Experiment 10: Implementing Firewall Using Iptables

Bhuvi Ghosh
60009210191

Aim:
The objective of this experiment is to gain hands-on experience in implementing a firewall using iptables on a Linux-based system. Participants will learn how to configure iptables rules to control incoming and outgoing network traffic, enhance network security, and protect the system from unauthorized access.

Equipment/Requirements:
Linux-based system (e.g., Ubuntu, CentOS)
Access to the terminal or SSH for command-line interface
Basic understanding of networking concepts
Administrative privileges (sudo access)

Background:
Iptables is a powerful tool for configuring the Linux kernel firewall, which controls network traffic on a system. It can be used to set up rules to allow or block traffic based on various criteria such as source IP, destination IP, ports, and protocols.

Procedures:

Step 1: Verify iptables Installation
Ensure that iptables is installed on your system. If not, install it using the package manager appropriate for your Linux distribution (e.g., apt, yum).

```
sudo apt-get install iptables
```

Step 2: View Current iptables Rules

Check the current iptables rules on your system using the following command

```
sudo iptables -L
```

Step 3: Define Firewall Rules
Create and implement firewall rules based on your network security requirements.
For example:

# Allow incoming SSH (replace <your_ip> with your actual IP address)
sudo iptables -A INPUT -p tcp --dport 22 -s <your_ip> -j ACCEPT

# Allow incoming HTTP traffic
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

# Drop all other incoming traffic
sudo iptables -A INPUT -j DROP

Step 4: Save iptables Rules
Save the iptables rules to ensure they persist after a system reboot.

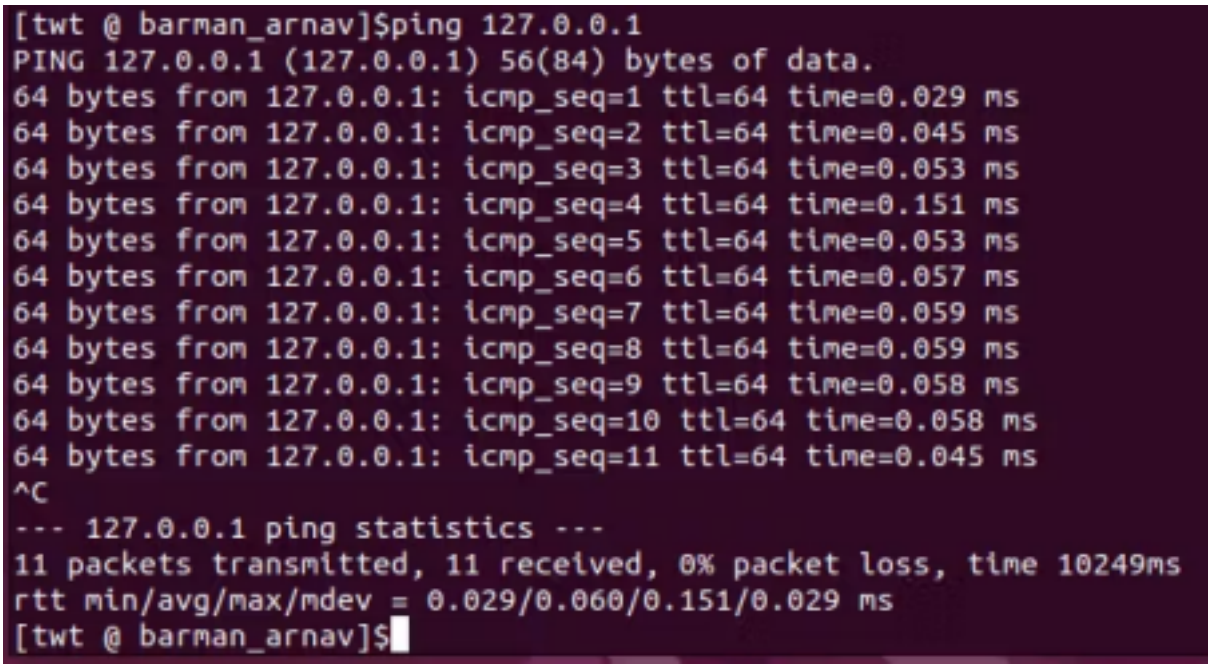
sudo service iptables save

Step 5: Test Firewall Rules
Test the firewall rules by attempting to access the system from a remote location. Ensure that allowed traffic is permitted, and blocked traffic is denied.

Step 6: Monitor Firewall Activity
Use the following command to monitor live firewall activity:

sudo iptables -L -v

Expected Outcomes:



Conclusion:

This experiment provides valuable hands-on experience in configuring and managing a firewall using iptables. Participants should now have a better understanding of how to enhance network security by controlling incoming and outgoing traffic on a Linux-based system.