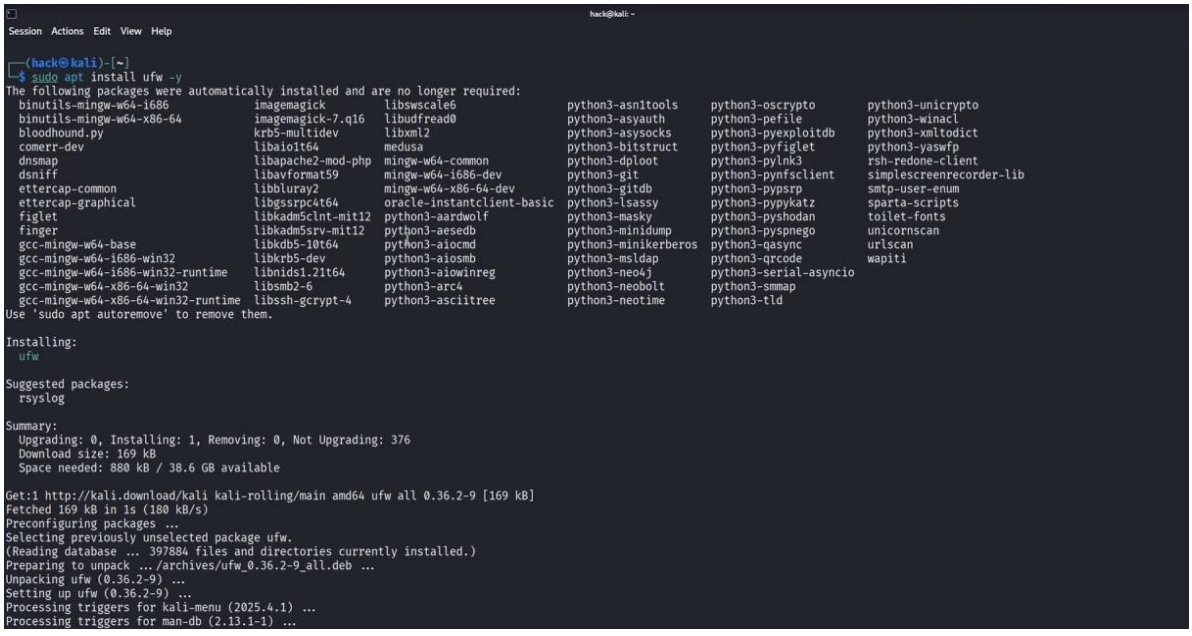
Task 2: Basic Firewall Configuration with UFW

INSTALL UFW:

To install **UFW (Uncomplicated Firewall)** on a Linux system, first update your package list using the command sudo apt update. Then install UFW by running **sudo apt install ufw -y**. Before turning it on, it's important to allow SSH connections (especially if you are connected remotely) using **sudo ufw allow ssh**. After that, enable the firewall with **sudo ufw enable**. You can then verify its status with **sudo ufw status verbose** or check the version using ufw version. This setup ensures that UFW is properly installed, running, and configured with safe access to your system via SSH.



SETTING UP UFW:

After installing UFW, you can begin configuring your firewall rules to control network traffic. Start by allowing essential services such as SSH using `**sudo ufw allow ssh**` to ensure remote access remains available. You can then deny or allow other ports based on your security needs — for example, `**sudo ufw deny http**` to block web traffic. Once your rules are set, enable the firewall with `**sudo ufw enable**` and verify the configuration using `**sudo ufw status verbose**`. This ensures that your system is protected and only trusted connections are allowed.