**John the Ripper** es una herramienta poderosa para el crackeo de contraseñas, incluyendo las contraseñas de llaves SSH privadas. Aquí te dejo una guía paso a paso sobre cómo utilizar John the Ripper para crackear una llave SSH privada.

**Requisitos previos**

1. **John the Ripper:** Asegúrate de tener John the Ripper instalado en tu sistema. Puedes instalar la versión "Jumbo" que incluye más funcionalidades y soporte para más formatos de hash.
2. **Llave SSH privada:** Necesitas tener una llave SSH privada que esté protegida por una contraseña.

**Instalación de John the Ripper (versión Jumbo)**

Si aún no tienes John the Ripper, puedes instalarlo utilizando los siguientes comandos:

bash

Copy code

# Clonar el repositorio de John the Ripper Jumbo

git clone https://github.com/openwall/john -b bleeding-jumbo john

# Entrar al directorio clonado

cd john/src

# Compilar John the Ripper

./configure && make -s clean && make -sj4

**Convertir la llave SSH a un formato crackeable**

Antes de poder crackear la contraseña de la llave SSH, necesitas convertirla a un formato que John the Ripper pueda entender. Para ello, puedes usar el script ssh2john.py incluido con John the Ripper.

bash

Copy code

# Convertir la llave SSH privada a un formato crackeable

python3 ../run/ssh2john.py id\_rsa > id\_rsa.hash

**Crackeo de la llave SSH con John the Ripper**

Una vez que tengas el archivo de hash generado (id\_rsa.hash), puedes utilizar John the Ripper para intentar crackear la contraseña.

bash

Copy code

# Ejecutar John the Ripper sobre el archivo de hash

../run/john id\_rsa.hash

John the Ripper comenzará a intentar diferentes contraseñas hasta encontrar la correcta. Dependiendo de la complejidad de la contraseña y de tu hardware, este proceso puede llevar desde unos minutos hasta varias horas o días.

**Utilizar diccionarios (Wordlists)**

Para acelerar el proceso, puedes utilizar diccionarios de contraseñas comunes. John the Ripper puede usar wordlists para probar contraseñas más rápidamente.

bash

Copy code

# Ejecutar John the Ripper con una wordlist específica

../run/john --wordlist=/ruta/a/tu/wordlist.txt id\_rsa.hash

**Ver el progreso y los resultados**

Puedes verificar el estado del proceso de crackeo y ver las contraseñas encontradas utilizando el siguiente comando:

bash

Copy code

# Mostrar el estado del crackeo

../run/john --status

# Mostrar las contraseñas encontradas

../run/john --show id\_rsa.hash

**Resumen**

1. Instala John the Ripper Jumbo.
2. Convierte la llave SSH a un formato crackeable usando ssh2john.py.
3. Utiliza John the Ripper para crackear la contraseña.
4. (Opcional) Utiliza diccionarios para acelerar el proceso.

Este proceso te permitirá intentar crackear la contraseña de una llave SSH privada utilizando John the Ripper. Recuerda que esto debe hacerse únicamente en un entorno controlado y con las autorizaciones necesarias para evitar cualquier actividad ilegal o no ética.

**Paso 1: Descargar e instalar John the Ripper Jumbo**

Si aún no tienes John the Ripper Jumbo instalado, sigue estos pasos para instalarlo:

bash

Copy code

# Clonar el repositorio de John the Ripper Jumbo

git clone https://github.com/openwall/john -b bleeding-jumbo john

# Entrar al directorio clonado

cd john/src

# Compilar John the Ripper

./configure && make -s clean && make -sj4

**Paso 2: Localizar el script ssh2john.py**

El script ssh2john.py se encuentra en el directorio run dentro del directorio principal de John the Ripper.

bash

Copy code

# Navegar al directorio donde se encuentra el script

cd ../run

**Paso 3: Convertir la llave SSH**

Sigue estos pasos para convertir la llave SSH privada a un formato que John the Ripper pueda entender:

1. Asegúrate de tener tu llave SSH privada, por ejemplo, id\_rsa.
2. Utiliza el script ssh2john.py para convertir la llave.

bash

Copy code

# Convertir la llave SSH privada a un formato crackeable

python3 ssh2john.py /ruta/a/tu/id\_rsa > id\_rsa.hash

**Ejemplo de conversión**

Si tu llave SSH privada se llama id\_rsa y está ubicada en tu directorio actual, puedes ejecutar:

bash

Copy code

python3 ssh2john.py id\_rsa > id\_rsa.hash

**Paso 4: Verificar el archivo de hash generado**

El archivo id\_rsa.hash ahora contiene la llave SSH en un formato que John the Ripper puede utilizar para crackear la contraseña.

bash

Copy code

# Verificar el contenido del archivo de hash

cat id\_rsa.hash

**Paso 5: Crackear la contraseña con John the Ripper**

Ahora puedes utilizar John the Ripper para intentar crackear la contraseña de la llave SSH:

bash

Copy code

# Ejecutar John the Ripper sobre el archivo de hash

../run/john id\_rsa.hash

**Utilizar diccionarios (Wordlists) para acelerar el proceso**

Para acelerar el proceso de crackeo, puedes utilizar diccionarios de contraseñas comunes:

bash

Copy code

# Ejecutar John the Ripper con una wordlist específica

../run/john --wordlist=/ruta/a/tu/wordlist.txt id\_rsa.hash

**Ver el progreso y los resultados**

Para verificar el estado del proceso de crackeo y ver las contraseñas encontradas, utiliza los siguientes comandos:

bash

Copy code

# Mostrar el estado del crackeo

../run/john --status

# Mostrar las contraseñas encontradas

../run/john --show id\_rsa.hash

Siguiendo estos pasos, podrás convertir tu llave SSH privada a un formato que John the Ripper pueda crackear y proceder con el proceso de crackeo de la contraseña. Recuerda que debes hacer esto únicamente en un entorno controlado y con las autorizaciones necesarias para evitar cualquier actividad ilegal o no ética.