YOUR NETWORK IS NOT SAFE!

THE SECURITY SCORE OF YOUR NETWORK IS:

35%

VULNERABILITY ASSESSMENT

LUCAS VIAENE

INTRODUCTION

Preface

Throughout this assessment I will describe the vulnerabilities I found on your network. I scanned the network, pentested the devices and generally tried to find all vulnerabilities present. For each vulnerability or cluster of vulnerabilities that belong together, I will propose a possible solution on how to erase these vulnerabilities out of your network and on how to prevent related issues to form in the future.

If any words or terminology appear unclear throughout the assessment, please refer to the Glossary of Terms at the end of this document.

Scope

For this assessment, I scanned the first 100 IP's of your network. This means that the information in this document only covers the devices present in the first 100 IP addresses.

DISCLAIMER

The information displayed in this report is accurate as of 03/06/2024 23:59:59. This pentest / network scan was provided on behalf of Howest. In no other case it is permitted to apply the following techniques to the company of Vault Vinyl or any other company, unless with clear written permission from the company itself.

TABLE OF CONTENTS

Introduction 1
Preface 1
Scope 1
Network Overview 5
Asset Discovery 5
Risk Assessment 6
Legend 6
Risk Classification 7
Critical Risk 7
High Risk 7
Medium Risk 7
Low Risk 7
Risk Overview 7
Vulnerabilities 8
Remote Code Execution (RCE) 8
Exposed Remote Desktop Protocol (RDP) 8
Insecure FTP Configuration 8
Weak Access Control 8
SMB Enumeration 8
Insecure Direct Object References (IDOR) 8
SAM Hashes Extraction 8
LDAP Enumeration 9
SSH Brute-Force 9
Pass-The-Hash Attack 9
MSRPC Specific Login 9
NFS Share 9
Weak Passwords 9
Information Disclosure 10
ARP Poisoning 10
DNS Enumeration 10
OPNsense Admin Panel Access 10
Robots.txt 10
Device Details 11

Device: amplifier.vault.vinyl (10.11.12.6) 11
Vulnerability Score 11
Nmap Scan Results 11
ARP Poisoning Attack 11
LDAP Enumeration 11
SMB Enumeration 11
NFS Share 11
DNS Enumeration 12
Pass-The-Hash Attack 12
MSRPC Specific Login 12
Mitigation 12
Device: turntable.vault.vinyl (10.11.12.13) 13
Vulnerability Score 13
Nmap Scan Results 13
OPNsense Admin Panel Access 13
Shell Access via Admin Panel 13
Mitigation 13
Device: record.vault.vinyl (10.11.12.28) 14
Vulnerability Score 14
Nmap Scan Results 14
Remote Desktop Protocol 14
Insecure Storage of Sensitive Information 14
SAM Hashes 14
Mitigation 14
Device: 10.11.12.38 15
Vulnerability Score 15
Nmap Scan Results 15
Remote Code Execution (RCE) 15
Mitigation 15
Device: www.vault.vinyl (10.11.12.53) 16
Vulnerability Score 16
Nmap Scan Results 16
Robots.txt and Insecure FTP Configuration 16
PKZIP Password Cracking 16

SSH Brute-force Attack 16
Nginx Version and Configuration Exposure 16
Weak Access Control and IDOR 16
Password Crack 17
Mitigation 17
Device: 10.11.12.75 18
Vulnerability Score 18
Nmap Scan Results 18
ARP Poisoning & Information Disclosure via ElasticSearch 18
RCE in ElasticSearch 18
Mitigation 18
Recommendations 19
Immediate Actions 19
Short-term Mitigations 20
Long-term Strategies 21
Conclusion 22
Summary 22
Next Steps 22
Glossary of Terms 23

