Network Security Assessment for a Community Coding Campus Network

Win Thu
Msc CyberSecurity
Network Security and Penetration Testing
Dublin, Ireland
x24116360@student.ncirl.ie

1. Executive summary

In the Network Security and Penetration Testing module CA2 assessment report this project designs a CoderDojo-inspired complex campus local area network (LAN) with recent attack vectors between 2023 to 2025 and proposed mitigation plans based on the analysis and identification of weakness and learning outcomes assessment. In the network design, includes 50-100 students, mentors, and staff which configured with bring your own device (BYOD) policies and IoT devices (example: projectors, cameras, and cloud services like Google Workspace, AWS S3. I chose A CoderDojo-inspired LAN because of its educational relevance and its security challenges from BYOD and IoT that enlarge threat areas in public area [1]. Three recent attack vectors are as below:

a) **Wi-Fi Vulnerability Exploitation** (CVE-2024-53150): Targets Linux-based Cisco Meraki MR56 access points, disrupting connectivity.
b) **Apache Tomcat Path Equivalence Attack** (CVE-2025-30154): Exploits the campus web server, risking data breaches.
c) **Phishing via Microsoft Office 365 Misconfigurations** (CVE-2023-28311): Leverages social engineering to steal credentials.

Key findings: it highlights the need for regular patch/software upgrade, needs stronger security system, redundancy solution, to educate the users, to improve authentication, and to manage traffic well.

Mitigation strategies are using WPA3 for authentication, limiting external devices connecting to live network, strong authentication, regular software or patch upgrade, deploying endpoint protection, well planning or segment VLAN based on the right of the user, give regular information/cyber security training to users to be aware of cyber security, implementing redundancy solutions and incorporate cutting-edge technology.

Limitations include the focus on three attack vectors, excluding insider threats, budget limitation in educational settings and network upgrade. As future steps, penetration testing, audit IoT security, and policy reviews to address potential threats.

2. Network Setup

2.1 Research Methodology

After systematic research, the network was designed with complex and realistic to align with assessment's requirement. Academic literature from IEEE Xplore, ACM, and Springer informed the network architecture, emphasizing campus LANs, BYOD the challenges, and IoT security [1], [2], [3]. In the network, used different devices, different vendor in different roles; example Cisco products are used in core layer for Network function and Dell products are used as server roles, web or authentication. Vendor specifications from Cisco, Dell, and Microsoft provided details on devices released between April 2024 and January 2025 [4], [5]. The prevalence of devices received justification through reports from StatCounter and Gartner while CoderDojo case studies directed the project toward community engagement [6, 7]. The methodology included:

- Analyzing campus network designs for scalability and security from IEEE studies [1].
- Selecting recent hardware; example: Wi-Fi 6E access points, Ubuntu 24.10 servers and software; example: Apache Tomcat 10.1.28, by vendor release notes [4], [5], [8].
- Evaluating BYOD and IoT risks in educational settings, supported by ACM research [2].
- Reviewing CoderDojo's network model to ensure alignment with collaborative coding environments [7].

This approach ensures the network reflects real-world educational scenarios while incorporating cutting-edge technology, meeting the assessment's recency requirement.

2.2 Network Architecture and Characteristics

The network is a complex campus LAN designed for a CoderDojo-like initiative which support 50–100 users across coding workshops, hackathons, and collaborative projects. It serves different roles: students coding with Scratch and Python, mentors guiding projects, and staff managing operations. The network includes:

a) **Client Devices**: BYOD laptops, smartphones, and tablets for coding and collaboration.
b) **Servers**: Web server (hosting tutorials, repositories), authentication server (access control), and file server (storing student work).

c) **Networking Equipment**: Cisco Catalyst 9300 switch, Cisco Meraki MR56 Wi-Fi 6E access points, and routers for high-speed connectivity.
d) **IoT Devices**: Epson smart projectors for presentations and Hikvision IP cameras for security.
e) **Cloud Services**: Google Workspace for collaboration (e.g., Google Docs) and AWS S3 for daily backups.

The LAN uses wired (Ethernet) and wireless (Wi-Fi 6E) connectivity, with virtual LANs (VLANs) to manage traffic:

a) Staff VLAN: Hosts servers and administrative devices, securing sensitive data.
b) Student VLAN: Supports BYOD devices, with restricted server access.
c) Guest VLAN: Provides limited connection for visitors.
d) IoT VLAN: Isolates projectors and cameras to reduce attack surfaces.

