1/24/2024

Task 1
Risk Assessment

Martin Phetla
INTERN CAREER

Introduction

Welcome to our cybersecurity risk assessment project!

In this initiative, we're taking a close look at the security of our computer network. The network is like a hub that connects our computers, phones, and printers, making it crucial to ensure it's safe from potential threats.

We're focusing on identifying possible problems like unauthorized access (people getting into our system without permission), unpatched software (outdated programs), firewall issues, physical security concerns, denial of service attacks, insecure remote access, and risks related to social engineering.

To dig deeper, we're using tools like Nmap to scan our network for vulnerabilities. The results will help us see where our network might be weak and what impact it could have on our system.

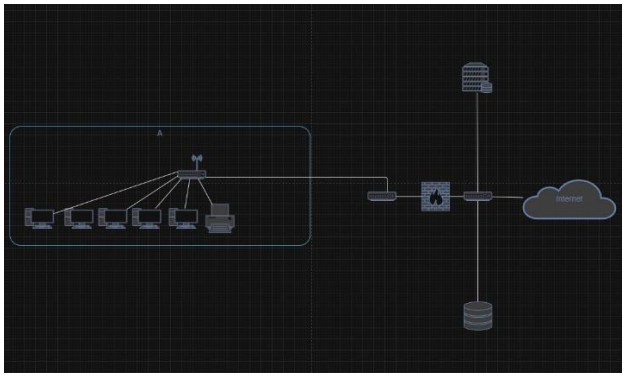
After identifying vulnerabilities, we'll analyze the risks they pose and prioritize them based on how severe they are and how likely they are to happen. Then, we'll come up with plans to fix or mitigate the high-risk issues. Our goal is to make our network more secure by addressing these concerns.

This document will be a detailed record of our assessment process, findings, and suggestions for making things safer. Additionally, we'll create a presentation to share the key points with everyone involved in keeping our network secure. Let's work together to strengthen our defenses in the digital world!

Methodology

In conducting the cybersecurity risk assessment for my network, I employed a systematic approach to comprehensively evaluate the security of the setup. The methodology encompassed the following key steps:

Network Overview:



I began by providing an insightful overview of my network infrastructure:

- Router: Serving as the central hub, the router connects laptops, cell phones, and printers.
- Switch 1: Links the router to the firewall, forming a crucial connection point.
- Firewall: Ensures secure connections, safeguarding the network from potential threats.
- Switch 2: Acts as the gateway to the internet, external storage, and more.

Tools Used:

NMAP Vulnerability Scanning:

Commencing with NMAP 7.94 on at 2024-01-17 15:36 South Africa Standard Time, the scan provided key insights into potential vulnerabilities within my network. Here's a breakdown of the findings:

Finding & ***Risk Analysis***

1. **Unpatched Software:**
    - Vulnerability: Delayed or missed software updates.
    - Severity: Medium.
    - Potential Impact: Risks associated with the exploitation of known vulnerabilities, compromising the integrity of the system.
2. **Firewall Configurations:**
    - Vulnerability: Misconfigured firewall rules.
    - Severity: High.
    - Potential Impact: Risks include unauthorized access, data leakage, and compromised overall network security.
3. **Physical Security:**
    - Vulnerability: Lack of physical access controls.
    - Severity: Medium.
    - Potential Impact: Risks involve unauthorized access, tampering, or potential theft of hardware.
4. **DoS Attacks:**
    - Vulnerability: Insufficient protection against Denial-of-Service attacks.
    - Severity: High.
    - Potential Impact: Risks include the disruption of network services, downtime, and resource exhaustion.
5. **Insecure Remote Access:**
    - Vulnerability: Weak or unsecured remote access methods.
    - Severity: High.
    - Potential Impact: Risks encompass unauthorized access, data interception, and the compromise of remote systems.
6. **Phishing & Social Engineering:**
    - Vulnerability: Lack of user awareness and training.
    - Severity: High.
    - Potential Impact: Risks involve unauthorized access, data breaches, and the compromise of sensitive information.

Mitigation Strategies:

To make our network safer based on the identified problems, we've come up with simple plans:

1. Unauthorized Access:

- **Make Strong Passwords:**
    - People need to use strong and complicated passwords. They should change them regularly.
    - Add an extra layer of security by using more than just a password (multi-factor authentication).

2. Unpatched Software:

- **Keep Everything Updated:**
    - Set up a regular schedule to update all our software.
    - Use tools that automatically update our software to make it easier.

3. Firewall Configurations:

- **Check and Update Firewall Settings:**
    - Review and update the rules in our firewall to make sure they are secure.
    - Keep an eye on changes in the rules and make sure they are still needed.

4. Physical Security:

- **Control Physical Access:**
    - Use systems like key cards or fingerprints to control who can get into our physical spaces.
    - Regularly check and fix any issues with physical security, like broken locks or cameras.

5. DoS Attacks:

- **Stop Overloading:**
    - Use special systems to notice and stop attacks that try to overload our network.
    - Have backup plans and extra systems to handle network traffic during attacks.

6. Insecure Remote Access:

- **Secure Remote Connections:**
    - Make sure people connecting remotely use secure and encrypted methods, like VPNs.
    - Ask for strong passwords and extra security steps when connecting remotely.

7. Phishing & Social Engineering:

- **Train People to Spot Tricks:**
    - Teach everyone how to recognize fake emails or messages that try to trick them.
    - Use tools to filter out suspicious emails before they reach our systems.

How We'll Do It:

- Start with the most urgent problems and fix those first.
- Get a team to take charge and make sure these plans happen.
- Keep checking and testing our security regularly.
- Teach everyone in our team to be careful and know how to spot potential issues.

These plans are like a guide to make our network safer. We'll keep learning and making things better to stay protected from potential problems.