Andree Salvo

Southern New Hampshire University

CYB 310 - 6-1 Project One Submission: Network Evaluation Report

Instructor: Raschid Muller

9/8/2025

I. Network Evaluation Report

A. Challenge One

1. Potential cause

I chose Remote_Access_PC because, upon examining the topology, it's open to the entire internal network. This is a problem because the machine can connect to more of its systems than it should. However, looking at the firewall, the whole internal network doesn't have any restrictions in place because firewall rules, VLAN segmentation, or access control lists would limit this kind of access. In theory, these controls are most likely causing the issue.

One possible reason for this issue is that the Remote_Access_PC was placed on the same subnet as all the internal systems, rather than being isolated in its own VLAN or DMZ. Another factor could be that the remote access setup was too broad, granting full network access by default instead of limiting it to just the file server. Additionally, the user account associated with this PC may have been assigned higher-level permissions than it should be, such as domain-wide rights, which could allow it to access systems it shouldn't.

Leaving it like that is a big security risk because if the Remote_Access_PC ever gets compromised, an attacker would have a clear path to move around the whole entire network and target other systems freely. In essence, Remote access points are already one of the most common attack vectors, so not restricting this PC just makes it even more vulnerable. Ideally, it should only connect to the file server and nothing else.

2. Approach

- Setting the the Remote_Access_PC into a separate VLAN to isolate the traffic.
- Configure the firewall and ACL rules so that the Remote_Access_PC can connect to the internal file server only!
- Applying the principle of least privilege to only limit certain permissions.
- Applying endpoint hardening and monitoring

Justification

Remote access systems often catch the eye of attackers because they can be a gateway to the entire network. If these systems are breached, attackers might gain access to explore the network. Isolating the Remote_Access_PC and restricting its access, we can minimize the potential attack surface. This method not only aligns with network security best practices but also safeguards both confidentiality and integrity.

B. Challenge two

1. Potential cause

The organization appears to lack a formal password policy. This means employees are setting weak or easily guessable passwords, and these passwords would never expire. As a result, accounts are at risk of brute force attacks, credential stuffing, and insider misuse. Without enforced controls, these accounts remain vulnerable over time.

2. Approach

- The organization must enforce a wide password policy with requirements that should be length, complexity, and uniqueness instead of using “Password123”

- Enforcing a regular password expiration up to (60-90 day period) this will help balance everything.
- Apply Multi-Factor authentication (MFA) for systems that are critical and for which someone is trying to gain remote access.
- Adopting user training and awareness so employees know how to maintain password policy hygiene.
- Implementing a centralized identity management system, so it makes it harder for someone to bypass security rules.

Justification

Passwords are the go-to method for someone to gain authentication but using weak or outdated passwords can pose a big risk inside the organization. By following best practices, we can keep user accounts secure and ensure that only authorized individuals have access. Adding Multi-Factor Authentication (MFA) gives an extra layer of security, because even if someone manages to steal a password, they need that second authentication.