

**Veermata Jijabai Technological Institute, Mumbai 400019**

**Experiment No.:** 04

**Aim:** Practical Experiment on Firewall

**Group :** Kiran Patil - 211070904

Mayuresh Murudkar - 211070903

Pratiksha Sankhe – 201071049

**Branch:** Final Year B.Tech Computer Engineering

**Batch:** D

**Theory:**

**Firewall**

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, software-as-a service (SaaS), public cloud, or private cloud (virtual).

**1. Firewall Software:**

* **Firewall Functionality**: Firewalls act as a barrier between your network and external networks, controlling incoming and outgoing traffic based on a set of predefined security rules.
* **Packet Filtering**: Most firewalls use packet filtering to allow or block traffic based on IP addresses, ports, and protocols.
* **Stateful Inspection**: This feature keeps track of the state of active connections and makes decisions based on the context of the traffic.
* **Proxy Services**: Some firewalls offer proxy services, which involve acting as an intermediary between internal and external clients to enhance security.
* **Deep Packet Inspection (DPI)**: DPI firewalls inspect the actual data within packets to identify and block specific content or threats.
* **Application Layer Filtering**: Modern firewalls often include application-layer filtering to control traffic based on specific applications and services.
* **Logging and Reporting**: Comprehensive logging and reporting capabilities help in monitoring and auditing network activity.

**Popular commercial firewall software includes:**

* Cisco ASA (Adaptive Security Appliance)
* Palo Alto Networks
* Fortinet FortiGate
* Check Point Firewall
* SonicWall

**2. Intrusion Detection System (IDS) Software:**

* **IDS Functionality**: IDS software monitors network traffic for suspicious activity or known attack patterns. It can be classified into two main types: Network-based (NIDS) and Host-based (HIDS).
* **Signature-Based Detection**: This method uses predefined patterns (signatures) to identify known threats, making it effective against known attacks.
* **Anomaly-Based Detection**: Anomaly-based IDS software establishes a baseline of normal network behavior and triggers alerts when deviations occur.
* **Heuristic-Based Detection**: These IDS systems use rules or heuristics to identify suspicious behavior that may indicate an attack.
* **Real-time Alerting**: IDS software generates alerts when it detects potentially malicious activity, which can be sent to administrators for further action.
* **Logging and Reporting**: Similar to firewalls, IDS systems offer logging and reporting features to help in post-incident analysis.

**Notable commercial IDS software includes:**

* Snort
* Suricata
* McAfee Network Security Platform
* IBM QRadar
* Trend Micro Deep Security

**When studying commercial firewall and IDS software, consider the following aspects:**

* **Licensing and pricing**: Understand the cost structure and licensing terms.
* **Scalability**: Assess whether the software can scale to meet your network's needs.
* **Integration**: Check if the software integrates with other security tools and SIEM systems.
* **Management and ease of use**: Evaluate the user interface and management capabilities.
* **Support and updates**: Look into the availability of support, documentation, and regular updates.
* Ultimately, the choice of commercial firewall and IDS software should align with your organization's security requirements, network architecture, and budget constraints. Conduct thorough research, consider trial versions, and, if possible, consult with experts in the field to make an informed decision.

**3. Graphical Uncomplicated Firewall**

Gufw, which stands for "Graphical Uncomplicated Firewall," is a user-friendly graphical interface for managing the Uncomplicated Firewall (UFW) on Linux systems. UFW is a front-end to the netfilter firewall, which is built into the Linux kernel and provides packet filtering and network address translation (NAT).

**1. Purpose:**

* Gufw is designed to simplify the process of configuring and managing firewall rules on a Linux system. It provides an easy-to-use, graphical interface for users who may not be comfortable with the command-line interface.