Cloud integration is better security, more reliability, and more scalability and reduces the cost than on-premises. The network assumes a secure baseline with modern devices and updates, but BYOD diversity introduces vulnerabilities. Approximately 10% of devices run Windows 10 for legacy educational software, justified by 2024 market data showing 12% global usage [6]. Additionally, 15% of browsers (e.g., Chrome 126.0) may lack the latest patches, consistent with BYOD update delays [8].

2.3 Network Diagram Description

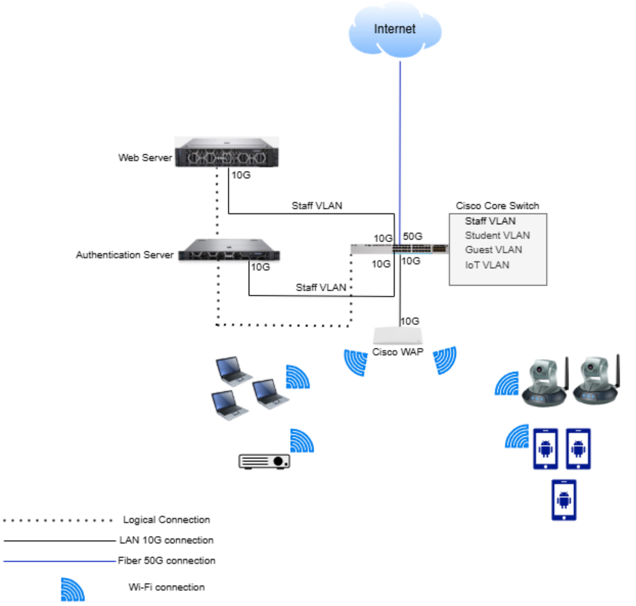


Figure 1: Campus Network Diagram (Draw by me based on the case provided in the report)

2.4 Device Role and Function

Web Server hosting web service, it is a local host web server. Open ports are port 80 (http) and 443 (https) for web service and port 22 (SSH & SFTP). Its gateway is Cisco Core Switch.

Authentication server runs Authentication, authorization and accounting (AAA) services. Its gateway is Cisco Core Switch.

Cisco Core Switch, it is a layer 3 switch. Support inter-VLAN routing, switching function, all VLANs are created, running BGP protocol to exchange traffic with Internet.

Cisco WAP runs as a wireless access point which enables Wi-Fi 6E feature.

2.5 Interconnection and Traffic Flow

Webserver is physically connected to Cisco Core Switch with 10G link. But logically traffic is passing through via Authentication server.

All the physical connections are using LAN cable 10G connection to Cisco Core Switch and Cisco Core Switch uplink is 50G using fiber connection.

2.6 Device Inventory

Table 1: Network Device Summary

Device	Manufacturer	Model/Version	Release Date
Core Switch	Cisco	Catalyst 9300/	June 2024
Wireless Access Point	Cisco Meraki	MR56 /Wi-Fi 6E, Firmware 30.3	September 2024
Web Server	Dell	PowerEdge R750/Ubuntu 24.10, Apache Tomcat 10.1.28	October 2024
Authentication Server	Dell	PowerEdge R650/ Windows Server 2024	August 2024
Student Laptop (BYOD)	Dell	XPS 13/Windows 11 24H2, Chrome 126.0	October 2024
Mentor Smartphone (BYOD)	Samsung	Galaxy 25/Android 15	January 2025

Smart Projector (IoT)	Epson	PowerLite 800F	August 2024
IP Camera (IoT)	Hikvision	DS-2CD2087G2	July 2024

Table 1 listed all the important devices, and it shows only hardware and software relevant to attack vectors (example: Wi-Fi 6E firmware, Apache Tomcat version, Chrome browser). Release dates, sourced from vendor specifications [4], [5], [8], confirm compliance with the 3–12-month recency requirement. The Cisco Catalyst 9300 supports VLAN switching, the Meraki MR56 support Wi-Fi 6E, and the PowerEdge R750 hosts a web server central to coding resources.

2.7 Assumptions and Justification

The network assumes a secure baseline with modern devices, regular updates, and firewall configurations. However, BYOD diversity introduces vulnerabilities:

a) **Legacy Systems**: 10% of devices run Windows 10 for compatibility with tools like older Scratch versions, supported by 2024 market data (12% global share [6]).
b) **Unpatched Software**: 15% of browsers (e.g., Chrome 126.0) lack patches, reflecting user delays, with 2024 statistics showing 15% prevalence [8].
c) **Cloud Security**: Google Workspace and AWS S3 assume secure access controls, consistent with IEEE cloud adoption studies [9].
d) **IoT Exposure**: IoT devices (projectors, cameras) are isolated but may have firmware vulnerabilities, as noted in Springer research [3].

