Cat's Company Vulnerabilities

By: Danielle Daza

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On December 12, 2024, three types of scans each were conducted on the Linux Host and Windows11 machines using OpenVAS Vulnerability Scanner – Discovery, Full and Fast, and Full and Fast with login credentials. With the ranges of these scans, varying tiers of access have revealed the overall security posture of the company network allowing for a holistic understanding of the vulnerabilities present and prioritize them appropriately for remediation.

From the scans conducted, there were several vulnerabilities of note found within the Linux Host, the most critical in severity revealing how susceptible the system is to Brute Force attacks and some vulnerabilities revealing that software and application versions being not properly updated. Though all the vulnerabilities found will be thoroughly explained within this report, the six most in-need of attention will have supplementary information in regards to recommended mitigations provided. Overall, the solutions come down to refining account use policies, implementing stricter password setting standards, updating/upgrading software and application versions, and ensuring transmissions of sensitive data are utilizing encrypted channels. Though the solutions and mitigations are not very numerous, that is precisely the reason they must be carried out. These vulnerabilities place the organization's data confidentiality, integrity and availability of use at risk as these three aspects of an organization's data systems effectively result in financial and reputational consequences. As such, the recommendations within this report have been carefully compiled to ensure a swift remediation of these most critical vulnerabilities.

SCAN RESULTS

The following table is a summary of the scan results from the scans conducted on both machines in order of the sophistication of the scans conducted. Within the table it includes the type of scan conducted that were able to discover the vulnerability, the machine it was found on, the date of discovery, the name and brief description of the vulnerability as well as a CVSS severity rating.

The **affected ports** simply identify the system's ports that are most affected by the vulnerability as in what methods of communications does the vulnerability utilize. This heading influences the impact, likelihood and consequently the risk ratings. The **CVE notes** provide relevant CVE vulnerability registered details (that could be found in the industry-standard NIST database) that are relevant to those vulnerabilities found within the systems. The **CVSS severity ratings** are the ratings determined by the Common Vulnerability Scoring System (CVSS) which is a standardized framework for measuring information system's severity of security flaws from 0-10. It is worth noting that as this rating system is standardized for use of all types of organizations and does not consider individual organizations' network infrastructure or business composition, it should not be the deciding factor in determining its priority ranking as a vulnerability.

Severity of Vulnerability	Scan Discovered Through	Machine	Date of Discovery	Name of Vulnerability	Description	Affected Ports	CVE Notes	CVSS Severity Rating (0-10)
Critical								
High	Discovery/ Full and Fast/ Full and Fast with credentials	Windows11	2024-12-12	TCP Timestamps Information Disclosure	A side effect of this feature is that the uptime of the remote host can sometimes be computed.	General TCP	N/A	2.6
Medium	Discovery/ Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	ICMP Timestamp Reply Information Disclosure	The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.	General ICMP	CVE-1999-0524	2.1
Low	Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	TCP Timestamps Information Disclosure	A side effect of this feature is that the uptime of the remote host can sometimes be computed.	General TCP	N/A	2.6
	Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	Weak MAC Algorithm(s) Supported (SSH)	The remote SSH server is configured to allow / support weak MAC algorithm(s).	22/TCP	N/A	2.6
	Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	FTP Unencrypted Cleartext Login	An attacker can uncover login names and passwords by sniffing traffic to the FTP service.	21/TCP	N/A	4.8
	Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	Cleartext Transmission of Sensitive Information via HTTP	An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.	80/TCP	N/A	4.8
	Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	Anonymous FTP Login Reporting	A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.	21/TCP	CVE-1999-0497	6.4
	Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	FTP Brute Force Logins Reporting	It was possible to login into the remote FTP server using weak/known credentials.	21/TCP	1999-0507CVE-1999-0508CVE-2001-1594CVE-2013-7404CVE-2014-9198CVE-2015-7261CVE-2016-6751CVE-2017-8218CVE-2018-9068CVE-2018-17771CVE-2018-	7.5
	Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	Riello NetMan 204 Default Credentials (SSH)	The remote Riello NetMan 204 network card is using known default credentials for the SSH login.This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.	22/TCP		7.5