**2. Features:**

* **Rule Management:** Gufw allows users to create, modify, and delete firewall rules to control network traffic. This includes both incoming and outgoing traffic.
* **Application Profiles:** Gufw can create and manage profiles for different applications or services. This feature simplifies the process of allowing or blocking network traffic for specific applications.
* **Preconfigured Profiles:** It comes with a set of preconfigured profiles for common services such as SSH, web servers, and file sharing. This simplifies the setup for users who don't want to create custom rules.
* **Logging:** Gufw provides logging capabilities, allowing users to monitor firewall activity and track allowed or denied traffic.
* **Status Toggle:** You can easily enable or disable the firewall with a simple toggle switch within the Gufw interface.

**3. Basic Concepts:**

* **Firewall Rules:** Gufw allows you to define rules that specify what network traffic should be allowed or denied. Rules typically include information like the direction of traffic (inbound or outbound), the protocol (e.g., TCP or UDP), and the port or application involved.
* **Default Policies:** You can set the default policies for incoming and outgoing traffic, specifying whether traffic not explicitly allowed by a rule should be denied or allowed by default.
* **Profiles:** Gufw uses profiles to group rules related to specific applications or services. For example, you might have a profile for a web server with rules allowing HTTP and HTTPS traffic.

**4. How Gufw Works:**

* Gufw is essentially a graphical front-end to UFW, which itself interacts with the netfilter framework in the Linux kernel. When you create or modify a rule in Gufw, it translates your settings into UFW commands that are then used to configure the underlying firewall.

**5. Advantages:**

* User-Friendly: Gufw makes firewall management more accessible to users who are not comfortable with the command line.
* Easy Setup: Preconfigured profiles and an intuitive interface simplify the setup of common firewall rules.
* Logging: Gufw provides logging capabilities to monitor and track firewall activity.

**6. Considerations:**

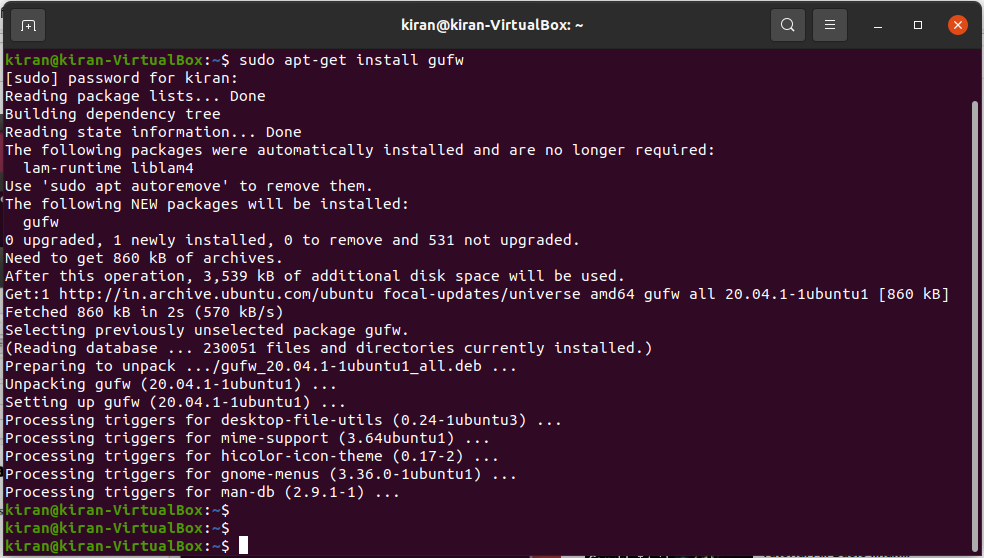
* While Gufw simplifies firewall management, it's important to understand the basics of networking and firewall rules to use it effectively.
* Misconfigured firewall rules can impact network connectivity and security, so it's essential to be cautious when setting up rules.

In summary, Gufw is a valuable tool for managing firewall rules on Linux systems, especially for users who prefer a graphical interface. It simplifies the process of configuring firewall rules and helps enhance the security of Linux systems by controlling network traffic. However, users should have a basic understanding of networking and firewall concepts to use Gufw effectively.

