Firewall Configuration & Testing Report

Cyber Security Internship – Task 10

Firewall Tool: UFW (Uncomplicated Firewall)

Operating System: Linux (Kali / Ubuntu)

Author: Mohammed Nihal

Abstract

This report documents the configuration and testing of a host-based firewall using UFW. The objective of this task is to understand firewall concepts, configure inbound and outbound rules, test connectivity, observe firewall logs, and analyze the impact of firewall rules on system security. All activities were conducted in a controlled lab environment for educational purposes.

1. Introduction

Firewalls are a critical component of network and system security. They act as a barrier between trusted and untrusted networks by filtering traffic based on predefined rules. Host-based firewalls such as UFW help protect individual systems by controlling incoming and outgoing network connections. This task focuses on practical firewall configuration and testing.

2. Firewall Concepts

A firewall enforces security policies by allowing or denying traffic based on parameters such as IP address, port number, protocol, and direction. Firewalls can be stateful, which track the state of active connections, or stateless, which inspect packets independently. UFW operates as a stateful firewall by default, providing enhanced security.

3. Configuration Environment

The firewall configuration was performed on a Linux-based system using UFW. The system was configured in a lab environment to ensure that no production systems were affected. Default firewall policies were reviewed prior to applying custom rules.

4. Firewall Setup and Rule Configuration

Initially, the firewall status was checked to confirm whether UFW was active. The firewall was then enabled with default policies that deny incoming traffic and allow outgoing traffic. Specific rules were added to allow necessary services such as SSH and to block unused or insecure ports.

5. Allowing and Denying Traffic

Firewall rules were configured to allow inbound SSH traffic on port 22 to ensure remote administration access. Inbound traffic on port 80 was explicitly denied to demonstrate how firewalls reduce the attack surface by blocking unnecessary services.

6. Firewall Testing and Verification

After configuring firewall rules, network connectivity was tested using Nmap. The scan results confirmed that allowed ports were accessible while denied ports were blocked. This verified that the firewall rules were functioning as intended.

7. Firewall Logging and Monitoring

Firewall logging was enabled to monitor blocked and allowed traffic. Logs were reviewed to observe how UFW records connection attempts and rule enforcement. Log monitoring is essential for detecting suspicious or unauthorized network activity.

8. Blocking Malicious IP Addresses

A sample IP address was blocked using UFW to simulate mitigation of malicious traffic. Blocking known malicious IPs helps prevent repeated unauthorized access attempts and enhances system security.

9. Impact and Security Benefits

Proper firewall configuration significantly improves system security by minimizing exposed services and controlling network access. While firewalls cannot prevent all attacks, they form a crucial first line of defense in a layered security strategy.

10. Conclusion

This task provided hands-on experience with firewall configuration and testing using UFW. Understanding how to manage firewall rules, test connectivity, and analyze logs is essential for maintaining secure systems. Firewall management is a fundamental skill for cyber security professionals.