Figure 1.1 – Compiled OpenVAS scans 1/2

	Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	SSH Brute Force Logins With Default Credentials Reporting	It was possible to login into the remote SSH server using default credentials.	22/TCP	CVE-1999-0501CVE-1999-0502CVE-1999-0507CVE-1999-0508CVE-2020-29583CVE-2020-9473CVE-2023-1944CVE-2024-22902CVE-2024-31970CVE-2024-46128	9.8
	Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark Security Update (wnpa-sec-2024-09) - Linux	Wireshark is prone to an use after free vulnerability.	General/TCP	CVE-2024-4853	2.6
	Full and Fast (with credentials)	Linux Host	2024-12-12	Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware vulnerabilities	The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'SSB - Speculative Store Bypass' hardware vulnerabilities.	General/TCP	CVE-2018-3639	5.5
	Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark Multiple Vulnerabilities (Jun 2024) - Linux	Successful exploitation allows an attacker to cause denial of service.	General/TCP	CVE-2024-4853CVE-2024-4854	6.6
	Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark < 4.2.0 DoS Vulnerabilities	Successful exploitation may allow remote attackers to perform denial of service on an affected system.	General/TCP	CVE-2024-24478CVE-2024-24479	6.6
	Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark Security Update (wnpa-sec-2023-08) - Linux	It may be possible to make Wireshark crash by injecting a malformed packet onto the wire or by convincing someone to read a malformed packet trace file.	General/TCP	CVE-2023-1161	7.1
	Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark Security Update (wnpa-sec-2023-29) - Linux	Successful exploitation allows an attacker to cause denial of service.	General/TCP	CVE-2023-6175	7.1
	Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark Security Multiple DoS Vulnerabilities (Apr 2023) - Linux	Wireshark is prone to multiple denial of service (DoS) vulnerabilities.	General/TCP	CVE-2023-1992CVE-2023-1993CVE-2023-1994	7.5

Figure 1.2 – Compiled OpenVAS scans 2/2

The results above contain only the information compiled from the OpenVAS vulnerability scans without any additional input in terms of risk assessment as a later section will cover that assessment. The following scans were conducted (sequentially):

1. Discovery
    - Very surface-level scan, collects information about open ports, used hardware, firewalls, used services, installed software and certificates (10 Scanning a System, 2022).
2. Full and Fast

- Configured scan based on information gathered in the previous port scan and uses almost all vulnerability tests to discover as much information as possible about the targeted system without credentials (10 Scanning a System, 2022).
- The vulnerability tests are optimized in order to keep potential false positive rates low (10 Scanning a System, 2022).

3. Full and Fast (with credentials/login details for network access)
    - Full and fast scan with additional access to discover vulnerabilities from the perspective of a user who has authorized access to the network (10 Scanning a System, 2022).
    - Discovers vulnerabilities that would affect specific applications on the system that could not be discovered without credentials.

Utilizing these types of scans gives a grounded view of what vulnerabilities are exploitable, at what level of access and the likelihoods of those vulnerabilities. In the following section, further rationale will be provided for why each specific scan was conducted.

METHODOLOGY

The main tool utilized for the scans was OpenVAS Vulnerability Scanner which offers several types of scans to conduct on a target system. This tool is an open-source vulnerability scanner and offers comprehensive vulnerability scanning that aims to detect a wide range of vulnerabilities such as network services, web applications, operating systems, databases, etc (Greenbone, 2024). Moreover, as OpenVAS relies on a constantly updated database of known vulnerabilities (CVE), its database contains tests for over 50,000 vulnerabilities which are continuously added or modified to remain current with the evolving threat landscape (Greenbone, 2024).

Below is the list of scans conducted and the rationale of the selected.

Scan Conducted	Rationale
Discovery scan	In order to confirm the most conspicuous vulnerabilities and determine the severity.
Full and fast	In order to discover the less evident vulnerabilities that are exploitable with a more actively-searching eye.
Full and fast (with login details)	In order to understand the vulnerabilities apparent within the system from a user that can access the system with credentials.

FINDINGS

Machine	Scan Conducted	Results	Notes
Windows11	Discovery scan	Successfully scanned	Revealed 1 vulnerability
	Full and fast	Successfully scanned	Revealed 1 vulnerability
	Full and fast (with login details)	Successfully scanned	Revealed 1 vulnerability
Linux	Discovery scan	Successfully scanned	Revealed 1 vulnerability.
	Full and fast	Successfully scanned	Revealed 9 vulnerabilities
	Full and fast (with login details)	Successfully scanned	Revealed 16 vulnerabilities

RISK ASSESSMENT

Within this section, a comprehensive table of the scan results have been compiled for ease of grasping the gravity of the vulnerabilities found and what systems it affects. However, a few notes on select headings within the table have been provided below:

- In regards to how the **impact** rating was determined, the CIA triad was used for reference which stipulates that any security concern would in some way affect the information systems' confidentiality (i.e. protection of sensitive information), integrity (protection of data from unauthorized modification or destruction) and availability (assurance of timely and reliable access to data and systems by authorized users) (How to Determine Cybersecurity Impact Level Using FIPS 199, 2023).
- The **impact** and **likelihood** ratings given for each vulnerability were determined after examining that particular systems, ports and applications the vulnerabilities affect as well

as if the vulnerabilities are dependent on if credentials need to be used in order to exploit the vulnerabilities.

