PROJECT REPORT

CYBER SHIELD: DEFENDING THE NETWORK

By

Kuncham Varun Teja

CMR Institute of Technology

CSE-DS Department

INTRODUCTION

In today's digitally driven academic environment, educational institutions rely extensively on interconnected networks to support learning, research, communication, and laboratory operations. With this growing dependence comes an increased exposure to cyber threats that can disrupt academic activities, compromise confidential data. As part of the **Cisco Virtual Internship Program 2025**, this project aims to analyze, evaluate, and strengthen the cybersecurity posture of the **CMR Institute of Technology (CMRIT)** network using industry-relevant tools and methodologies.

This project focuses on the **CMRIT Main Academic Block**, which consists of multiple computer laboratories, faculty offices, departmental server rooms, and student-access areas. The network within this block supports hundreds of connected devices daily and therefore requires structured design, segmentation, and robust security mechanisms to ensure efficient and secure operations. By leveraging Cisco Packet Tracer, the project simulates a realistic representation of the block's network infrastructure, allowing the identification of vulnerabilities, misconfigurations, and potential attack vectors.

The broader goal of this work is not only to map the existing network but to **approach it from a red-team perspective**, evaluating the system as an attacker would. This analysis helps reveal weak points in segmentation, authentication, access control, firewall rules, and monitoring mechanisms. Building upon the findings, the project further proposes a secure **Hybrid Access Model**, enabling authenticated and role-based access for faculty, students, and remote users. Finally, a comprehensive **Web Access Policy Framework** is developed to ensure controlled, monitored, and responsible usage of the institutional network.

This project aligns directly with the cybersecurity principles taught in the **Cisco Networking Academy**, combining theoretical knowledge with hands-on practical application.

PART 1: RED TEAM AUDIT

1.1 Network Layout

- Main campus router & core switch
- ASA Firewall securing connectivity
- Wi-Fi Network (192.168.10.0/24)
- Authentication Server

VLAN Allocation:

- VLAN 10 – Ground Floor Lab (192.168.1.0/24)
- VLAN 20 – Faculty (192.168.2.0/24)
- VLAN 30 – Project Hub (192.168.3.0/24)
- VLAN 40 – 1st Floor Lab (192.168.4.0/24)
- VLAN 50 – 2nd Floor Lab (192.168.5.0/24)
- VLAN 60 – 3rd Floor Lab (192.168.6.0/24)
- VLAN 70 – Server Room (192.168.7.0/24)

