5/28/2024

Cat’s Vulnerability Scan

Fahad Shahzad

Executive summary

Our organization conducted a vulnerability scan on three critical assets: Windows Server, Windows 1, and Ubuntu Linux, using OpenVAS. This scan revealed several significant vulnerabilities that need immediate attention to ensure the security and integrity of our systems. The scan results are presented in alignment with NIST standards to provide a comprehensive security framework for remediation.

Key Findings:

1. Outdated Greenbone Community Edition

   The scan engine, Greenbone Community Edition, used across all three assets, is outdated or at the end of its lifecycle. This version lacks the latest functionalities and bug fixes, potentially missing critical vulnerabilities in the scan.
2. Missing Passwords on Linux OS

   The Ubuntu Linux asset has high vulnerabilities due to missing passwords for both the web application and the OSSEC-authd service. This oversight allows unauthorized access to sensitive information and system configuration.
3. Outdated TLS Versions

   The Windows 1 asset is using TLSv1.0 and TLSv1.1 protocols, which are susceptible to eavesdropping due to known cryptographic weaknesses.
4. Incorrect TLS Setup on Ubuntu Linux

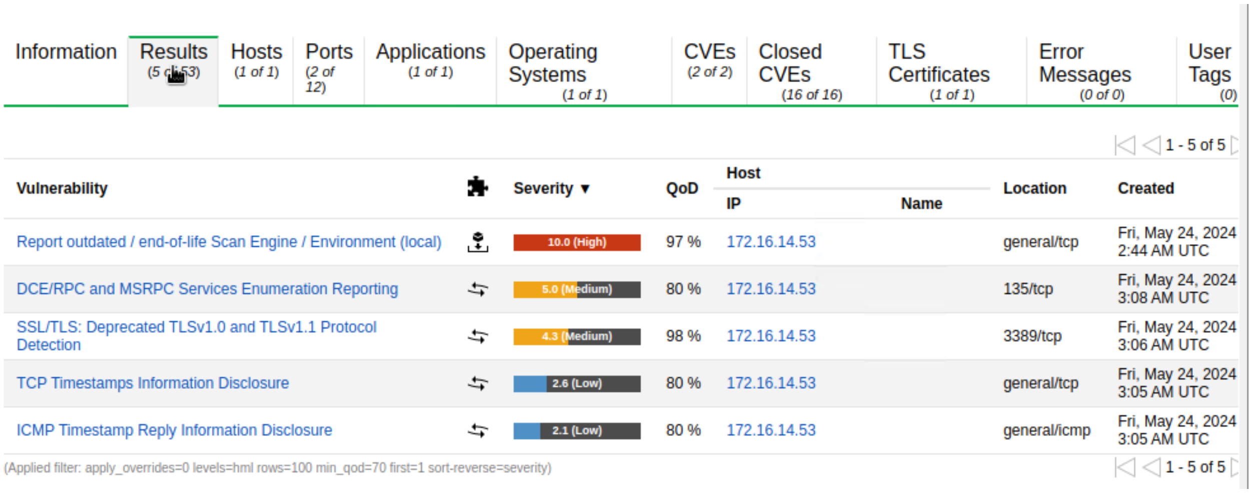
   The TLS configuration on the Ubuntu Linux asset is incorrect, making it vulnerable to Denial of Service (DoS) attacks. The service does not properly restrict client-initiated renegotiation, which can be exploited to exhaust system resources.
5. Excessive Open Ports on Windows Server

   The Windows Server has multiple open ports, allowing unauthorized connections and potential exploitation.
6. Service Enumeration

   Description: DCE/RPC or MSRPC services running on port 135 of the Windows Server can be enumerated, allowing attackers to gain information about the remote host and potentially exploit it.

By applying these remediation measures and protecting these assets, we will be able to better control and enhance the security of our organization.

