CYBER SECURITY
LAB 1

Identify network resources like switches, router, hub, firewall and security issues for the same

SOLUTION:

The Network resources are :

1. Switch
2. Router
3. Hub
4. Firewall
5. Access point
6. Servers
7. Gateway
8. Modem
9. Network Interface Card(NIC)
10. VPN(Virtual private Network)
11. Load Balancer
12. Intrusion Detection System(IDS)

SWITCH:

Definition: A networking device that connects devices on a computer network by using packet switching to forward data to the destination device.

Secuirty Issues:

1. **MAC Flooding**
   - **Issue description:** Attackers can flood the switch with fake MAC addresses, causing it to send data to all ports.
   - **Solution:** Implement port security and rate limiting
2. **VLAN Hopping**
   - **Issue description:** Improper VLAN configuration can allow attackers to send packets to unauthorized VLANs.
   - **Solution:** Proper VLAN configuration and tagging
3. **Port Security**

- **Issue description:** Lack of port security can lead to unauthorized devices connecting to the network.
- **Solution:** Limit the number of devices per port

4. **Spanning Tree Protocol (STP) Attacks**
    - **Issue description:** STP can be manipulated to alter the network topology and cause disruptions
    - **Solution:** Use STP security features (e.g., BPDU Guard)

HUB

Definition: A basic networking device that connects multiple Ethernet devices, making them act as a single network segment.

Security Issues:

1. **Lack of Security Features**:
    - **Issue description**: Hubs do not filter or secure traffic, making all connected devices susceptible to sniffing.
    - **Solution**: Replace with switches where possible.
2. **Broadcast Traffic**:
    - **Issue description**: All data packets are sent to every device on the network, increasing interception risk.
    - **Solution**: Use network segmentation.

Router

Definition: A networking device that forwards data packets between computer networks, creating an overlay network.

Security Issues:

1. **Default Credentials**:
    - **Issue description** :Many routers come with default usernames and passwords that are easily exploitable.
    - **Solution**: Change default usernames and passwords.
2. **Outdated Firmware**:
    - **Issue description** Failure to update router firmware can leave vulnerabilities open to exploitation.
    - **Solution**: Keep firmware up-to-date.
3. **Weak Encryption**:

- **Issue description** :Using weak encryption protocols (e.g., WEP) makes it easier for attackers to intercept data.
- **Solution**: Use strong encryption protocols (e.g., WPA3).

4. **Remote Management**:
   - **Issue description** :Enabled remote management interfaces can be accessed by attackers if not secured.
   - **Solution**: Limit access and disable if not needed.
5. **Open Ports**:
   - **Issue description** :Unnecessarily open ports can be entry points for attackers.
   - **Solution**: Close unnecessary ports.

Firewall

Definition: A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Security Issues:

1. **Misconfiguration**:
   - **Issue description** :Incorrectly configured firewalls can allow unauthorized traffic or block legitimate traffic.
   - **Solution**: Ensure proper configuration and regular audits.
2. **Policy Bypass**:
   - **Issue description** :Complex rules and policies might be improperly enforced, leading to security loopholes.
   - **Solution**: Simplify and regularly review rules.
3. **Outdated Software**:
   - **Issue description** :Firewalls that are not updated may have vulnerabilities that can be exploited.
   - **Solution**: Keep software up-to-date.
4. **Logging and Monitoring**:
   - **Issue description:** Insufficient logging and monitoring can delay detection of breaches.
   - **Solution**: Implement robust logging and monitoring.