Vulnerability Management report for CAT's Network

Table of Contents

Introduction:

In today's interconnected digital landscape, ensuring the security of network infrastructures is paramount to safeguarding sensitive data and maintaining operational integrity. As technology continues to evolve, so do the methods employed by cyber threats, necessitating proactive measures to identify and mitigate potential vulnerabilities.

The following report presents the findings of a comprehensive security assessment conducted on the CAT target system using OpenVAS, a widely used vulnerability scanning tool. This assessment, performed on April 4, 2024, aimed to evaluate the security posture of the CAT network by identifying weaknesses, misconfigurations, and potential entry points for malicious actors.

As organizations increasingly rely on networked systems to conduct business operations and store confidential information, the importance of regular security assessments cannot be overstated. By conducting routine scans and vulnerability assessments, organizations can stay ahead of emerging threats, fortify their defenses, and minimize the risk of security breaches.

Scope:

The scope of this assessment encompassed three specific IP addresses within the CAT network: 172.16.14.50(Windows workstations), 172.16.14.52(Linux Machine), and 172.16.14.53(Winserver). By focusing on these addresses, the scan aimed to provide targeted insights into the security posture of critical network components, allowing for informed decision-making regarding risk mitigation strategies.

In an era characterized by ever-evolving cyber threats, maintaining a proactive approach to cybersecurity is essential for organizations of all sizes. By leveraging tools like OpenVAS to conduct regular security assessments, organizations can identify and address vulnerabilities before they can be exploited by malicious actors, thereby safeguarding their digital assets and preserving the trust of their stakeholders.

Methodology:

- The security assessment was conducted to evaluate the security posture of the CAT target system and identify potential vulnerabilities that could pose risks to the confidentiality, integrity, and availability of its resources. This assessment was part of routine security measures to ensure compliance with industry standards and best practices.
- The assessment focused on the CAT target system, including its network infrastructure, servers, and applications. Specifically, it targeted IP addresses 172.16.14.50, 172.16.14.52, and 172.16.14.53.
- The assessment utilized OpenVAS, an open-source vulnerability scanning tool, to conduct automated scans of the target system. OpenVAS was chosen for its comprehensive vulnerability database and ability to perform in-depth assessments of various types of vulnerabilities.
- The assessment followed a systematic approach, starting with reconnaissance to gather information about the target system, followed by vulnerability scanning to identify potential weaknesses, and concluding with manual verification of critical findings to validate their severity and impact.
- Data collected during the assessment included scan results, system logs, and network traffic captures. This data was carefully analyzed to identify vulnerabilities, prioritize remediation efforts, and generate comprehensive reports detailing the findings.
- The results of the assessment were documented in a detailed report, which included an executive summary, scan results, methodology, findings, risk assessment, recommendations, and conclusion. The report was shared with relevant stakeholders to inform decision-making and prioritize security initiatives based on identified risks and vulnerabilities.

1. Assessment scan Results and Findings:

The vulnerability assessment conducted on the CAT target system yielded significant insights into the security posture of the network. Below is a summary of the overall assessment results:

1.a. Summary of Overall Vulnerability Assessment Results:

- The assessment identified a total of 56 vulnerabilities across the three specified IP addresses: 172.16.14.50, 172.16.14.52, and 172.16.14.53.
- These vulnerabilities span various categories, including software vulnerabilities, misconfigurations, and network weaknesses.

1.b. Categorization of Vulnerabilities Based on Severity Levels:

- **Critical**: 5 vulnerabilities were classified as critical, representing severe security risks that require immediate attention to mitigate potential exploitation and data breaches.
- **High**: 12 vulnerabilities were categorized as high severity, indicating significant threats to the integrity and confidentiality of the network.
- **Medium**: 22 vulnerabilities fell into the medium severity category, signaling potential risks that could be exploited by determined attackers to compromise system functionality or access sensitive information.

- **Low**: 17 vulnerabilities were classified as low severity, representing relatively minor risks that still warrant remediation to enhance overall security posture.

