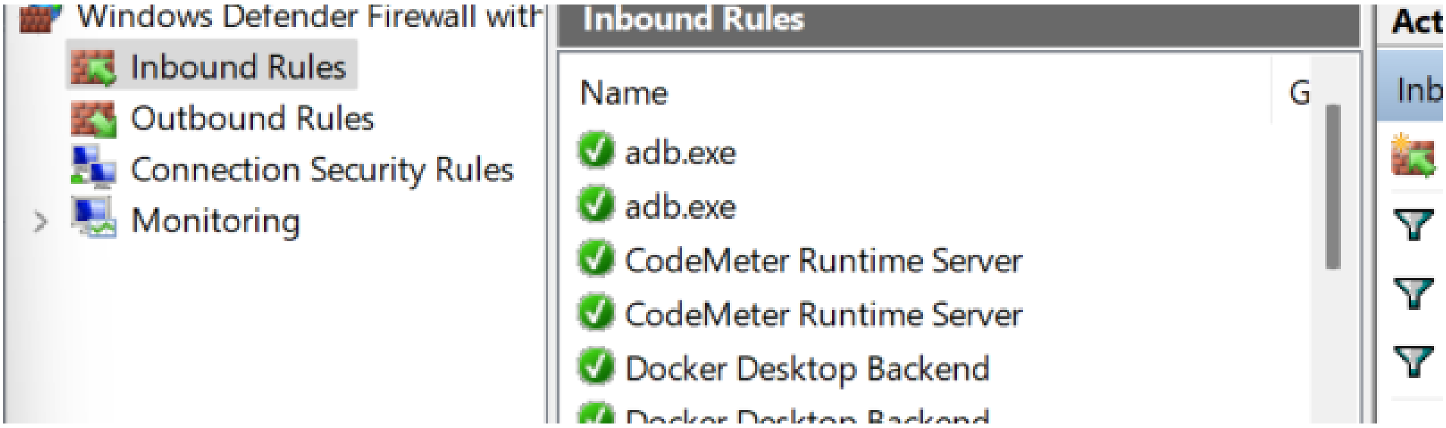
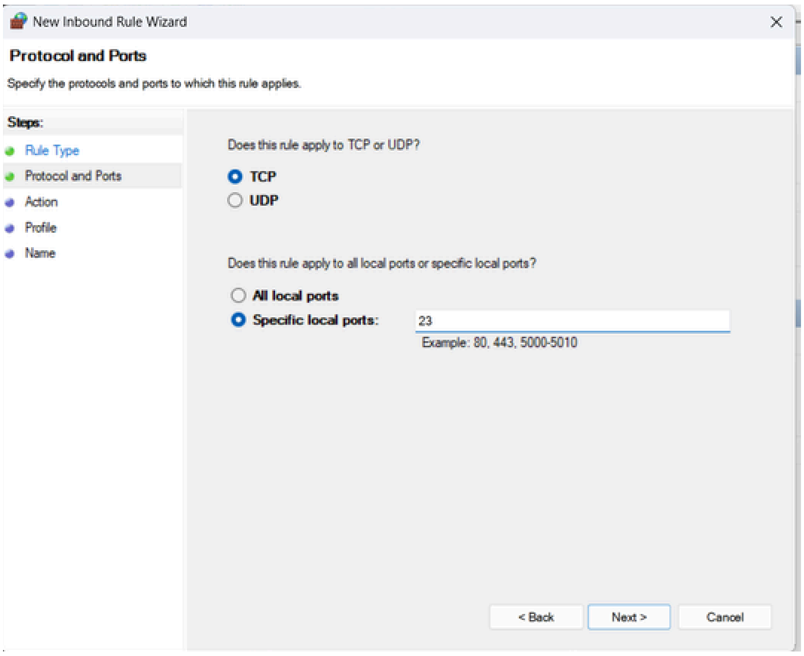
Elevate Labs Task 4

