Vulnerability Report

Zehra Nur Ozer

June 2024

Table of Contents

Video Presentation

The link for the video presentation is below.

https://docs.google.com/presentation/d/1pnRbh7kT090xII05zAa_H2EzaSaPwsxA/edit?usp=drive_link&ouid=116449824947486147238&rtpof=true&sd=true

1. Executive Summary

As part of the system's security enhancement, the team conducted a series of vulnerability scans using the OpenVAS tool to identify potential security weaknesses in IT infrastructure. The scans targeted a Windows workstation, a Windows server, and a Linux system. The objective was to identify and prioritize vulnerabilities to mitigate potential security risks. The findings revealed several vulnerabilities, including high and medium-severity issues. This report details these findings, the potential impact on the business, and recommendations for mitigating the identified risks.

2. Scan Results

Methodology

The team used OpenVAS as the primary tool within the KaliOpenVAS environment to perform the scanning. for the vulnerability scan, which is well known for its comprehensive capabilities and vast database.

The scan is performed on the following targets, and the result is separated by the systems to explain the details below.

a. Windows1 (172.16.14.50)

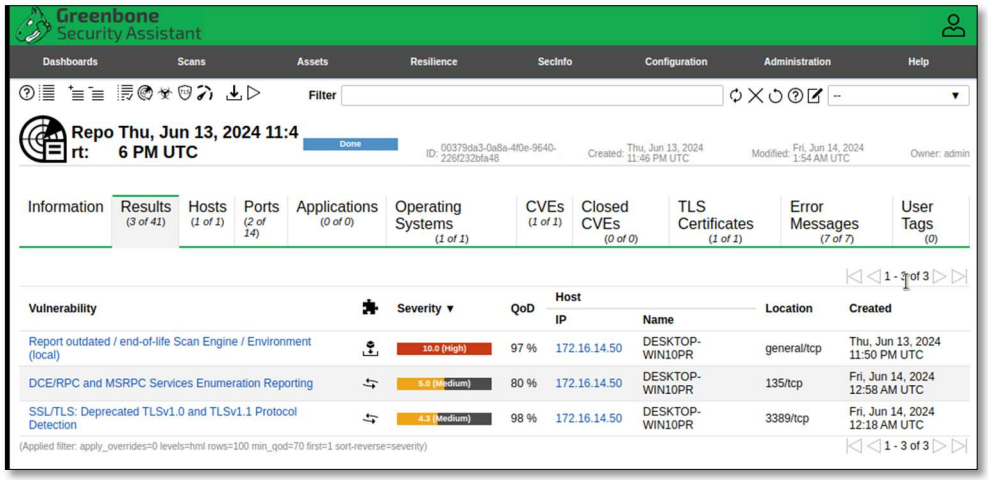


Figure 1 OpenVAS Windows1 scan results

1 - 2 of 2

Port	Hosts	Severity ▼
135/tcp	1	5.0 (Medium)
3389/tcp	1	4.3 (Medium)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 2 of 2

Ports

135/TCP (DCE/RPC and MSRPC Services Enumeration Reporting): The potential information disclosure through enumeration. Restricting access and implementing network segmentation can be a solution.

3389/TCP: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection. This can impact insecure TLS protocols can be exploited. An update to TLSv1.2 can be a solution.

1 - 1 of 1

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	1	1	4.3 (Medium)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 1 of 1