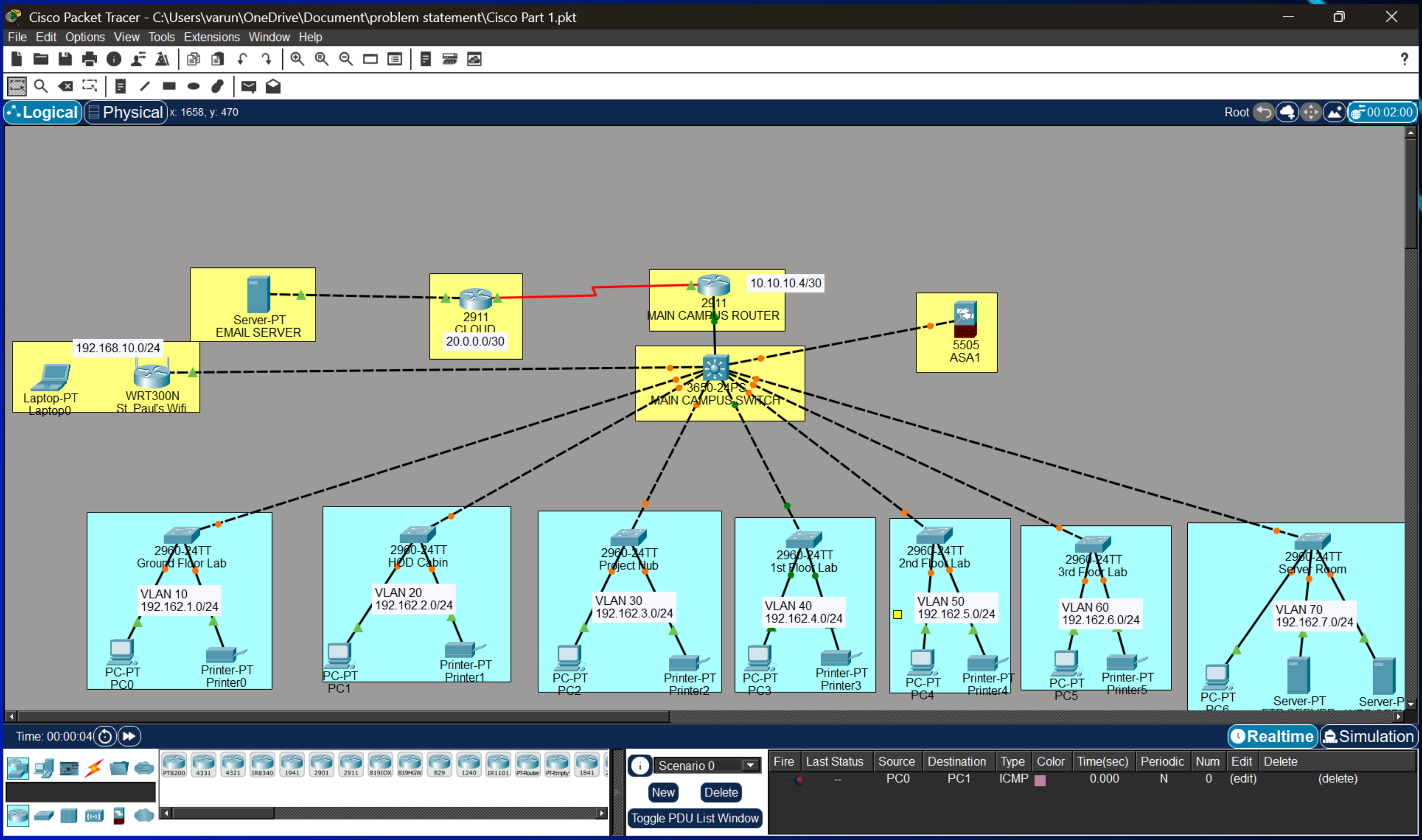
1.2 Weaknesses Identified

- Shared Wi-Fi credentials
- VLANs lack ACL restrictions
- Firewall missing DPI
- Server VLAN reachable by students
- No centralized logging system

1.3 Recommendations

- Enforce ACLs between VLANs
- Enable RADIUS-based authentication

- Strengthen firewall with IDS/IPS
- Restrict access to Server VLAN
- Deploy Syslog server



Cisco Packet Tracer - C:\Users\varun\OneDrive\Document\problem statement\Cisco Part 1.pkt

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	--	PC0	PC1	ICMP	■	0.000	N	0	(edit)	(delete)

PART 2: HYBRID SECURE ACCESS DESIGN

- Firewall segmentation
- Faculty VLAN (10) authenticated
- Student VLAN (20) restricted
- VPN for remote secure access

Risks & Fallback:

- VPN overload → Split tunneling
- Auth server downtime → Local backup accounts

2.1 Purpose of Hybrid Model

CMRIT faculty require secure remote access for:

- Preparing lectures
- Accessing research files
- Managing internal portals

Students typically access learning resources on campus, using personal devices. The design must ensure:

- Internal services remain protected
- Remote access is authenticated & encrypted
- User roles are separated

2.2 Proposed Hybrid Network Architecture

Key Components

- **VPN Gateway:** Enables SSL/IPSec-based remote faculty access.
- **Identity-Aware Proxy (IAP):** Validates role and identity before granting access.
- **RADIUS Server:** Centralized authentication for both Wi-Fi and VPN.

