**Task 4 : Setup and Use a Firewall on Windows/Linux**

**Objective**: Configure and test basic firewall rules to allow or block traffic.

**Tools**: Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

**Deliverables**: Screenshot/configuration file showing firewall rules applied.

Report according to the checklist

### ****1. Opening the Firewall Configuration Tool (UFW)****

The Uncomplicated Firewall (UFW) is a command-line tool used in Linux systems to manage firewall rules in a simplified manner. It is a frontend for iptables and helps users allow or deny traffic without complex commands.

### ****2. Listing Current Firewall Rules****

Before modifying the firewall configuration, it's important to view existing rules to avoid conflicts. The command sudo ufw status numbered displays all active firewall rules, along with their assigned numbers, which helps in identifying or removing specific rules later.

### ****3. Adding a Rule to Block Inbound Traffic on a Specific Port (Port 23 for Telnet)****

To enhance security, you may block unused or vulnerable ports. Port 23 is commonly used by the Telnet protocol, which transmits data in plaintext and is insecure. Using the command sudo ufw deny 23, all inbound traffic on this port is blocked, preventing potential unauthorized access via Telnet.

### ****4. Testing the Block Rule****

After applying the block rule, it is important to verify whether it is effective. This can be done by attempting to establish a connection to the port (e.g., using telnet <ip> 23). If the rule is working, the connection attempt will fail, confirming that the firewall is properly filtering the traffic.

### ****5. Adding a Rule to Allow SSH (Port 22)****

While securing the system, it's important to ensure that essential services remain accessible. SSH (Secure Shell) typically uses port 22 and is widely used for secure remote logins. Adding a rule with sudo ufw allow 22 ensures that SSH connections are not blocked, allowing administrators to manage the system remotely.

### ****6. Removing the Test Block Rule to Restore the Original State****

Once testing is complete, the temporary rule blocking port 23 can be removed to return the firewall to its original state. This is done using sudo ufw delete deny 23, or by referencing the rule number shown in the status list. This step helps maintain a clean and manageable rule set.

### ****7. Documenting the Commands Used****

All firewall actions should be documented for future reference and troubleshooting. Documenting commands such as sudo ufw deny 23 and sudo ufw allow 22 provides a clear log of the configurations applied, which is essential for auditing and maintaining system security.

### ****8. Summary: How Firewalls Filter Traffic****

Firewalls operate by monitoring and controlling incoming and outgoing network traffic based on predefined security rules. In the case of UFW:

**Inbound rules** determine what kind of traffic is allowed to enter the system.

**Outbound rules** (less commonly used in UFW) control what traffic the system can send out.

Rules can be set to:

**Allow** traffic on trusted ports (like 22 for SSH)

**Deny** traffic on vulnerable or unused ports (like 23 for Telnet).

By using such rules, firewalls act as gatekeepers that protect the system from unauthorized access and attacks.

**Related Screenshots**