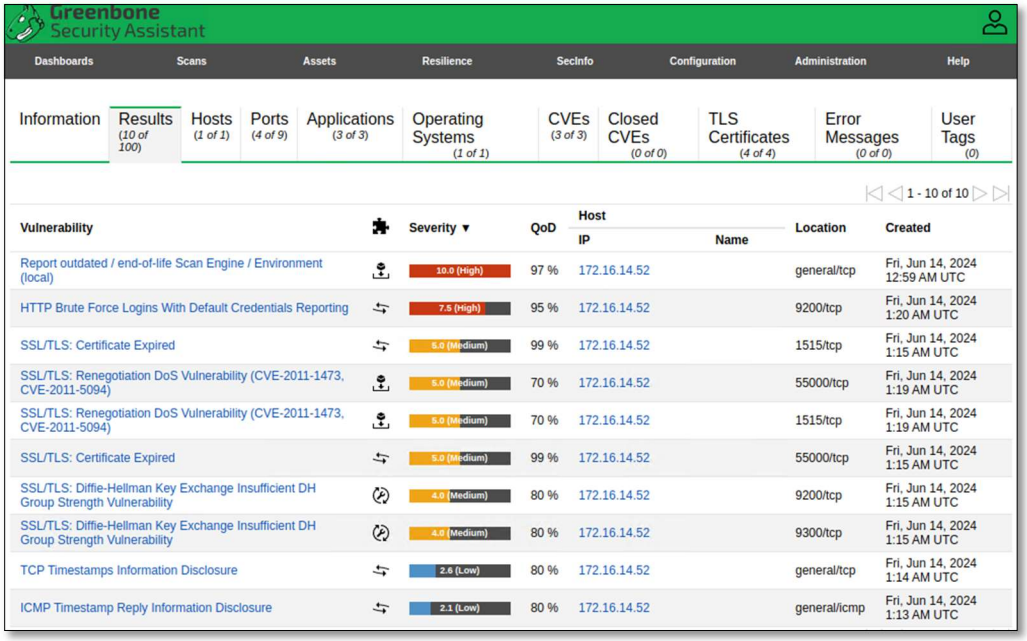
CVE-2011-3389: This vulnerability is due to the use of deprecated TLS protocols (TLSv1.0 and TLSv1.1). These protocols are considered insecure and can be exploited by attackers to perform various attacks, including man-in-the-middle attacks. Using deprecated protocols can compromise communication security. Attackers may intercept or manipulate data being transmitted. (NVD - Cve-2011-3389, n.d.)

Solution: Update all systems to use TLSv1.2 or higher.

CVE-2015-0204: This vulnerability relates to the use of weak Diffie-Hellman key exchange parameters in SSL/TLS, allowing attackers to potentially decrypt encrypted traffic. Attackers can intercept and decrypt sensitive information transmitted over SSL/TLS connections. (NATIONAL VULNERABILITY DATABASE, 2024)

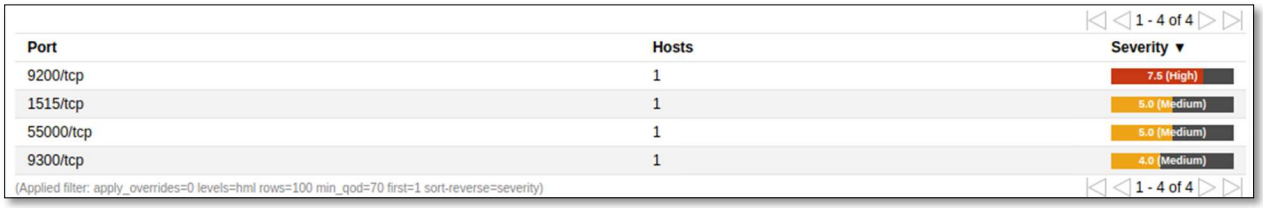
Solution: Configure servers to use strong Diffie-Hellman groups and update to TLSv1.2 or higher.

b. Linux (172.16.14.52)



Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	172.16.14.52		general/tcp	Fri, Jun 14, 2024 12:59 AM UTC
HTTP Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	172.16.14.52		9200/tcp	Fri, Jun 14, 2024 1:20 AM UTC
SSL/TLS: Certificate Expired	5.0 (Medium)	99 %	172.16.14.52		1515/tcp	Fri, Jun 14, 2024 1:15 AM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70 %	172.16.14.52		55000/tcp	Fri, Jun 14, 2024 1:19 AM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70 %	172.16.14.52		1515/tcp	Fri, Jun 14, 2024 1:19 AM UTC
SSL/TLS: Certificate Expired	5.0 (Medium)	99 %	172.16.14.52		55000/tcp	Fri, Jun 14, 2024 1:15 AM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	172.16.14.52		9200/tcp	Fri, Jun 14, 2024 1:15 AM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	172.16.14.52		9300/tcp	Fri, Jun 14, 2024 1:15 AM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	172.16.14.52		general/tcp	Fri, Jun 14, 2024 1:14 AM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	172.16.14.52		general/icmp	Fri, Jun 14, 2024 1:13 AM UTC

Figure 2 OpenVAS Linux scan results



Port	Hosts	Severity ▼
9200/tcp	1	7.5 (High)
1515/tcp	1	5.0 (Medium)
55000/tcp	1	5.0 (Medium)
9300/tcp	1	4.0 (Medium)

<u>Ports</u>

9200/TCP (HTTP Brute Force Logins with Default Credentials Reporting and SSL/TLS) Certificate Expired Risk of unauthorized access and man-in-the-middle attacks.