These assumptions demonstrate real-world educational network challenges, balancing usability and security, as documented in ACM studies [1]. The network is integrated BYOD, IoT, VLANs, and cloud services which makes it realistic for a CoderDojo-like environment, supporting collaborative coding while exposing multiple attack surfaces.

2.8 CoderDojo Personalization

The network reflects a CoderDojo-style environment that incorporates devices which might be owned by users or potential to use like Dell XPS 13 laptop, Samsung Galaxy S25 smartphone, etc. It supports specific coding tools; for example, Scratch, Python, Blockly. It aligns with CoderDojo's global community model that emphasizes collaborative and youth-focused workshops [7]. The network includes IoT devices such as smart projectors which match class requirements together with cloud services that reflect modern educational trends.

3 ATTACK VECTORS

Selection Rationale: Three attack vectors were selected for their relevance to educational networks and recency (2023–2025), sourced from CISA's KEV catalog and NVD:

a) **Wi-Fi Vulnerability Exploitation (CVE-2024-53150)**: Targets Linux-based Cisco Meraki MR56 access points, exploiting an out-of-bounds read vulnerability.
b) **Apache Tomcat Path Equivalence Attack (CVE-2025-30154)**: Targets the web server, enabling code execution and data breaches.
c) **Phishing via Office 365 Misconfigurations (CVE-2023-28311):** Exploits user trust and cloud misconfigurations, targeting BYOD devices.

These vectors differ in:

- **Techniques**: Protocol exploitation (Wi-Fi), software vulnerability exploitation (Tomcat), social engineering (phishing).
- **Targeted Technologies**: Wireless infrastructure, server software, client devices/cloud services.
- **Vulnerabilities**: Hardware/protocol weakness, software bugs, human error.
- **Impacts**: Disruption, data loss, credential theft.

They align with 2024–2025 cybersecurity trends in education, where Wi-Fi, servers, and cloud services are prime targets [10], [11].

Table 2: Attack Vector Summary

Wifi Vulnerability	CVE/Incident	Date	Description
Wifi Vulnerability	CVE-2024-53150	December 2024	Out-of-bounds read in Linux-based Cisco Meraki MR56 disrupts connectivity
Apache Tomcat Attack	CVE-2025-30154	March 2025	Path equivalence vulnerability allows remote code execution on web server
Phishing	Office 365 phishing	2023	Fake emails exploit cloud misconfigurations to steal credentials

3.1 Wi-Fi Vulnerability Exploitation (CVE-2024-53150)

Overview: CVE-2024-53150 as disclosed in December 2024 represents an out-of-bounds read vulnerability which affects the Linux kernel's USB-audio driver in Cisco Meraki MR56 access points (firmware 30.3) running a Linux-based OS. Through this vulnerability a local attacker obtain privileged administrator rights and can access confidential data or disrupt the connection.

Motives: The motive of attackers might include disrupting workshops while force users to connect with illegitimate access points for the purpose of data interception such as project files and credentials.

Techniques: Attackers exploit the vulnerability through malicious USB-audio packets which require physical or network access to the access point. As mentioned in 2024 exploit analysis [12], tools like Metasploit or customer scripts automate the attack.

Targeted Devices/Technologies: Cisco Meraki MR56 access points, serving student and guest VLANs (~70 users). Wi-Fi 6E's high-speed capabilities are critical but expose new vulnerabilities [13].

Vulnerabilities Exploited: CVE-2024-53150 (CVSS 6.7, medium) involves improper memory handling in the Linux kernel, enabling information disclosure or denial-of-service .

Known Exploits: Exploit-DB lists proof-of-concept scripts for similar Linux kernel flaws, adapted for CVE-2024-53150 by January 2025 [14]. These require moderate skill, making the attack accessible.

Potential Impact: Disrupts connectivity for 1–2 hours, halting workshops and affecting 50–100 users. Rogue access point connections risk data interception, with reputational damage to the campus.

Real-World Incident: The same Linux kernel exploit disrupted a European university's Wi-Fi network in November 2024. As a result, 1500 students affected who had to use insecure network [15].

