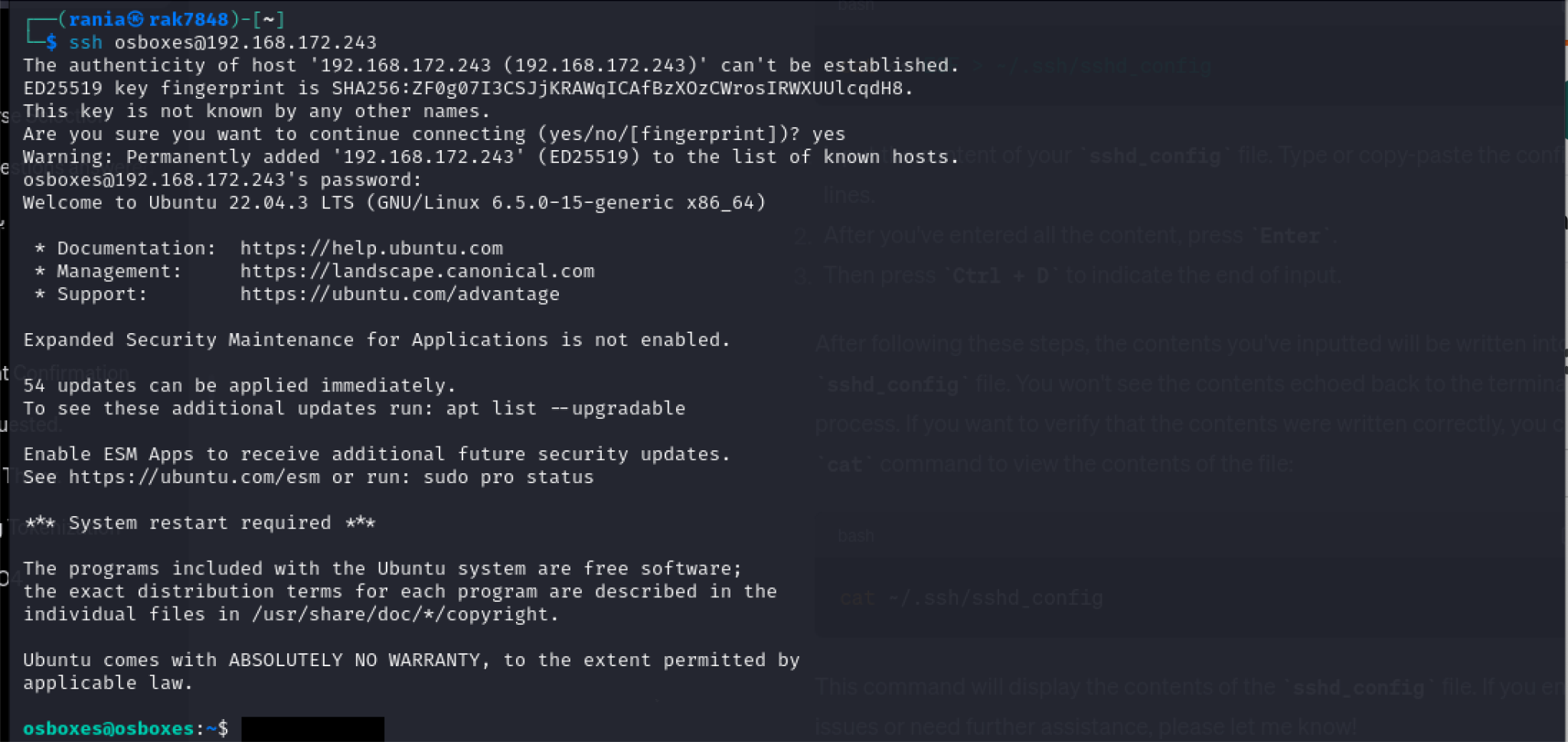
**Course: NSSA.245.60L1**

**Names: Suhaila Alfalasi - Rania Kanaan**

**Tuesday 13th February**

