CYBER SECURITY INTERNSHIP

Task 10: Firewall Configuration & Testing (Full Explanation)

Aim:

The aim of this task is to understand firewall concepts and configure firewall rules to control network traffic, protect systems from unauthorized access, and test the effectiveness of security rules.

Introduction:

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. Firewalls act as a barrier between trusted internal networks and untrusted external networks such as the internet. Proper firewall configuration is essential to prevent cyber attacks.

Tools Used:

1. UFW (Uncomplicated Firewall) – Linux based firewall management tool
2. Windows Defender Firewall – Built-in firewall in Windows OS
3. iptables – Advanced Linux firewall utility

Firewall Concepts:

1. Inbound Rules: Control incoming traffic to the system
2. Outbound Rules: Control outgoing traffic from the system
3. Stateful Firewall: Tracks active connections
4. Stateless Firewall: Filters packets without tracking sessions
5. Port-based Filtering: Allows or blocks specific ports

Procedure:

1. Install and enable the firewall tool
2. Set default rules to deny unauthorized access
3. Allow necessary ports such as SSH (22) or HTTP (80)
4. Block unused or risky ports
5. Add rules to block malicious IP addresses
6. Enable logging to monitor firewall activity
7. Test connectivity using ping or browser
8. Verify logs to ensure rules are working correctly

Testing & Verification:

After configuring firewall rules, connectivity testing is performed to verify allowed services are accessible and blocked services are restricted. Logs are analyzed to confirm firewall decisions.

Deliverables:

Documentation of firewall rules, screenshots of configuration, and explanation of security impact.

Final Outcome:

This task improves practical knowledge of firewall management, network security, and threat prevention techniques.

Interview Questions & Answers:

1. **What is a firewall?** A firewall is a security system that controls network traffic using rules.
2. **Stateful vs Stateless firewall?** Stateful tracks connections, stateless filters packets individually.
3. **Why are firewalls needed?** To prevent unauthorized access and cyber attacks.
4. **What is inbound and outbound rule?** Inbound controls incoming traffic, outbound controls outgoing traffic.
5. **Can firewall stop all attacks?** No, firewalls reduce risk but cannot stop all attacks.