NETWORK OVERVIEW

Asset Discovery

Below you find a list of the devices I identified and their roles and services

- 10.11.12.6 (amplifier.vault.vinyl)
  - ✓ DNS Server
  - ✓ Domain Controller
  - ✓ Windows System (version 10.0)
- 10.11.12.13 (turntable.vault.vinyl)
  - ✓ OPN Sense Router
- 10.11.12.28 (record.vault.vinyl)
  - ✓ Client
  - ✓ Windows System
- 10.11.12.38
  - ✓ Debian client
  - ✓ Postgres
- 10.11.12.48
- 10.11.12.53 (www.vault.vynil)
  - ✓ Web Server
  - ✓ Nginx
- 10.11.12.75 (catalog.vault.vinyl)
  - ✓ ElasticSearch

RISK ASSESSMENT

Let’s place all vulnerabilities on a Risk Assessment Scale. We’ll take 4 levels of risk, from highest risk (critical) to lowest risk (low). This way you can get a clear view on the state of the security of the network. The vulnerabilities themselves will be explained later.

Legend

- **Critical Risk**
  - Immediate and severe impact, leading to full system compromise, data loss, and potential further network infiltration.
  - High likelihood due to easily exploitable vulnerabilities and high-value targets.
- **High Risk**
  - Significant impact, allowing unauthorized access, data manipulation, or service disruptions.
  - Moderate to high likelihood based on the visibility and accessibility of the vulnerabilities.
- **Medium Risk**
  - Moderate impact, potentially enabling lateral movement within the network or privilege escalation.
  - Moderate likelihood, depending on the attacker's access level and persistence.
- **Low Risk**
  - Limited impact, mostly facilitating information gathering or minor service disruptions.
  - Lower likelihood, often requiring specific conditions or insider knowledge.

Risk Classification

CRITICAL RISK

- Remote Code Execution (RCE)
- Exposed Remote Desktop Protocol (RDP)

HIGH RISK

- Insecure FTP Configuration
- Weak Access Control
- SMB Enumeration
- Insecure Direct Object References

MEDIUM RISK

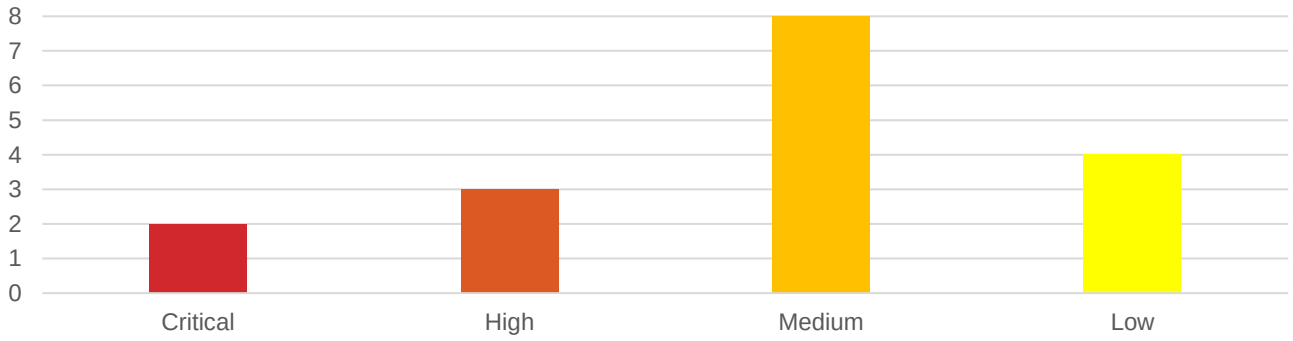
- SAM Hashes Extraction
- LDAP Enumeration
- SSH Brute-Force
- Pass-The-Hash Attack
- MSRPC Specific Login
- NFS Share
- Weak Passwords
- Information Disclosure

LOW RISK

- ARP Poisoning
- DNS Enumeration
- OPNsense Admin Panel Access
- Robots.txt

Risk Overview

Below you can find a brief overview of security issues. I have found 18 total vulnerabilities from which most of them are classed “Medium risk”. This might look decent, but the high amount of “lower than high” risks should not distract you from the fact that there are 18 vulnerabilities present on your system from which 6 are very dangerous.