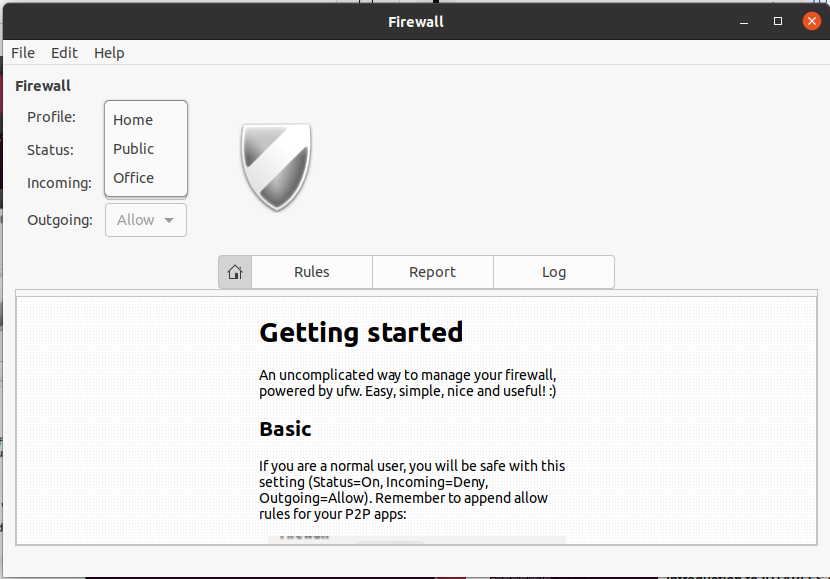
**Implementation:**

**Install gufw tool**

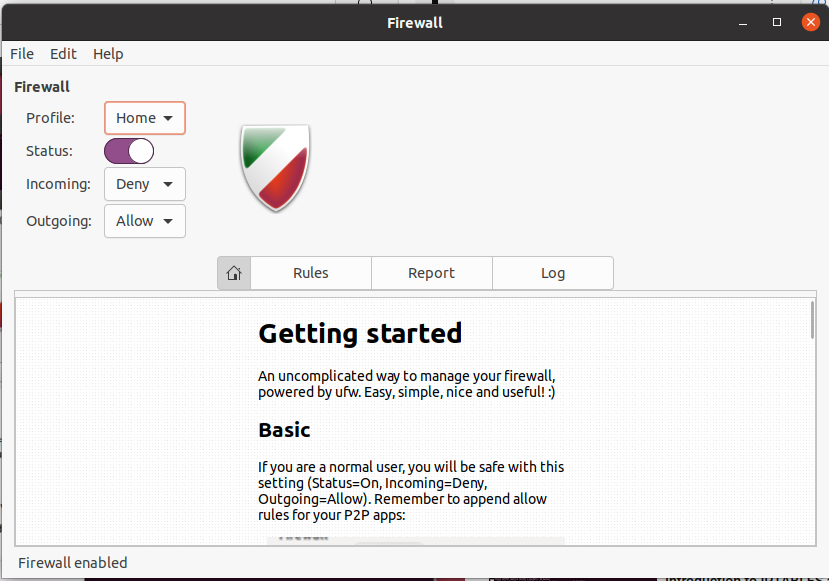
sudo apt-get install gufw



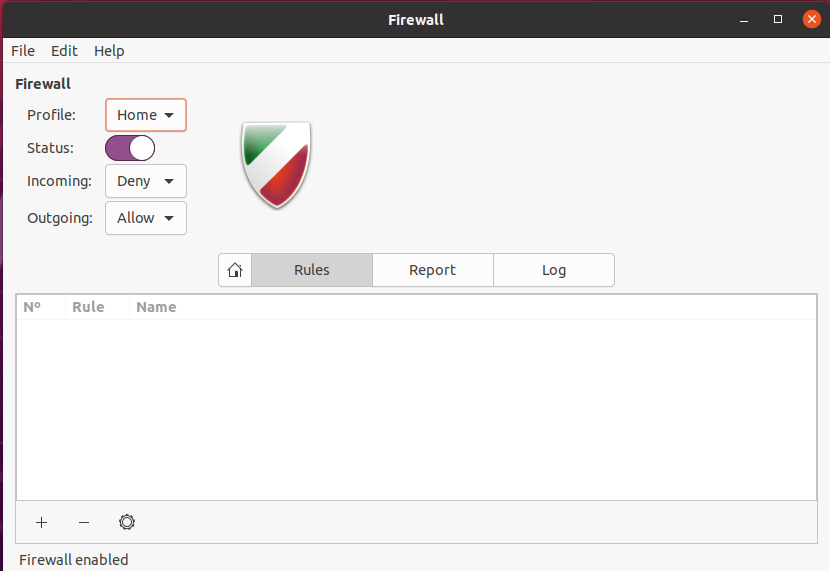
