CYBER SECURITY INTERNSHIP

Task 10

FIREWALL CONFIGURATION & TESTING

JASHMI KS

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a barrier between a trusted internal network and untrusted external networks (like the Internet).

Types of Firewalls

- **Host-based firewall** – Runs on individual systems (UFW, Windows Firewall)
- **Network firewall** – Protects entire networks (hardware firewalls)
- **Packet-filtering firewall** – Filters traffic based on IP, port, protocol (iptables)
- **Stateful firewall** – Tracks connection states
- **Application-level firewall** – Filters traffic at application layer

Importance

- Prevent unauthorized access
- Block malicious traffic
- Protect services and data
- Control network usage
- Improve overall system security

Configure Firewall Rules

Firewall rules define **what traffic is allowed or blocked**.

Each rule is based on:

- **Source IP address**
- **Destination IP address**
- **Port number**
- **Protocol** (TCP / UDP / ICMP)
- **Action** (ALLOW / DENY / REJECT)

Example:

- Allow SSH only from trusted IP
- Block unused ports
- Deny traffic from suspicious IPs

In Linux:

- **UFW** → Beginner-friendly
- **iptables** → Advanced, low-level control

Allow / Deny Ports

Ports are communication endpoints used by services.

Common Ports

Service	Port
HTTP	80
HTTPS	443
SSH	22
FTP	21
MySQL	3306

Using UFW (Linux)

- Allow a port:

```
sudo ufw allow 22
```

- Deny a port:

```
sudo ufw deny 23
```

- Allow specific protocol:

```
sudo ufw allow 80/tcp
```

Using iptables

- Allow port:

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

- Block port:

```
sudo iptables -A INPUT -p tcp --dport 23 -j DROP
```

Test Connectivity

After configuring rules, **testing is essential** to verify firewall behavior.

Testing Methods

- **ping** → Tests ICMP connectivity
- **telnet / nc** → Tests port accessibility
- **nmap** → Scans open/closed ports
- **browser access** → Tests web services

Example:

```
nmap localhost
```

Expected results:

- Allowed ports → OPEN
- Blocked ports → FILTERED or CLOSED

Testing ensures:

- No critical services are blocked
- Unauthorized ports are inaccessible

Firewall Logs

Firewall logs record allowed and blocked traffic events.

Why Logs Matter

- Detect intrusion attempts
- Analyze suspicious activity
- Troubleshoot connectivity issues
- Maintain audit records

Enable Logging in UFW

```
sudo ufw logging on
```

Log Location (Linux)

```
/var/log/ufw.log
```

Logs include:

- Source IP
- Destination port
- Protocol
- Action taken (ALLOW/DROP)

Block Malicious IP Address

Firewalls can block known malicious or suspicious IP addresses to prevent attacks.

Using UFW

```
sudo ufw deny from 192.168.1.100
```

Using iptables

```
sudo iptables -A INPUT -s 192.168.1.100 -j DROP
```

This prevents:

- Brute-force attacks
- Unauthorized access attempts
- Malware communication

Blocking IPs enhances **active defense**.

Document Firewall Rules

Example Entry

Rule	**Description**
Allow 22	SSH access for admin
Block 23	Disable Telnet
Block IP	Prevent brute-force

Documentation helps in:

- Future troubleshooting
- Security audits
- Team coordination

Explain Firewall Impact

Firewall configuration impacts system security and performance.

Positive Impacts

- Increased security
- Reduced attack surface
- Controlled access
- Better monitoring

Possible Negative Impacts

- Misconfiguration can block services
- Performance overhead (minimal)
- Maintenance required

Overall Impact

A properly configured firewall:

- Protects systems from attacks
- Ensures secure communication
- Maintains system integrity

Firewall configuration using **UFW, Windows Firewall, or iptables** is a critical aspect of network security. By understanding firewall concepts, configuring rules, allowing or denying ports, testing connectivity, monitoring logs, blocking malicious IPs, documenting rules, and analyzing impact, organizations can build a **strong and effective security defence system**.