Scan Results



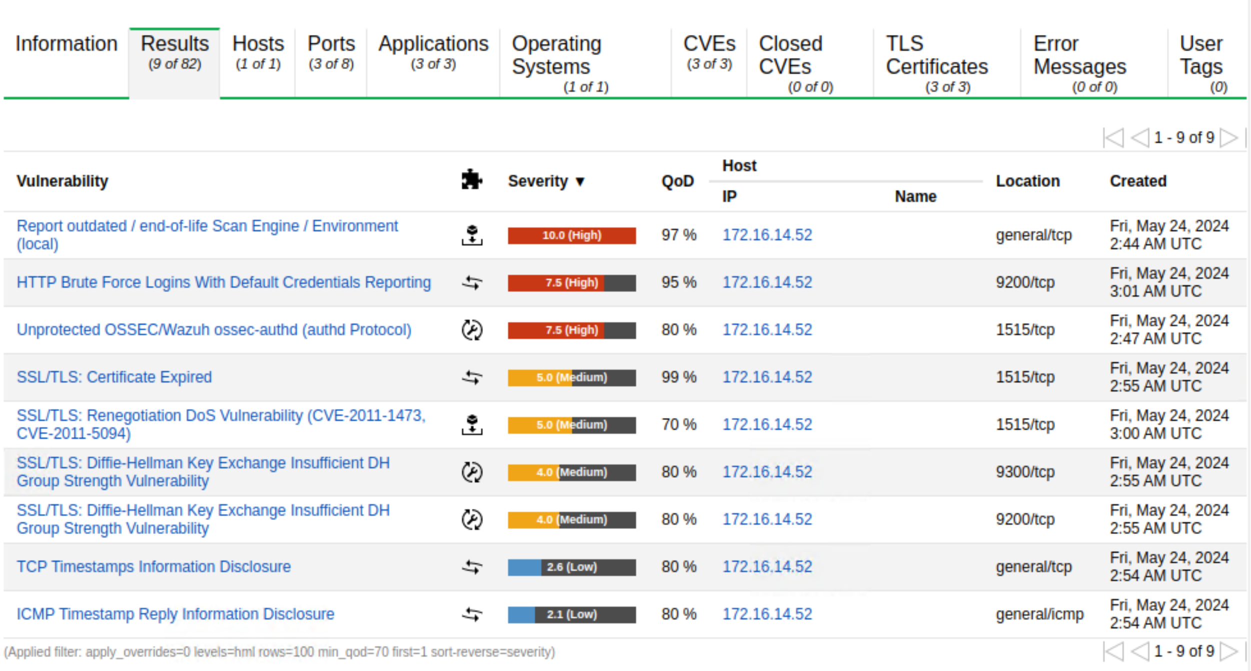
Information | Results (5 of 53) | Hosts (1 of 1) | Ports (2 of 12) | Applications (1 of 1) | Operating Systems (1 of 1) | CVEs (2 of 2) | Closed CVEs (16 of 16) | TLS Certificates (1 of 1) | Error Messages (0 of 0) | User Tags (0)

1 - 5 of 5

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	172.16.14.53		general/tcp	Fri, May 24, 2024 2:44 AM UTC
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80 %	172.16.14.53		135/tcp	Fri, May 24, 2024 3:08 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection		4.3 (Medium)	98 %	172.16.14.53		3389/tcp	Fri, May 24, 2024 3:06 AM UTC
TCP Timestamps Information Disclosure		2.6 (Low)	80 %	172.16.14.53		general/tcp	Fri, May 24, 2024 3:05 AM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	172.16.14.53		general/icmp	Fri, May 24, 2024 3:05 AM UTC

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

1 - 5 of 5



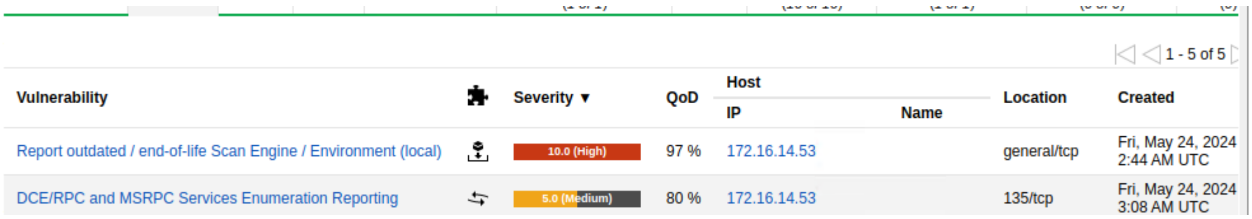
Information | Results (9 of 82) | Hosts (1 of 1) | Ports (3 of 8) | Applications (3 of 3) | Operating Systems (1 of 1) | CVEs (3 of 3) | Closed CVEs (0 of 0) | TLS Certificates (3 of 3) | Error Messages (0 of 0) | User Tags (0)