VULNERABILITIES

Let's dig deeper into each of these vulnerabilities to understand the importance of mitigating them.

Remote Code Execution (RCE)

Remote Code Execution (RCE) is a critical vulnerability that allows an attacker to execute arbitrary commands on a server from a remote location. This type of vulnerability can lead to full system compromise, unauthorized access, and data theft.

Exposed Remote Desktop Protocol (RDP)

Exposed Remote Desktop Protocol (RDP) is a critical vulnerability that allows unauthorized remote access to a system. RDP is commonly used for remote administration and, if not properly secured, can lead to full system compromise, data theft, and unauthorized network access.

Insecure FTP Configuration

Insecure FTP Configuration is a significant vulnerability that allows unauthorized access to an FTP server due to improper settings. This can lead to unauthorized data access, file manipulation, and potential data breaches.

Weak Access Control

Weak Access Control is a vulnerability that arises when access to sensitive systems or data is not adequately restricted. This can lead to unauthorized access and manipulation of critical information.

SMB Enumeration

SMB (Server Message Block) Enumeration is a vulnerability where an attacker utilizes compromised or weak credentials to connect to a server via SMB and access sensitive files. By exploiting credentials vulnerabilities, the attacker can enumerate shares on the server and retrieve confidential data.

Insecure Direct Object References (IDOR)

Insecure Direct Object References (IDOR) is a vulnerability that occurs when an application exposes internal implementation objects, such as files, database entries, or keys, without proper authorization checks. This can allow attackers to manipulate references to access unauthorized data.

SAM Hashes Extraction

SAM (Security Account Manager) Hashes Extraction is a vulnerability that involves retrieving hashed passwords from the SAM database of a target system using SMB (Server Message Block) enumeration. These hashes can be used by attackers in various ways, including pass-the-hash attacks, to gain unauthorized access to other systems.

LDAP Enumeration

LDAP (Lightweight Directory Access Protocol) Enumeration is a vulnerability where an attacker can gather detailed information about network users and their attributes by leveraging intercepted network traffic and compromised credentials. This process often involves performing a man-in-the-middle (MITM) attack to capture network packets, extracting credentials, and then using those credentials to query an LDAP server.

SSH Brute-Force

SSH Brute-Force is a vulnerability that arises from the insecure configuration of the SSH (Secure Shell) service on a target system. Attackers exploit this vulnerability by attempting to gain unauthorized access via SSH using default, weak, or commonly used credentials, or by employing brute-force techniques to systematically guess passwords. Once access is obtained, attackers can escalate privileges and perform malicious activities on the compromised system.

Pass-The-Hash Attack

A Pass-The-Hash attack is a type of authentication attack where an attacker obtains the hashed credentials (NTLM or LM hash) of a user and uses them to authenticate to a system without needing the plaintext password. This attack exploits the weakness of the Windows authentication protocol, allowing attackers to gain unauthorized access to systems and sensitive data.

MSRPC Specific Login

The MSRPC (Microsoft Remote Procedure Call) Specific Login vulnerability involves unauthorized access to the RPC service (on port 135) on a target system using valid credentials. Attackers can gather detailed information about domain users, groups, and service accounts, potentially exposing sensitive information and facilitating privilege escalation attacks.

NFS Share

The NFS Share vulnerability involves the insecure configuration of Network File System (NFS) shares, allowing unrestricted access to shared directories without proper authentication or access controls. Attackers can mount these shares and access sensitive files, potentially leading to data breaches and compromising data integrity.

Weak Passwords

Weak passwords pose a significant security risk by providing attackers with an easy entry point to compromise systems or gain unauthorized access to sensitive information. These passwords are often predictable, easily guessable, or based on common patterns, making them vulnerable to brute-force attacks and password cracking techniques.