G.Harshith

I have opened the Windows firewall for inbound and outbond rules



Now i want to block telnet requests in my system


New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

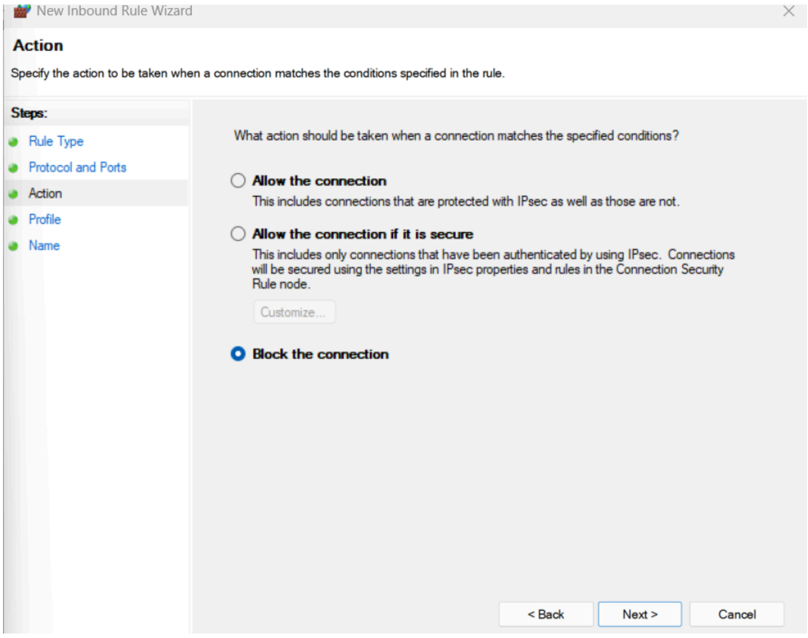
Does this rule apply to TCP or UDP?

● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 23

Example: 80, 443, 5000-5010



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

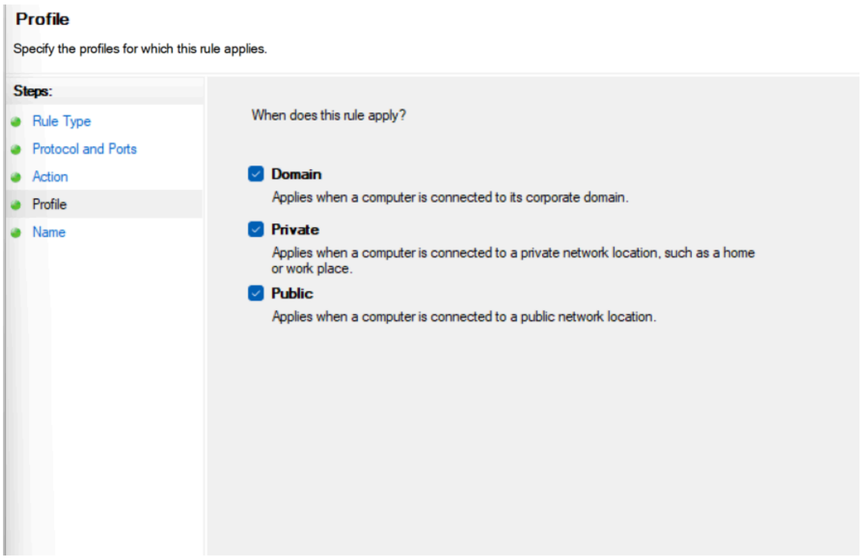
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**



Profile

Specify the profiles for which this rule applies.

Steps:

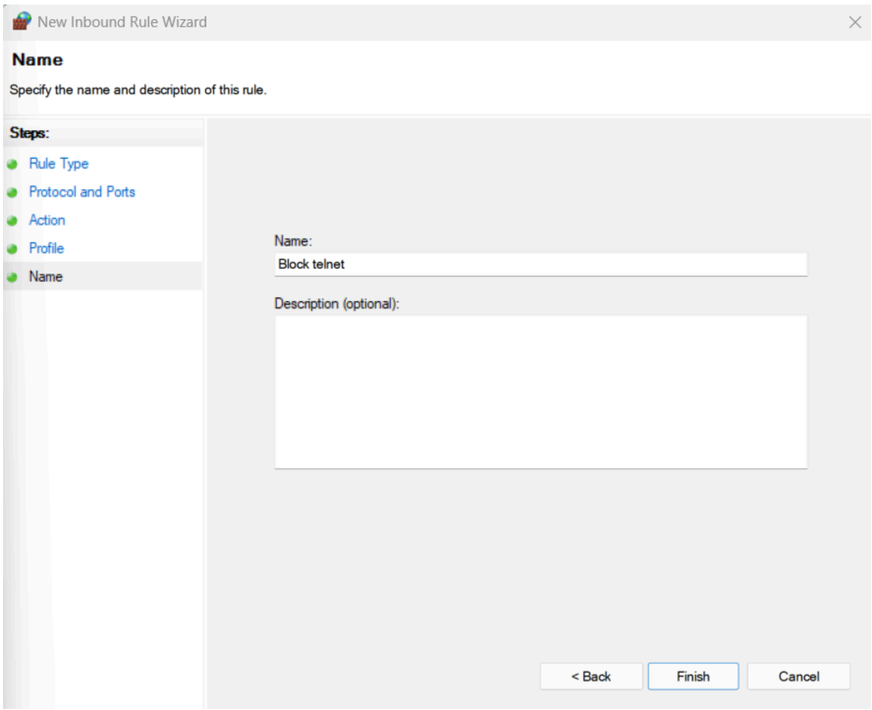
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.



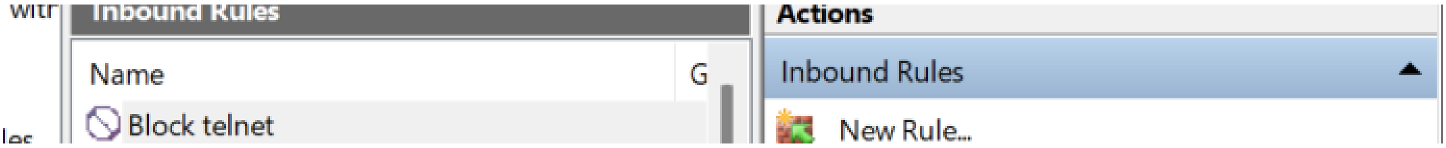
New Inbound Rule Wizard

Name

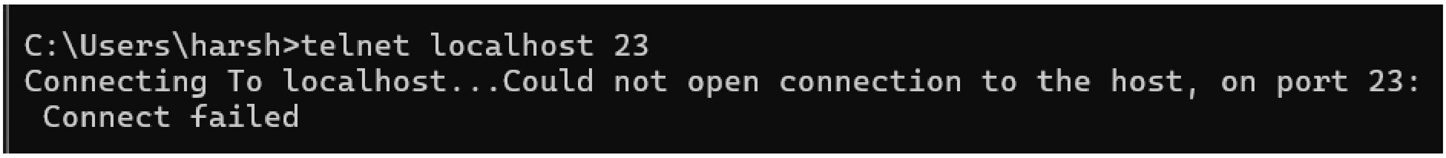
Specify the name and description of this rule.

Name: Block telnet

Description (optional):



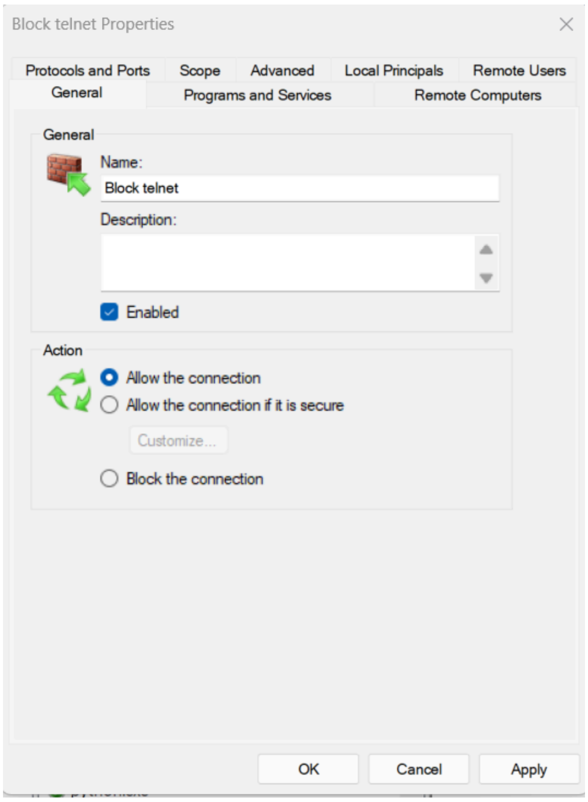
Therefore the Telnet requests are blocked by the fire wall



```
C:\Users\harsh>telnet localhost 23
Connecting To localhost...Could not open connection to the host, on port 23:
 Connect failed
```

As we can see telnet connection cannot be accessed since the fire wall is blocking it.

