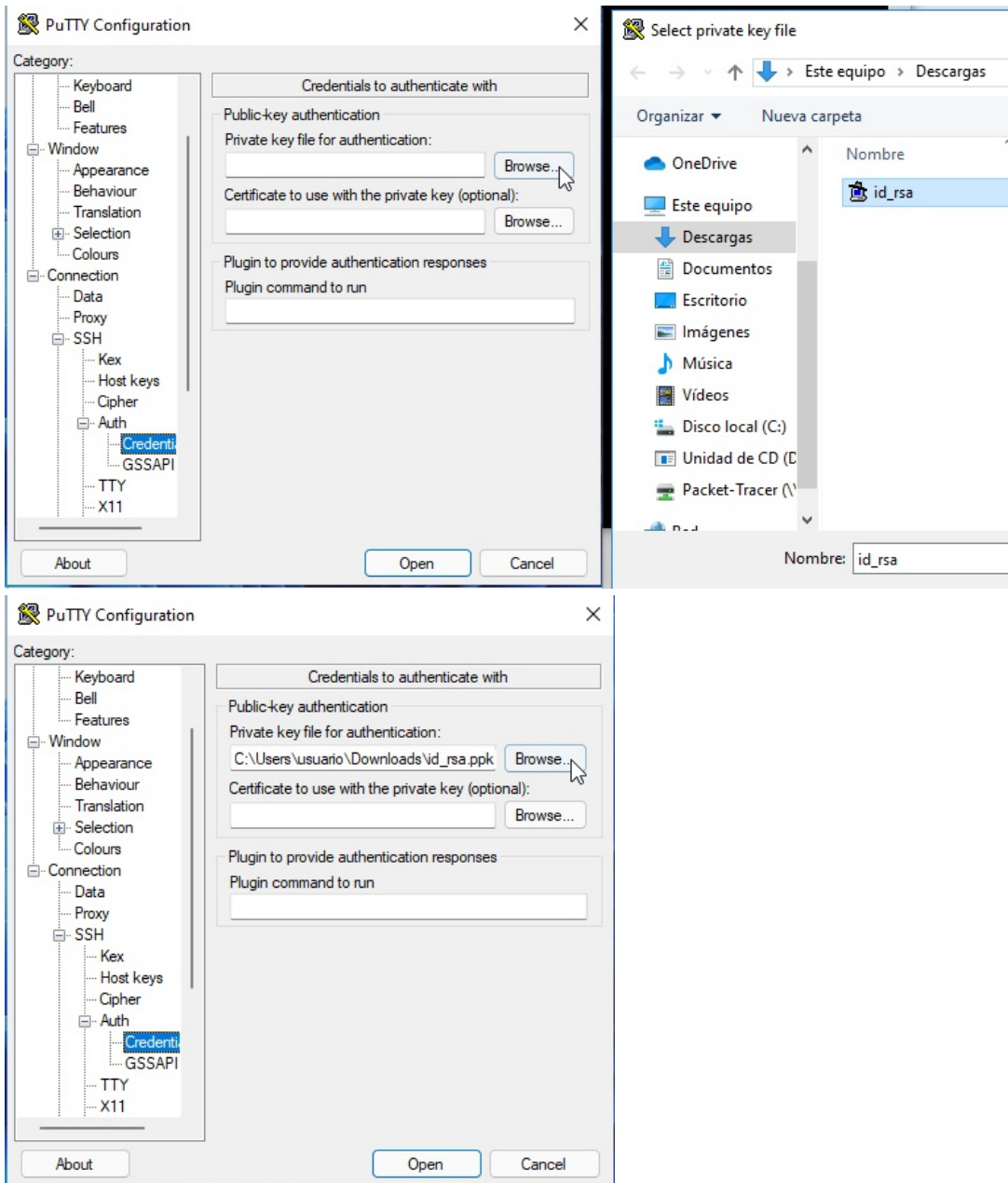
- b. Convertir esa chave privada ao formato entendible polo aplicativo putty gardándoa en formato PPK



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: Picar no botón Open para acceder sen contrasinal mediante conexión cifrada co usuario kali.