Information Disclosure

Information disclosure vulnerabilities involve the unintentional exposure of sensitive data to unauthorized parties. Attackers exploit these vulnerabilities to gather valuable information about systems, networks, or users, which can aid in further attacks or compromise security.

ARP Poisoning

ARP (Address Resolution Protocol) poisoning, also known as ARP spoofing, is a technique used by attackers to intercept network traffic by manipulating ARP messages. By sending falsified ARP messages onto a local area network, an attacker can associate their MAC address with the IP address of a legitimate network device, causing traffic intended for that device to be redirected to the attacker's system.

DNS Enumeration

DNS enumeration is a reconnaissance technique used by attackers to gather information about a target organization's DNS infrastructure. By querying DNS servers for specific types of records, such as TXT records, attackers can uncover sensitive information such as system configurations, service details, or even confidential data inadvertently stored in DNS records.

OPNsense Admin Panel Access

Accessing the OPNsense admin panel through a web browser reveals a login screen where administrative credentials are required for access. OPNsense is a firewall and routing platform based on FreeBSD, designed for network configuration and management. The vulnerability lies in the use of default credentials, allowing unauthorized users to access the admin panel and potentially compromise network security.

Robots.txt

The robots.txt file, which is intended to instruct web crawlers on which parts of a website to avoid indexing, contains sensitive information. This vulnerability arises from misconfigurations or improper handling of data within the robots.txt file, leading to the exposure of sensitive information to unauthorized users.

DEVICE DETAILS

For each device I created an overview of its weak points and listed mitigations on how to generally maximize the security of this device.

I gave each device a vulnerability score which has been subtracted of the total network safety score (you can find the total network safety score on the frontpage). The higher the vulnerability score of a device, the more vulnerable the device is. To proof that I legitimately found these vulnerabilities, I will briefly explain my ways of working and provide small proof of my research if necessary.

Device: amplifier.vault.vinyl (10.11.12.6)

VULNERABILITY SCORE

The device has a high vulnerability score due to multiple critical vulnerabilities found on this device. The score is 15, resulting in a 15% reduction in the total network safety score.

NMAP SCAN RESULTS

- Open ports: 22, 53, 88, 111, 135, 139, 389, 445, 464, 593, 636, 3268, 3269
- Services: SSH, DNS, Kerberos, MSRPC, NetBIOS, LDAP, SMB, HTTP, LDAPS, Global Catalog

ARP POISONING ATTACK

Methodology: Performed ARP spoofing using a man-in-the-middle tool to intercept network traffic.

Findings: Captured sensitive credentials and data being transmitted across the network, which can lead to unauthorized access and data breaches.

Proof: There's a user "ftpuser" with password "FLAG-5***".

LDAP ENUMERATION

Methodology: Executed LDAP enumeration using a tool to query the LDAP server for user and group information.

Findings: Extracted detailed user information including usernames and organizational structure, which could be used for further attacks.

Proof: The "phyiscalDeliverOfficeName" of the user "ed" is "FLAG-66**".

SMB ENUMERATION

Methodology: Used SMB enumeration tools to list shared resources on the device.

Findings: Identified accessible shares containing sensitive files, which can be exploited to gain unauthorized access to data.

Proof: On the Share //10.11.12.6/Financial there's a file "FLAG.txt".

NFS SHARE

Methodology: Used tool to show mounted directories.

Findings: Found mounted directory "/Data" and its contents.

Proof: There's a file in the "/Data" directory called "FLAG.txt".

DNS ENUMERATION

Methodology: Used lookup tool to uncover TXT records.

Findings: Found mail server details.

Proof: There's "FLAG-6***" in these records.

PASS-THE-HASH ATTACK

Methodology: Used tool to pass "Amelia Turner's" password hash.

