Task 4 – Firewall Setup and Configuration (Windows & Kali Linux)

Overview

This report documents Task 4 of the Cyber Security Internship, which focuses on configuring and testing firewall rules on both Windows and Kali Linux systems. The task demonstrates practical understanding of host-based firewalls and network traffic filtering.

Objective

- Configure firewall rules on Windows and Kali Linux
- Block insecure services using port-based filtering
- Test and verify firewall behavior
- Understand the role of firewalls in system security

Tools and Environment

Windows: Windows Defender Firewall with Advanced Security
Kali Linux: UFW (Uncomplicated Firewall)

Task Description

In this task, Telnet traffic on port 23 was blocked on both Windows and Kali Linux systems. Telnet is an insecure protocol that transmits data in plain text. Blocking this port reduces security risks and prevents unauthorized access.

Implementation – Windows Firewall

An inbound firewall rule was created to block TCP traffic on port 23. The rule was applied to all network profiles and tested using the Telnet client. The failed connection confirmed that the rule was successfully enforced.

Implementation – Kali Linux (UFW)

UFW was enabled on Kali Linux, and a deny rule was added for port 23. SSH access on port 22 was allowed to maintain secure remote access. The rule was verified using Telnet, which failed as expected.

Testing and Verification

On both operating systems, connection attempts to localhost on port 23 failed after applying the firewall rules. This confirms that the firewall configurations effectively blocked Telnet traffic.

Outcome

The task was completed successfully on both Windows and Kali Linux. Firewall rules were configured, tested, and validated, providing hands-on experience in firewall management and network security.

Conclusion

This task demonstrated practical firewall configuration across multiple platforms. Blocking Telnet traffic and validating the results highlighted the importance of firewalls in protecting systems from insecure services.