I will delete the rule , so that telnet can be used



General

Name: Block telnet

Description:

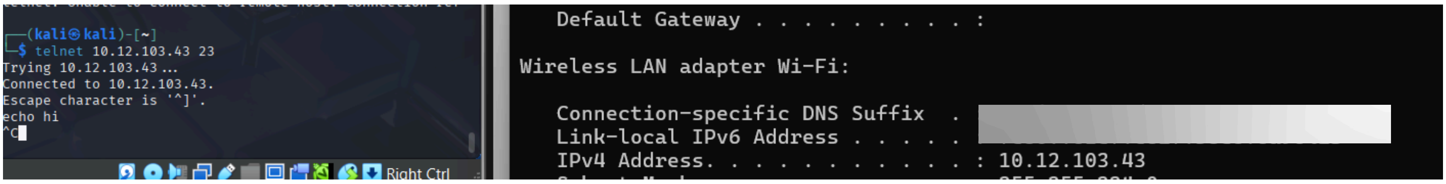
☑ Enabled

Action

● Allow the connection

○ Allow the connection if it is secure

○ Block the connection

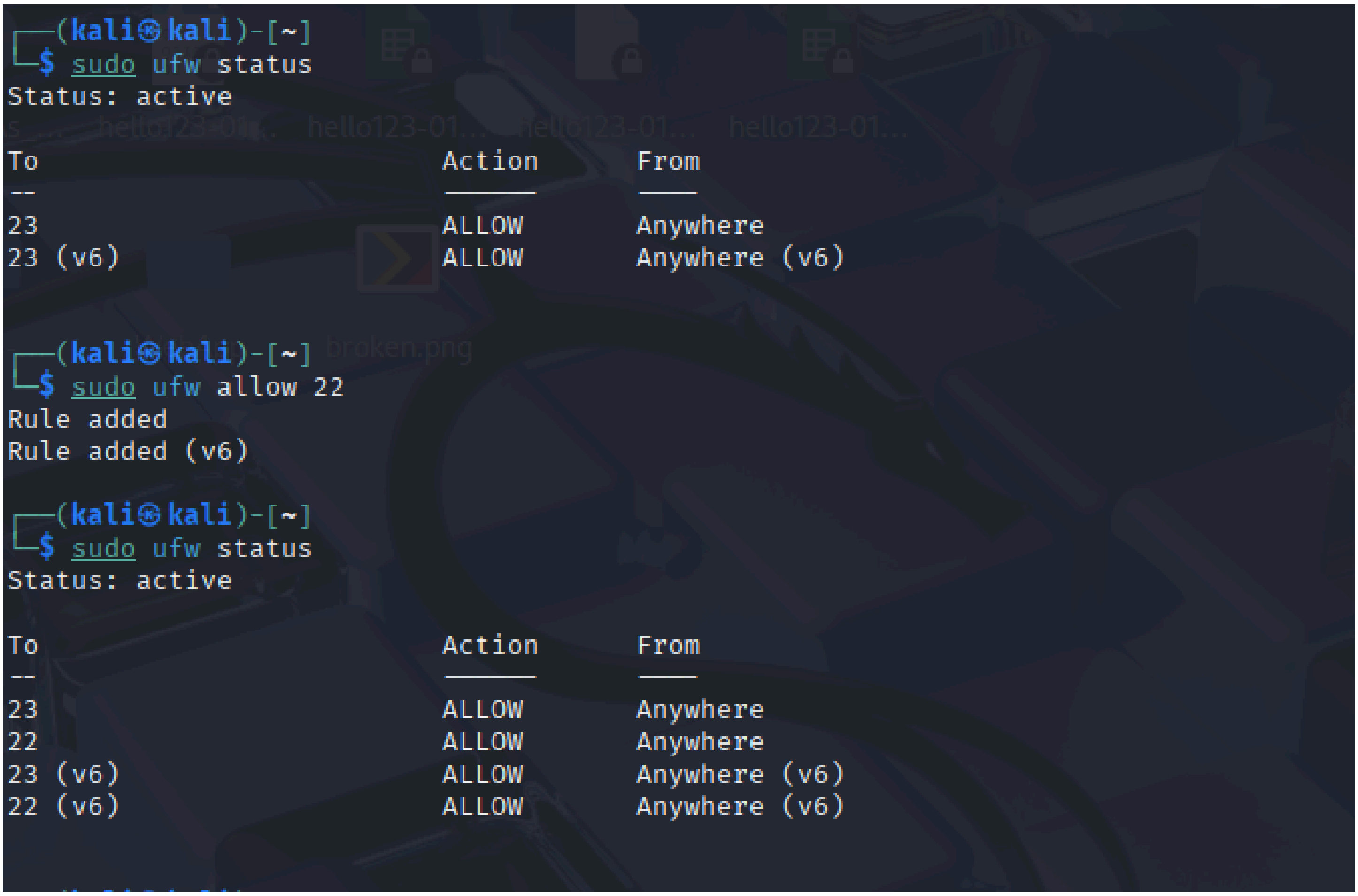


```
┌──(kali㉿kali)-[~]
└─$ telnet 10.12.103.43 23
Trying 10.12.103.43 ...
Connected to 10.12.103.43.
Escape character is '^]'.
echo hi
^C
```

```
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . [redacted]
   Link-local IPv6 Address . . . . .
   IPv4 Address. . . . . . . . . . . : 10.12.103.43
```

