| **Course Name:** | **Information Security (116U01L602)** | **Semester:** | **VI** |
| --- | --- | --- | --- |
| **Date of Performance:** | **20/03/2025** | **DIV/ Batch No:** | **C – 3** |
| **Student Name:** | **Romil Lodaya** | **Roll No:** | **16010122096** |

| **Title: Implementation and configuration of Firewall using Iptable.**  **Demo of Palo Alto Next Gen Firewall** |
| --- |

| **Objectives:** |
| --- |
| * **To understand and implement firewall configuration using iptables in a Linux environment**: This will help in gaining practical knowledge of basic firewall functionalities and their configuration. * **To explore and demonstrate the capabilities of Palo Alto Next Generation Firewalls (NGFW)**: This aims at showcasing the advanced features of modern NGFWs, including traffic monitoring, VPN setup, and intrusion prevention. * **To compare network security mechanisms used by traditional firewalls (like iptables) and next-gen firewalls (like Palo Alto)**: This objective aims at identifying the strengths and weaknesses of both approaches. |

| **Expected Outcome of Experiment:** |
| --- |
| **CO4:** Illustrate and Compare network security mechanisms |

| **Books/ Journals/ Websites referred:** |
| --- |
| * <https://www.geeksforgeeks.org/iptables-command-in-linux-with-examples/> * <https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands> * <https://www.youtube.com/watch?app=desktop&v=vbhr4csDeI4&t=326s> * <https://www.youtube.com/watch?v=H1WPwAjMXRo> * <https://www.youtube.com/watch?v=eC8scXX1_1M> |

| **Pre Lab/ Prior Concepts:** |
| --- |
| * **Basic Networking Concepts**: Understanding of TCP/IP, IP addressing, DNS, and HTTP/HTTPS protocols. * **Firewall Fundamentals**: Knowledge of what firewalls are, their types (stateful vs stateless), and their role in network security. * **Linux Command Line Basics**: Familiarity with Linux commands and the terminal, especially for iptables commands. * **Basic Security Protocols**: Awareness of protocols like VPN, IPSec, SSL/TLS, and their relevance in network security. |

| **New Concepts to be learned:** |
| --- |
| * **iptables Configuration**: Learning the syntax and rules of iptables to create filtering and NAT (Network Address Translation) rules for traffic management. * **Palo Alto Next Gen Firewall**: Gaining hands-on experience with Palo Alto firewalls and understanding their advanced features such as traffic analysis, intrusion prevention, SSL decryption, and user-based security policies. * **Comparison of Network Security Mechanisms**: Exploring the differences between traditional firewalls like iptables (which is more focused on packet filtering) and next-gen firewalls (which provide deeper inspection, visibility, and control of network traffic). |

| **Abstract:** |
| --- |
| This experiment focuses on the implementation and configuration of firewalls using iptables on a Linux system, as well as exploring the features and functionality of Palo Alto’s Next Generation Firewalls (NGFW). The experiment begins with the basic configuration of iptables for managing inbound and outbound traffic, setting rules for filtering, and monitoring network activity. The second part of the experiment introduces Palo Alto NGFWs, demonstrating how they go beyond simple traffic filtering to provide deeper traffic inspection, VPN management, and intrusion detection/prevention. The final aspect of the experiment involves a comparison between traditional firewalls like iptables and NGFWs in terms of security mechanisms, highlighting the improvements made in the realm of network security with the advent of NGFW technologies. |

| **Related Theory:** |
| --- |
|  **Firewall Types**:   * **Packet Filtering Firewalls**: The most basic type of firewall that inspects packets in isolation and allows or blocks them based on predefined rules. * **Stateful Inspection Firewalls**: These firewalls track the state of active connections and make decisions based on the context of the traffic, not just individual packets. * **Next-Generation Firewalls (NGFW)**: These firewalls offer features such as integrated intrusion prevention systems (IPS), application awareness, and deep packet inspection (DPI) to identify and block advanced threats.    **Iptables Basics**:   * iptables is a user-space utility program that allows a system administrator to configure the Linux kernel firewall (netfilter). It provides filtering rules for traffic to and from the system, allowing administrators to create a customized set of rules to secure their network. * **Chains in iptables**: The built-in chains are INPUT, OUTPUT, and FORWARD, with each handling different types of traffic. * **Types of Rules**: Rules can be based on IP addresses, protocols, ports, and connection states (e.g., new, established).    **Palo Alto Next Gen Firewall Features**:   * **Application Awareness**: Allows for identification of applications (not just ports) to better control traffic. * **Deep Packet Inspection (DPI)**: Inspects the payload of network packets to detect malware, unauthorized applications, and threats. * **SSL Decryption**: Intercepts SSL traffic to inspect encrypted communications for threats. * **Intrusion Prevention System (IPS)**: Monitors network traffic for signs of malicious activity or known attack patterns.    **Comparison of Firewalls**:   * **Performance**: Traditional firewalls like iptables focus mainly on packet-level filtering, whereas NGFWs inspect deeper layers of network traffic, which can increase processing demands but provide stronger protection against sophisticated attacks. * **Ease of Configuration**: iptables configuration is command-line based and requires precise syntax, while NGFWs typically offer more user-friendly GUI-based interfaces for configuring complex rules. * **Security Features**: NGFWs provide advanced threat detection, including botnet detection, zero-day protection, and malware inspection, which are not natively available in traditional firewalls like iptables. |

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

| **Post Lab Questions:** |
| --- |
| Q1] What is the difference between stateful and stateless firewalls?  **Stateful Firewall:**   * Monitors the **state of active connections** and makes decisions based on connection state, traffic patterns, and context. * Keeps a record of ongoing connections and dynamically allows or blocks traffic. * More secure as it detects malicious patterns over multiple packets. * Examples: Cisco ASA, Check Point, and pfSense.   **Stateless Firewall:**   * Evaluates traffic **packet by packet** without considering the state of the connection. * Only uses pre-defined rules for allowing or denying traffic. * Less resource-intensive but easier for attackers to bypass. * Examples: iptables (basic configurations), Access Control Lists (ACLs).   Q2] How does a firewall protect data?  **Traffic Filtering:** Blocks unauthorized access by allowing or denying packets based on defined rules.  **Port and Protocol Control:** Limits traffic to only approved ports and protocols, reducing exposure.  **Packet Inspection:** Examines incoming and outgoing packets for anomalies or malicious behavior.  **Preventing Unauthorized Access:** Restricts access to sensitive data by controlling traffic between trusted and untrusted networks.  Q3] What can't a firewall protect against?  **Internal Threats:** Insider attacks or compromised internal devices.  **Phishing and Social Engineering:** Firewalls cannot prevent users from clicking malicious links or sharing sensitive data.  **Zero-Day Exploits:** New vulnerabilities not yet identified may bypass firewall rules.  **Encrypted Traffic Attacks:** Malicious data inside encrypted packets may pass undetected if the firewall cannot inspect encrypted traffic.  Q4] How is a firewall different from an IDS and an IPS? Explain.  **Firewall:**   * Controls traffic between networks based on rules. * Prevents unauthorized access and filters traffic.   **IDS (Intrusion Detection System):**   * **Monitors traffic** for suspicious activities and generates alerts. * **Passive system**—does not take action, only notifies.   **IPS (Intrusion Prevention System):**   * Monitors traffic like IDS but also **actively blocks** suspicious activity. * **Proactive system** that prevents attacks in real-time. |

| **Conclusion:** |
| --- |
| Iptables secures Linux systems through rule-based traffic control, while Palo Alto Next-Gen Firewall offers advanced threat prevention capabilities. |