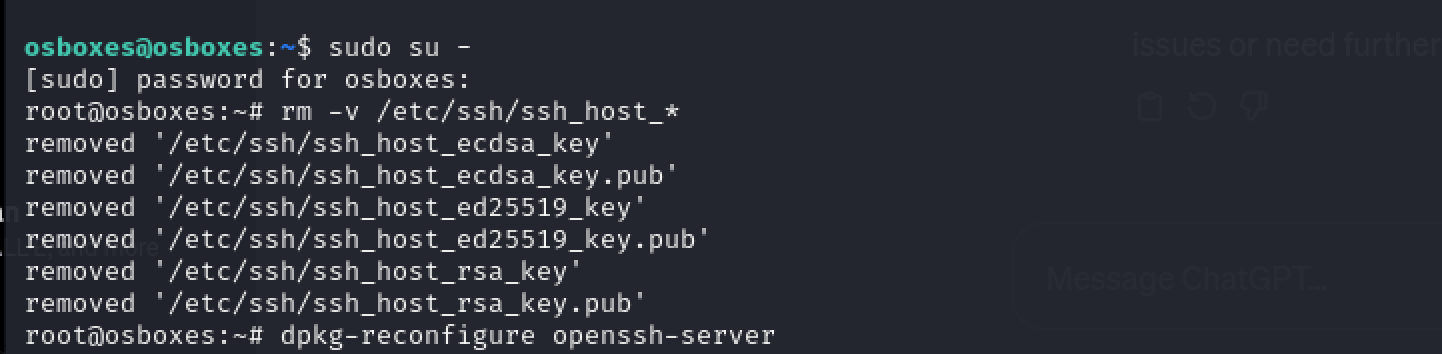
**Lab-01 SSH**

**Task 1**

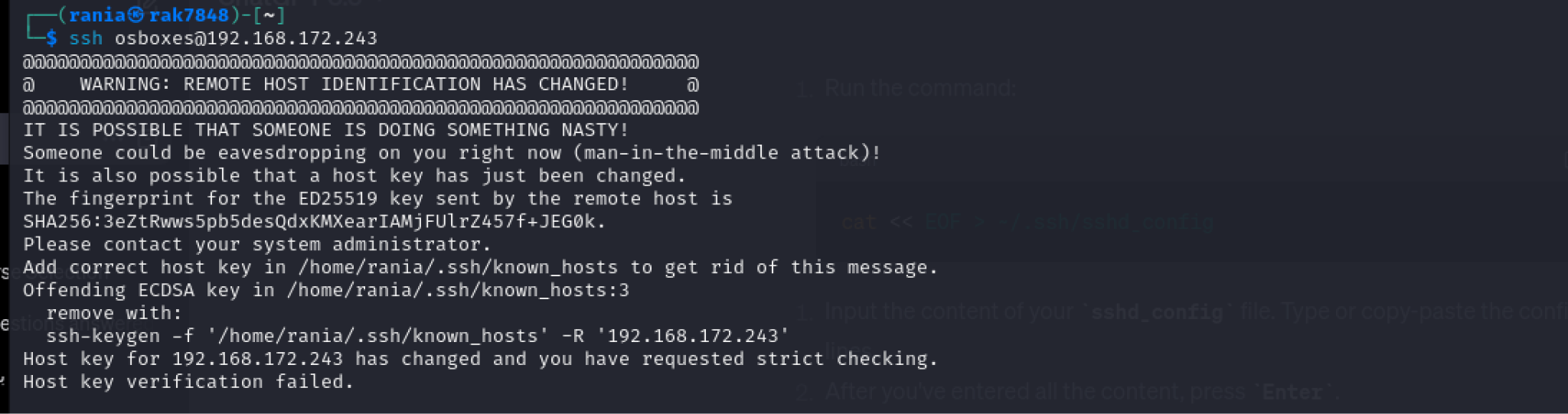
****

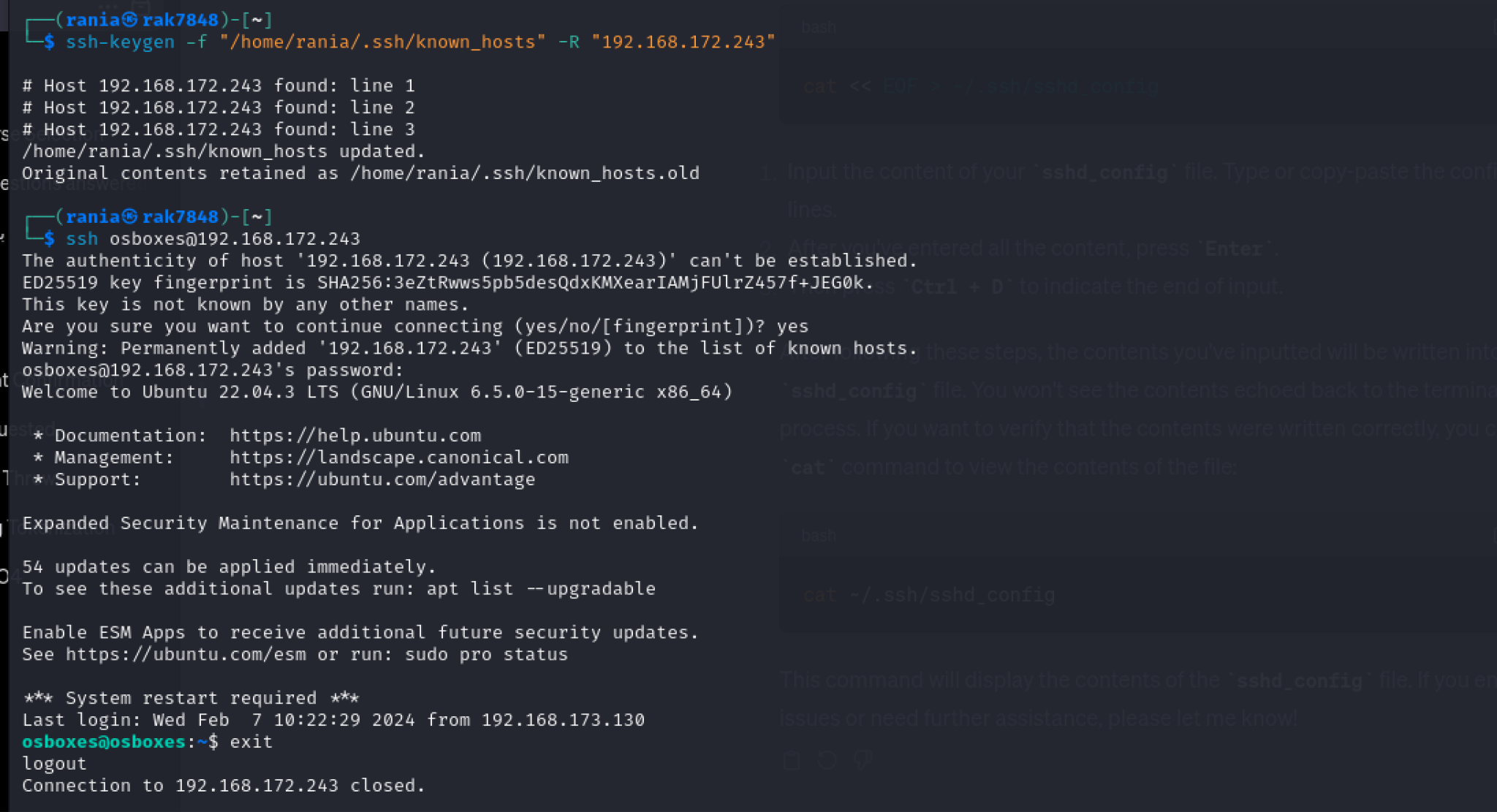
The goal of this command is to try to connect the Ubuntu computer to the Kali system over SSH using the IP address 192.168.172.243.