- For example, if there is a vulnerability with a high CVSS Severity Rating only affects a specific application after credentials have been authenticated in a generally isolated capacity, it may not be as high of a priority as something of a medium severity rating that affects a high-traffic port.

Below is a comprehensive table of the vulnerabilities and risk assessment.

Scan Discovered Through	Machine	Data of Discovery	Name of Vulnerability	Description	CVSS Severity Rating (0-10)	Impact (0-3)			Likelihood	Risk (I+L)	Priority (Severity Rating+Risk)
						Confidentiality	Integrity	Availability			
Discovery/ Full and Fast/ Full and Fast with credentials	Windows11	2024-12-12	TCP Timestamps Information Disclosure	A side effect of this feature is that the uptime of the remote host can sometimes be computed.	2.6	0	2	0	2	4	6.6
Discovery/ Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	ICMP Timestamp Reply Information Disclosure	The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.	2.1	1	0	0	2	3	5.1
Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	TCP Timestamps Information Disclosure	A side effect of this feature is that the uptime of the remote host can sometimes be computed.	2.6	0	2	0	2	4	6.6
Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	Weak MAC Algorithm(s) Supported (SSH)	The remote SSH server is configured to allow / support weak MAC algorithm(s).	2.6	1	2	0	3	6	8.6
Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	FTP Unencrypted Cleartext Login	An attacker can uncover login names and passwords by sniffing traffic to the FTP service.	4.8	3	0	2	7	12	16.8
Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	Cleartext Transmission of Sensitive Information via HTTP	An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.	4.8	3	3	1	6	13	17.8
Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	Anonymous FTP Login Reporting	A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.	6.4	3	2	0	7	12	18.4
Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	FTP Brute Force Logins Reporting	It was possible to login into the remote FTP server using weak/known credentials.	7.5	3	3	2	8	18	25.5
Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	Riello NetMan 204 Default Credentials (SSH)	The remote Riello NetMan 204 network card is using known default credentials for the SSH login.This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.	7.5	3	3	2	8	18	25.5
Full and Fast/ Full and Fast (with credentials)	Linux Host	2024-12-12	SSH Brute Force Logins With Default Credentials Reporting	It was possible to login into the remote SSH server using default credentials.	9.8	3	3	2	8	18	25.8
Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark Security Update (wnpa-sec-2024-09) - Linux	Wireshark is prone to an use after free vulnerability.	2.6	2	0	0	2	4	6.6

Figure 2.1 – Risk assessment and relevant ratings 1/2

Full and Fast (with credentials)	Linux Host	2024-12-12	Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware vulnerabilities	The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'SSB - Speculative Store Bypass' hardware vulnerabilities.	5.5	0	0	2	5	7	12.5
Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark Multiple Vulnerabilities (Jun 2024) - Linux	Successful exploitation allows an attacker to cause denial of service.	8.8	0	0	3	7	10	18.8
Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark < 4.2.0 DoS Vulnerabilities	Successful exploitation may allow remote attackers to perform denial of service on an affected system.	8.8	0	0	3	7	10	18.8
Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark Security Update (wnpa-sec-2023-08) - Linux	It may be possible to make Wireshark crash by injecting a malformed packet onto the wire or by convincing someone to read a malformed packet trace file.	7.1	1	3	3	8	15	22.1
Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark Security Update (wnpa-sec-2023-29) - Linux	Successful exploitation allows an attacker to cause denial of service.	7.2	0	0	3	7	10	17.2
Full and Fast (with credentials)	Linux Host	2024-12-12	Wireshark Security Multiple DoS Vulnerabilities (Apr 2023) - Linux	Wireshark is prone to multiple denial of service (DoS) vulnerabilities.	7.5	0	0	3	7	10	17.5

Figure 2.2 – Risk assessment and relevant ratings 2/2

Below is a shortened table of the vulnerabilities ordered by its priority score that was calculated in the previous table.

