**Project 1 : Built and Configure a Firewall**

**By Sumit**

**Building and configuring a firewall is crucial for protecting networks from unauthorized access and potential threats. This project helped me setting up and configuring a firewall on an Ubuntu system using UFW (Uncomplicated Firewall).**

**Objective: Successfully built and configured a firewall using UFW on Ubuntu to enhance network security.**

**Steps Involved:**

1. **System Update:**
   * **Updated the Ubuntu system to ensure all packages were current.**
   * **By using : Sudo apt Update**
   * **Sudo apt upgrade -y**
2. **UFW Installation:**
   * **Installed the Uncomplicated Firewall (UFW) for managing firewall rules.**
   * **By Using : sudo apt install ufw**
3. **UFW Enablement:**
   * **Enabled UFW to start managing incoming and outgoing traffic.**
   * **By using : sudo ufw enable**
4. **SSH Connections:**
   * **Configured UFW to allow secure SSH connections for remote access.**
   * **By Using : sudo ufw allow ssh**
   * **Sudo ufw allow 22/tcp (default is 22)**
5. **Service and Port Management:**
   * **Allowed specific services and ports to ensure necessary communication (e.g., HTTP, HTTPS).**

**Sudo ufw allow http**

**Sudo ufw allow https**

* + **Or by specifying the ports :**

**Sudo ufw allow 80/tcp**

**Sudo ufw allow 443/tcp**

* **Allowed a specific ports like :**

**Sudo ufw allow 8080/tcp**

* **Allowed a range of ports :**

**Sudo ufw allow 1000:2000/tcp**

* **Allowed Specific IP Address**

**Sudo ufw allow from 192.168.1.100**

* **Allowed specific Subnets**

**Sudo ufw allow from 192.168.1.0/24**

* + **Denied specific services and ports to block unwanted traffic and enhance security.**

**Sudo ufw deny 23/tcp**

* + **Deny a specific IP Address**

**Sudo ufw deny from 203.0.113.0**

1. **Status and Rules Monitoring:**
   * **Viewed UFW status and rules to verify correct configuration.**
   * **By using : sudo ufw status verbose**
2. **Rule Management:**
   * **Listed a rules with numbers :**

**By using : sudo ufw status numbered**

* + **Deleted obsolete or incorrect UFW rules to maintain a clean and efficient rule set.**

**Sudo ufw delete 2 (deleted using numbers)**

* + **Using rules specification :**

**Sudo ufw delete allow 8080/tcp**

1. **Advanced Configuration:**
   * **Performed advanced UFW configuration for more granular control over network traffic.**
   * **Enabled logging to monitor UFW Activity :**

**Sudo ufw logging on**

* + **Set default policies to deny all incoming and allow all outgoing traffic by using :**

**Sudo ufw default deny incoming**

**Sudo ufw default allow outgoing**

* + **Ufw includes profiles for some common applications , listed these profiles :**

**Sudo ufw app list**

* + **Allowing a specific application :**

**Sudo ufw allow ‘Nginx Full’**

1. **Testing:**
   * **Tested the firewall to ensure all rules were correctly applied and effective.**
   * **Checked open ports :**

**Used nmap from another machine to scan the open on your firewall- protected machine :**

**Nmap -v -A 192.168.1.10 # replace with the actual IP of your Firewall- protected machine**

**Skills Acquired:**

* **Network Security**
* **Linux Administration**
* **UFW Configuration**
* **Service and Port Management**
* **Troubleshooting and Testing**

**Tools:**

* **Ubuntu**
* **Uncomplicated Firewall (UFW)**

**Achieved a robust and secure firewall configuration, improving the overall security posture of the system.**