Campus Network Security Assessment & Attack Surface Report

# Problem Statement

You are a part of the cybersecurity student team at your college, freshly enrolled in the Cisco NetAcad Cybersecurity course. With access to Cisco Packet Tracer and your growing knowledge of security fundamentals, you've been given your first real-world challenge.  
  
Your task is to analyze your own college network as if you were part of an internal red team. You’ll begin by mapping the current infrastructure using Cisco Packet Tracer, identifying devices, access points, firewalls, segmentation boundaries, and any existing security controls.  
  
But this isn’t just a drawing exercise. You are expected to assess how effective these controls are in today’s threat landscape. Where are the weak points? Are there flat zones that allow lateral movement? What would an attacker target first, and how would you stop them?  
  
Using the knowledge from your NetAcad course and insights gained through simulation, conduct an attack surface analysis, and present your findings. Your recommendations should reflect real-world thinking: assume budgets are tight, staff are limited, and security is everyone’s afterthought until something breaks.

# 1. Scope & Objective

This assessment covers the existing college campus network layout, identifying core devices (routers, switches, firewalls, access points), zones (academic, administrative, student, guest Wi-Fi), and current segmentation. The objective is to evaluate existing security controls, map potential attack surfaces, and suggest risk-based countermeasures.

# 2. Network Topology Overview

The college network is built using Cisco routers, distribution/access switches, and multiple access points. Segmentation exists across VLANs for Administration, Faculty, Students, and Guest users. A central firewall enforces limited traffic filtering.

# 3. Device Inventory

Key devices in the network include:

• Core Router – Gateway to ISP / Internet.  
• Layer 3 Switch – VLAN segmentation and inter-VLAN routing.  
• Access Switches – Faculty labs, classrooms, and dorm access.  
• Wireless Access Points – Campus Wi-Fi (Student & Guest zones).  
• Firewall – Central enforcement point with ACLs.  
• Servers – Authentication server, Web server, File server.  
• Endpoints – Faculty PCs, student laptops, IoT devices.

# 4. Trust Zones & Segmentation

• Administrative Zone – High trust, sensitive data.  
• Faculty Zone – Moderate trust, academic resources.  
• Student Zone – Lower trust, bulk of traffic.  
• Guest Wi-Fi – Untrusted, isolated network.  
• Server Zone (DMZ) – Medium trust, external-facing services.

# 5. Existing Security Controls

• Firewall configured with ACLs for inbound/outbound traffic.  
• VLAN segmentation for administrative, student, and guest networks.  
• WPA2 Wi-Fi security for faculty/student SSIDs.  
• Authentication server (local RADIUS) for staff logins.  
• Antivirus/EDR on faculty endpoints.

# 6. Attack Surface Mapping

Potential weaknesses identified:  
• Flat VLANs in Student Zone – risk of lateral movement.  
• Guest Wi-Fi with weak isolation – possible pivot into campus network.  
• Outdated firmware on switches and access points.  
• Limited monitoring – no IDS/IPS in place.  
• Firewall ACLs too permissive in certain zones.  
• Lack of network segmentation between IoT devices and main network.

# 7. Recommendations

1. Introduce an IDS/IPS (Snort or Suricata) for real-time threat detection.  
2. Harden ACLs at firewall and router to enforce least privilege.  
3. Segment IoT devices into a dedicated VLAN with restricted Internet-only access.  
4. Enforce WPA3 for Wi-Fi security and isolate Guest SSID.  
5. Enable centralized logging (Syslog, SIEM-lite) for monitoring.  
6. Conduct regular firmware updates and vulnerability scans.  
7. Apply principle of least privilege for faculty/student access.  
8. Provide cybersecurity awareness training to staff and students.

# 8. Conclusion

The current campus network provides a strong foundation but suffers from flat zones, limited visibility, and insufficient segmentation. By adopting the above recommendations—particularly improved ACLs, IDS/IPS deployment, and network segmentation—the attack surface can be significantly reduced while staying within budget and resource constraints.