Cyber Security Internship – Task 10: Firewall Configuration & Testing

Objective

The objective of this task is to configure, test, and document firewall rules to regulate inbound and outbound traffic, ensuring secure access to services.

Tools & Environment

Firewall Tool: UFW (Uncomplicated Firewall) Operating System: Linux Firewall rules were implemented on a test system to simulate real-world security scenarios.

Firewall Concepts

A firewall acts as a security barrier between trusted and untrusted networks. It filters traffic based on defined rules to prevent unauthorized access.

Configuration Steps

Firewall was enabled and configured to allow essential services such as SSH and HTTP. Unused and insecure ports like FTP were blocked. A simulated malicious IP address was also denied.

Testing & Validation

Firewall effectiveness was tested using connectivity checks. Allowed services were accessible, while blocked ports and IPs were denied, confirming correct rule implementation.

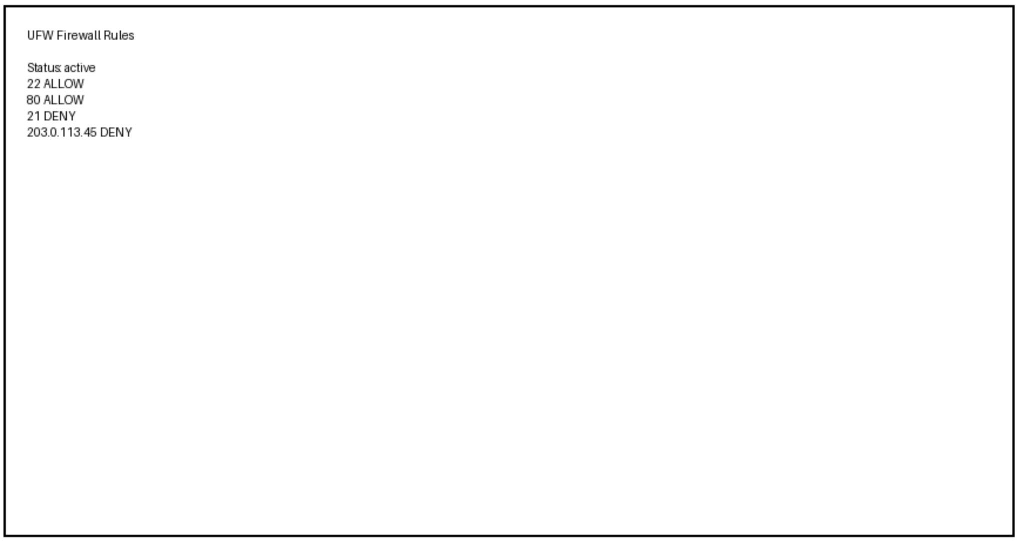
Impact & Security Benefits

Proper firewall configuration significantly reduces attack surface, prevents unauthorized access, and enhances system resilience.

Conclusion

Firewall management is a critical defensive security skill. Correctly implemented rules ensure operational continuity while maintaining security.

Screenshots / Evidence



```
UFW Firewall Rules

Status: active
22 ALLOW
80 ALLOW
21 DENY
203.0.113.45 DENY
```