**Task 2**

****

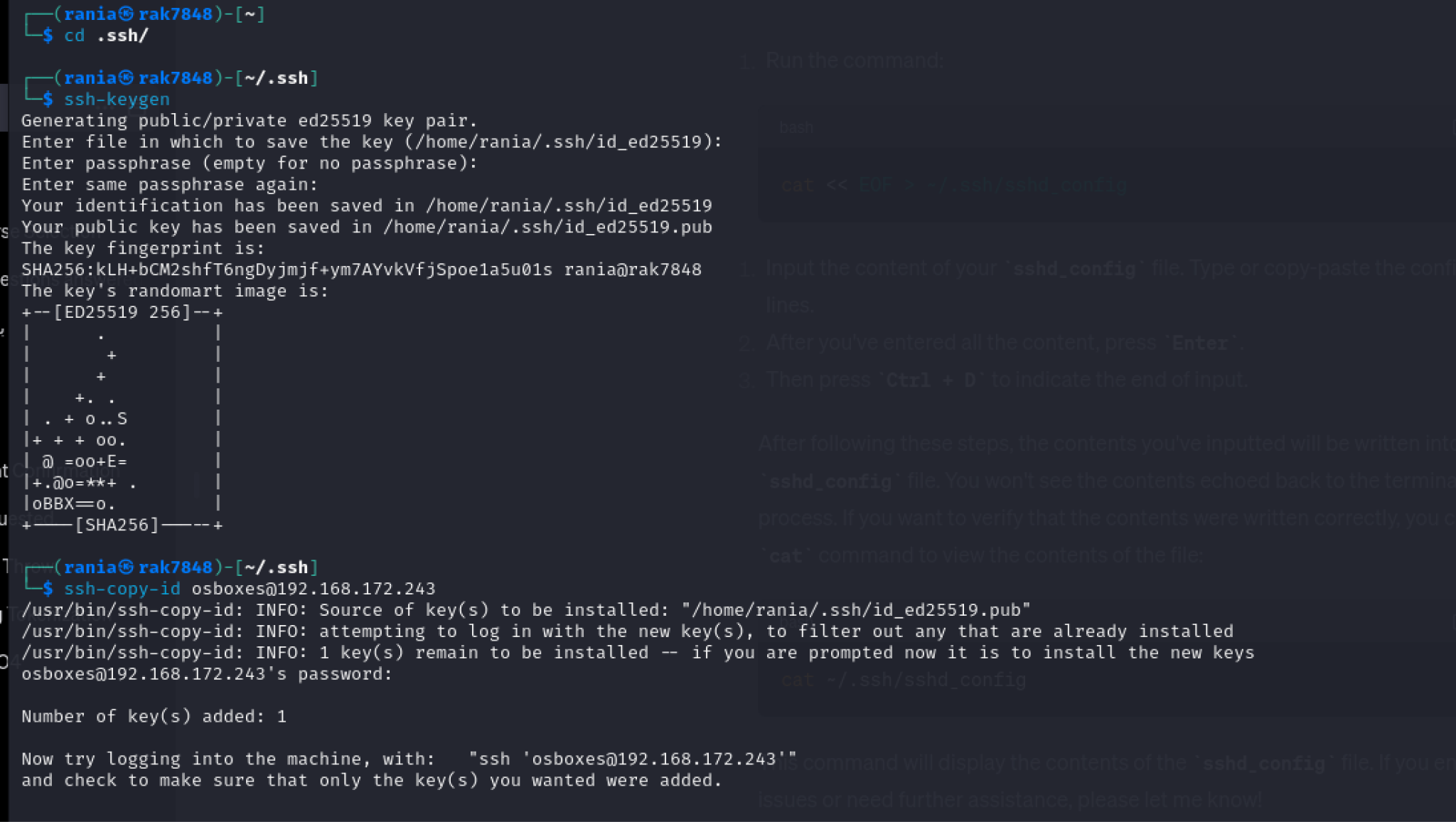
With the use of this command, the current user can become the root user and take complete control of the system's resources and configuration settings.