Findings: Gained access to user "Amelia's" filesystem.

Proof: In "Amelia's" root folder, there's a file "FLAG.txt" with inside "FLAG-6***".

MSRPC SPECIFIC LOGIN

Methodology: Investigated RPC service using "ed@vault.vinyl's" credentials.

Findings: List of registered users, groups, …

Proof: There's a user "flag". There's a group "Enterprise Admins".

MITIGATION

- ☐ Implement ARP spoofing detection and prevention mechanisms.
- ☐ Restrict LDAP queries to authorized users and limit the information disclosed.
- ☐ Secure SMB shares with strong access controls and regularly review permissions.
- ☐ Ensure NFS shares are properly configured with appropriate access controls and monitor for unauthorized mounts.
- ☐ Secure DNS records and limit exposure of sensitive information.
- ☐ Implement multi-factor authentication and use robust password policies to prevent pass-the-hash attacks.
- ☐ Restrict RPC service access to authorized users and implement stringent monitoring of service activities.

Device: turntable.vault.vinyl (10.11.12.13)

VULNERABILITY SCORE

The device has a high vulnerability score due to significant vulnerabilities found on this device. The score is 10, resulting in a 10% reduction in the total network safety score.

NMAP SCAN RESULTS

- Open ports: 80, 443, 53
- Services: Web server, DNS

OPNSENSE ADMIN PANEL ACCESS

Methodology: Accessed the OPNsense admin panel using default credentials.

Findings: Obtained administrative access to the firewall and routing configuration, which could be used to alter network settings and disrupt services.

Proof: There's an image on the dashboard with the text "FLAG-1**8".

SHELL ACCESS VIA ADMIN PANEL

Methodology: Used admin panel access to execute commands on the underlying operating system.

Findings: Gained shell access, allowing full control over the device, including the ability to install malicious software.

Proof: In the root of the turntable user's shell, there's a file called "FLAG.txt" with inside "FLAG-1**7".

MITIGATION

- ☐ Change default credentials and enforce strong password policies.
- ☐ Implement two-factor authentication for admin panel access.
- ☐ Regularly audit access logs and configurations for unauthorized changes.

Device: record.vault.vinyl (10.11.12.28)

VULNERABILITY SCORE
The device has a medium vulnerability score due to critical vulnerabilities found on this specific device. The score is 8, resulting in a 8% reduction in the total network safety score.

NMAP SCAN RESULTS
- Open ports: 135, 139, 445, 3389
- Services: MSRPC, NetBIOS, SMB, Remote Desktop Protocol

REMOTE DESKTOP PROTOCOL
Methodology: Attempted RDP connections using known credentials.

Findings: Successfully logged in using credentials for "ed@vault.vinyl" and accessed sensitive user data.

Proof: The users directory contains a file called “FLAG.txt”. The users who have logged onto this device are “Administrator”, “ed”, and “Amelia Turner”.

INSECURE STORAGE OF SENSITIVE INFORMATION
Methodology: Analyzed stored files and configurations.

Findings: Discovered sensitive information stored in plain text, including passwords and personal data.

Proof: The user’s password for the website “http://flag.vault.vinyl/” is “FLAG-2***”.

SAM HASHES
Methodology: Extracted SAM hashes using a privileged account.

Findings: Retrieved hashed passwords, which can be cracked offline to gain further access.

Proof: Amelia Turner’s SAM hash starts with “1001” and ends in “2f8:::”

MITIGATION
- ☐ Disable unnecessary RDP services and use VPN for remote access.
- ☐ Encrypt sensitive information and avoid storing passwords in plain text.
- ☐ Regularly change passwords and use strong hashing algorithms.

Device: 10.11.12.38

VULNERABILITY SCORE

The device has a critical vulnerability score due to severe vulnerabilities found on this device. The score is 12, resulting in a 12% reduction in the total network safety score.