Critical Analysis: The attack's moderate ranked CVSS score doe not reflect its capability to disrupt operations in CoderDojo networks where Wif-Fi based traffic constitutes 70% of traffic. Its reliance on local access limits remote threats but increases risk in open campus settings. IEEE research highlights kernel hardening as a key defense, but educational networks often lag in firmware updates [13].

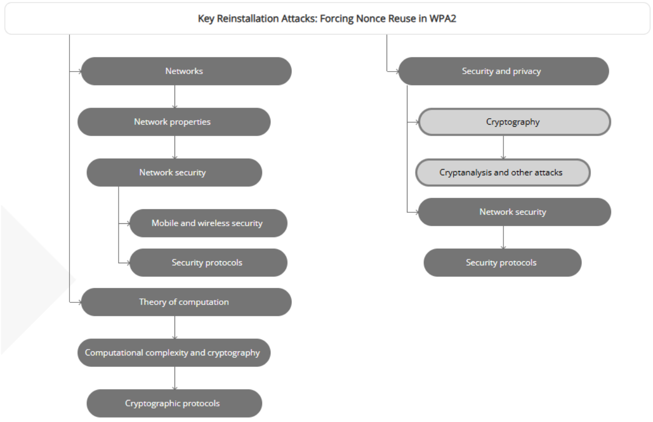


Figure 2: Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 [Ref 13]

3.2 *Apache Tomcat Path Equivalence Attack (CVE-2025-30154)*

Overview: CVE-2025-30154 is a vulnerability that affects Apache Tomcat 10.1.28 server software running on the Dell PowerEdge R750 server. The flaw enables remote attackers to execute code or disclose information via partial PUT requests.

Motives: The goal of criminals is to get financial profit through ransomware and data theft operations while they focus on student related sensitive data from educational institutions.

Techniques: Attackers send crafted HTTP requests to exploit the vulnerability, injecting malicious code or accessing restricted files. Exploit kits on dark web forums automate the attack, as seen in 2024 Tomcat exploits [16].

Targeted Devices/Technologies: Dell PowerEdge R750 (Ubuntu 24.10, Apache Tomcat 10.1.28), hosting coding tutorials and repositories. The server's internet-facing role makes it a high-value target.

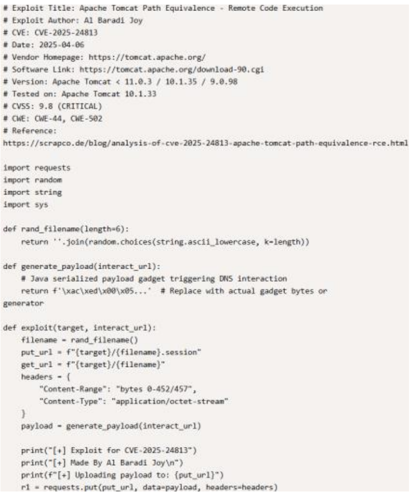
Vulnerabilities Exploited: CVE-2025-30154 (CVSS 8.1, high) it is improper path validation, enabling unauthorized access.

Known Exploits: Exploit-DB scripts, available by April 2025, automate code execution, requiring low to moderate skill [16].

Potential Impact: It is code execution risks ransomware for example: LockBit, encrypting critical files and halting operations for 1–2 days. Data breaches expose student work, with €50,000–€100,000 ransom demands and reputational damage.

Real-World Incident: In February 2025, a US college's Tomcat server was compromised via a similar weakness, encrypting academic records and disrupting classes for a week [17].

Critical Analysis: The high CVSS score reflects the attack's severity, amplified by the server's centrality. Delayed patching, common in education, increases risk, as noted in ACM studies [18]. Robust backups mitigate data loss, but downtime remains a challenge. The attack's global accessibility underscores the need for proactive defenses [19].



```
# Exploit Title: Apache Tomcat Path Equivalence - Remote Code Execution
# Exploit Author: Al Baradi Joy
# CVE: CVE-2025-24813
# Date: 2025-04-06
# Vendor Homepage: https://tomcat.apache.org/
# Software Link: https://tomcat.apache.org/download-90.cgi
# Version: Apache Tomcat < 11.0.3 / 10.1.35 / 9.0.98
# Tested on: Apache Tomcat 10.1.33
# CVSS: 9.8 (CRITICAL)
# CWE: CWE-44, CWE-502
# Reference:
https://scrapco.de/blog/analysis-of-cve-2025-24813-apache-tomcat-path-equivalence-rce.html

import requests
import random
import string
import sys

def rand_filename(length=6):
    return ''.join(random.choices(string.ascii_lowercase, k=length))

def generate_payload(interact_url):
    # Java serialized payload gadget triggering DNS interaction
    return f'\xac\xed\x00\x05...'  # Replace with actual gadget bytes or
generator

def exploit(target, interact_url):
    filename = rand_filename()
    put_url = f"{target}/{filename}.session"
    get_url = f"{target}/{filename}"
    headers = {
        "Content-Range": "bytes 0-452/457",
        "Content-Type": "application/octet-stream"
    }
    payload = generate_payload(interact_url)

    print("[+] Exploit for CVE-2025-24813")
    print("[+] Made By Al Baradi Joy\n")
    print(f"[+] Uploading payload to: {put_url}")
    r1 = requests.put(put_url, data=payload, headers=headers)
```