****

****

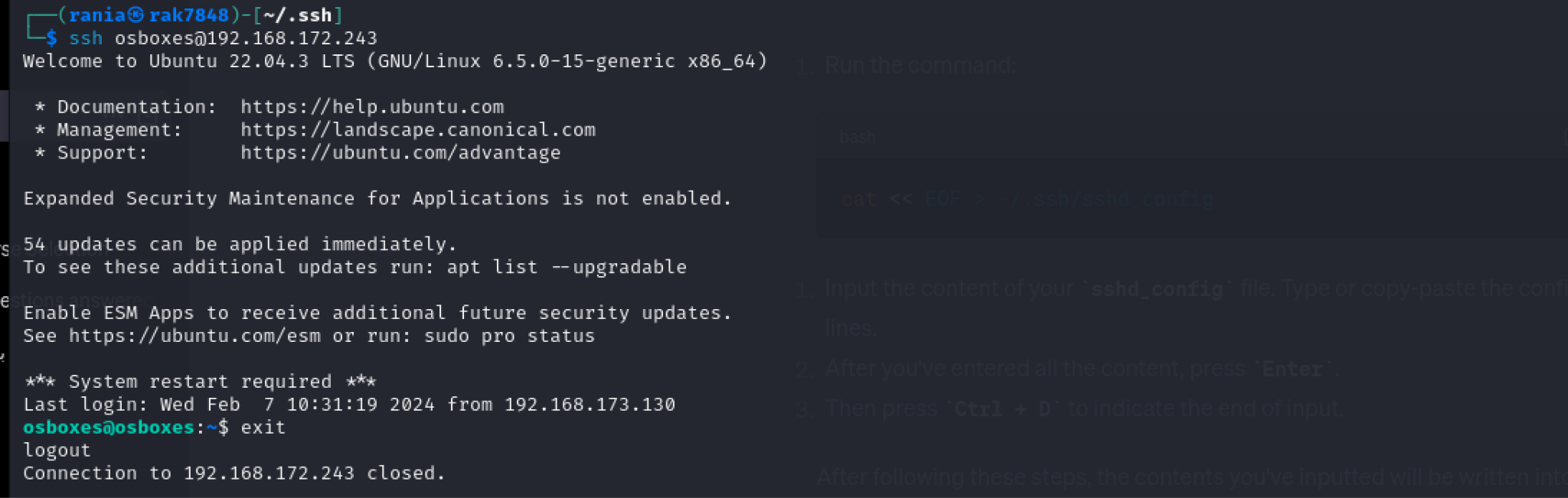
The command eliminates the entry for the host with the IP address "192.168.172.243" from the user's home directory's {`/home/rania/.ssh/known\_hosts} file within the `known\_hosts` file. In order to update the file, the entry has been deleted and backed up as `known\_hosts.old}.

**Task 3**

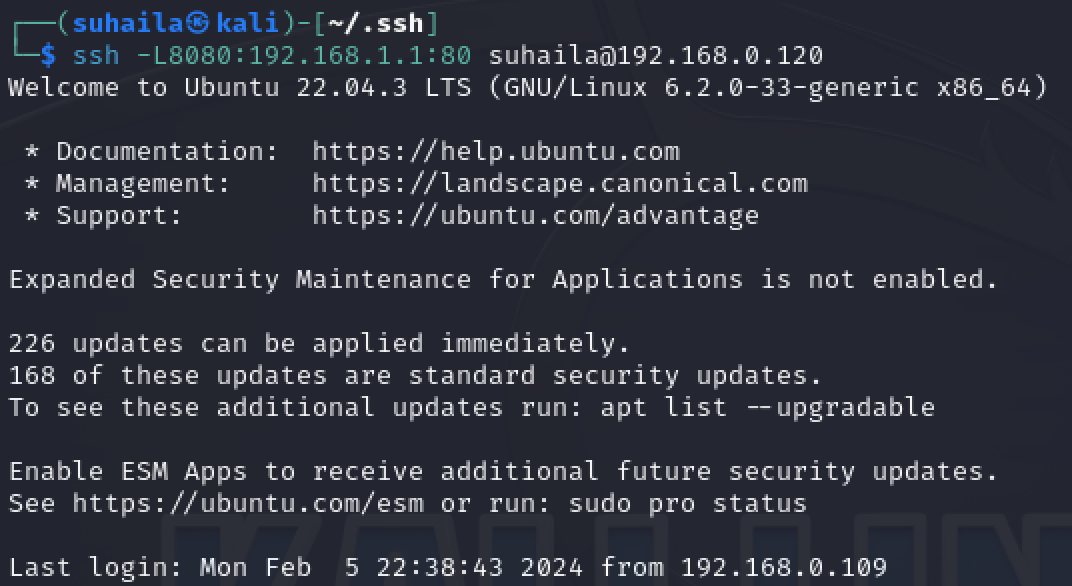
****

The command ssh-keygen is used to create, control, and modify SSH keys for authentication.

