Problem Statement for Cyber Security stream

Cyber Shield: Defending the network

Problem Statement:

PART 1:

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.

Tasks:

- Conduct a complete analysis of the existing college campus network layout, devices, and zones.
- Use Cisco Packet Tracer to create a visual representation of routers, switches, firewalls, and access points.
- Assess how the network is segmented and which trust zones exist.
- Identify and document any security controls such as firewalls, IDS/IPS, authentication servers, or ACLs.
- Perform an attack surface mapping exercise to locate potential weaknesses.
- Suggest risk-based countermeasures, policy changes, and improved control placement

Deliverables:

- A detailed network topology diagram highlighting infrastructure, zones, and attack surface.
- Security assessment report highlighting identified security risks, suggested solutions and countermeasures to mitigate attack surface risks.

PART 2:

Problem Statement: After your impressive audit in Part 1, the college IT department has invited you to contribute to a new project: enabling a hybrid access model for students and faculty.

Faculty members will now work flexibly from home or campus, and require uninterrupted, secure access to teaching tools, research repositories, and internal services. Students, on the other hand, will continue using personal devices to access shared academic portals and lab resources.

But here’s the catch: the administration has made it clear that the internal services must never be exposed directly to the internet.

Your task is to design a secure hybrid network architecture that supports remote access while enforcing strict boundaries. Think like a network engineer and evaluate options like VPN, SASE, identity-aware proxies, or split tunneling. Consider not only how to connect, but how to ensure the right people access the right services at the right time.

Can your design balance simplicity, security, and scale without overwhelming the existing infrastructure?

Tasks & Deliverables:

- Design network segmentation based on user roles (faculty vs student).
- Recommend secure access tools like VPN, SASE, identity-aware proxies, or split tunnelling.
- Define trust models, authentication flows, and control access to internal apps.
- Update the campus network topology to show remote access pathways, gateways, and policy enforcement zones.
- Justify your architecture with risks, use cases, and fallback strategies.

Deliverables:

- Updated network diagram with new hybrid access components.
- Technical documentation explaining chosen solutions, technologies, risks, and advantages.

PART 3:

Problem Statement: Soon after the hybrid model rolls out, complaints start coming in: students are streaming videos during lectures, torrenting files in labs, and bypassing basic restrictions using browser extensions and proxies.

The administration turns to you again, and this time for a solution that restricts web access smartly, without creating backlash or blocking legitimate research.

You must design a policy framework that considers:

- Who the user is (student, faculty, guest)
- When they're online (class hours, weekends)
- What content they're trying to access (education, social media, games, etc.)

Explore modern filtering tools: DNS-based filtering, L7 firewalls, proxies, and endpoint-based enforcement. Draft simple, understandable rules, but back them with solid policy logic and enforcement mechanisms.

Don't just stop at blocking sites but instead log events, anticipate circumvention attempts, and define how violations should be reported.

Tasks:

- Compare filtering solutions: DNS filtering, Layer 7 firewalls, proxy-based, or client-side enforcement.
- Design policies that vary by user groups, access time, or category.
- Simulate the enforcement using simple commands or pseudo-policies.
- Add components to the network that enforce and monitor these rules.
- Plan logging and alerting for any access violations.

Deliverables:

- Updated topology with filtering appliance or cloud service locations.
- Web access policy document (in natural language or policy syntax).
- Overview of policy intent, enforcement logic, and advantages.