



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Course Name:** | | **Information Security (116U01L602)** | **Semester:** | **VI** | |
| **Date of**  **Performance:** | | **16 / 04 / 2025** | **DIV/ Batch No:** | **A-3** | |
| **Student Name:** | | **Kashish Mamania** | **Roll No:** | **16010122104** | |
|  | | | | | |
|  | **Title: Implementation and configuration of Firewall using Iptable / Fortinet / Palo Alto.** | | | |  |

* To understand the concept of a firewall and its importance in network security.
* To implement and configure a basic firewall using iptables in Linux.
* To explore different options and rule specifications in iptables.

**Objectives:**

* Students will be able to configure and manage firewall rules using iptables.
* Students will understand how to secure a system by controlling network traffic.
* Students will gain hands-on experience with various iptables commands and concepts.

**Expected Outcome of Experiment:**

* https://linux.die.net/man/8/iptables
* [https://www.netfilter.org](https://www.netfilter.org/)
* Official Ubuntu and CentOS documentation on iptables

**Books/ Journals/ Websites referred:**

* Basics of Linux command-line usage.
* TCP/IP networking fundamentals.
* Understanding of ports, protocols, and IP addressing.

**Pre Lab/ Prior Concepts:**

* Host-based and router-based firewalls.
* Use of iptables for packet filtering and network traffic control.
* Chain policies (INPUT, OUTPUT, FORWARD).

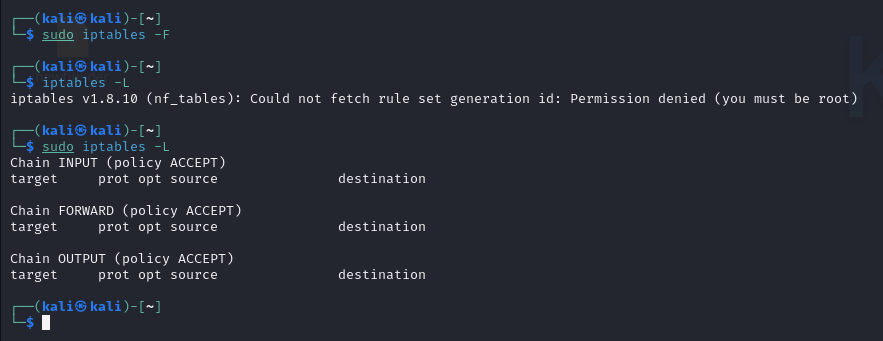
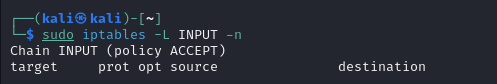
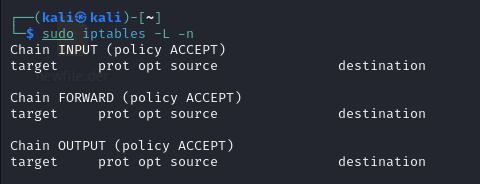
**New Concepts to be learned:**

|  |
| --- |
| **Abstract:** |
| This experiment focuses on understanding the concept, types, and working of firewalls, along with hands-on implementation using iptables in a Linux environment. Firewalls are essential network security components that monitor, filter, and control traffic based on defined security rules. The objective of the experiment is to explore both host-based and router-based firewalls and configure various rule sets to manage traffic flowing into, out of, or through a system.  Using the iptables tool, students learn to list active rules, add and delete specific rules, flush rule sets, and print chain-specific policies. The experiment covers rule specifications such as allowing loopback traffic, accepting established connections, dropping invalid packets, blocking specific IP addresses, and enabling or restricting access to services like HTTP, SSH, and SSL. Additionally, the concept of Stateful Packet Inspection (SPI) is introduced, where the firewall maintains a table of active connections and filters packets based on their connection state.  Through this practical exercise, students gain foundational knowledge in firewall configuration, network traffic control, and basic intrusion prevention techniques using Linux-based tools. |

|  |  |  |
| --- | --- | --- |
|  | **Related Theory:** |  |
| A **firewall** is a critical component in network security that helps in monitoring and filtering incoming and outgoing traffic based on an organization’s or system administrator’s pre-configured rules. It serves as a protective barrier between a trusted internal network and untrusted external sources, such as the internet. Firewalls are used to prevent unauthorized access, detect suspicious traffic, and enforce security policies across systems and networks. |
|  | **Types of Firewalls:**   1. **Host-Based Firewall**:   These are firewalls installed directly on individual devices (hosts), such as laptops or servers. They monitor and control traffic specific to that system. An example is iptables on a Linux machine or Windows Defender Firewall on a Windows system.   1. **Router-Based Firewall (or Network Firewall)**:   Deployed at the network perimeter, typically on routers or dedicated firewall appliances. These firewalls filter traffic between different networks (e.g., LAN and Internet). They are usually the first line of defense in enterprise environments. |  |