Priority Score (Severity+Risk)	Machine	Vulnerability	Description
25.8	Linux host	SSH Brute Force Logins With Default Credentials Reporting	It was possible to login into the remote SSH server using default credentials.
23.5	Linux host	FTP Brute Force Logins Reporting	It was possible to login into the remote FTP server using weak/known credentials.
22.1	Linux host	Wireshark Security Update (wnpa-sec-2023-08) - Linux	It may be possible to make Wireshark crash by injecting a malformed packet onto the wire or by convincing someone to read a malformed packet trace file.
21.5	Linux host	Riello NetMan 204 Default Credentials (SSH)	The remote Riello NetMan 204 network card is using known default credentials for the SSH login.This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.
18.4	Linux host	Anonymous FTP Login Reporting	A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.
17.8	Linux host	Cleartext Transmission of Sensitive Information via HTTP	An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
17.5	Linux host	Wireshark Security Multiple DoS Vulnerabilities (Apr 2023) - Linux	Wireshark is prone to multiple denial of service (DoS) vulnerabilities.
17.2	Linux host	Wireshark Security Update (wnpa-sec-2023-29) - Linux	Successful exploitation allows an attacker to cause denial of service.
16.8	Linux host	FTP Unencrypted Cleartext Login	An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
16.8	Linux host	Wireshark < 4.2.0 DoS Vulnerabilities	Successful exploitation may allow remote attackers to perform denial of service on an affected system.
16.6	Linux host	Wireshark Multiple Vulnerabilities (Jun 2024) -	Successful exploitation allows an attacker to cause denial of service.
12.5	Linux host	Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass'	The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'SSB - Speculative Store Bypass' hardware vulnerabilities.

Figure 3.1 – Prioritized vulnerabilities 1/2

8.6	Linux host	Weak MAC Algorithm(s) Supported (SSH)	The remote SSH server is configured to allow / support weak MAC algorithm(s).
6.6	Windows11	TCP Timestamps Information Disclosure	A side effect of this feature is that the uptime of the remote host can sometimes be computed.
6.6	Linux host	TCP Timestamps Information Disclosure	A side effect of this feature is that the uptime of the remote host can sometimes be computed.
6.6	Linux host	Wireshark Security Update (wnpa-sec-2024-09) - Linux	Wireshark is prone to an use after free vulnerability.
5.1	Linux host	ICMP Timestamp Reply Information Disclosure	The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Figure 3.2 – Prioritized vulnerabilities 2/2

With the vulnerabilities thoroughly explored, the following section further explains the effects on the security posture of the company and the potential consequences of the exploitation of these vulnerabilities as well as recommended remediations.

RECOMMENDATIONS

The following table will summarize recommendations for what would most likely minimize the likelihood of exploiting the discovered vulnerabilities. The following table will only address the vulnerabilities with critical severity rankings along with the first three highest vulnerabilities under the high severity rating in order to best relegate resources to the most vulnerable aspects present in the systems.

Below is a summary table outlining the main effects of the six most urgent vulnerabilities discovered.

Priority Score (Severity+Risk	Machine	Vulnerability	Effect on security posture	Recommended Mitigations	Description
25.8	Linux host	SSH Brute Force Logins With Default Credentials Reporting	Security breach risk, data integrity and confidentiality risks, operational disruption, reputation damage	Account Use Policies	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges (Brute Force, 2024).
				Multi-Factor Authentication	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services (Brute Force, 2024).
				Password Policies	Refer to NIST guidenlines when creating password policies (Brute Force, 2024).
				User Account Management	Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts (Brute Force, 2024).
23.5	Linux host	FTP Brute Force Logins Reporting	Security breach risk and unauthorized access, lateral movement for attacks, loss of data integrity, reputation damage	Account Use Policies	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges (Brute Force: Password Guessing , 2024).
				Multi-Factor Authentication	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services (Brute Force: Password Guessing , 2024)
				Password Policies	Refer to NIST guidenlines when creating password policies (Brute Force: Password Guessing , 2024)
				Update Software	Upgrade management services to the latest supported and compatible version. Specifically, any version providing increased password complexity or policy enforcement preventing default or weak passwords (Brute Force: Password Guessing , 2024).
22.1	Linux host	Wireshark Security Update (wnpa-sec-2023-08) - Linux	Remote code execution, compromise of network security, access to internal systems, loss of confidentiality, integrity, availability, reputation damage	Upgrade Application	Upgrade to Wireshark 4.0.4, 3.6.12 or later (Wireshark, 2023).