**UI for the gufw tool**



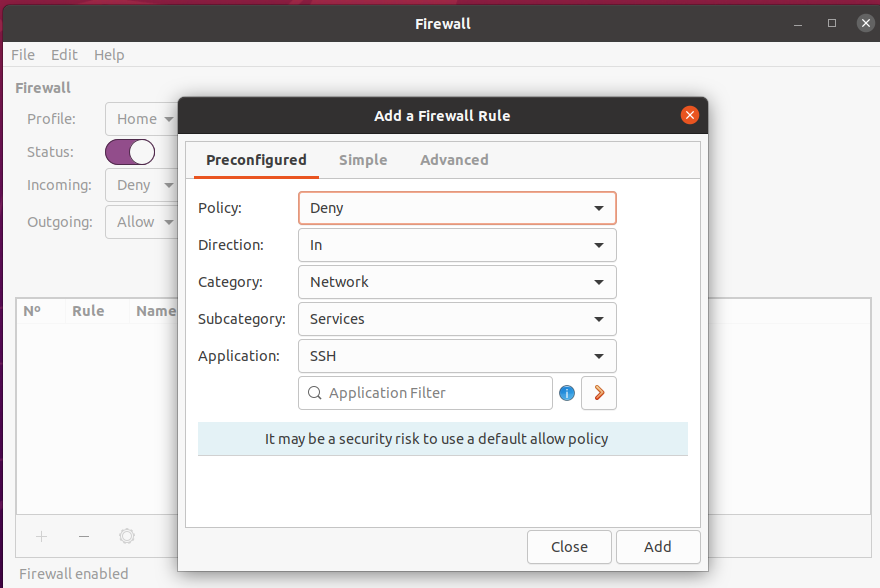
**Enable the firewall**



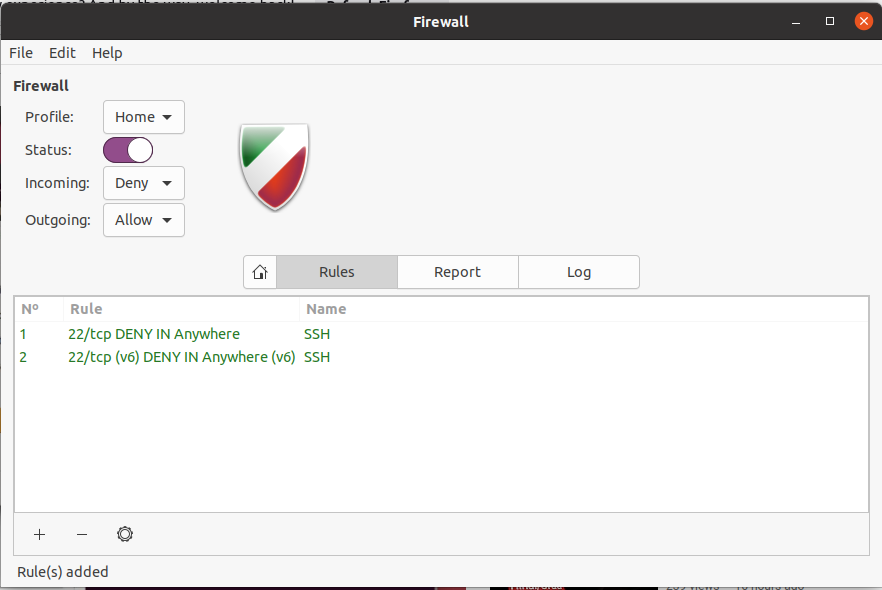
**Set the options as below and click on “+” under Rules tab to add firewall rules**