2.3 Authentication Workflow

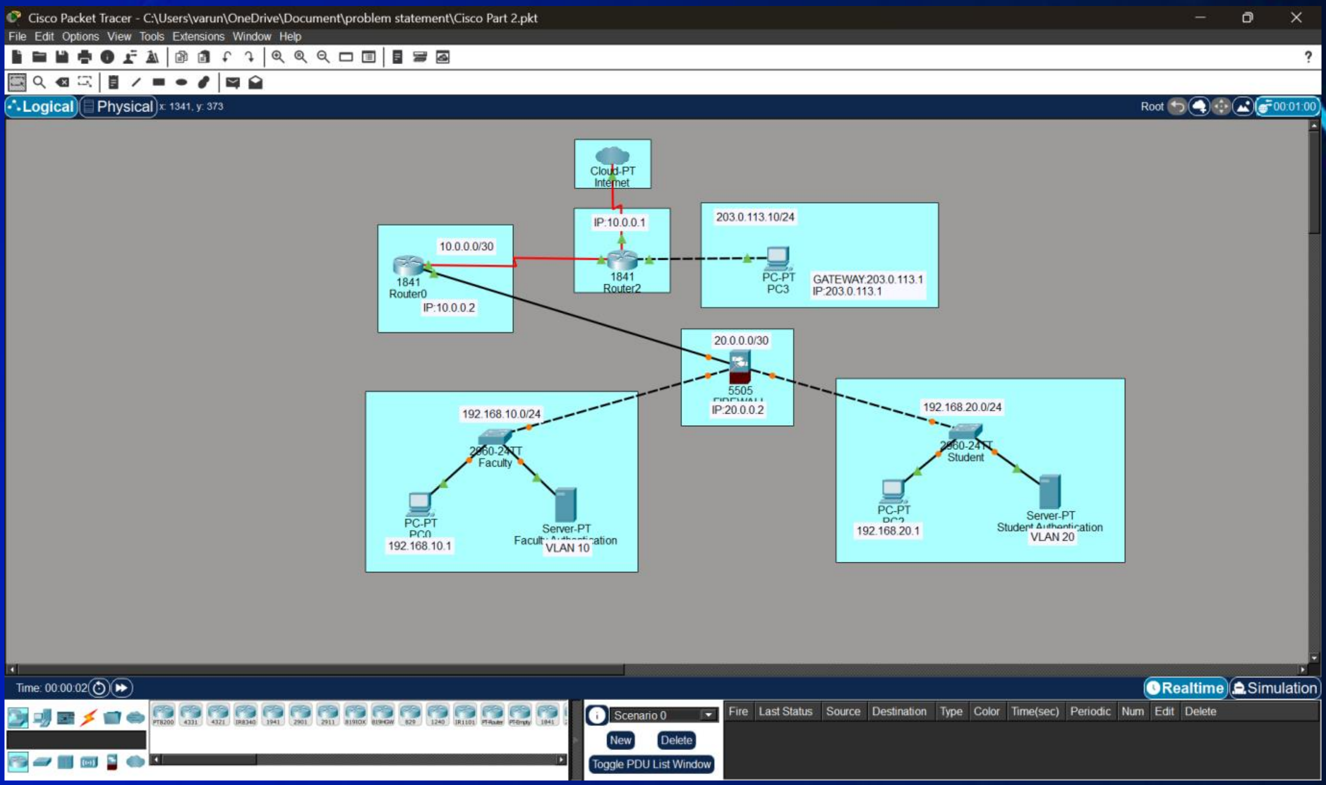
1. User initiates login (Wi-Fi/VPN/IAP).
2. RADIUS verifies credentials.
3. Firewall checks Access Policies.
4. Traffic allowed only to authorized VLAN subnets.

2.4 Risk & Fallback Strategy

Risk: VPN Overload
Solution: Enable route-based split tunneling for safe traffic.

Risk: Authentication Server Failure
Solution: Use backup local credentials or secondary RADIUS server.

.



PART 3: WEB ACCESS POLICY FRAMEWORK

3.1 Subnet & Servers

• Web Server – 192.168.20.10

• FTP Server – 192.168.20.20

• Syslog Server – 192.168.20.30

3.2 Policy Rules

Students:

• Block social media, torrents, gaming during class hours

Faculty:

• Allow full access; log activities

Guests:

• Only HTTP/HTTPS allowed

3.3 Enforcement Logic

IF Student AND Class Hours → Block entertainment categories

IF Faculty → Allow all + log

IF Guest → Allow only basic internet

3.4 Need for Web Filtering

Issues identified:

- Students streaming videos during lectures
- Torrenting and P2P traffic in labs
- Use of proxy extensions to bypass restrictions

3.5 Web Access Policy – CMRIT

Student Rules

- Block: Social media, entertainment, torrenting during class hours.
- Allow: Educational platforms.
- Monitor: All suspicious or repeated patterns.