NMAP SCAN RESULTS

- Open ports: 22, 3826, 5432
- Services: SSH, RTSP, PostgreSQL

REMOTE CODE EXECUTION (RCE)

Methodology: Injected commands through a vulnerable input field in the web application.

Findings: Executed arbitrary commands on the server, retrieved system information, and accessed sensitive files such as the shadow file containing password hashes.

Proof: The user “flag” has a password “FLAG-3***”.

MITIGATION

- ☐ Sanitize and validate all user inputs to prevent injection attacks.
- ☐ Implement application-level firewalls to detect and block malicious activities.
- ☐ Regularly update and patch software to fix known vulnerabilities.

Device: www.vault.vinyl (10.11.12.53)

VULNERABILITY SCORE

The device has a low safety score due to multiple issues found on this device. The score is 8, resulting in a 8% reduction in the total network safety score.

NMAP SCAN RESULTS

- Open ports: 21, 22, 80, 443, 2121, 3703
- Services: FTP, SSH, Web server, Adobe Server

ROBOTS.TXT AND INSECURE FTP CONFIGURATION

Methodology: Accessed robots.txt file and listed FTP directory contents.

Findings: Robots.txt file disclosed sensitive URLs, and FTP was configured without encryption, exposing data to interception.

Proof: There's a disallowed webpage that starts in "ATWTM" and an anonymous account with a "flag.txt" file in his homedirectory.

PKZIP PASSWORD CRACKING

Methodology: Attempted to crack passwords for encrypted PKZIP files found on the FTP server.

Findings: Successfully cracked passwords, gaining access to sensitive compressed files.

Proof: The password of the protected zip is "FLAG-*3*0".

SSH BRUTE-FORCE ATTACK

Methodology: Performed brute-force attack on SSH service.

Findings: Gained access using weak passwords, compromising the system.

Proof: On the IP "192.168.30.10" there's a file "index.html" with contents "FLAG-08**".

NGINX VERSION AND CONFIGURATION EXPOSURE

Methodology: Enumerated Nginx version and checked configuration files.

Findings: Exposed outdated Nginx version with known vulnerabilities.

Proof: The nginx version is 1.22.1 and the root path of flag.conf is "/var/www/html/flag" with index "index.html"

WEAK ACCESS CONTROL AND IDOR

Methodology: Tested for access control issues and IDOR vulnerabilities.

Findings: Accessed unauthorized resources and sensitive data.

Proof: There's a user "real_admin" with a hashed password that starts with "PB00ZEsoarn"

PASSWORD CRACK

Methodology: Used password cracking tools on stored hashes.

Findings: Recovered several weak passwords.

Proof: The hashes password of the admin in plaintext is “FLAG-**95”.

MITIGATION

- ☐ Secure robots.txt file and remove sensitive URLs.
- ☐ Use SFTP instead of FTP to encrypt data in transit.
- ☐ Implement strong password policies and account lockout mechanisms.
- ☐ Regularly update Nginx and other software to the latest versions.
- ☐ Enforce strict access controls and conduct regular audits for IDOR vulnerabilities.

Device: 10.11.12.75

VULNERABILITY SCORE
The device has a critical safety score due to severe vulnerabilities found on this device. The score is 12, resulting in an 12% reduction in the total network safety score.

NMAP SCAN RESULTS
- Open ports: 22, 1072, 5961, 9200, 32778
- Services: SSH, ElasticSearch

ARP POISONING & INFORMATION DISCLOSURE VIA ELASTICSEARCH
Methodology: Performed ARP spoofing and accessed ElasticSearch service.

Findings: Intercepted network traffic and accessed sensitive information stored in ElasticSearch, including configuration details and user data.

Proof: The album's name of the artist "Flynn Aglow" in the year 2024 is "FLAG-7*7*".

RCE IN ELASTICSEARCH
Methodology: Exploited RCE vulnerability in ElasticSearch.