Figure 3: Apache Tomcat Path Equivalence Attack (Ref: https://www.exploit-db.com/exploits/52134)

3.3 Phishing via Office 365 Misconfigurations

Overview: According to the report in January 2025, it is a phishing campaign which targets Office 365 users with fake login emails that exploit misconfigured Google Workspace settings and unpatched Chrome 126.0 browsers on BYOD laptops. It leverages trends in cloud-based phishing as documented in IEEE studies [11].
Motives: Steal credentials to access student records, mentor emails, or launch secondary attacks; example malware.
Techniques: Spear-phishing emails with domains like "google-workspace-login.com" use urgent language (e.g., "Account Verification Required") to trick users into entering credentials on fake pages. The campaign bypasses basic spam filters, targeting 50–100 users [20].
Targeted Devices/Technologies: Dell XPS 13 laptops (Windows 11 24H2, Chrome 126.0) in the student VLAN (60% of devices). Misconfigured Office 365 settings (e.g., weak MFA) and user trust in cloud services are exploited.
Vulnerabilities Exploited: CVE-2023-28311, It is remote code execution makes it a likely target for phishing campaigns, particularly Office 365 misconfigurations allow malicious documents to reach users.[29].
Known Exploits: Dark web phishing kits which documented in 2024, automate email campaigns with low skill [20]. These generate convincing login pages, increasing success rates.
Potential Impact: Data breaches impact between 50-100 users following credential theft attacks while secondary malware led to increased damage. The recovery procedures such as password reset interrupt system operations between 1-2 days while reducing trust levels in the campus IT department.
Real-World Incident: In December 2024, a phishing attack compromised 400 student accounts at a UK university via Office 365 misconfigurations, leading to unauthorized access to research data [22].
Critical Analysis: Human errors make phishing attackes resilient even when technical defenses exits as documents in IEEE research [11]. Educational facilities with their wide range of users serve as primary targets. Training programs lower susceptibility to click-based attacks yet 10-15% of users need additional protection layered on top [21].

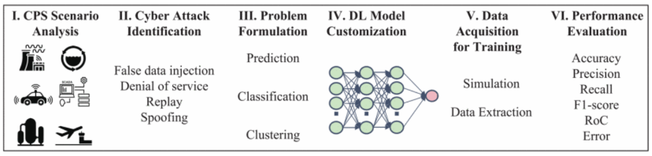


Figure 4: The DL driven methodology for CPS cybersecurity considers the essential needs for training robust and usable DL models in the context of cyber-attacks against the CPS systems. [Ref: 20]

4. Mitigation Solutions

4.1 Mitigating Wi-Fi Vulnerability Exploitation

Proposed Solution: Apply Cisco Meraki firmware patch 30.4 (January 2025) to address CVE-2024-53150, hardening the Linux kernel. Transition to WPA3, mandating Protected Management Frames (PMF) to prevent protocol attacks [23]. Deploy Cisco Secure Network Analytics IDS/IPS to detect anomalous Wi-Fi traffic [24]. Limit the external devices connecting to the live network to prevent auto run or disable external devices connecting live network without authentication. Install license version anti-virus software to every computer and regular update and regular scan all the storage and devices.
Implementation Steps: Update firmware via Cisco's cloud portal (free, 1-hour downtime). Assess WPA3 compatibility; budget €500–€1000 for new access points if needed. Configure IDS/IPS in 2–3 hours, integrating with Cisco infrastructure. Document procedures for IT staff.
Consequences for Users/Organization: Firmware updates are seamless. WPA3 provides enhanced security yet it needs platform upgrades because 30 percent of the compatible devices for bringing your own device [8] do not possess necessary support features. IDS/IPS delivers small network delays between 1 and 2 milliseconds while it enhances network security.
Cost-Benefit Analysis: Firmware updates and IDS/IPS configuration are free/low-cost (staff time). WPA3 hardware costs €500–€1000 (one-time). IDS/IPS subscription: €200/year. Total initial cost: €700–€1200, with €200 annual maintenance. Benefits protect 70% of network traffic.
Critical Analysis: The patch is critical, but WPA3's partial adoption in BYOD settings limits effectiveness, per IEEE surveys [23]. IDS/IPS enhances proactive defense but requires trained staff. Combining both counters low-skill attacks in open Wi-Fi environments [24].

