**TASK – 4**

## **Setup and Use a Firewall on Linux.**

1. **CHECKING AND INSTALLING FIREWALL CONFIGURATION TOOL :**

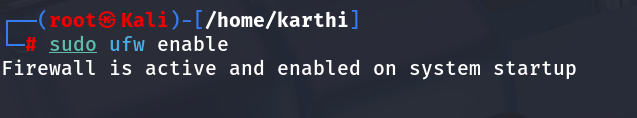
****

* I have switched to root user and checked the status of ufw (uncomplicated firewall).
* As it returned command not found , I have installed it after updating my current system.

**COMMANDS USED :**

* **sudo su**
* **sudo ufw status**
* **sudo apt update**
* **“ sudo apt install ufw “**

1. **ENABLING THE FIREWALL TOOL (UFW) :**

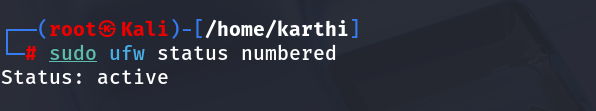
****

* We have to enable the tool to use.

**COMMAND USED :**

* **sudo ufw enable**

1. **LISTING ALL CURRENT RULES :**

****

* When I ran the command to list all the rules, it returned nothing but status.
* So, there are no current rules that are defined or running.

**COMMAND USED :**

* **sudo ufw status numbered**

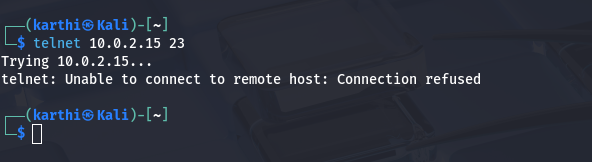
**4) ADDING RULE TO BLOCK INBOUND TRAFFIC FOR A PORT :**

****

**COMMAND USED :**

* **sudo ufw deny 23**

**5) TESTING FROM ANOTHER DEVICE :**

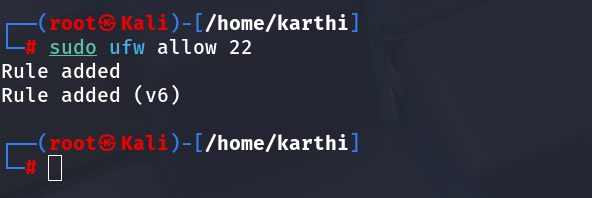
****

* We got connection refused when we tried to reach the ip with port 23.
* So the port is blocking the incoming traffic.

**COMMAND USED :**

* **telnet <ip> 23**

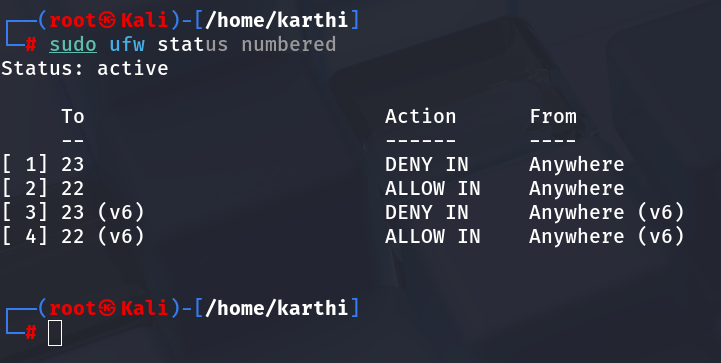
**6) ADDING ANOTHER RULE :**

****

**COMMAND USED :**

* **sudo ufw allow 22**

**7) LISTING / CHECKING ALL THE CURRENT RULES :**

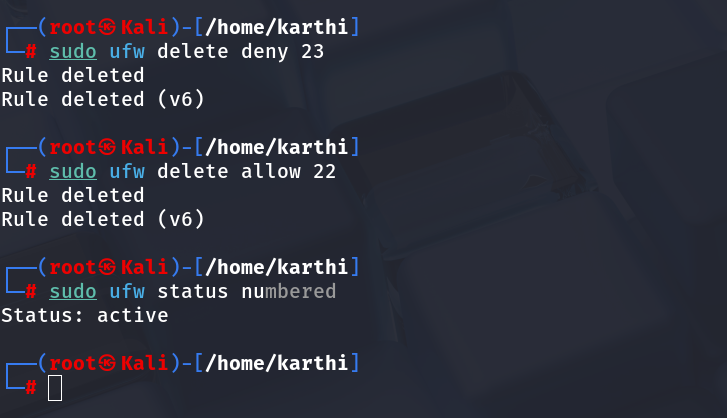
****

* Here, we can see that traffic denied to port 23 , allowed to port 22.
* So, The rules we have created are applied.

**COMMAND USED :**

* **sudo ufw status numbered**

**7) REMOVING RULES AND RESTORING TO ORIGINAL :**

****

* I have run commands to remove rules that I have applied.
* We can see “Rule deleted” message from the above terminal screenshot.
* Then I have again checked with the listing command and I found nothing just as same as in the 3rd step.

**COMMAND USED :**

* **sudo ufw delete deny 23**
* **sudo ufw delete allow 22**
* **sudo ufw status numbered**

**WORKING OF FIREWALL (SUMMARY) :**

**Watches Traffic:**  
 Every time your computer sends or receives data, the firewall checks it.

**Checks the Rules:**  
 It compares that data with rules like:

* "Allow port 22 for SSH"
* "Block port 23 for Telnet"

**Takes Action:**

* If the data is safe or allowed, it lets it pass.
* If it’s suspicious or not allowed, it blocks it.

**Keeps In & Out in Control:**

* Inbound rules control who can reach your system.
* Outbound rules control what your system can connect to.

**Nanduri Karthikeya.**