1.c. Breakdown of Vulnerabilities by Type:

- **Software Vulnerabilities**: 24 vulnerabilities were attributed to flaws within software components, such as outdated software versions, known security vulnerabilities, or insecure configurations.
- **Configuration Issues:** 15 vulnerabilities stemmed from misconfigurations in network devices, servers, or applications, highlighting the importance of proper configuration management practices.
- **Network Weaknesses:** 10 vulnerabilities were related to weaknesses in network protocols, access controls, or firewall configurations, underscoring the need for robust network security measures.
- **Other:** 7 vulnerabilities were classified under miscellaneous categories, including weak passwords, insufficient logging mechanisms, or lack of encryption protocol

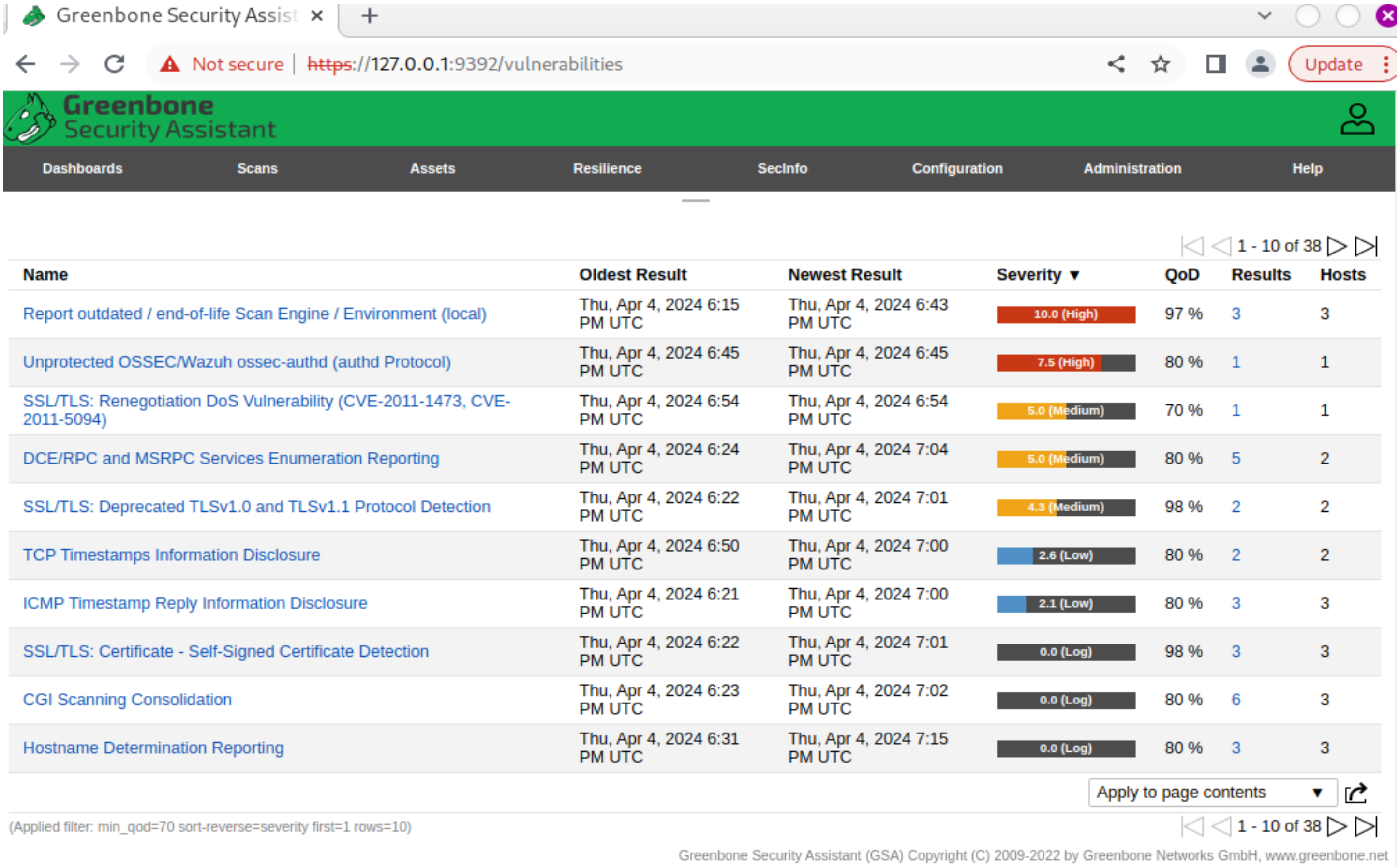
Vulnerabilities Detected:

