**Day 13**

**Exploitation Analyst**

**SSH Protocol:**

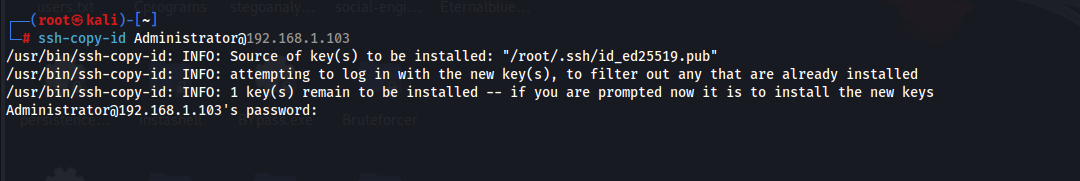
**How to connect SSH using keys:**

Steps:

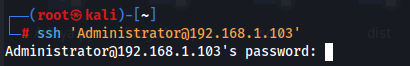
Generate the key using the following command:

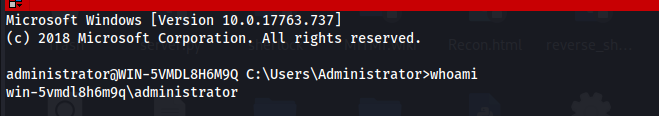


To copy keys to the Windows 2019 server: IP of 2019 server is 192.168.1.103



Now, try to enter in:



We can confirm like this:  


**Why SSH Key-Based Authentication Is Safe:**

Instead of sending a password (which can be guessed, stolen, or intercepted), this method uses a private-public key pair. The private key stays securely on your Kali machine, and only the public key is placed on the Windows server. When you connect, the server challenges you in a way that can only be answered using the private key. No secret is ever sent over the network, making it immune to sniffing (even with tools like Wireshark). Also, private keys are much longer and complex than passwords, making brute-force attacks practically impossible. You can even add a passphrase to your private key for extra protection, so even if it’s stolen, it can’t be misused easily.

**Ways SSH Can Be Hacked:**

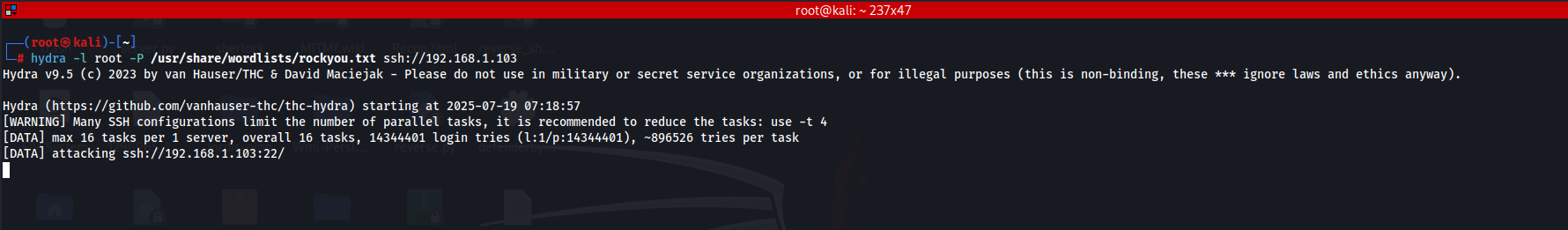
1. **Brute Force Attacks**  
   Attackers use automated tools like Hydra or Medusa to try thousands or millions of username-password combinations to guess valid SSH credentials.
2. **Stolen Private Keys**  
   If a user’s private key file is stolen (e.g., via malware or misconfigured file permissions), an attacker can gain access — especially if the key is not protected with a passphrase.
3. **Man-in-the-Middle (MITM) Attacks**  
   If a client connects without verifying the server’s fingerprint, an attacker on the same network can intercept the session and impersonate the server.
4. **Keyloggers and Malware**  
   If the client system is compromised, attackers can capture keystrokes, including passwords and session data, or even steal private SSH keys.
5. **Weak SSH Configuration**  
   Common misconfigurations include:
   1. Allowing root login via SSH
   2. Enabling password-based login instead of keys
   3. Using outdated or weak encryption algorithms
   4. Leaving the default SSH port (22) open to the internet
6. **Backdoors or Rogue SSH Servers**  
   Attackers may install unauthorized SSH servers or backdoors on compromised machines to collect credentials or monitor SSH sessions.
7. **Credential Reuse**  
   If users reuse the same password across services, a leak from one service can let attackers try the same credentials on SSH.