Solution: Implement strong passwords and renew certificates.

1515/TCP: (SSL/TLS: Renegotiation DOS Vulnerability) Potential denial-of-service attacks.

Solution: Disable SSL/TLS renegotiation or upgrade.

9300/TCP: (SSL/TLS: Diffie-Hellman Key Exchange) Insufficient DH Group Strength Vulnerability

Weaker encryption and susceptible to attacks.

Solution: Use strong DH groups.

Information | Results (10 of 100) | Hosts (1 of 1) | Ports (4 of 9) | Applications (3 of 3) | Operating Systems (1 of 1) | CVEs (3 of 3) | Closed CVEs (0 of 0) | TLS Certificates (4 of 4) | Error Messages (0 of 0) | User Tags (0)

1 - 3 of 3

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508	HTTP Brute Force Logins With Default Credentials Reporting	1	1	7.5 (High)
CVE-2011-1473 CVE-2011-5094	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	1	2	5.0 (Medium)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	1	1	2.1 (Low)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 3 of 3

CVE-1999-0502, CVE-1999-0507, CVE-1999-0508: HTTP Brute Force Logins with Default Credentials Reporting

Indicates using default credentials that can be easily brute-forced, leading to unauthorized access. (NATIONAL VULNERABILITY DATABASE, 2024)

Solution: Change default credentials and implement account lockout mechanisms

CVE-2011-1473 & CVE-2011-5094: SSL/TLS Renegotiation DoS Vulnerability

Exploits in SSL/TLS renegotiation can lead to denial-of-service attacks. (NATIONAL VULNERABILITY DATABASE, 2024)

Solution: Disable insecure renegotiation or apply necessary patches.

CVE-1999-0524: ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts. (NATIONAL VULNERABILITY DATABASE, 2024)

Solution: Users may configure the firewall to prevent a system from responding to certain ICMP requests.

c. WinServer (172.16.14.53)

