**Project Report**

**Implementing a Firewall in Linux**

**-Vankadara Uma Gayathri**

**Motivation:**

The main motivation for selecting the Configure a firewell in linux project is familiarity with the technologies involved. Working on this project aims to improve skills and upgrade knowledge in these areas. Additionally, this project will facilitate professional growth and bring immediate value to the company by leveraging existing skills to deliver a high-quality product.

**Introduction:**

This project aims to implement a firewall on a Linux system using iptables to control incoming and outgoing network traffic. Iptables is a powerful tool for configuring firewall rules in Linux, allowing control over incoming, outgoing, and forwarded network traffic.

**What is Firewall?**

* A firewall is a security system designed to monitor and control incoming and outgoing network traffic. Its primary objective is to establish a barrier between a trusted internal network and untrusted external networks.
* Firewalls are fundamental to protecting networks from a wide range of cyber threats. They provide essential security controls at the network perimeter and within internal segments, helping organizations maintain the confidentiality, integrity, and availability of their critical data and systems. As cyber threats continue to evolve, firewalls remain a cornerstone of network security worldwide**.**

**Key Functions of a firewall include:**

* Packet Filtering: Examining packets of data and allowing or blocking them based on predetermined rules.
* Stateful Inspection: Tracking the state of active connections and only allowing packets that belong to established connections.
* Proxy Service: Acting as an intermediary for client requests, shielding the internal network by forwarding requests from clients and returning responses from servers.
* Network Address Translation (NAT): Modifying the source or destination IP addresses of packets to hide the internal network's structure.
* Virtual Private Network (VPN) Management: Facilitating secure remote access to the internal network through encrypted VPN connections**.**

**Types of Firewall in Linux:**

* **Netfilter:**

The core firewall framework in Linux, providing packet filtering and network address translation capabilities.

* **Iptables:**

The command-line utility for configuring and managing the Netfilter firewall, offering flexibility and fine-grained control.

* **Firewalld:**

A user-friendly firewall management tool that simplifies the configuration process with interfaces and services.

**Terminology:**

**IP Address:**

An IP address (Internet Protocol address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves as a unique identifier for that device within its network and allows other devices to locate and communicate with it.

**Types of IP Addresses:**

* **Public IP Address**: A public IP address is globally unique and routable on the Internet. It is assigned by an ISP (Internet Service Provider) or network administrator and allows devices to communicate across different networks worldwide.
* **Private IP Address**: A private IP address is used within a local network, such as a home or office network. It is not globally unique and cannot be routed on the Internet directly.

**Components of an IP Address:**

* **IPv4 Format**: IPv4 addresses are typically represented as four decimal numbers separated by periods. Each number, known as an octet, ranges from 0 to 255.
* **Example**: 192.168.1.1
* **IPv6 Format:** IPv6 addresses are longer and represented as eight groups of hexadecimal digits separated by colons. IPv6 was introduced to address the limitations of IPv4, primarily the exhaustion of available addresses due to the rapid growth of devices connecting to the Internet.
* **Example**: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

**LAN:**

LAN stands for Local Area Network. It refers to a network that connects computers and other devices within a limited geographical area such as a home, office building, school, or campus. LANs are typically owned, controlled, and managed by a single organization or individual.

**Uses and Applications:**

* **File Sharing** : LANs allow users to share files and resources easily within the same network.
* **Internet Access** : LANs provide shared access to the Internet through a single connection, typically managed by a router.
* **Communication** : LANs support communication applications such as email, instant messaging, and VoIP (Voice over IP) within the organization.
* **Collaboration** : LANs facilitate collaboration among users by enabling shared access to databases, applications, and collaborative tools.

**WAN :**

WAN stands for Wide Area Network. It is a type of computer network that covers a large geographical area, typically spanning across cities, countries, or continents. Unlike Local Area Networks (LANs), which are confined to a specific location like a home, office building, or campus, WANs connect multiple LANs and other types of networks together to enable communication and data exchange over long distances.

**Components of a WAN:**

* **Routers**: Routers are essential components in WANs that forward data packets between different networks. They use routing protocols to determine the best path for data transmission across the network based on factors like network conditions and destination addresses.
* **Modems and Multiplexers**: Modems and multiplexers are used to interface with different types of WAN connections, converting digital data signals into appropriate formats for transmission over the network.
* **Network Protocols**: WANs support multiple network protocols, such as TCP/IP (Transmission Control Protocol/Internet Protocol), which enable devices from different networks to communicate and exchange data effectively.

