Pragadeesh V S

Task 4 – Setup and Use a Firewall on Windows/Linux

Objective

To configure and test basic firewall rules to allow or block traffic using Windows Firewall or UFW (Uncomplicated Firewall) on Linux.

Tools Used

- Operating System: Ubuntu 22.04 LTS (Linux)
- Firewall Tool: UFW (Uncomplicated Firewall)
- Terminal for testing and rule application

Steps Performed

1. View Current Firewall Rules

Command:

```
sudo ufw status numbered
```

Checked the list of existing rules.
Confirmed UFW was active.

2. Block Inbound Traffic on Port 23 (Telnet)

Command:

```
sudo ufw deny 23
```

Added a rule to block Telnet (which is insecure and outdated).
Verified the rule was added successfully.

3. Allow Inbound SSH on Port 22

Command:

```
sudo ufw allow 22
```

Ensured remote access via SSH was still allowed after applying firewall rules.

4. Verify Firewall Status

Command:

```
sudo ufw status verbose
```

Checked the rules applied to confirm correct configuration.

5. Test the Firewall Rule

Command:

```
telnet localhost 23
```

Result: Connection was refused, indicating the rule worked as expected.

6. Remove the Test Rule (Restore State)

Command:

```
sudo ufw delete deny 23
```

Removed the Telnet block rule to restore the system to its original state.

Summary: How Firewall Filters Traffic

A firewall filters traffic by evaluating network packets against a set of rules. If a packet matches a rule (e.g., block port 23), the firewall will take the specified action (deny/allow). UFW simplifies this by providing a user-friendly syntax to define such rules.

Interview Questions & Answers

What is a firewall?

A firewall is a network security device or software that monitors and controls incoming and outgoing traffic based on predefined rules.

Difference between stateful and stateless firewall?

- Stateful: Tracks active connections and makes decisions based on connection state.
- Stateless: Filters packets solely on predefined rules without tracking state.

What are inbound and outbound rules?

- Inbound: Controls traffic coming into your system.
- Outbound: Controls traffic going out of your system.

How does UFW simplify firewall management?

UFW provides a simplified command-line interface to manage iptables, which are otherwise complex to configure manually.

Why block port 23 (Telnet)?

Telnet is insecure and transmits data in plaintext, making it vulnerable to interception.

What are common firewall mistakes?

- Blocking essential ports (like SSH).
- Leaving unnecessary ports open.
- Misconfiguring rule directions (inbound vs. outbound).

How does a firewall improve network security?

By blocking unauthorized access, filtering unwanted traffic, and protecting against exploits and malware.

What is NAT in firewalls?

NAT (Network Address Translation) modifies IP address information in packet headers, allowing private IP addresses to communicate with external networks securely.