|  |  |  |
| --- | --- | --- |
|  | **How Firewalls Work:**  Firewalls operate using a set of **rules** that define what kind of traffic is permitted or denied. These rules evaluate various parameters of packets such as:   * Source and destination IP addresses * Port numbers * Protocols (TCP, UDP, ICMP) * Connection states (NEW, ESTABLISHED, RELATED, INVALID)   When a packet arrives, the firewall examines it according to the defined rules and takes appropriate action — typically to **ACCEPT**, **DROP**, or **REJECT** the packet.   * ACCEPT: Allows the packet through. * DROP: Silently discards the packet with no feedback to the sender. * REJECT: Discards the packet and sends an error ressponse to the sender. |  |
|  | * **iptables in Linux:**   iptables is a user-space command-line tool used to configure the Linux kernel firewall (Netfilter). It allows administrators to define rules within tables that process packets through **chains**. The most common chains are:   * + **INPUT**: Handles packets destined for the host system.   + **OUTPUT**: Handles packets originating from the host.   + **FORWARD**: Handles packets being routed through the system (not destined to or from the host).   Each rule in a chain matches specific traffic and defines what action to take on that traffic. Rules are evaluated in order from top to bottom, and the first match determines the outcome. |  |

|  |
| --- |
| **Implementation Details:** |
|  |



|  |
| --- |
| **Post Lab Questions:** |
| 7.1 What is the difference between stateful and stateless firewalls?  Ans:   | **Feature** | **Stateless Firewall** | **Stateful Firewall** | | --- | --- | --- | | Packet Context | None | Maintains connection state | | Filtering Criteria | Individual packet fields | Packet fields + connection history | | Security Level | Basic | Higher, context-aware | | Performance | Fast, simple | More resource-intensive | | Example | iptables (basic rules) | Fortinet, Palo Alto, iptables with connection tracking |   7.2 How does a firewall protect data?  Ans:  A firewall acts as a barrier between trusted and untrusted networks, filtering all traffic based on a defined security policy. It enforces rules that determine which traffic is allowed or denied, thus:   * **Blocking Unauthorized Access:** Only permitted traffic is allowed to enter or leave the protected network, reducing the risk of intrusion. * **Segmentation:** Firewalls can separate network zones (e.g., DMZ, internal network), limiting the spread of attacks. * **Enforcing Security Policies:** By specifying allowed protocols, ports, and IP addresses, firewalls reduce the attack surface. * **Concealing Internal Network Structure:** Techniques like Network Address Translation (NAT) hide internal IP addresses from external entities, making targeted attacks more difficult1. * **Logging and Monitoring:** Firewalls provide logs for security monitoring and incident response.   However, firewalls primarily protect data in transit by controlling access to network resources; they do not encrypt data or protect data at rest.  7.3 What can't a firewall protect against?  Ans:  Firewalls have important limitations:   * **Attacks Bypassing the Perimeter:** If an attacker gains physical access or uses a modem, VPN, or infected device inside the network, the firewall is bypassed. * **Malicious Content in Allowed Traffic:** Firewalls cannot detect malware hidden in permitted traffic (e.g., a virus in an allowed email or web download). * **Application-layer Attacks:** Basic firewalls may not inspect application data, so attacks like SQL injection or XSS can pass through unless advanced filtering/proxying is used. * **Insider Threats:** Firewalls do not protect against malicious or careless insiders who have legitimate access. * **Encrypted Traffic:** Unless configured for deep packet inspection, firewalls cannot inspect the contents of encrypted traffic. * **Misconfiguration:** An incorrectly configured firewall may allow unauthorized access or block legitimate traffic, reducing its effectiveness.   7.4 How is a firewall different from an IDS and an IPS? Explain.  Ans:   | **Feature** | **Firewall** | **IDS (Intrusion Detection System)** | **IPS (Intrusion Prevention System)** | | --- | --- | --- | --- | | Primary Function | Filters traffic based on rules | Monitors and alerts on suspicious activity | Detects and blocks suspicious activity | | Placement | Network perimeter or host | Network or host (passive) | Network or host (inline/active) | | Action | Allows/blocks traffic | Alerts/logs events | Alerts and actively blocks/throttles | | Response | Preventive (policy enforcement) | Detective (no direct blocking) | Preventive (can block/mitigate threats) | | Example | iptables, Fortinet, Palo Alto | Snort, OSSEC | Snort (in IPS mode), Suricata | |

|  |
| --- |
| **Conclusion:** |
| This experiment helped me develop a clear understanding of firewalls and their critical role in protecting systems and networks from unauthorized access. I explored the core functionality of firewalls and learned how they act as a filter between internal and external traffic, enforcing security policies by allowing or blocking packets based on defined rules. The distinction between host-based and router-based firewalls became clear through theoretical study and practical application. |