**Hacking SSH protocol:**

**Brute force attack on SSH:**

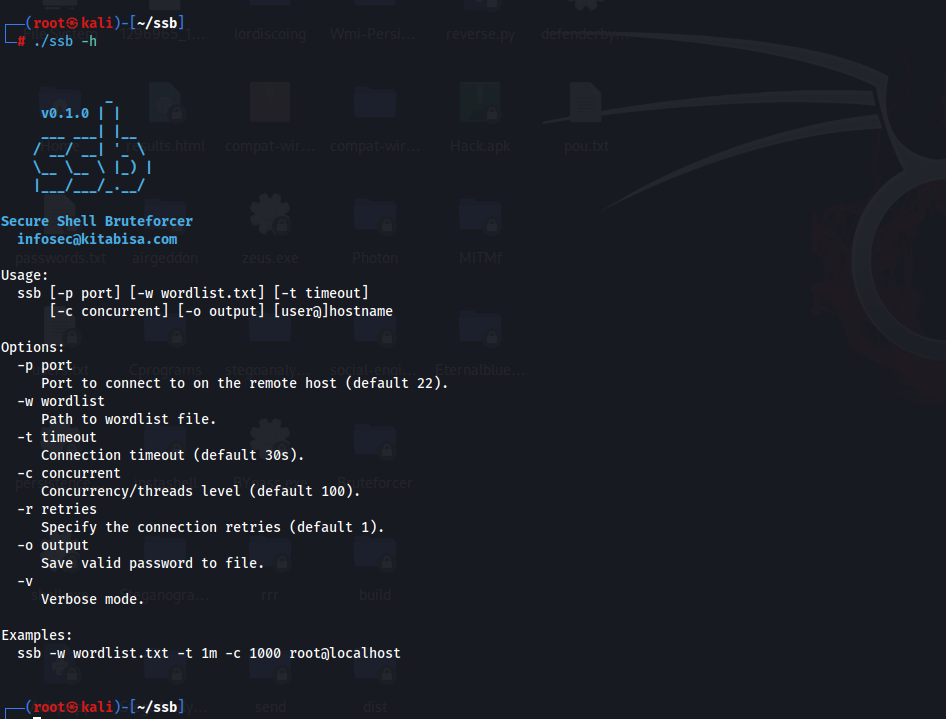
Steps:

Run the folloiwng command with specified password list and the IP address:

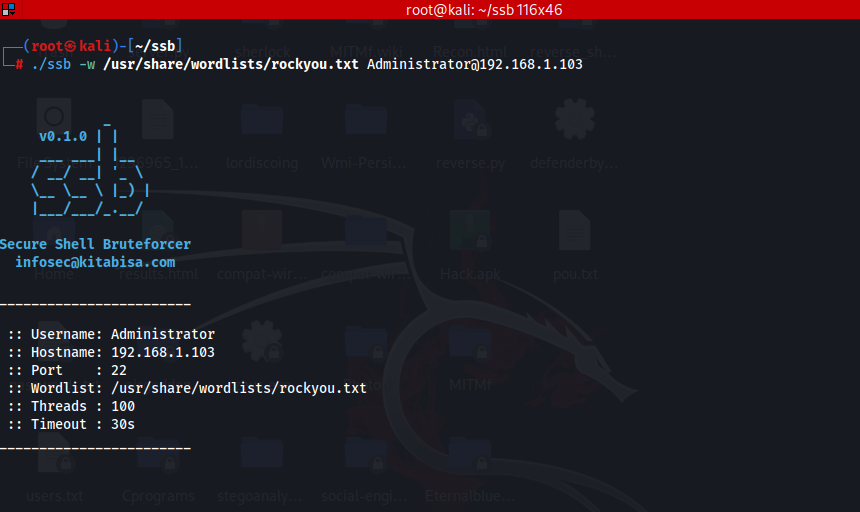


**OR,**

Try this:



Then to start the attack:



--The End--