1 - 9 of 9

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, May 24, 2024 2:44 AM UTC
HTTP Brute Force Logins With Default Credentials Reporting		7.5 (High)	95 %	172.16.14.52		9200/tcp	Fri, May 24, 2024 3:01 AM UTC
Unprotected OSSEC/Wazuh ossec-authd (authd Protocol)		7.5 (High)	80 %	172.16.14.52		1515/tcp	Fri, May 24, 2024 2:47 AM UTC
SSL/TLS: Certificate Expired		5.0 (Medium)	99 %	172.16.14.52		1515/tcp	Fri, May 24, 2024 2:55 AM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)		5.0 (Medium)	70 %	172.16.14.52		1515/tcp	Fri, May 24, 2024 3:00 AM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	172.16.14.52		9300/tcp	Fri, May 24, 2024 2:55 AM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	172.16.14.52		9200/tcp	Fri, May 24, 2024 2:55 AM UTC
TCP Timestamps Information Disclosure		2.6 (Low)	80 %	172.16.14.52		general/tcp	Fri, May 24, 2024 2:54 AM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	172.16.14.52		general/icmp	Fri, May 24, 2024 2:54 AM UTC

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

1 - 9 of 9



1 - 5 of 5

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	172.16.14.53		general/tcp	Fri, May 24, 2024 2:44 AM UTC
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80 %	172.16.14.53		135/tcp	Fri, May 24, 2024 3:08 AM UTC

Methodology

For the vulnerability scan we used the OpenVAS tool; Greenbone Security Assistant to scan three assets on the network. We used this tool and executed the scan on a Kali Linux distribution machine. The scanner itself is a web GUI interface which allows us to control scans and access vulnerabilities.

We then made sure that our assets which we wanted to scan for any vulnerabilities were on the network and functioning, the assets we used are Windows 1, Ubuntu Linux, and Windows Server.

For the scan itself, we performed a quick scan, which was selected from under the Scans tab, then the wand icon, and finally selecting the "task wizard" option. This allowed us to get the most relevant data and vulnerabilities in a time effective manner. This scan was used on all 3 assets.

Findings

We were able to scan all three assets, the Windows 1, the Ubuntu Linux, and the Windows server respectively. All the scan completed successfully, and the following are the vulnerabilities which should be focused on.

Windows 1 - (172.16.14.50)

Vulnerability – High 10:

- Greenbone Community Edition used for the scan is an outdated or end of life scan engine. Having an outdated version of the scanner impacts the scan by losing certain functionalities not having the most recent of bug fixes.
- **NIST SP 800-53 Rev. 5 SI-2: Flaw Remediation**.
    - According to the National Vulnerability Database (NVD), the presence of outdated software components is a common source of vulnerabilities. For instance, outdated scanning engines may fail to detect newer threats that have emerged since the last update. **CVE-2019-25047** and **CVE-2018-25016**

Vulnerability – Medium 4.3:

- All services providing an encrypted communication using TLSv1.0 or TLSv1.1 protocol are affected, with the impact allowing attackers the ability to use unknown cryptographic flaws to eavesdrop the connection between client and the service to get access to sensitive data.