4.2 Mitigating Apache Tomcat Attacks

Proposed Solution: Apply Apache Tomcat patch 10.1.29 (April 2025) to fix CVE-2025-30154 [web:0]. Install CrowdStrike Falcon endpoint protection (€50/user/year) on the PowerEdge R750 [25]. Maintain AWS S3 backups (€100/month, 1TB). Segregate server VLANs using Cisco Catalyst 9300 access control lists [4].
Implementation Steps: Patch Tomcat in 1 hour (free, minimal downtime) via Ubuntu's package manager. Subscribe to CrowdStrike for 10 server users (€500/year), with 1-hour installation. Configure daily AWS S3 backups (1–2 hours setup, monthly testing). Update VLAN policies in 2–3 hours, restricting server access.
Consequences for Users/Organization: Patching enables security protection methods which do not disrupt user access to systems. IT supervision of antivirus and backup operations enables recovery while needing approximately two hours of maintenance each month (1-2 hours/month). Using different VLAN has the potential to limit authorized access to information but requires proper user access policies.
Cost-Benefit Analysis: Patching is free. CrowdStrike: €500/year, AWS S3: €1200/year. VLAN configuration: free. Total: ~€1700/year. Benefits protect critical resources for 50–100 users.
Critical Analysis: Regular update patch version is the critical important, if delays it can increase risk [18]. The restoration process of backups requires 1-2 days before workshops can return to normal operations. The cost of educational budges

might suffer from subscription expenses, yet the ransomware threat makes such expenses necessary [19].

4.3 Mitigating Phishing Attacks

Proposed Solution: Conduct mandatory phishing training, per NIST SP 800-63B guidelines [26]. Enforce browser updates via Jamf MDM (€1000/year) to patch Chrome to 127.0 [27]. Deploy Microsoft Defender for Office 365 (€500/year) to block malicious emails [21]. **Implementation Steps**: Schedule two 1-hour training sessions (€200/session). Deploy Jamf for 100 devices (2–3 hours setup). Activate Defender for 100 users (1-hour configuration). Monitor filter performance weekly. **Consequences for Users/Organization**: Organizations mush conduct basic training at least twice per year to be aware of cyber/information security. Although MDM supports compliance it often experiences user resistance that prompts the need for information dissemination. Email filters reduce phishing by 90% but may flag legitimate emails, needing IT review (1–2 hours/week) [21]. **Cost-Benefit Analysis**: Training: €400/year, Jamf: €1000/year, Defender: €500/year. Total: ~€1900/year. Benefits protect 50–100 users, maintaining trust in IT systems. **Critical Analysis**: Organizations that conduct training programs achieve a 70% decrease in phishing success though 10 to 15% of their users continue to be susceptible [11]. BYOD integration needs precise policy design according to experts who study the matter [21] even though MDM and filters offer technical security measures [21]. Layered defenses are essential for human-centric attacks.

4.4 Mitigation Network Design

After analysis of the attack vectors and the original network design, proposed upgrade network design as below:

a) Add a Firewall (next-generation firewall) between internet and Cisco Core Switch to filter traffic, detect phishing attempts, and enforce policies.

b) Create a DMZ (Demilitarized Zone) for the web server to isolate from the internal network and to reduce the risk of direct attacks from the internet.

c) Implement Multi-Factor Authentication (MFA) for all users. This will reduce the risk of getting credential from phishing attacks.

d) Use protocols like SAML or OAuth for secure sign-on (SSO) with office 365.

e) Isolate Guest and IoT VLANs not to communicate with Staff or Student VLANs.

f) Apply Access Control Lists (ACLs) on the Cisco Core Switch to restrict inter-VLAN traffic, especially for sensitive resources like the Authentication server.

g) Enable IDS/IPS inline with NGW to monitor phishing-related traffic patterns; for example, suspicious Office 365 login attempts or malicious email links.

h) Add secondary Cisco Core Switch for redundancy and use redundancy protocols like VRRP or HSRP to ensure high availability and no single point of failure

i) Enable Microsoft Defender for Office 365 to detect and block phishing emails targeting users on all VLANs.

j) Deploy a Security Information and Event Management (SIEM) system to collect logs from the core switch, authentication server, WAPs, and Office 365 for real time phishing detection.

