Campus Network Analysis and Security Assessment

1. Network Topology Analysis

To analyze your college campus network topology:

1. Gather information:
   - Obtain network documentation if available
   - Interview IT staff
   - Conduct a physical walkthrough of the campus
2. Identify key components:
   - Core routers and switches
   - Distribution switches
   - Access switches
   - Firewalls
   - Wireless access points
   - Servers (web, email, database, etc.)
   - Client devices (computers, printers, IoT devices)
3. Map out connections:
   - Determine how devices are interconnected
   - Identify VLANs and subnets
   - Note the types of connections (Ethernet, fiber, wireless)
4. Document IP addressing scheme and routing protocols

2. Cisco Packet Tracer Network Mapping

Use Cisco Packet Tracer to create a simplified model of your campus network:

1. Place core routers and switches
2. Add distribution and access layer switches
3. Include firewalls and other security devices
4. Add representative end devices (servers, computers, etc.)
5. Connect devices using appropriate cable types
6. Configure IP addresses, VLANs, and routing protocols to match your actual network

3. Attack Surface Mapping

Conduct an attack surface mapping exercise:

1. External attack vectors:
   - Internet-facing services (web servers, email servers)
   - VPN endpoints
   - Wireless networks
2. Internal vulnerabilities:
   - Unpatched systems

   - Misconfigured devices
   - Weak access controls
   - Insecure protocols
3. Physical security risks:
   - Unsecured network closets
   - Public access areas with network ports
4. Social engineering risks:
   - Phishing susceptibility
   - Insider threats
5. Data flow analysis:
   - Identify sensitive data repositories
   - Map data transmission paths

Security Assessment Report

Identified Security Risks:

1. Unauthorized Access:
   - Weak passwords on network devices
   - Unencrypted wireless networks
   - Open network ports in public areas
2. Data Breaches:
   - Unencrypted data transmission
   - Inadequate access controls on sensitive servers
   - Lack of data loss prevention measures
3. Network Availability:
   - Single points of failure in core infrastructure
   - Lack of redundancy in internet connections
   - Insufficient DDoS protection

Proposed Solutions and Countermeasures:

1. Implement strong password policies and multi-factor authentication
2. Encrypt all wireless networks with WPA3
3. Disable or secure unused network ports in public areas
4. Implement end-to-end encryption for sensitive data transmission
5. Enhance access controls with principle of least privilege
6. Deploy data loss prevention (DLP) solutions
7. Introduce redundancy in core network infrastructure
8. Establish backup internet connections
9. Implement DDoS mitigation services
10. Regularly update and patch all systems and devices
11. Conduct ongoing security awareness training for all users
12. Implement network segmentation to isolate sensitive systems
13. Deploy and maintain next-generation firewalls
14. Establish a robust incident response plan