- **NIST SP 800-52 Rev. 2: Guidelines for TLS Implementations**.
    - The NVD lists several vulnerabilities associated with outdated versions of TLS, such as TLSv1.0 and TLSv1.1. These vulnerabilities often allow attackers to intercept and decrypt communications. The NVD recommends upgrading to TLSv1.2 or higher to avoid these risks and ensure secure data transmission. **CVE-2011-3389** and **CVE-2015-0204**

Ubuntu Linux – (172.16.14.52)

Vulnerability – High 7.5:

- It was possible to log into web application using default credentials. This issue may be exploited by remote attacker to perhaps gain access to sensitive information or modify system configuration.
- **NIST SP 800-53 Rev. 5 CM-7: Least Functionality**.
    - Limiting functionality to the minimum necessary for business operations is a key principle of this guideline. Allowing service enumeration exposes unnecessary information, violating this principle and increasing the risk of exploitation. **CVE-1999-0501**, **CVE-1999-0502**, **CVE-1999-0507**, and **CVE-1999-0508**

Vulnerability – High 7.5:

- Remote OSSEC-authd service is not protected by password authentication or client certification verification. During the detection method, a test was conducted, and we were able to connect to the remote service with out having to provide a password or a client certificate. This issue may be exploited by a remote attacker to register arbitrary agents at the remote service or overwrite the registration of existing ones taking them out of service.
- **NIST SP 800-53 Rev. 5 IA-5: Authenticator Management.**
    - The NVD frequently highlights the risks associated with weak or missing passwords. For example, missing passwords can lead to unauthorized access, as documented in numerous vulnerability entries. The NVD advises implementing strong password policies and multi-factor authentication to mitigate such risks. **CVE-2020-8447**

Vulnerability – Medium 5.0:

- Remote SSL/TLS service is prone to a DoS attack since the service does not properly restrict client-initiated renegotiation with the SSL and TLS protocol. This vulnerability might make it easier for the remote attacker to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

- **NIST SP 800-52 Rev. 2: Guidelines for TLS Implementations.**
    - Misconfigurations in TLS setups are commonly reported in the NVD, especially those that enable DoS attacks. The NVD details the importance of correctly configuring TLS settings to prevent renegotiation vulnerabilities, which can lead to resource exhaustion and service disruption. **CVE-2011-1473** and **CVE-2011-5094**

Windows Server – (172.16.14.53)

Vulnerability - Medium 5.0:

- DCE/RPC or MSRPC services running on the remote host can be enumerated by connect on port 135 and doing the appropriate queries. This opening allows the attacker to use these ports to gain access to and abuse knowledge about the remote host.
- **NIST SP 800-53 Rev. 5 SC-7: Boundary Protection.**
    - The NVD describes service enumeration as a significant risk, as it can reveal valuable information to attackers. Entries in the NVD recommend restricting access to services and implementing network segmentation to reduce the risk of enumeration and subsequent exploitation. **CVE-2015-2370**

Risk Assessment

The process:

Risk Assessment is implemented through the Risk Assessment Table. The Risk Assessment process is coordinated by the information security analyst, identification of threats and vulnerabilities is performed by asset owners, and assessment of consequences and likelihood is performed by risk owners. Cat in selective situations will have the same asset owner and risk owner for a given asset.

Cat and the executive team will be the main risk and asset owners (due to the limited information provided).

The Assets:

- Windows 1 (scanned asset)
- Windows Server (scanned asset)
- Ubuntu Linux (scanned asset)
- Kali Linux (used to host scanner)