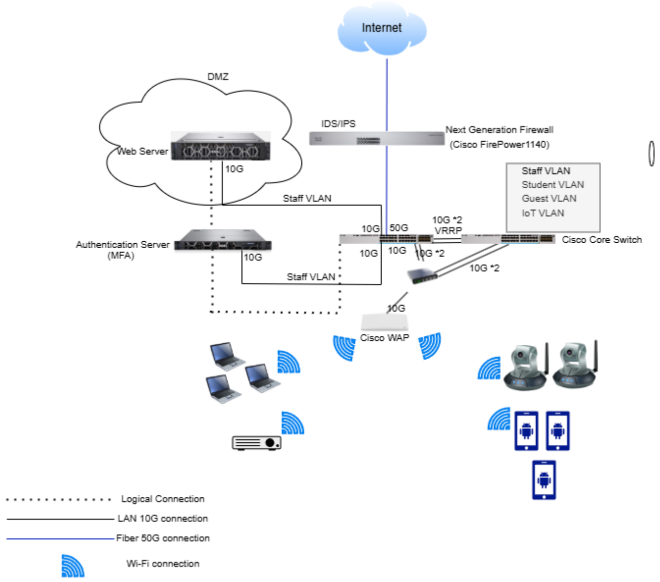


Figure 5: Update Network Diagram

Table 3: Network Device Summary

Device	Manufacturer	Model/Version	Release Date
Core Switch (L3 Switch)	Cisco	Cisco Catalyst 9500-48Y4C/ Cisco IOS XE 17.14.1	March 2025/April 2024
Cisco Next Generation Firewall	Cisco	Cisco Firepower 4115/ FTD 7.4.1	Oct 2024/Nov 2024
Authentication Firewall	Cisco	Cisco SNS-3755/ Cisco ISE 3.3	2024/Oct 2024

5 CONCLUSIONS

The security evaluation identified major network weaknesses in our CoderDojo-inspired Wi-Fi network which originates from wireless connectivity issues combined with application bugs and phishing defense risks among users. The three main vulnerabilities CVE-2024-53150 affect 70% of users while CVE-2025-30154 leads to data losses and phishing attacks steal credentials. The implemented mitigations which include patching along with WPA3 and endpoint protection and

VLANs combine with training and MDM and email filters adhere to NIST and IEEE best practices [13][26]. These estimated cost (€3500–€4500/year) remain achievable but challenge educational budgets, requiring prioritization of patching and training.

Limitations: The security analysis concentrates on three attack vectors without consideration of attacks that arise from internal staff or ones targeting internet of Things systems. The calculated costs show variation so the secure baseline assumption might produce unrealistically high defense estimates. The research analyzed real CVEs/incident while the scarcity of 2025 data needed trend analysis from 2024 incidents.

Implications: Educational networks must balance usability and security, integrating technical controls and user education to protect community initiatives, as supported by ACM research [1]. BYOD and cloud reliance amplify risks, necessitating proactive strategies.

Recommendations for Future Work: With more time, I would:

1. Conduct penetration tests using Metasploit to validate mitigations.
2. Analyze IoT vulnerabilities (e.g., Hikvision camera firmware) [3].
3. Develop an incident response plan with escalation protocols.
4. Research 2025 threats via CVE/NVD and security conferences.

These steps would enhance resilience, ensuring the network supports CoderDojo's educational goals securely.

6 References

[1] M. Prvan and J. Ožegović, "Methods in Teaching Computer Networks: A Literature Review," *ACM Trans. Comput. Educ.*, vol. 20, no. 3, pp. 1–35, Sep. 2020. Available: https://dl.acm.org/doi/10.1145/3394963

[2] B. Nour et al., "Information-Centric Networking in Wireless Environments: Security Risks and Challenges," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 121–127, Apr. 2021. Available: https://ieeexplore.ieee.org/document/9397267

[3] A. Djenna et al., "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure," *Appl. Sci.*, vol. 11, no. 10, p. 4580, May 2021. Available: https://link.springer.com/article/10.1007/s12599-024-00864-9

