Project: Cyber Shield Internship – Cisco Packet Tracer Network Defense

Submitted by KSHITIJ PAWAR

Date: August 2025

Tools Used: Cisco Packet Tracer, Markdown, GitHub, CLI

🔑 Overview

Phase 2 focused on auditing and hardening the network topology across all zones, with special emphasis on the DMZ web server. The goal was to identify vulnerabilities, implement layered security controls, and simulate external threats to validate the network's resilience.

 Part 1: **Security Assessment Summary**

🔎 Network Zones Audited

- Student Zone (VLAN 10)

- Faculty Zone (VLAN 20)

- Guest Zone (VLAN 30)

- Core Zone (VLAN 99)

- DMZ Zone (VLAN 50)

🔐 **Key Findings**

| Zone | Vulnerability Identified | Recommended Control |

| Guest | Open access to internal VLANs | ACL to restrict inter-VLAN traffic |

| Faculty | No endpoint firewall | Host-based firewall configuration |

| DMZ | Web server exposed to all zones | Isolate via ACL and DMZ segmentation |

| Core | No logging or monitoring | Enable syslog and SNMP traps |

🗂 ACL Implementation

- Inbound ACLs on router interfaces to block unauthorized access

- Outbound ACLs to limit data exfiltration from sensitive zones

- Explicit deny statements for Guest-to-Core and Guest-to-DMZ traffic

📡 Wireless Security

- Configured Access Point-PT-N in DMZ

- Enabled WPA2-PSK with strong passphrase

- Assigned to VLAN 50 (WEB_DMZ)

🔧 Part 2**: DMZ Hardening & Attack Simulation**

🛠️ DMZ Web Server Hardening

- Firewall ACLs applied to restrict HTTP/HTTPS access to external users only

- Static IP binding and MAC filtering enabled

- Disabled unused services (FTP, Telnet)

- Configured logging for access attempts and errors

□ Attack Simulation

| Attack Type | Source Zone | Outcome | Mitigation Verified |

| Ping Flood (DoS) | Guest | Dropped by ACL | ✅ Yes |

| Spoofed HTTP Req | Student | Blocked by DMZ ACL | ✅ Yes |

| Unauthorized SSH | Faculty | Denied by firewall | ✅ Yes |

📊 **Impact Analysis**

- No data breach observed during simulated attacks

- DMZ remained isolated from internal zones

- Firewall and ACLs successfully enforced zone boundaries

- Wireless access restricted to authorized devices only

✅ Conclusion

The Phase 2 implementation significantly improved the network's security posture. All zones are now segmented with ACLs, the DMZ is hardened against external threats, and wireless access is secured. The simulated attack