Mark Ngugi
I132/g/1614/21
COURSE CODE: ICB 1409
COURSE TITLE: NETWORK MANAGEMENT AND SECURITY

Securing TechNova Inc.'s Digital Ecosystem

Part A: Identifying Vulnerabilities (15 Marks)

1. **Default Credentials on Switches**
    - Default credentials were left unchanged on the switches, allowing the attacker to access the management interfaces easily. Default credentials are widely known and can be exploited without sophisticated tools, granting administrative control over the network devices.
2. **MAC Flooding Attacks**
    - The attacker launched MAC flooding attacks, causing the switches' MAC address tables to overflow. This forced the switches to broadcast all traffic across all ports, exposing sensitive data and degrading network performance.
3. **Misconfigured VLANs**
    - VLANs were improperly configured, enabling the attacker to gain unauthorized access to the segregated financial department VLAN. This misconfiguration violated the principle of least privilege and facilitated lateral movement within the network.

Part B: Impact Analysis (10 Marks)

1. **Consequences of MAC Flooding Attacks**
    - **Network Performance Degradation**: By overflowing the MAC address table, switches operated in broadcast mode, increasing network congestion and reducing performance.

    - **Data Exposure**: Sensitive data intended for specific devices was broadcast to all devices, increasing the likelihood of unauthorized access or interception.
2. **Consequences of VLAN Misconfigurations**
    - **Unauthorized Access**: Misconfigured VLANs allowed attackers to bypass logical segmentation, accessing sensitive data from restricted VLANs, such as the financial department.
    - **Compliance Violations**: Failing to ensure proper VLAN segmentation could lead to non-compliance with data protection regulations, exposing the company to legal and financial penalties.

Part C: Best Practices (15 Marks)

1. **Change Default Credentials**
    - All default credentials should be replaced with strong, unique passwords. This reduces the risk of unauthorized access to network devices.
2. **Enable Port Security**
    - Port security limits the number of MAC addresses that can connect to a port, preventing MAC flooding attacks by blocking unauthorized devices.
3. **Implement VLAN Segmentation and Access Control**
    - Properly configure VLANs with strong access control policies to enforce logical segmentation. This ensures sensitive data is accessible only to authorized users.

Part D: Technical Solutions (20 Marks)

1. **Port Security**
    - **How it Works** : Port security restricts the number of MAC addresses allowed on a switch port. It can also block or shut down ports when unauthorized devices attempt to connect.
    - **How it Addresses Vulnerabilities** : By limiting allowed MAC addresses, port security mitigates MAC flooding attacks and prevents unauthorized access to the network.

2. **VLAN Trunking Protocol (VTP) Pruning**
    - **How it Works** : VTP pruning restricts VLAN traffic on trunk links to only those VLANs required on the connected switches. This reduces unnecessary traffic.
    - **How it Addresses Vulnerabilities** : By restricting VLAN traffic, VTP pruning prevents VLAN hopping and limits the attack surface available to potential intruders.

3. **Dynamic ARP Inspection (DAI)**
    - **How it Works** : DAI validates ARP packets in the network, ensuring that the ARP requests and replies match the known IP-MAC bindings in the DHCP snooping database.
    - **How it Addresses Vulnerabilities** : DAI prevents ARP spoofing attacks by ensuring the integrity of ARP communications, safeguarding against IP-MAC mismatches.