Faculty Rules

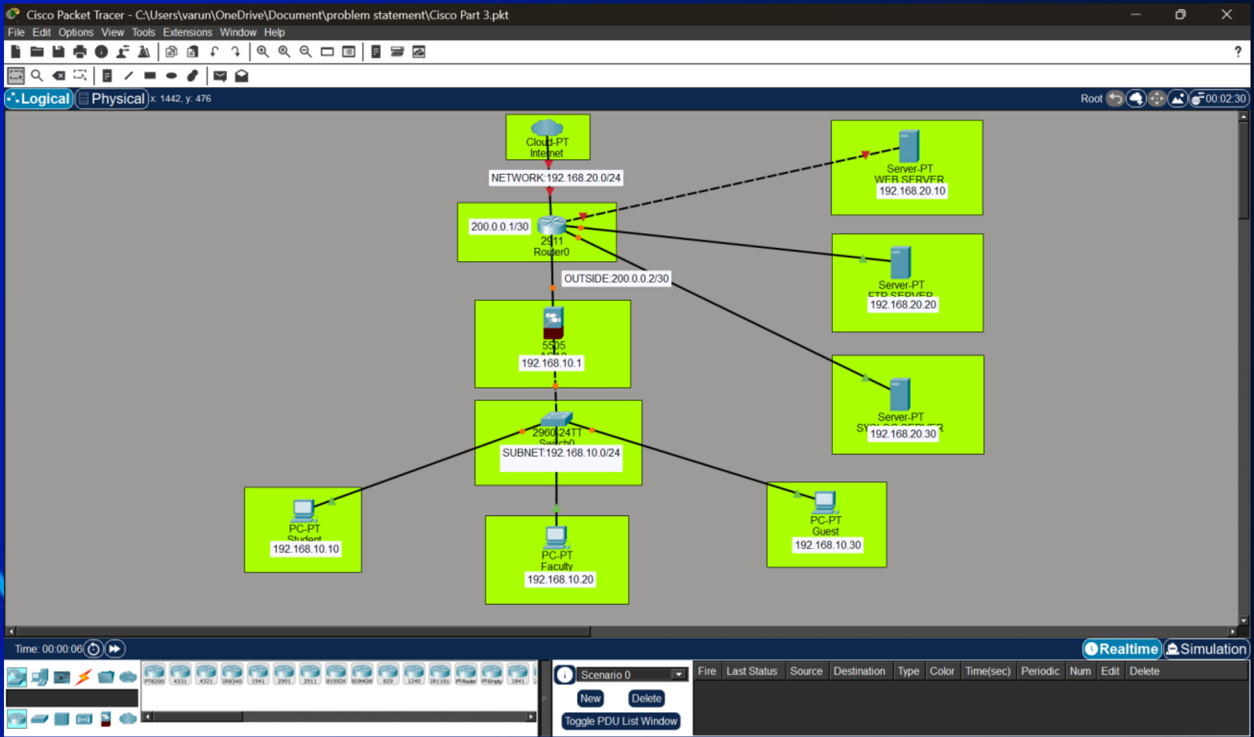
- Allow unrestricted access for research.
- Log entire session activity for auditing

Guest Users

- Only HTTP/HTTPS access.
- Block file sharing, downloads, and internal subnets

3.6 Enforcement Logic

```
IF User = Student AND Time = Class Hours
 → Block: Social Media, Gaming, Torrents
IF User = Faculty
  → Allow All + Log Activity
IF User = Guest
    → Allow Only HTTP/HTTPS
```



CONCLUSION

This extended project demonstrates a full-cycle cybersecurity approach beginning with red-team analysis, followed by secure architecture redesign and finally policy enforcement. Through Cisco Packet Tracer simulations, the redesigned CMRIT Academic Block network showcases improvements in:

- Segmentation
- Authentication
- Access control
- Firewall policies
- Web usage governance

The implemented recommendations significantly enhance the security posture of the institution, making it more resilient to internal misuse and external cyber threats.