Cybersecurity Audit Report

Prepared by: Pooja Sharma | Freelance Cybersecurity Analyst

1. Executive Summary

This audit was conducted to evaluate the security posture of the client's infrastructure including AWS, Office 365, and on-premise systems. The objective was to identify vulnerabilities, assess security controls, and recommend improvements.

2. Scope and Methodology

The scope included:

- AWS IAM and S3 configurations
- Office 365 email security settings
- Endpoint and network configurations

Tools used: Nmap, Wireshark, AWS CLI, Microsoft Secure Score, Splunk

Methodology: Vulnerability scanning, configuration review, log analysis, phishing simulation.

3. Key Findings

- S3 buckets with public access permissions
- MFA not enforced for Office 365 users
- Weak email filtering rules - phishing emails bypassed filters
- Excessive permissions assigned to IAM users
- Lack of centralized logging for Windows endpoints

4. Recommendations

- Apply least-privilege IAM policies and enable MFA for all users
- Restrict public access to S3 buckets
- Update Office 365 policies to enhance anti-phishing protection
- Configure Splunk or centralized logging for all endpoints

- Regularly audit access controls and perform phishing awareness training

5. Appendix

- Tools: Nmap, AWS CLI, Wireshark, Microsoft Secure Score, Splunk
- Platforms: AWS, Office 365, Windows 10
- Audit Date: March 2025
- Analyst: Pooja Sharma