**Adding a Firewall rule to deny the SSH**

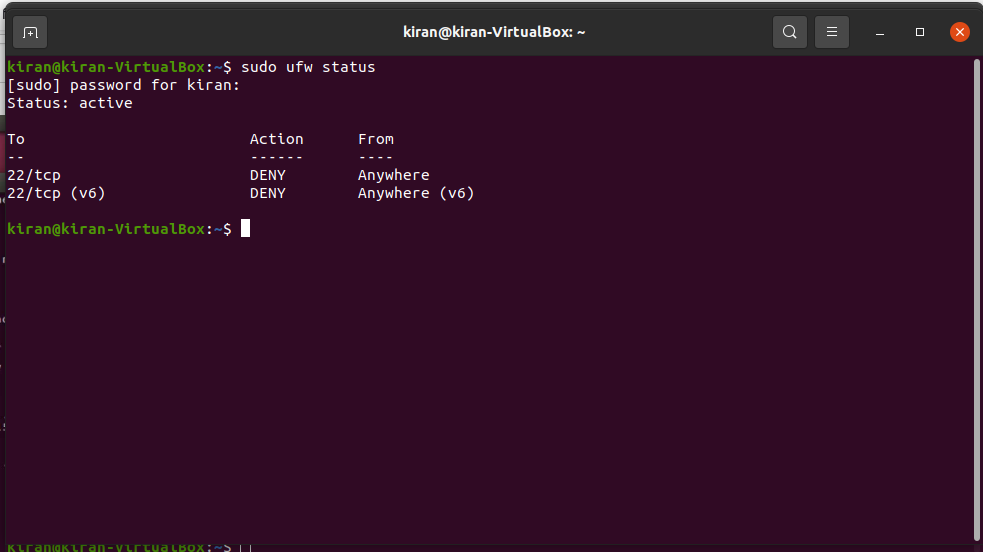


**The Rules are added**



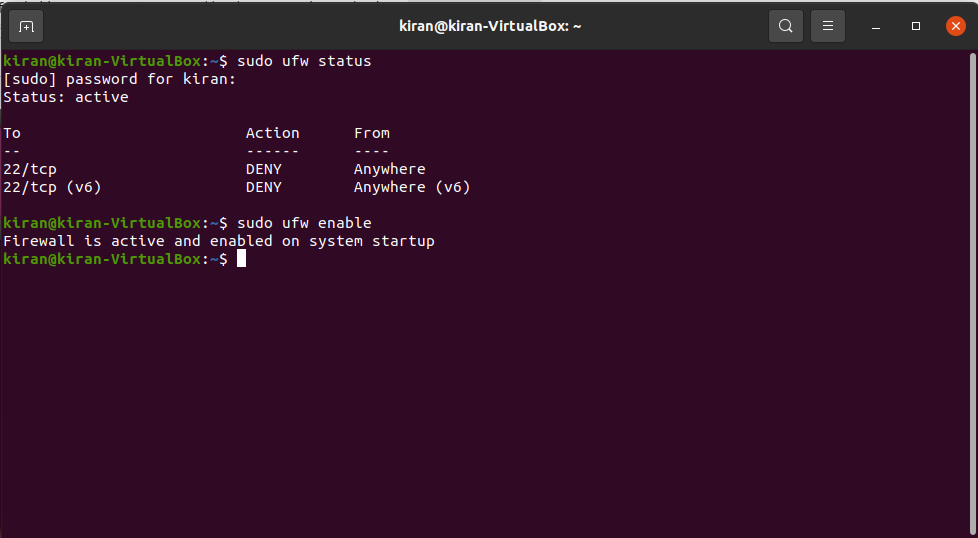
**Verify the the firewall rules from trminal**