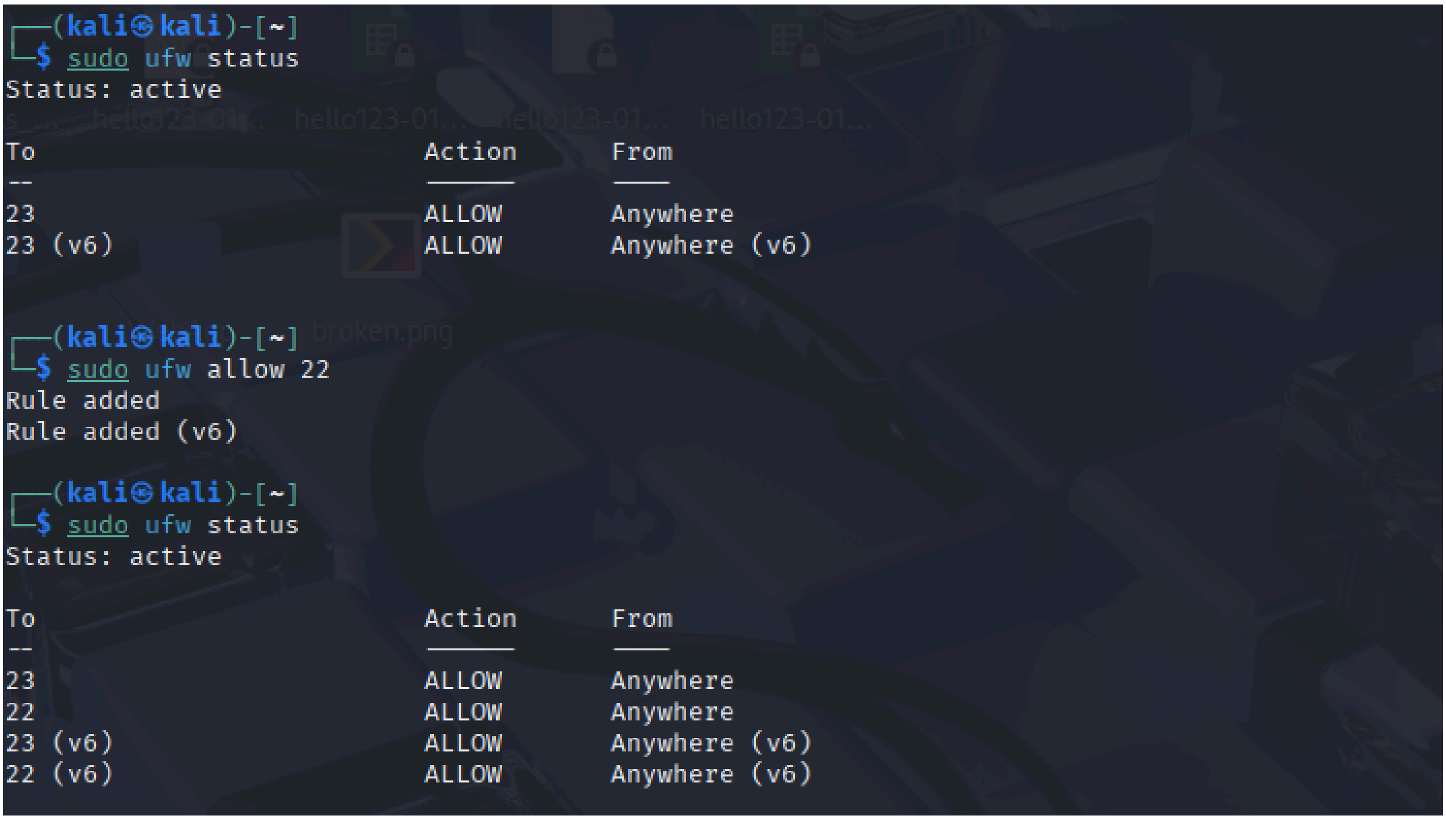
Now the telnet Connection can be done

Now on Linux

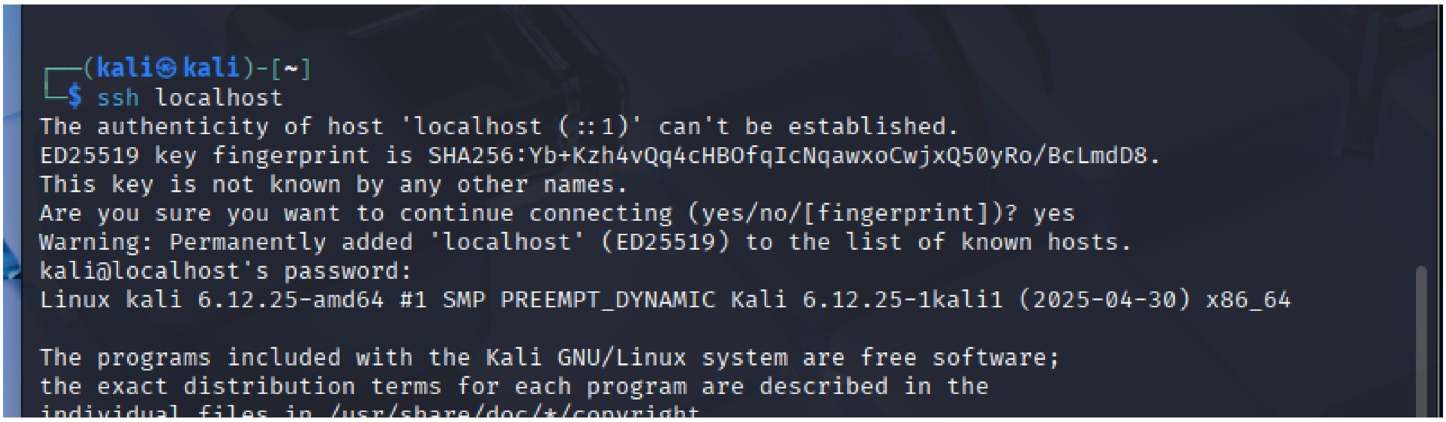


```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         ALLOW       Anywhere
23 (v6)                    ALLOW       Anywhere (v6)


┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         ALLOW       Anywhere
22                         ALLOW       Anywhere
23 (v6)                    ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)
```

This setup in firewall allows both telnet and ssh to work on it



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         ALLOW       Anywhere
23 (v6)                    ALLOW       Anywhere (v6)


┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22
Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         ALLOW       Anywhere
22                         ALLOW       Anywhere
23 (v6)                    ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)
```



```
┌──(kali㉿kali)-[~]
└─$ ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:Yb+Kzh4vQq4cHBOfqIcNqawxoCwjxQ50yRo/BcLmdD8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
kali@localhost's password:
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright
```

By this Exercise i understood how firewall rules can be made and edited