Figure 4.1 – Highest-priority vulnerabilities and recommended Mitigations 1/2

21.5	Linux host	Riello NetMan 204 Default Credentials (SSH)	Network compromise, denial of service (DoS), data loss, corruption, reputation damage	Account Use Policies	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges (Brute Force, 2024).
				Multi-Factor Authentication	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services (Brute Force, 2024).
				Password Policies	Refer to NIST guidenlines when creating password policies (Brute Force, 2024).
				User Account Management	Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts (Brute Force, 2024).
18.4	Linux host	Anonymous FTP Login Reporting	Security breach risk, malware distribution, integrity compromise, reputation damage	Disable Anonymous Logins	If sharing files is not necessary, anonymous logins should be disabled (Anonymous FTP Login Reporting , 2018).
17.8	Linux host	Cleartext Transmission of Sensitive Information via HTTP	Data intercepting and eavesdropping, data breach, loss of confidential information, reputation damage	Utilize SSL/TLS Connections	Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions (CWE, 2023).

Figure 4.2 – Highest-priority vulnerabilities and recommended Mitigations 2/2

Evident from the table above, there are overlapping solutions to the most urgent vulnerabilities as well as simple updates/upgrades required of some applications in order to mitigate the possibility of these vulnerabilities being exploited. As such, these mitigations have been carefully compiled and recommended to ensure these vulnerabilities do not pose neither a financial nor a reputational risk before the next vulnerability assessment. It is highly recommended

that these mitigations be enforced within the company's security policies as without these implementations, the security posture of the company is left susceptible to incidents of compromise.

CAT'S 5-7 MINUTE BRIEFING SUMMARY

On December 12, 2024, three types of scans each were conducted on the Linux Host and Windows11 machines using OpenVAS Vulnerability Scanner – Discovery, Full and Fast, and Full and Fast with login credentials. With the ranges of these scans, varying tiers of access have revealed the overall security posture of the company network allowing for a holistic understanding of the vulnerabilities present and prioritize them appropriately for remediation.

From the scans conducted, there were several vulnerabilities of note found within the Linux Host, the most critical in severity revealing how susceptible the system is to Brute Force attacks and some vulnerabilities revealing that software and application versions being not properly updated. All discovered vulnerabilities will not be discussed in detail, however the six most critical in severity will be the focus of this presentation and succinctly explained along with the necessary recommendations for remediation.

The common denominators of these vulnerabilities in terms of Incidents of Compromise (IoCs) associated are Brute Force attacks, Denial-of-Service attacks, and Remote Code Execution. To briefly overview the effects of these types of attacks, they generally entail security data breaches, data loss or tampering, unauthorized user access into the organization network. These all ultimately result in financial loss (e.g. ransomware, operations rendered unavailable, sensitive data becoming known to competitors, tampered data influencing high stakes decisions) and/or reputational damage (e.g. due to data breaches becoming public knowledge, services being perceived as unreliable, mistakes made based on inaccurate data).

Overall, the solutions come down to refining account use policies, implementing stricter password setting standards, updating/upgrading software and application versions, and ensuring transmissions of sensitive data are utilizing encrypted channels. Though the solutions and

mitigations are not very numerous, that is precisely the reason they must be carried out. These vulnerabilities place the organization's data confidentiality, integrity and availability of use at risk as these three aspects of an organization's data systems effectively result in financial and reputational consequences. As such, the recommendations within this report have been carefully compiled to ensure a swift remediation of these most critical vulnerabilities.

REFERENCES

Brute Force: Password Guessing . (2024, October 14). Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1110/001/

CWE-319: Cleartext Transmission of Sensitive Information . (2023, January 24). Retrieved from Common Weakness Enumeration (CWE): https://cwe.mitre.org/data/definitions/319.html

10 Scanning a System. (2022). Retrieved from Greenbone: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/scanning.html

Anonymous FTP Login Reporting . (2018, October 22). Retrieved from Pentest tools: https://pentest-tools.com/vulnerabilities-exploits/anonymous-ftp-login-reporting_14315

Brute Force. (2024, October 14). Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1110/

Discovery Scan. (2023). Retrieved from Rapid7: https://help.rapid7.com/metasploit/Content/scanning/discovery-scan.html

Greenbone. (2024). Retrieved from Greenbone Background: https://greenbone.github.io/docs/latest/background.html

How to Determine Cybersecurity Impact Level Using FIPS 199. (2023, Aug 16). Retrieved from LinkedIn: https://www.linkedin.com/pulse/how-determine-cybersecurity-impact-level-using-fips-199

wnpa-sec-2023-08 · ISO 15765 and ISO 10681 dissector crash. (2023, March 2). Retrieved from Wireshark: https://www.wireshark.org/security/wnpa-sec-2023-08.html