Task 10: Firewall Configuration & Testing (Solved)

🎯 Objective

Understand firewall concepts, configure firewall rules to **allow/deny traffic**, test connectivity, observe logs, block malicious IPs, and document the **security impact**.

🛠 Tools Used

Choose **ONE** (recommended based on OS):

🔹 **Linux / Kali / Ubuntu**

- **UFW (Uncomplicated Firewall)**

🔹 **Windows**

- **Windows Defender Firewall (Advanced Security)**

🔁 **Alternative**

- iptables (advanced, not mandatory)

🧠 1️⃣ Firewall Concepts (Theory)

What a Firewall Does

A firewall:

- Monitors network traffic
- Applies security rules
- Allows or blocks traffic based on policy

🔐 Acts as a **gatekeeper** between trusted and untrusted networks.

🧪 LAB SETUP (Example)

- Attacker/Tester: Kali Linux
- Target: Ubuntu VM or Windows 10/11
- Network: Same LAN / Host-only / NAT

⚠️ Only configure firewalls on **your own system or lab VM**

🐧 PART A: UFW (Linux Firewall)

2️⃣ Check Firewall Status

```
sudo ufw status verbose
```

If inactive:

```
sudo ufw enable
```

3️⃣ Default Firewall Rules (Best Practice)

```
sudo ufw default deny incoming

sudo ufw default allow outgoing
```

🔎 Impact

- Blocks all unsolicited inbound traffic
- Allows system to access internet

4️⃣ Allow Specific Ports (Service Access)

Allow SSH (Port 22)

```
sudo ufw allow 22
```

Allow HTTP & HTTPS

```
sudo ufw allow 80

sudo ufw allow 443
```

5️⃣ Deny a Specific Port

```
sudo ufw deny 21
```

🔎 Blocks FTP service (common attack target)

6️⃣ Block a Malicious IP Address

```
sudo ufw deny from 192.168.1.100
```

📌 **Use case:**

- Brute-force attacker
- Suspicious scanner
- IDS alert IP

7️⃣ Test Connectivity

From another machine:

```
ping <target-ip>
ssh <target-ip>
nmap <target-ip>
```

Expected Result:

Service	Result
Allowed port	Accessible
Blocked port	Filtered / Timeout

8️⃣ Observe Firewall Logs

```
sudo ufw logging on
sudo tail -f /var/log/ufw.log
```

🔍 Shows:

- Blocked packets
- Source IP

- Destination port

🪟 PART B: Windows Firewall (Advanced)

2️⃣ Open Firewall Console

Control Panel → Windows Defender Firewall → Advanced Settings

---

3️⃣ Create Inbound Rule (Block Port)

Example: Block FTP (Port 21)

- Inbound Rules → New Rule
- Port → TCP → 21
- Action → Block
- Apply to all profiles
- Name: Block FTP Port 21

4️⃣ Allow SSH or HTTP (Inbound)

Example: Allow HTTP

- Port → TCP → 80
- Action → Allow

5️⃣ Block Malicious IP (Windows)

- Inbound Rules → New Rule
- Custom → Scope
- Remote IP: 192.168.1.100
- Action: Block

6️⃣ Test Firewall Rules

```
Test-NetConnection -Port 21 <target-ip>
```

or from Kali:

```
nmap <target-ip>
```

📄 FIREWALL RULES DOCUMENTATION (Deliverable)

Firewall Summary

Rule	Direction	Port/IP	Action
Default inbound	Inbound	All	Deny
SSH access	Inbound	22	Allow
Web access	Inbound	80/443	Allow
FTP	Inbound	21	Deny
Malicious IP	Inbound	192.168.1.100	Block

📊 IMPACT ANALYSIS

✅ Security Improvements

- Reduced attack surface
- Blocked unauthorized access
- Prevented brute-force attempts
- Improved network hygiene

⚠️ Limitations

- Firewall cannot stop:
    - Phishing
    - Malware via allowed ports
    - Insider attacks

    - Zero-day exploits