Findings: Executed arbitrary commands, retrieved system information, and accessed sensitive files.

Proof: The flag.txt file size on 10.11.12.75 was is 10 bytes.

MITIGATION
- ☐ Implement ARP spoofing detection and prevention mechanisms.
- ☐ Secure ElasticSearch with authentication and access controls.
- ☐ Regularly update and patch ElasticSearch to fix vulnerabilities.
- ☐ Monitor and log access to detect and respond to suspicious activities.

RECOMMENDATIONS

The recommendations aim to address the immediate actions for the most critical vulnerabilities found during the assessment, strengthen the security posture in the short term, and ensure long-term resilience against potential threats.

Immediate Actions

- ☐ **Change Default Credentials**
  - ☐ Update default credentials on all devices, especially the OPNsense admin panel and any other systems with factory-set passwords.
- ☐ **Restrict Remote Access**
  - ☐ Disable unnecessary remote access services like RDP on devices where it is not required.
  - ☐ Implement VPN for secure remote access where necessary.
- ☐ **Implement ARP Spoofing Detection**
  - ☐ Deploy ARP spoofing detection tools across the network to identify and block ARP poisoning attempts.
- ☐ **Sanitize Inputs to Prevent RCE**
  - ☐ Immediately update applications to sanitize and validate all user inputs, preventing remote code execution attacks.
- ☐ **Secure SMB and NFS Shares**
  - ☐ Review and restrict access permissions on SMB and NFS shares, ensuring only authorized users have access.
- ☐ **Remove Sensitive Data from Public Files**
  - ☐ Secure robots.txt files by removing references to sensitive URLs and securing any exposed data.

Short-term Mitigations

- ☐ **Implement Multi-Factor Authentication (MFA)**
  - ☐ Enable MFA for accessing critical systems, especially administrative panels and remote access services.
- ☐ **Audit and Enforce Strong Password Policies**
  - ☐ Implement strong password policies across the network and ensure regular password updates.
  - ☐ Use robust hashing algorithms for password storage.
- ☐ **Regular Patching and Software Updates**
  - ☐ Establish a regular schedule for patching and updating software, including Nginx, ElasticSearch, and other critical applications.
- ☐ **Enhance Access Controls**
  - ☐ Implement role-based access controls (RBAC) and ensure strict enforcement of access policies.
  - ☐ Restrict LDAP queries to authorized users and limit the information disclosed.
- ☐ **Encrypt Data in Transit**
  - ☐ Switch from FTP to SFTP to encrypt data during transmission.
  - ☐ Ensure all sensitive data being transmitted over the network is encrypted.
- ☐ **Conduct Regular Security Audits**
  - ☐ Perform frequent security audits and vulnerability scans to identify and address new vulnerabilities promptly.

Long-term Strategies

- **Network Segmentation**
  - Implement network segmentation to isolate critical systems and reduce the attack surface.
  - Use firewalls and VLANs to control and monitor traffic between segments.
- **Security Awareness Training**
  - Conduct regular security awareness training for employees to recognize and respond to potential security threats.
- **Implement Comprehensive Monitoring and Logging**
  - Deploy advanced monitoring and logging solutions to detect and respond to suspicious activities.
  - Monitor access logs and system activities to identify and mitigate potential threats in real-time.
- **Develop an Incident Response Plan**
  - Establish a robust incident response plan that outlines procedures for responding to security breaches.
  - Regularly test and update the plan to ensure its effectiveness.
- **Adopt a Zero Trust Security Model**
  - Implement a zero trust security model, ensuring that every access request is authenticated, authorized, and encrypted regardless of the requestor's location within or outside the network.
- **Invest in Advanced Security Technologies**
  - Explore and deploy advanced security technologies such as AI-based threat detection, endpoint protection platforms, and intrusion prevention systems.

