Cybersecurity Risk Assessment Report

Organization: ABC Startup Company

Date: August 1, 2024

Prepared by: Darlene Opeña

Scope and Objectives

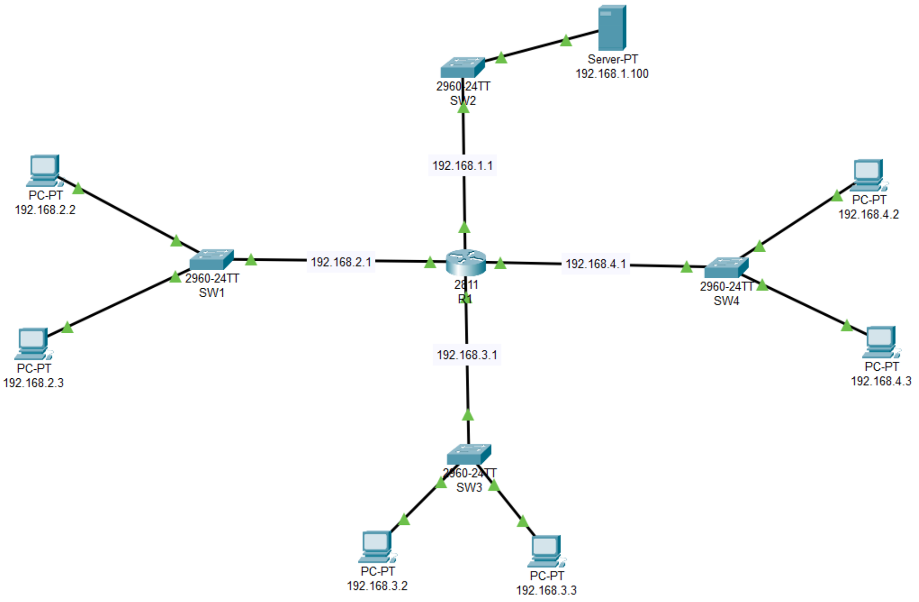
Scope:

- Systems
  - Internal Network
  - Server
  - PC's
  - Connected Devices
- Data
  - Network Traffic
  - Configurations
  - User Access Information

Objectives:

- Identify and evaluate cybersecurity risks.
- Prioritize risks on impact and likelihood.
- Recommend mitigation strategies to enhance security.

Network Diagram/Topology



Subnets and Connected Nodes:

- Subnet 192.168.1.10/24
  - Server: 192.168.1.100
  - Router: 192.168.1.1
  - Switch: SW2
- Subnet 192.168.2.0/24
  - PC: 192.168.2.2
  - PC: 192.168.2.3
  - Router: 192.168.2.1
  - Switch: SW1
- Subnet 192.168.3.0/24
  - PC: 192.168.3.2
  - PC: 192.168.3.3
  - Router: 192.168.3.1
  - Switch: SW3
- Subnet 192.168.4.0/24
  - PC: 192.168.4.2
  - PC: 192.168.4.3
  - Router: 192.168.4.1
  - Switch: SW4

Threat Identification

Objective:

- Identify potential threats that could exploit vulnerabilities within the network.

Identified Threats:

- Unauthorized Access
  - Potential for attackers to gain unauthorized entry into the network.
- Data Breach
  - Unauthorized access to sensitive information.
- Insider Threat
  - Malicious actions by employees or individuals with access to the network.
- DDoS Attack
  - Distributed denial of service attacks that could overwhelm network resources.
- Man-in-the-Middle Attacks
  - Interception of data transmission between network devices.

Vulnerability Scanning

Objective:

- Used Nmap tool to identify vulnerabilities within the network that could be exploited by threats.

Nmap Scan Result:

- Live Host = 8

Ping Scan:

- All host are up (6 PC's and 1 server).

Service Version Detection:

- All ports are using Apache HTTP Server 2.4.18.

Port Scan:

- All the scanned devices show common open ports most notable will be the HTTP or port 80 and HTTPS or the port 443, which indicates that web services are active.

Identified Vulnerabilities:

Vulnerability	Description	Severity	Potential Impact
Default Password	Use of default credentials on network devices	High	Unauthorized access, data breaches
Lack of Encryption	Insufficient encryption for data in transit and at rest	High	Data interception, MitM attacks
Inadequate Access Controls	Weak access control policies and insufficient role-based access controls	High	Unauthorized access, insider threats
Single Point of Failure	Central server without redundancy	Medium	Network downtime
No IDS/IPS	Absence of intrusion detection systems and intrusion prevention systems	High	Undetected and unmitigated attacks

---

Risk Analysis

Objective:

- Evaluate the likelihood and impact of identified threats exploiting vulnerabilities.

Risk	Likelihood	Impact	Risk Rating	Description
Unauthorized Access	High	High	High	Default passwords and weak access controls
Data Breach	Low	Very High	High	Insufficient encryption and access controls

Insider Threat	Medium	High	Medium	Weak access control policies
DDoS Attack	Medium	Medium	Medium	Limited bandwidth and no DDoS mitigation
Man-in-the-Middle Attack	Medium	High	High	Lack of Encryption for data in transit

---

Mitigation Strategies

Objective:

- Recommend strategies to mitigate identified risks.

Risk	Mitigation Strategy	Responsible Party
Unauthorized Access	Implement strong passwords and multi-factor authentication	IT Department
Data Breach	Implement strong encryption (AES-256) and enhance access controls	Security Team
Insider Threat	Enhance access control policies and conduct regular audits	Security Team
DDoS Attack	Increase network bandwidth and deploy DDoS mitigation solutions	Network Team
Man-in-the-Middle Attack	Implement encryption (TLS) for data in transit	IT Department

---

Comprehensive Report

The purpose of this cybersecurity risk assessment is to identify potential threats, vulnerabilities, and risks within the network topology of ABC Startup Company. This report details the assessment process, findings, and recommended mitigation strategies.

Threat Identification:

Using industry-standard methodologies, the following threats were identified: unauthorized access, data breaches, insider threats, DDoS attacks, and MitM attacks.

Vulnerability Scanning:

Vulnerability scanning was conducted using Nmap. Key vulnerabilities identified include default passwords, lack of encryption, inadequate access controls, single points of failure, and the absence of IDS/IPS.

Risk Analysis:

Each identified risk was evaluated based on its likelihood and potential impact. High-risk areas include unauthorized access, and data breaches. Mitigation strategies have been prioritized accordingly.

Mitigation Strategies:

A detailed mitigation plan has been developed to address each identified risk. This includes implementing strong passwords, deploying encryption, enhancing access controls, increasing network bandwidth, and deploying DDoS mitigation solutions.

This cybersecurity risk assessment highlights critical areas requiring immediate attention to enhance the security posture of ABC Startup Company. Implementing the recommended mitigation strategies will significantly reduce the identified risks and improve overall network security.

Next Steps:

- Begin implementation of mitigation strategies.
- Conduct regular security audits and vulnerability assessments.
- Ensure continuous monitoring and improvement of security measures.