Cyber Security Internship - Revision Notes

Cyber Security Internship - Revision Notes

Task 4: Setup and Use a Firewall (Parrot OS with UFW)

1. Firewall Basics:

- Firewall monitors and controls incoming/outgoing network traffic.

- UFW is a simple front-end for managing firewall rules on Linux.

2. Common Commands:

- Check status: sudo ufw status verbose

- Allow port: sudo ufw allow <port>

- Deny port: sudo ufw deny <port>

- Enable firewall: sudo ufw enable

- Disable firewall: sudo ufw disable

- Delete rule: sudo ufw delete deny <port>

3. Important Steps:

- Always allow SSH (port 22) before enabling UFW to avoid lockout.

- Use 'sudo ufw status verbose' to verify rules and status.

- Block unnecessary or insecure ports like Telnet (port 23).

- Use IPv4 and IPv6 rules as required.

4. Default Policies:

- Incoming traffic default: deny

- Outgoing traffic default: allow

5. Testing Firewall Rules:

- After adding rules, test connectivity (e.g., telnet or ssh).
- Remove or update rules as needed to restore original state.

6. Key Learnings:

- How to enable/disable UFW safely.
- Managing firewall rules to control network traffic.
- Understanding the difference between allow and deny rules.
- Importance of firewall in network security.

Remember: Always backup firewall settings before making changes.