The command `ssh-copy-id osboxes@192.168.172.243` copies the public key to the authorized\_keys on the remote machine `192.168.172.243`, enabling SSH authentication for the osboxes user.

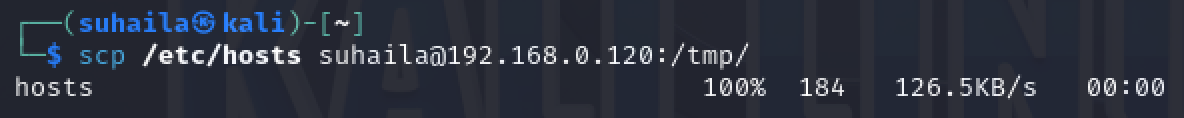
****

**Task 4**

****

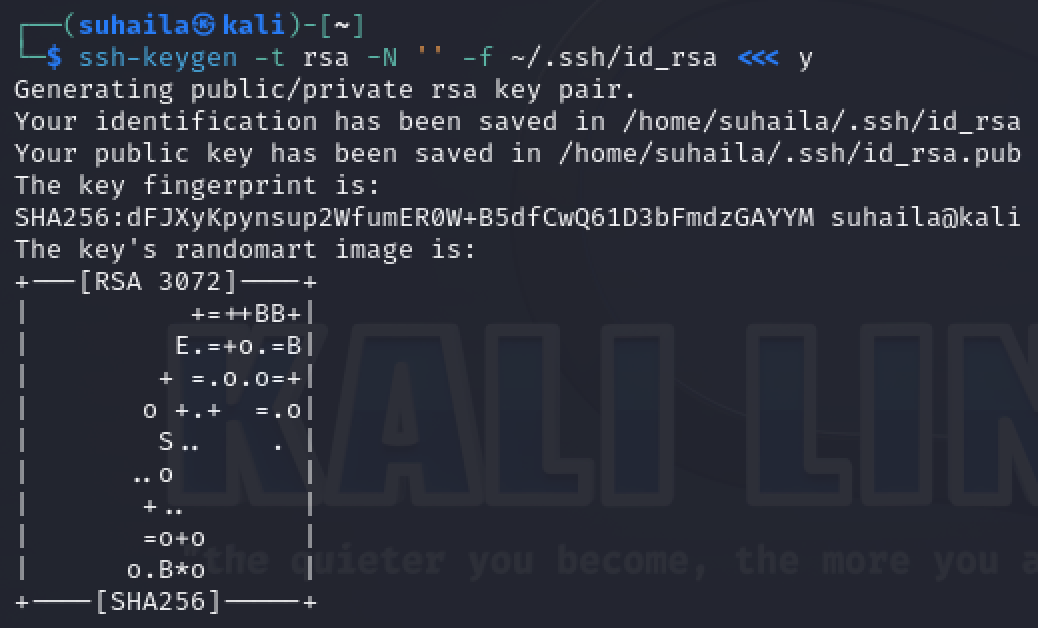
This command enables the ssh to connect to our ubuntu virtual machine with an IP address of 192.168.0.120 and any traffic that will be sent from local port 8080 will be forwarded to port 80.

**Task 5**

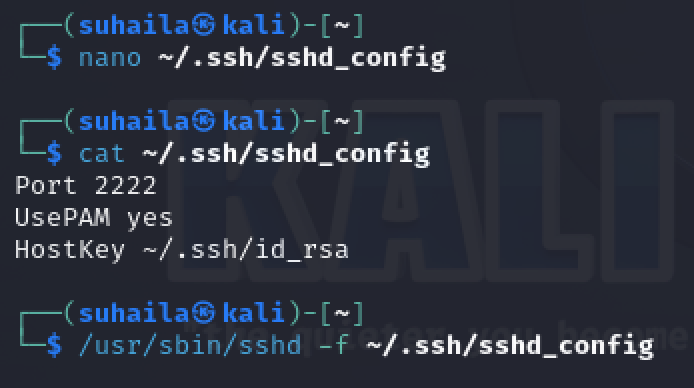
****

Scp means that it will copy the file securely from the path /etc/hosts to the destination of the Ubuntu virtual machine /tmp/. This will copy the file securely from the kali to the ubuntu over the network.

