***1.Title:***

Cyber Shield – Network Security Assessment

***2. Network Overview***

*Write:*

*“This is a college network with routers, switches, servers, PCs, and access points. It has zones for students, faculty, guests, and a DMZ****.”***

***3. Device List***

*Make a table like this:*

*| Device Name | Type | Zone |*

*| ISP | Router | External |*

*| R\_EDGE | Router | Edge |*

*| SW\_CORE | Switch | Core |*

*| SRV\_DC | Server | Core |*

*| Server1 | Server | DMZ |*

*| WEB\_DMZ | Access Point | DMZ |*

*| PC\_STUD | PC | Student |*

*| PC\_FAC | PC | Faculty |*

*| PC\_GUEST | Laptop | Guest |*

***4. Security Controls***

*Write:*

*- Firewall between DMZ and Core*

*- IDS/IPS watching traffic*

*- Authentication server for login*

***5. Attack Surface***

*Write:*

*- Guest PC can reach Core Zone (bad!)*

*- No VLANs to separate zones*

*- No ACLs (Access Control Lists)*

***6. Recommendations***

*Write:*

*- Add VLANs to separate zones*

*- Use ACLs to block unwanted traffic*

*- Use strong passwords*

*- Monitor traffic with ID*

***Phase 1 :***

This phase covers the full setup of tools, version control, and initial network configuration for the WEB\_DMZ zone. All components have been successfully installed, configured, and validated.

🔷 PHASE 1: Setup & Installation

✅ Step 1: Install Cisco Packet Tracer

- Logged into Cisco NetAcad

- Enrolled in Cybersecurity Essentials course

- Downloaded and installed Cisco Packet Tracer

- Verified installation by launching a blank project

🔷 PHASE 1: WEB\_DMZ Configuration

🔹 Device Overview

| Attribute | Value |

| Device Name | WEB\_DMZ |

| Device Type | AccessPoint-PT-N |

| Role | DMZ wireless access point |

🔹 Port 0 (Wired Interface)

| Setting | Value |

| Port Status | ON |

| Bandwidth | 100 Mbps |

| Duplex Mode | Half Duplex |

| VLAN Assignment | VLAN 50 |

| IP Address | 192.168.50.10 |

| Subnet Mask | 255.255.255.0 |

| Default Gateway | 192.168.50.1 |

✅ Verified connectivity via ping from router and VLAN 50 clients.

🔹 Port 1 (Wireless Interface)

| Setting | Value |

| Port Status | ON |

| SSID | WEB\_DMZ\_WiFi |

| 2.4 GHz Channel | 6 |

| 5 GHz Channel | 112 |

| Coverage Range | 250 meters |

| Authentication | WPA2-PSK |

| PSK Passphrase | CyberShield2025! |

| Encryption Type | AES (if available) |

✅ Wireless security configured and tested with client connection.

🔹 Network Integration

- Switch Port VLAN Configuration:

interface FastEthernet0/x

switchport mode access

switchport access vlan 50

- Router Subinterface for VLAN 50:

- IP: 192.168.50.1

- Inter-VLAN routing enabled

🔹 Validation Summary

- ✅ Ping test successful

- ✅ Wireless client connected securely

- ✅ SSID broadcast verified

- ✅ VLAN segmentation confirmed

- ✅ Security posture hardened