**Task-4 Findings / Observations**

| **Test Case** | **Expected Behavior** | **Observed Result** | **Conclusion** |
| --- | --- | --- | --- |
| Before UFW enabled | All ports open locally | Connection on port 23 succeeded | Unfiltered traffic |
| After deny 23/tcp | Port 23 blocked | Connection refused message | Inbound Telnet blocked successfully |
| After allow 22/tcp | SSH allowed | Connection succeeded | Selective allow verified |
| After deleting rule | Port 23 open again | Connection restored | Rule removal effective |

**Conclusion**

UFW correctly enforces firewall rules to block or permit specific ports, confirming proper packet filtering on Kali Linux.

**Firewall Summary**

* **Total rules applied:** 2 (active during test)
* **Default policy:** deny (incoming), allow (outgoing)
* **Blocked port:** 23 (Telnet – unsecured protocol)
* **Allowed port:** 22 (SSH – secure remote access)
* **Testing tool:** netcat for port connectivity check

**Learnings**

* Learned to enable and manage UFW from terminal.
* Understood the difference between **inbound** and **outbound** traffic.
* Realized why insecure services like Telnet should be blocked.
* Gained insight into how firewalls enforce least-privilege network access.