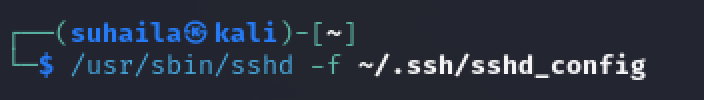
**Task 6**

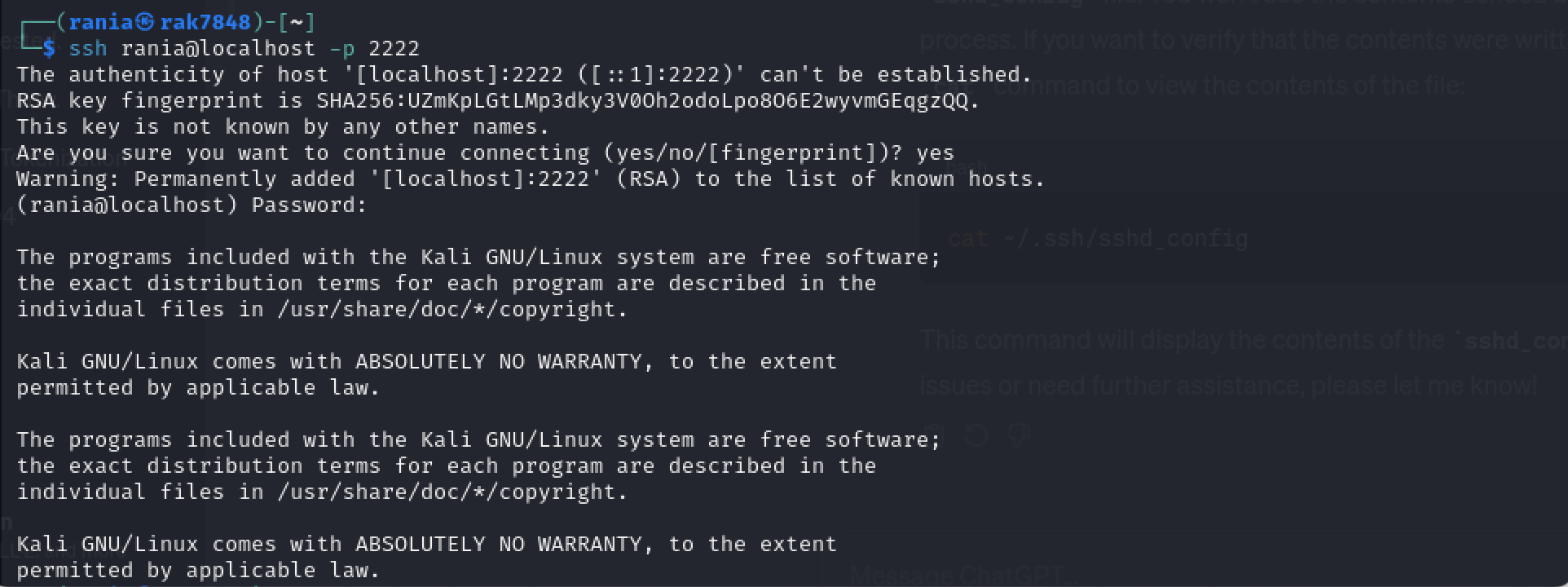


The “Ssh-keygen -t rsa -N ‘’ -f ~/.ssh/id\_rsa” command generates an RSA SSH key pair and saves it into ~/.ssh/id\_rsa with setting an empty password and “ <<< y “ indicates that its an automated yes to generate the key pair.



Nano is a text editor that opens the configuration file and inside the file we have typed the “Port 2222” that sets the server to listen to port 2222 instead of port 22, the “UsePAM yes” is enables the administrator to change the configuration policies, and the “HostKey ~/.ssh/id\_rsa” is the location where the host key file in stored. The “cat” command prints the given location content.





The first command `/usr/sbin/sshd -f ~/.ssh/sshd\_config` starts the daemon (`sshd`) with a configuration file `~/.ssh/sshd\_config`. It make the system use the specified configuration file instead of the default one.

Also for the second command which is the last one `ssh rania@localhost -p 2222` it establishes an ssh connection to the localhost, using port 2222 instead of port 22.