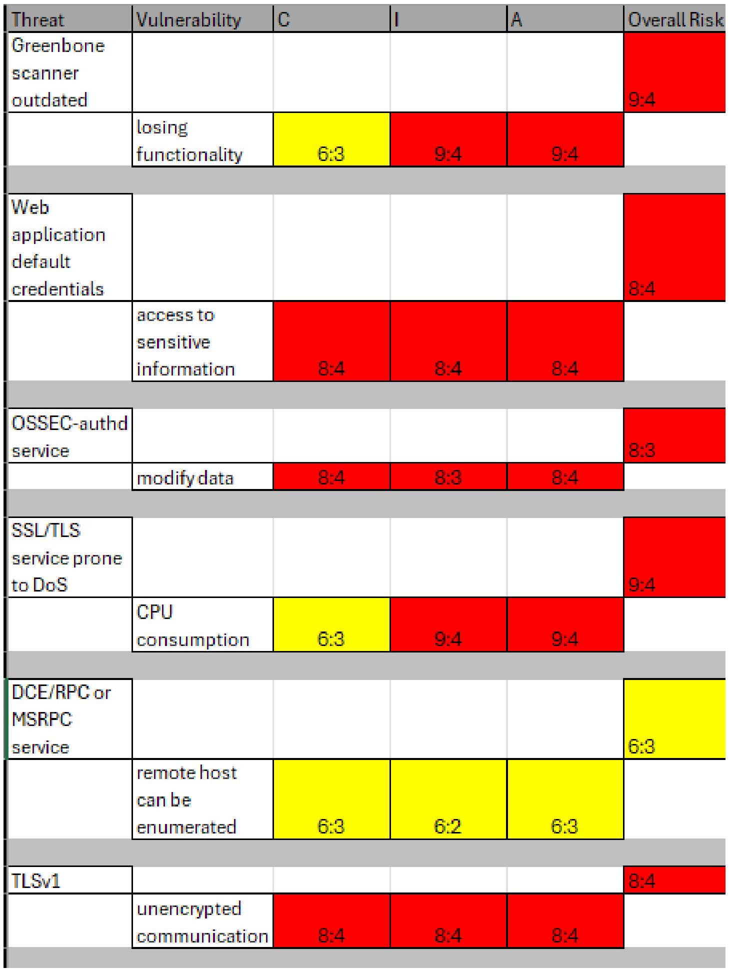
Impact and likelihood:

After risk owners have been identified, it is necessary to assess impacts for each combination of threats and vulnerabilities for an individual asset if such a risk materializes:

High Impact	7-10	Loss of confidentiality, availability, or integrity has considerable and/or immediate impact on the organization's cash flow, operations, legal or contractual obligations, or its reputation.
Mid Impact	4-6	Loss of confidentiality, availability, or integrity incurs costs and has a low or moderate impact on legal or contractual obligations, or the organization's reputation.
Low Impact	0-3	Loss of confidentiality, availability, or integrity does not affect the organization's cash flow, legal or contractual obligations, or its reputation.

After the assessment of consequences, it is necessary to assess the likelihood of occurrence of such a risk.

High Likelihood	4-5	Existing security controls are low or ineffective. Such incidents have a high likelihood of occurring in the future.
Mid Likelihood	2-3	Existing security controls are moderate and have mostly provided an adequate level of protection. New incidents are possible, but not highly likely.
Low Likelihood	0-1	Existing security controls are strong and have so far provided an adequate level of protection. No new incidents are expected in the future



Threat	Vulnerability	C	I	A	Overall Risk
Greenbone scanner outdated					9:4
	losing functionality	6:3	9:4	9:4	
Web application default credentials					8:4
	access to sensitive information	8:4	8:4	8:4	
OSSEC-authd service					8:3
	modify data	8:4	8:3	8:4	
SSL/TLS service prone to DoS					9:4
	CPU consumption	6:3	9:4	9:4	
DCE/RPC or MSRPC service					6:3
	remote host can be enumerated	6:3	6:2	6:3	
TLSv1					8:4
	unencrypted communication	8:4	8:4	8:4	

Recommendation

The top 6 recommendations we want to focus on are as listed below with (1) being the most important and (6) being the least important:

1. Greenbone scanner outdated.
2. Web application default credentials.
3. OSSEC-authd service no password and no certifications.
4. SSL/TLS service prone to DoS.
5. DCE/RPC or MSRPC service running on remote host can be enumerated.
6. TLSv1 used for encrypted communication.

After reviewing the vulnerabilities, the following are a list of actions that can be taken as per the above vulnerability ranking from 1-6 along with the NIST framework used:

Vulnerability 1 – Greenbone scanner outdated.

A scan engine is a core component of a vulnerability scanner, responsible for identifying and reporting security vulnerabilities. An outdated scan engine lacks the latest updates, which could result in missed vulnerabilities.

For this vulnerability we can apply a quick and easy fix such as update the scanner to the latest version. By doing so we can make sure that the scans being executed are capturing the most accurate and complete of vulnerabilities, free from bugs.

MITRE ATT&CK: Defense Evasion - Software Update.