CONCLUSION

Summary

The security audit uncovered several critical vulnerabilities in the network infrastructure. The network's overall security score was determined to be 35%, highlighting the need for significant improvements. Key findings include exposed remote desktop protocols, weak password policies, and insecure configurations in various services. Immediate actions have been recommended to address these vulnerabilities and enhance the security posture of the network. These actions include changing default credentials, restricting remote access, and implementing ARP spoofing detection mechanisms.

Next Steps

We recommend that you urgently address the immediate actions outlined in this report. The other stated recommendations should neither be left without action any longer. We understand that addressing these recommendations can be complex and resource-intensive. Our team is available to assist you in implementing these measures and ensuring that your network is secure. Please do not hesitate to contact us for further guidance or support in fulfilling the recommendations provided in this report. Together, we can enhance your organization's security posture and protect your valuable data from potential threats.

GLOSSARY OF TERMS

ARP (Address Resolution Protocol) Poisoning: A technique used by attackers to intercept network traffic by sending falsified ARP messages. This manipulation can redirect traffic intended for a legitimate device to the attacker's device, potentially leading to data breaches.

Authentication: The process of verifying the identity of a user, device, or other entity in a computer system, often through the use of passwords, tokens, or other credentials.

Brute-Force Attack: A method used by attackers to gain access to systems by systematically trying all possible passwords or keys until the correct one is found.

Credential: A set of information (such as a username and password) used to verify the identity of a user or system.

DNS (Domain Name System) Enumeration: A technique used by attackers to gather information about a target's DNS infrastructure, which can reveal details about the network, such as server names and IP addresses.

FTP (File Transfer Protocol): A standard network protocol used to transfer files between a client and a server on a computer network.

Hash: A function that converts input data (such as a password) into a fixed-size string of characters, which is typically a representation of the original data. Hashes are used to ensure data integrity and secure passwords.

LDAP (Lightweight Directory Access Protocol) Enumeration: A vulnerability where an attacker gathers detailed information about network users and their attributes by querying an LDAP server using compromised credentials.

MAC (Media Access Control) Address: A unique identifier assigned to network interfaces for communications on the physical network segment.

MSRPC (Microsoft Remote Procedure Call): A protocol that allows programs to communicate over a network. MSRPC is used by Windows systems for various services and administrative tasks.

NFS (Network File System) Share: A distributed file system protocol that allows users to access files over a network as if they were on their local hard drives. Insecure NFS shares can be exploited by attackers to access sensitive data.

OPNsense: An open-source firewall and routing platform based on FreeBSD, used for network configuration and management. Vulnerabilities can arise if default credentials are not changed or if the admin panel is not secured.

Pass-The-Hash Attack: An attack where an attacker uses the hashed version of a password (rather than the plaintext version) to authenticate to a remote server and gain unauthorized access.

Remote Code Execution (RCE): A critical vulnerability that allows an attacker to execute arbitrary commands on a server from a remote location, potentially leading to full system compromise.

RDP (Remote Desktop Protocol): A protocol used to remotely access and manage computers. Exposed RDP services can lead to unauthorized access if not properly secured.

SAM (Security Account Manager) Hashes: Hashed versions of user passwords stored in the SAM database on Windows systems. These hashes can be targeted by attackers to perform various types of authentication attacks.

SMB (Server Message Block) Enumeration: A vulnerability where attackers use compromised credentials to connect to an SMB server and access sensitive files.

SSH (Secure Shell): A protocol used to securely access and manage remote systems. SSH brute-force attacks exploit weak or default passwords to gain unauthorized access.

Two-Factor Authentication (2FA): An additional layer of security used to ensure that people trying to gain access to an online account are who they say they are. First, a user enters their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information.

Vulnerability: A weakness in a system or network that can be exploited by attackers to gain unauthorized access or cause damage.

Weak Password: A password that is easy to guess or crack due to its simplicity or common usage. Weak passwords pose a significant security risk as they can be exploited through brute-force attacks or other methods.