Internship Report - Task 4

Objective

The objective of this task was to configure and test basic firewall rules on a Linux system using UFW (Uncomplicated Firewall). The task involved enabling the firewall, applying rules to allow or block specific ports, verifying functionality, and restoring the system to its original state.

Tools

- Operating System: Kali Linux
- Firewall Utility: UFW (Uncomplicated Firewall)
- Testing Utility: Telnet

Procedure

Step 1: Checking Firewall Status

The current firewall status was checked with the command:

sudo ufw status verbose

The firewall was initially inactive. It was then enabled using:

sudo ufw enable

Step 2: Listing Current Rules

Existing firewall rules were listed with:

sudo ufw status numbered

No custom rules were present at this stage.

Step 3: Blocking Telnet (Port 23)

A rule was added to block inbound Telnet traffic:
sudo ufw deny 23

This was verified by running:
sudo ufw status numbered

Step 4: Testing the Rule

The block was tested by attempting a connection on port 23 using Telnet:
telnet localhost 23

The connection was denied, confirming that the rule was effective.

Step 5: Allowing SSH (Port 22)

To ensure secure remote access, SSH traffic was explicitly allowed:
sudo ufw allow 22

Step 6: Removing the Test Rule

The Telnet block rule was removed to restore the firewall configuration to its original state.
The rule number was first identified with:
sudo ufw status numbered

It was then deleted with:
sudo ufw delete <rule_number>

Firewall Configuration Snapshot

During testing, the firewall rules were displayed as follows:

Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From

22/tcp ALLOW Anywhere
23 DENY Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
23 (v6) DENY Anywhere (v6)

Explanation of the configuration:

- The firewall was active with logging enabled.
- Default policies denied all incoming traffic and allowed all outgoing traffic.

- Port 22 (SSH) was allowed for both IPv4 and IPv6.
- Port 23 (Telnet) was explicitly denied for both IPv4 and IPv6.

Results

- The firewall was successfully enabled and configured.
- Rules to allow and deny traffic were applied and verified through testing.
- Telnet (port 23) was successfully blocked, while SSH (port 22) remained accessible.
- The test rule was removed, restoring the firewall to a clean state.

Summary of Firewall Functionality

A firewall filters network traffic by applying predefined rules to incoming and outgoing connections. In this case, UFW provided a simplified interface to manage firewall rules without requiring direct interaction with complex iptables syntax. Blocking Telnet demonstrated how insecure services can be denied, while allowing SSH showed how essential services remain available.

Interview-Style Questions & Answers

1. What is a firewall?
   A firewall is a security mechanism that monitors and filters network traffic according to defined rules, controlling which connections are allowed or blocked.
2. Difference between stateful and stateless firewalls?
   - Stateful firewalls track the state of connections and automatically allow return traffic.
   - Stateless firewalls evaluate each packet individually without considering connection states.
3. What are inbound and outbound rules?
   - Inbound rules control traffic entering a system.
   - Outbound rules control traffic leaving a system.
4. How does UFW simplify firewall management?
   UFW provides user-friendly commands (e.g., allow, deny) that simplify rule management compared to the complex syntax of iptables.
5. Why block port 23 (Telnet)?
   Telnet is insecure because it transmits data, including credentials, in plain text. Attackers often target it, making it a common security risk.

6. What are common firewall mistakes?
    - Forgetting to allow SSH before enabling the firewall.
    - Leaving unused ports open.
    - Failing to document rule changes.
7. How does a firewall improve network security?
   By blocking unnecessary or insecure services and only allowing required traffic, a firewall reduces the system's attack surface.
8. What is NAT in firewalls?
   NAT (Network Address Translation) maps private internal IP addresses to a public address, providing both security and efficient use of IP addresses.

Conclusion

The task demonstrated basic firewall configuration using UFW on Linux. Rules were applied, tested, and removed as required. The exercise highlighted the importance of firewalls in controlling network access, preventing insecure connections, and ensuring that essential services remain available.