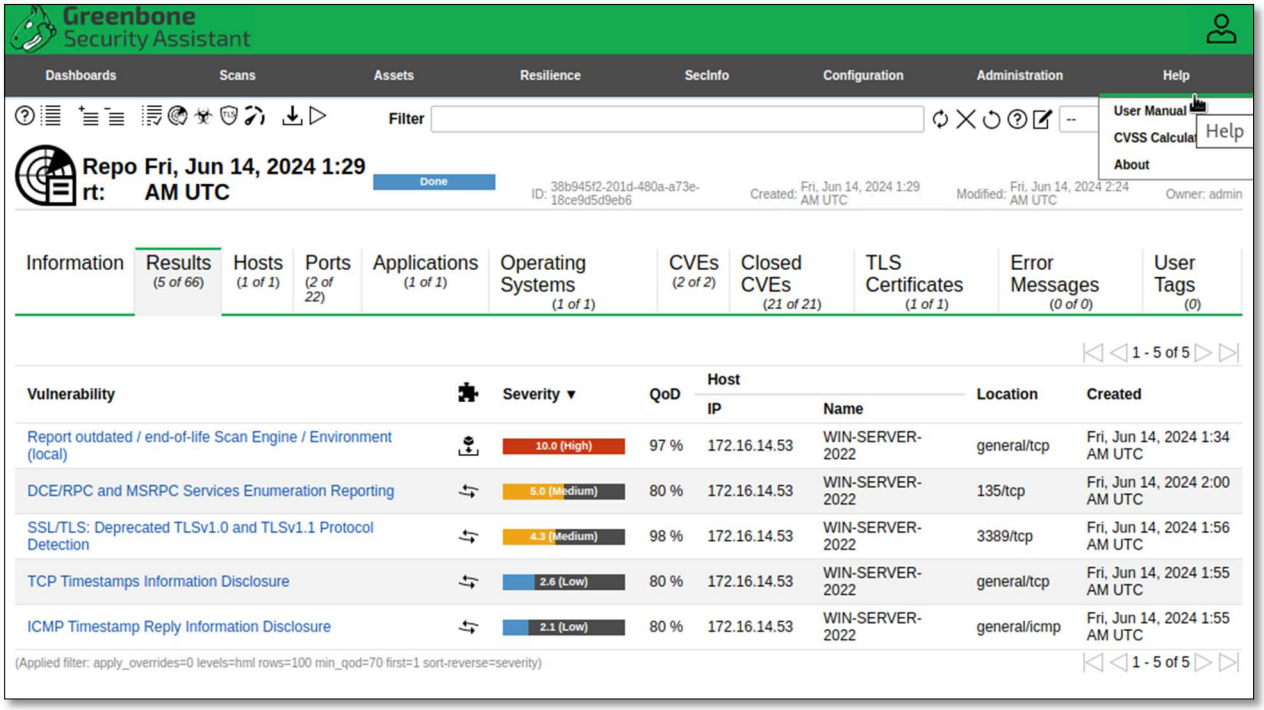


Figure 3 OpenVAS WinServer scan results

<u>Ports</u>

135/TCP (DCE/RPC and MSRPC Services) Enumeration Reporting. Potential information disclosure through enumeration.

Solution: Restrict access and implement network segmentation.

3389/TCP (SSL/TLS) Deprecated TLSv1.0 and TLSv1.1 Protocol Detection. Insecure TLS protocols can be exploited.

Solution: Update to TLSv1.2 or higher.

General/TCP: Report outdated / end-of-life Scan Engine / Environment (local) Exposure to unpatched vulnerabilities.

Solution: Update or replace the scan engine.

General/ICMP: ICMP Timestamp Reply Information Disclosure. Potential information disclosure.

Solution: Disable ICMP timestamp responses

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	1	1	4.3 (Medium)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	1	1	2.1 (Low)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity) 1 - 2 of 2

CVE-2011-3389 & CVE-2015-0204: SSL/TLS Renegotiation DoS Vulnerability Vulnerabilities in SSL/TLS that allow attackers to perform denial-of-service attacks by exploiting the renegotiation feature. (NATIONAL VULNERABILITY DATABASE, 2024)

Solution: Apply patches and configuration updates to mitigate these vulnerabilities.

CVE-1999-0524: ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts. (NATIONAL VULNERABILITY DATABASE, 2024)

Solution: Users may configure the firewall to prevent a system from responding to certain ICMP requests.

3. Our Findings

As the scanning results show, a detailed risk assessment is conducted below. The vulnerability will be classified into high, medium, and low severity.

The findings are listed below, and a detailed chart is prepared in the risk assessment section.

High Vulnerabilities:

- HTTP Brute Force Logins with Default Credentials Reporting
  - **Impact:** Risk of unauthorized access through default credentials.
  - **Solution:** Implement strong password policies and disable default credentials.
- DCE/RPC and MSRPC Services Enumeration Reporting
  - **Impact:** Potential information disclosure through enumeration.
  - **Solution:** Restrict access to DCE/RPC services and implement network segmentation.

Medium Vulnerabilities:

- SSL/TLS: Certificate Expired
  - **Impact:** Potential exposure to man-in-the-middle attacks.
  - **Solution:** Renew SSL/TLS certificates.
- SSL/TLS: Renegotiation DOS Vulnerability (CVE-2011-1473, CVE-2011-5048)
  - **Impact:** Potential denial of service attack.
  - **Solution:** Disable SSL/TLS renegotiation or upgrade to a secure version.

- SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
  - **Impact:** Weaker encryption, susceptible to attacks.
  - **Solution:** Configure servers to use a stronger DH group.
- SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
  - **Impact:** Exposure to attacks exploiting deprecated protocols.
  - **Solution:** Upgrade to TLSv1.2 or higher.
- TCP Timestamps Information Disclosure
  - **Impact:** Potential information disclosure.
  - **Solution:** Disable TCP timestamps on network devices.