Sudo ufw status

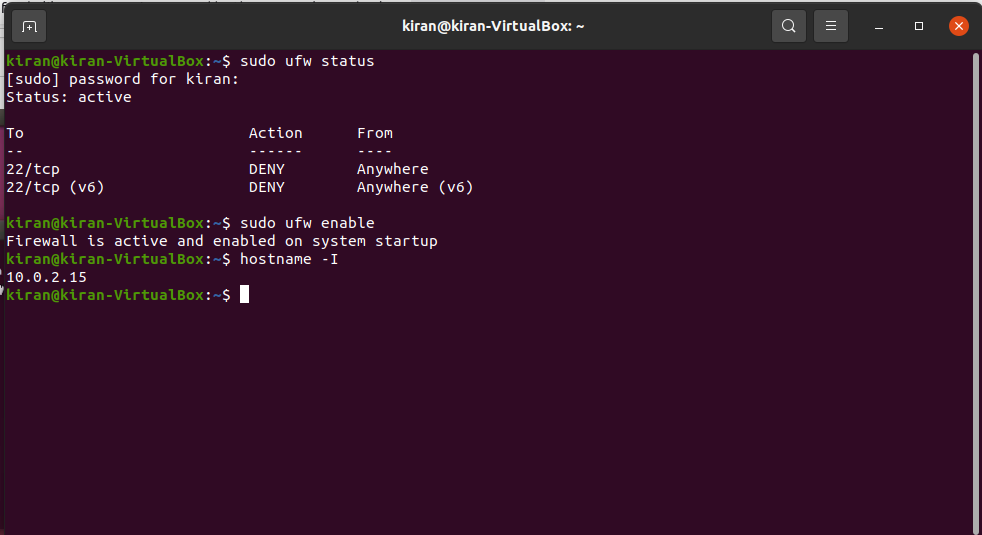


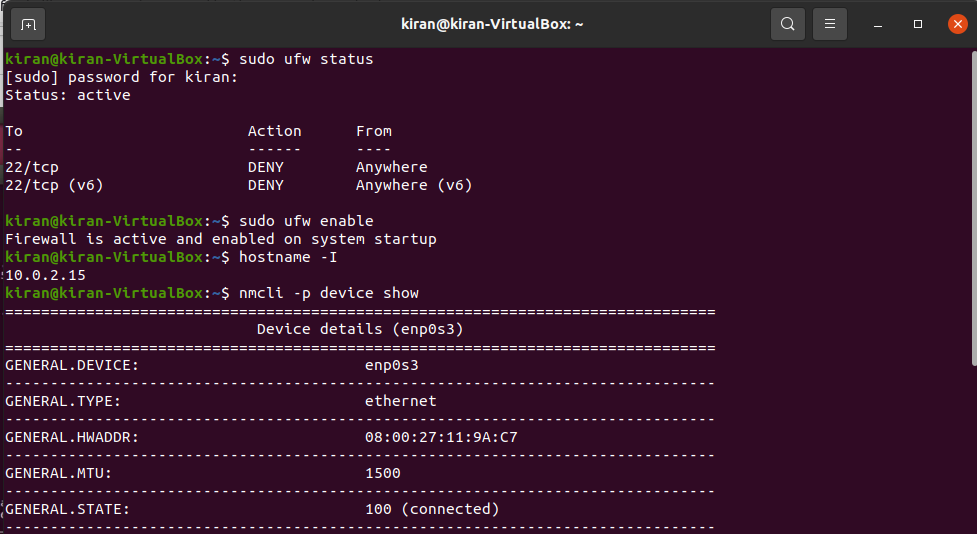
**Enable the firewall**

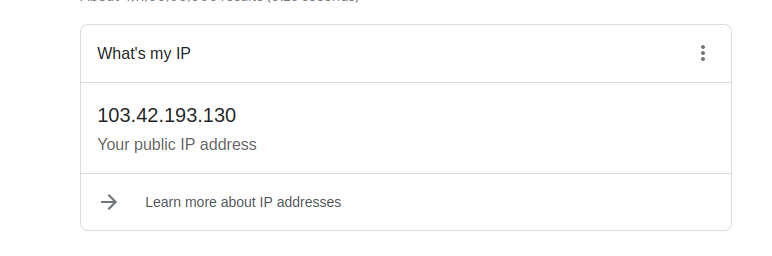
Sudo ufw enable



**Checking the IP address of the system to validate the firewall rules**



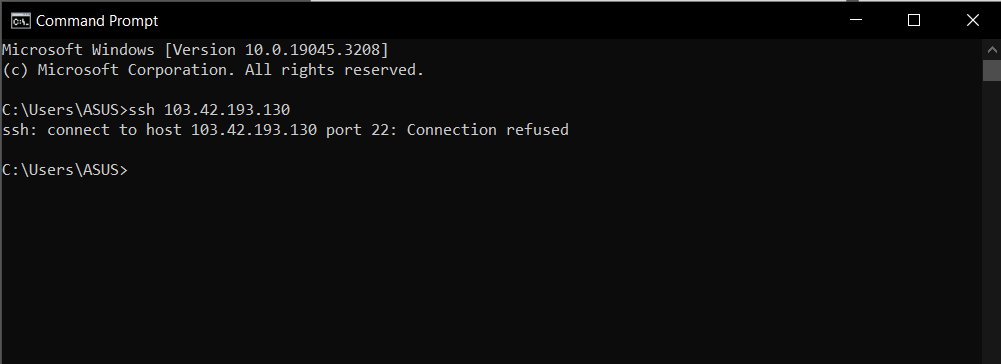




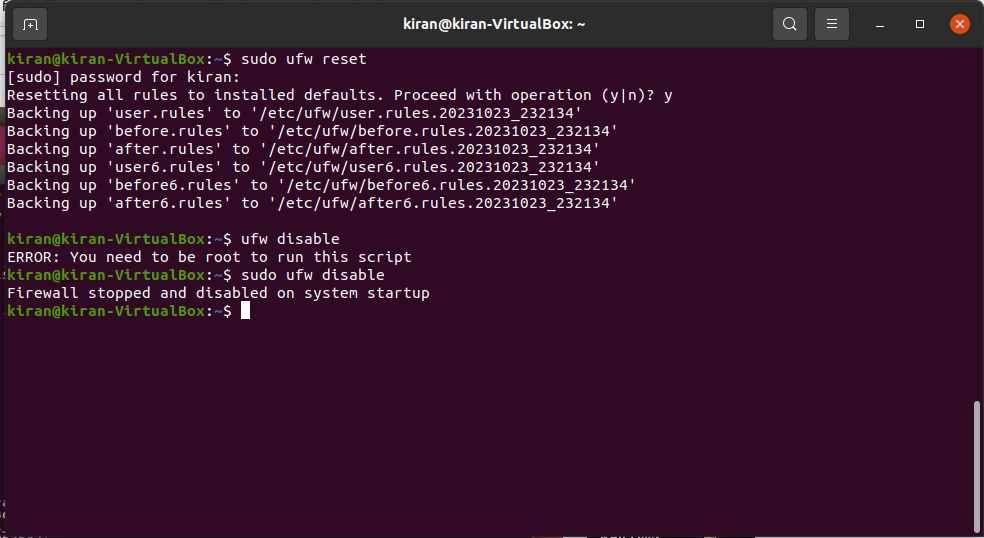
**Here 103.42.193.130 is my public Ip address**

**Verifying from other machine :**

SSH 103.42.193.130



**Reset The firewall rules and disabling it**



**Conclusion**:

In Conclusion, the practical experiment with the UFW (Uncomplicated Firewall) tool demonstrated its user-friendly and effective approach to network security and setting up the firewall While UFW offers straightforward firewall management, it's vital to remember that it should be integrated into a broader security strategy