Report 1 – Network Audit and Attack Surface Analysis

Prepared for: Cisco Networking Academy – Virtual Internship Program 2025

Prepared by: Kasmya Bhatia (23FE10CAI00010)

Date: August 2025

Part 1 – Network Audit and Attack Surface Analysis

Objective: To conduct a complete analysis of the existing college campus network using Cisco Packet Tracer, identify all devices, access points, firewalls, and segmentation boundaries, assess the effectiveness of current security controls, locate potential weaknesses, and propose risk based countermeasures that consider tight budgets and limited staff resources.

Current Network Mapping

The network interconnects multiple departments and labs:

- Departments: Computer Department, IT Department, Exam Cell, Principal Room
- Labs: Internet Lab
- Server Room: Hosts FTP, WEB, and DNS services

Key Observations:

- Logical separation between departments exists but lacks depth.
- No dedicated internal firewalls between critical areas.
- Internet Lab directly connects to the internet, creating an exposed entry point.

Identified Trust Zones

- High Trust: Server Room
- Medium Trust: Department VLANs
- Low Trust: Internet Lab, guest access points

Security Controls Identified

- Standard network routing between departments
- Basic switch-level segmentation
- No perimeter firewall or IDS/IPS present
- No ACLs restricting inter-department or lab-to-server traffic

Attack Surface Analysis

1. Missing Perimeter Firewall – Entire network exposed to inbound/outbound threats from the internet.
2. Flat Network Structure – Minimal segmentation allows easy lateral movement from compromised areas like the Internet Lab to sensitive zones like the Server Room.
3. No IDS/IPS – No detection or prevention of suspicious network activity.
4. Lack of Internal Access Controls – Unrestricted communication between departments increases attack spread potential.
5. Server Exposure – FTP, WEB, and DNS servers accessible without additional protective barriers.

Risk-Based Countermeasures

- Install a Perimeter Firewall at the internet gateway, default-deny policy except for explicitly allowed traffic.
- Strengthen Segmentation with ACLs:
    - Block direct Internet Lab to Server Room traffic.
    - Implement department-to-department communication restrictions.
- Create a DMZ: Move FTP, WEB, and DNS servers into a controlled segment accessible only through secure, filtered channels.
- Deploy IDS/IPS: Monitor and detect unusual traffic or intrusion attempts.
- Adopt Strong Security Policies:
    - Secure authentication for all devices and accounts.
    - Regular configuration and log audits.
    - Security awareness training for staff and students.

Deliverables

- Network Topology Diagram: Cisco Packet Tracer diagram showing routers, switches, access points, VLANs, trust zones, and security controls.
- Security Assessment Report: Documentation of identified risks, vulnerabilities, and mitigation strategies.

Conclusion

The audit revealed significant security gaps in the current campus network, primarily due to lack of perimeter defenses, insufficient segmentation, and absence of monitoring systems. By implementing the proposed firewall, segmentation improvements, IDS/IPS deployment, and policy changes, the college can substantially reduce its attack surface while maintaining operational efficiency.