**Internet Traffic Type:**

Internet traffic types refer to the data flows that traverse the Internet. These traffic types are categorized based on their characteristics, protocols used, and the purposes they serve.

**Web Traffic (HTTP/HTTPS)**:

* **Description**: Web traffic comprises requests and responses exchanged between web browsers (clients) and web servers. It includes accessing websites, downloading web pages, images, videos, and other resources.
* **Protocols**: HTTP (Hypertext Transfer Protocol) and its secure version HTTPS (HTTP Secure) are used for transmitting web traffic securely over the Internet.

**File Transfer Traffic (FTP/SFTP)**:

* **Description**: File transfer traffic involves transferring files between clients and servers over the Internet. It includes uploading, downloading, and managing files stored on remote servers.
* **Protocols**: FTP (File Transfer Protocol) and its secure counterpart SFTP (SSH File Transfer Protocol) are commonly used protocols for file transfer.

**IP Header:**

The IP header (Internet Protocol header) is a fundamental component of the IP (Internet Protocol) suite, which is responsible for routing data packets across networks. It is added to the beginning of each IP packet and contains crucial information that routers and other network devices use to properly forward the packet to its destination.

**TCP Header:**

The TCP header (Transmission Control Protocol header) is a critical part of the TCP/IP defining how data is structured and transmitted across networks using the TCP protocol. TCP is a connection-oriented protocol that provides reliable, ordered, and error-checked delivery of data between applications running on hosts on a network.

* **Source Port (16 bits)**: Specifies the source port number used by the sending application to establish communication. It identifies the sender's application process on the local host.
* **Destination Port (16 bits)**: Specifies the destination port number used by the receiving application to identify the intended recipient. It identifies the application process on the remote host.

**Objectives:**

* To secure the Linux system by restricting unauthorized access.
* To allow only necessary network services (e.g., YouTube) .
* To understand and apply basic firewall concepts using iptables.

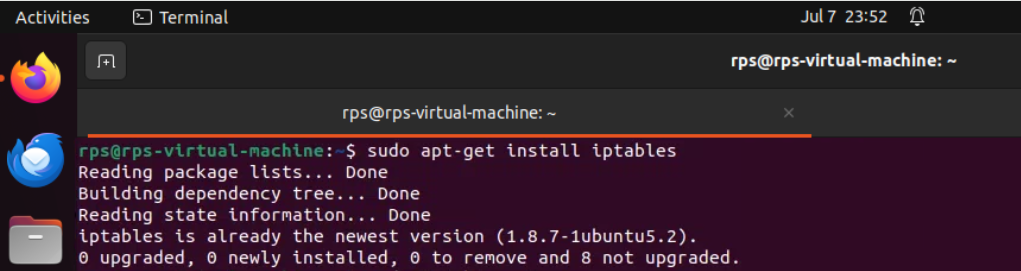
**Methodology:**

**Tools and Technologies:**

* **Linux Operating System:** Ubuntu
* **Firewall Software:** iptables

**Implementation Steps:**

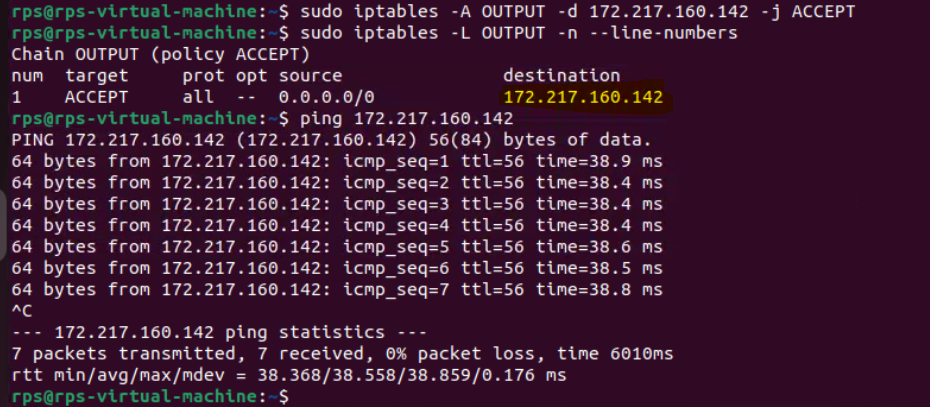
1. **Installation of iptables:**
   * Installed iptables using apt-get if not already present.