- Regularly updating security tools ensures that the latest vulnerabilities are detected and mitigated, aligning with industry best practices for maintaining robust defense mechanisms.

Vulnerability 2 – Web application default credentials.

Default credentials are predefined username and password combinations set by software vendors. Missing or default credentials pose significant security risks as they can be easily exploited by attackers.

For this vulnerability we should implement a strong password protection and consider using additional layers of authentication such as MFA

MITRE ATT&CK: Credential Access - Password Policies.

- Implementing strong password policies and additional authentication layers prevents unauthorized access, thereby enhancing the overall security posture.

Vulnerability 3 – OSEC-authd service which has no password and no certifications.

Service enumeration involves identifying active services on a networked device, which can provide attackers with critical information to exploit vulnerabilities.

Similarly, as the prior resolutions, we will need to implement client certifications and password authentication for the service to secure the vulnerability.

MITRE ATT&CK: Credential Access - Password Policies.

- Implementing strong password policies and additional authentication layers prevents unauthorized access, thereby enhancing the overall security posture.

Vulnerability 4 – SSL/TLS Service prone to DoS attack.

DoS (Denial of Service) attacks aim to make a machine or network resource unavailable to its intended users by overwhelming it with traffic. Improper TLS configuration can make systems susceptible to such attacks.

For this vulnerability a possible resolution is to either remove or disable the renegotiation option altogether. Or alternatively we can also contact the vendor to obtain a patch for the service.

MITRE ATT&CK: Denial of Service - Network DoS.

- Proper configuration and patch management are critical to preventing DoS attacks, ensuring the availability and reliability of services.

Vulnerability 5 – DCE/RPC or MSRPC service running on remote host which can be enumerated.

Open ports are communication endpoints through which data enters or exits a network. Having too many open ports increases the risk of unauthorized access and exploitation.

For this vulnerability since the risk are the ports, we can implement a filter for incoming traffic on the following ports: 2103, 2105, 2107, 49664, 49665, 49666, 49667, 49668, 49669, 49671, 49672, 49673.

MITRE ATT&CK: Defense Evasion - Network Segmentation.

- By restricting and regularly auditing open ports, organizations can reduce the likelihood of unauthorized access and limit the potential attack vectors.

MITRE ATT&CK: Defense Evasion - Firewall Rules.

- Properly configured firewall rules and network segmentation help in minimizing the risk of service enumeration and potential exploitation.

Vulnerability 6 – TLSv1 used for encrypted communications.

TLS (Transport Layer Security) is a protocol for securing communications over a computer network. Older versions (TLSv1.0 and TLSv1.1) have known vulnerabilities that can be exploited to intercept or manipulate data.

Like the first vulnerability, instead of using version of TLS which allows for eavesdropping over the communication, we can upgrade to a version which is above TLSv1.2 allowing us to truly secure our communications in transit and at rest.

MITRE ATT&CK: Network Evasion - Protocol Upgrades.

- Using the latest and most secure versions of communication protocols ensures data integrity and confidentiality, protecting against interception and manipulation.

References

Feilner, M. (2024, May 21). *Vulnerability Management | Open source and GDPR-compliant - Greenbone*. Greenbone. https://www.greenbone.net/en/

MITRE ATT&CK®. (n.d.-c). https://attack.mitre.org/

CSF Tools. (2021, March 5). *Flaw remediation - CSF tools*. CSF Tools - the Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/si/si-2/

CSF Tools. (2021a, March 5). *Authenticator Management - CSF Tools*. CSF Tools - the Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r4/ia/ia-5/

CSF Tools. (2021c, March 5). *Least functionality - CSF tools*. CSF Tools - the Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r5/cm/cm-7/

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.-b). *TLS Guidelines: NIST Publishes SP 800-52 Revision 2 | CSRC*. https://csrc.nist.gov/News/2019/nist-publishes-sp-800-52-revision-2

CSF Tools. (2021b, March 5). *Boundary Protection - CSF tools*. CSF Tools - the Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r4/sc/sc-7/

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.-b). *Release Search - NIST Risk Management Framework | CSRC | CSRC*. https://csrc.nist.rip/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=RA-5