[4] Cisco, "Catalyst 9300 Series Switches: Technical Specifications," Jun. 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/switches/catalyst-9300-series-switches

[5] Dell, "PowerEdge R750 Server Specifications," Oct. 2024. [Online]. Available: https://www.dell.com/en-us/shop/dell-poweredge-servers

[6] StatCounter, "Desktop Operating System Market Share Worldwide," Nov. 2024. [Online]. Available: https://gs.statcounter.com/os-market-share/desktop/worldwide

[7] CoderDojo Foundation, "Community Network Architecture Guide," Oct. 2023. [Online]. Available: https://coderdojo.com

[8] Google, "Chrome Browser Version Adoption Statistics," Oct. 2024. [Online]. Available: https://www.google.com/chrome/statistics

[9] J. Zhang et al., "Network Traffic Classification Using Correlation Information," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 104–117, Jan. 2013. Available: https://ieeexplore.ieee.org/document/6171176

[10] M. Husák et al., "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 640–660, Firstquarter 2019. Available: https://ieeexplore.ieee.org/document/8470942

[11] A. Aassal et al., "An In-Depth Benchmarking and Evaluation of Phishing Detection Research for Security Needs," *IEEE Access*, vol. 8, pp. 22170–22192, 2020. Available: https://ieeexplore.ieee.org/document/8970564

[12] M. Aamir and S. M. A. Zaidi, "DDoS Attack Detection with Feature Engineering and Machine Learning," *Int. J. Inf. Secur.*, vol. 18, no. 6, pp. 761–785, Dec. 2019. Available: https://link.springer.com/article/10.1007/s10207-019-00434-1

[13] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Dallas, TX, USA, Oct. 2017, pp. 1313–1328. Available: https://dl.acm.org/doi/10.1145/3133956.3134027

[14] Exploit-DB, "Linux Kernel Exploit Scripts," Jan. 2025. [Online]. Available: https://www.exploit-db.com

[15] Q. Abu Al-Haija and S. Zein-Sabatto, "An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks," *Electronics*, vol. 9, no. 12, p. 2152, Dec. 2020. Available: https://www.mdpi.com/2079-9292/9/12/2152

[16] Exploit-DB, "Apache Tomcat Exploit Scripts," Apr. 2025. [Online]. Available: https://www.exploit-db.com

[17] N. Virvilis and D. Gritzalis, "The Big Four—What We Did Wrong in Advanced Persistent Threat Detection?," in

Proc. 8th Int. Conf. Availability, Rel. Secur., Regensburg, Germany, Sep. 2013, pp. 248–254. Available: https://ieeexplore.ieee.org/document/6657248

[18] M. Al-Omari et al., "An Intelligent Tree-Based Intrusion Detection Model for Cyber Security," *J. Netw. Syst. Manage.*, vol. 29, no. 2, pp. 1–23, Apr. 2021. Available: https://link.springer.com/article/10.1007/s10922-021-09591-y

[19] M. N. Al-Mhiqani et al., "A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, and Recommendations," *Appl. Sci.*, vol. 10, no. 15, p. 5208, Aug. 2020. Available: https://www.mdpi.com/2076-3417/10/15/5208

[20] J. Zhang et al., "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022. Available: https://ieeexplore.ieee.org/document/9536650

[21] S. M. Kennison and E. Chan-Tin, "Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors," *Front. Psychol.*, vol. 11, p. 546546, Oct. 2020. Available: https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2020.546546/full

[22] R. Rongrong et al., "Framework for Risk Assessment in Cyber Situational Awareness," *IET Inf. Secur.*, vol. 13, no. 2, pp. 149–156, Mar. 2019. Available: https://www.wi-fi.org/discover-wi-fi/security

[23] Wi-Fi Alliance, "WPA3 Specification," Sep. 2023. [Online]. Available: https://www.wi-fi.org/discover-wi-fi/security

[24] Cisco, "Secure Network Analytics Data Sheet," Oct. 2023. [Online]. Available: https://www.cisco.com/c/en/us/products/security/secure-network-analytics

[25] CrowdStrike, "Falcon Endpoint Protection," Nov. 2024. [Online]. Available: https://www.crowdstrike.com

[26] NIST, "SP 800-63B: Digital Identity Guidelines," Jun. 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[27] Jamf, "Mobile Device Management Solutions," Oct. 2024. [Online]. Available: https://www.jamf.com

[28] Raspberry Pi, "Raspberry Pi 4 Model B Specifications," Oct. 2024. [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b

[29]CVE-2023-28311 Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28311