Low Vulnerabilities:

- ICMP Timestamp Reply Information Disclosure

  - **Impact:** Potential information disclosure.
  - **Solution:** Disable ICMP timestamp responses on network devices

4. Risk Assessment

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Thu, Jun 13, 2024 11:46 PM UTC	Done	Windows1 - Vulnerabilities with creds	10.0 (High)	1	2	0	37	0	

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Fri, Jun 14, 2024 12:55 AM UTC	Done	Linux	10.0 (High)	2	6	2	70	0	

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Fri, Jun 14, 2024 1:29 AM UTC	Done	WinServer - No host	10.0 (High)	1	2	2	59	0	

The report identifies security risks that could significantly impact business operations.

a. High Severity Vulnerability

VULNERABILITY	DESCRIPTION	SOLUTION
Report outdated / end-of-life Scan Engine / Environment (local)	The scan engine or environment used for vulnerability scanning is outdated or has reached end-of-life, which means it may no longer receive updates or patches. This could lead to missing new vulnerabilities or	Update the scan engine or switch to a supported environment to ensure it is up to date with the latest vulnerability definitions and patches.

	having unresolved known vulnerabilities.	
HTTP Brute Force Logins with Default Credentials Reporting	The scan detected the presence of default credentials being used, which attackers could exploit to gain unauthorized access through brute-force attacks.	Change default credentials to strong, unique passwords and implement account lockout mechanisms.
SSL/TLS: Certificate Expired	The system's SSL/TLS certificate has expired, which could lead to untrusted connections and potential man-in-the-middle attacks.	Renew the expired certificate and ensure it is properly installed.

b. Medium Severity Vulnerability

VULNERABILITY	DESCRIPTION	SOLUTION
DCE/RPC and MSRPC Services Enumeration Reporting	DCE/RPC (Distributed Computing Environment / Remote Procedure Calls) and MSRPC (Microsoft RPC) services were detected. These services can sometimes be exploited by attackers to gain unauthorized access or perform actions on remote systems.	Limit access to these services, apply patches, and ensure proper authentication and authorization controls are in place.
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	The scan detected the use of deprecated TLSv1.0 and TLSv1.1 protocols. These protocols are considered insecure and may be vulnerable to various attacks.	Disable TLSv1.0 and TLSv1.1 and upgrade to TLSv1.2 or higher.
Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5044)	The system is vulnerable to a denial of service (DoS) attack due to SSL/TLS renegotiation issues.	Apply patches or configuration changes to disable renegotiation or ensure it is secure.
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	The Diffie-Hellman key exchange used by the system has insufficient group strength, making it potentially vulnerable to certain attacks.	Use stronger Diffie-Hellman groups (2048-bit or higher).

c. Low Severity Vulnerability

VULNERABILITY	DESCRIPTION	SOLUTION

TCP Timestamps Information Disclosure	TCP timestamps are enabled, which could allow attackers to estimate the system's uptime and plan attacks accordingly.	Disable TCP timestamps if not needed.

5. Recommendations

The assessment has identified several critical and high-risk vulnerabilities that need immediate attention. By prioritizing these issues and following the recommendations provided.

Immediate updates to the scan engine should be made to a supported version to ensure all vulnerabilities can be identified and mitigated. Additionally, implementing a strong password policy and network segmentation is crucial to mitigate the high severity vulnerabilities.

Upgrade to SSL/TLS protocols as well as disable ICMP timestamp also prevents potential information disclosure.