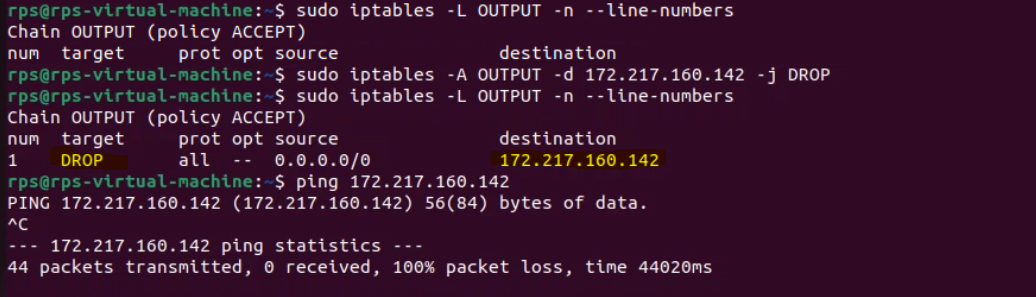


1. **Configuration of Firewall Rules:**
   * Defined default policies for INPUT, FORWARD, and OUTPUT chains.
   * Created specific rules to allow necessary services (e.g., YOUTUBE) and protocols.
   * Tested and adjusted rules to ensure they met security and operational requirements.



1. **Testing and Validation:**
   * Conducted thorough testing to verify that desired traffic was allowed
   * Utilized logging (-j LOG) to monitor and troubleshoot denied packets.
   * Ensured the firewall configuration did not disrupt essential network services.

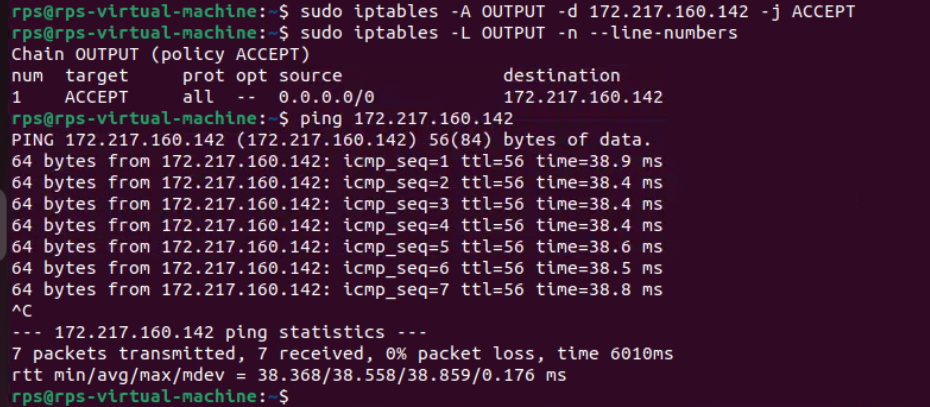




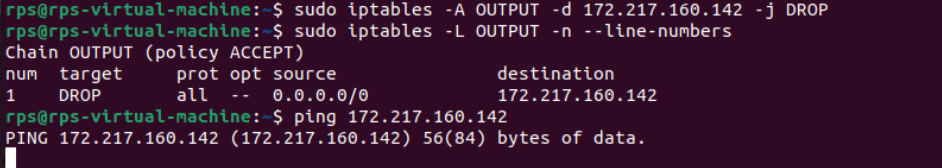
**Results and Discussion:**

**Firewall Configuration:**

* Implemented iptables rules to:
  + Allow specific services (e.g., YouTube).
* Allowing YouTube IP and checking the line numbers.



* Restricting YouTube IP



**Testing and Validation:**

* Successfully restricted incoming traffic to only necessary services.
* Validated that outgoing traffic was unrestricted as per policy.

**Conclusion:**

**Achievements**

* Implemented an effective firewall using iptables to enhance system security.
* Gained practical experience in configuring and managing network security policies on Linux.