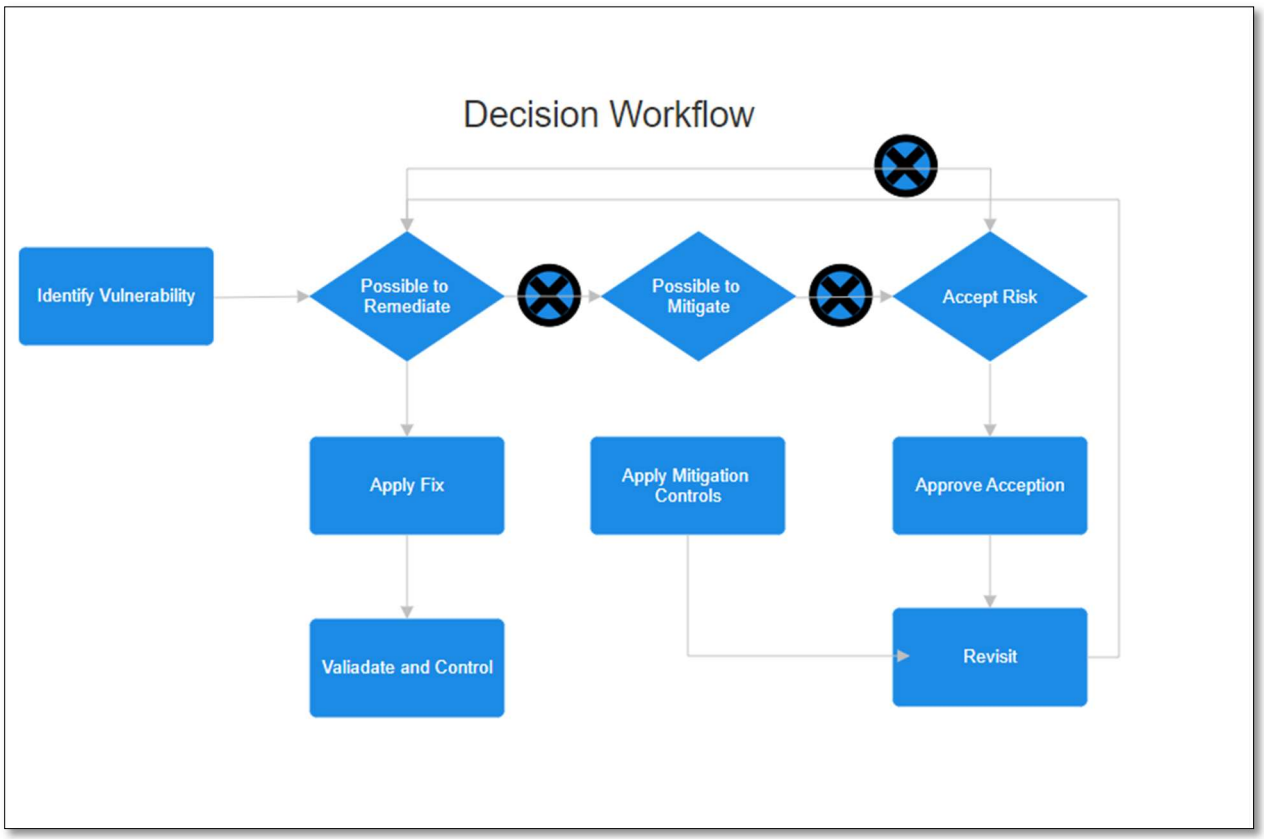


Figure 4 Company Vulnerability Decision Workflow created with Smartdraw (Cyber Security Bootcamp, 2023)

6. References

Carnegie Mellon University. (2016). *CRR Supplemental Resource Guide* (Vol. 4). https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf

ChatGPT. (2024). Retrieved June 12, 2024, from https://chatgpt.com/

Cyber Security Bootcamp. (2023). Vulnerabilities and the risk management process. In *Cyber Security Bootcamp* [Report].

Ec-Council. (2023, November 7). *How to write a vulnerability assessment report*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/how-to-write-vulnerability-assessment-report/

Everyone, S. F. (n.d.). *Five steps of a good vulnerability assessment and how to write report*. https://securityforeveryone.com/blog/a-good-vulnerability-assessment-and-how-to-write-report

HackerSploit. (2018, September 2). *Vulnerability analysis with OpenVAS* [Video]. YouTube. https://www.youtube.com/watch?v=koMo_fSQGlk

NVD - cve-2011-3389. (n.d.). https://nvd.nist.gov/vuln/detail/cve-2011-3389

Purplesec. (n.d.). Sample Network Vulnerability Assessment report. In *Purplesec* (pp. 1–8). https://purplesec.us/wp-content/uploads/2019/03/Sample-Network-Security-Vulnerability-Assessment-Report-Purplesec.pdf

Security, R., & Security, R. (2019, September 26). Tips for creating a strong vulnerability assessment report. *RSI Security*. https://blog.rsisecurity.com/tips-for-creating-a-strong-vulnerability-assessment-report/