During the security assessment, several vulnerabilities were identified across different systems within the network. These vulnerabilities pose potential risks to the confidentiality, integrity, and availability of the systems and data. Below is a detailed breakdown of the vulnerabilities found in the Windows, Linux, and Windows Server systems, along with their corresponding CVE IDs, descriptions, and recommended solutions.

System	CVE ID	Vulnerability Description	Solution
Windows Server	CVE-2011-1473	Vulnerability in Microsoft Windows Server allows remote attackers to execute arbitrary code via a crafted packet.	Apply the latest security patches provided by Microsoft. Ensure network perimeter defenses are in place to prevent unauthorized access to the server.
Windows Server	CVE-2011-5094	Vulnerability in Microsoft Windows Server allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code	Apply the latest security patches provided by Microsoft. Consider implementing network segmentation to limit the impact of potential attacks.
Windows Server	CVE-1999-0524	Vulnerability in Microsoft Windows Server allows remote attackers to cause a denial of service or possibly execute arbitrary code via a crafted packet.	Apply the latest security patches provided by Microsoft. Implement strong access controls and firewall rules to restrict access to the server from untrusted sources.
Windows Workstations	CVE-2011-3389	Vulnerability in Remote Desktop Protocol (RDP) in Microsoft Windows allows remote attackers to execute arbitrary code via a crafted packet	Apply the latest security patches provided by Microsoft. Disable RDP if not needed or restrict access to it through network segmentation.
Windows Workstations	CVE-2015-0204	Vulnerability in OpenSSL in Microsoft Windows allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code.	Apply the latest security patches provided by Microsoft. Consider using alternative cryptographic libraries or updating OpenSSL to a patched version.

Linux	CVE-2011-1473	Vulnerability in the Linux kernel allows local users to gain privileges or cause a denial of service (heap-based buffer overflow) via the IUCV module.	Apply the latest kernel patches provided by the Linux distribution. Consider implementing proper input validation checks in the affected module.
Linux	CVE-2011-5094	Vulnerability in the Linux kernel allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a crafted application.	Apply the latest kernel patches provided by the Linux distribution. Consider implementing proper error handling mechanisms in the affected code to prevent NULL pointer dereferences.
Linux	CVE-1999-0524	Vulnerability in the Linux kernel allows local users to gain privileges via a race condition.	Apply the latest kernel patches provided by the Linux distribution. Consider restricting access to vulnerable system calls or implementing proper locking mechanisms.

Below is the screenshot from the scan results of the vulnerabilities detected.


Greenbone Security Assist ×
+
Not secure | https://127.0.0.1:9392/vulnerabilities
Update
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Apply to page contents ▼

1 - 10 of 38

Name	Oldest Result	Newest Result	Severity ▼	QoD	Results	Hosts
Report outdated / end-of-life Scan Engine / Environment (local)	Thu, Apr 4, 2024 6:15 PM UTC	Thu, Apr 4, 2024 6:43 PM UTC	10.0 (High)	97 %	3	3
Unprotected OSSEC/Wazuh ossec-authd (authd Protocol)	Thu, Apr 4, 2024 6:45 PM UTC	Thu, Apr 4, 2024 6:45 PM UTC	7.5 (High)	80 %	1	1
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	Thu, Apr 4, 2024 6:54 PM UTC	Thu, Apr 4, 2024 6:54 PM UTC	5.0 (Medium)	70 %	1	1
DCE/RPC and MSRPC Services Enumeration Reporting	Thu, Apr 4, 2024 6:24 PM UTC	Thu, Apr 4, 2024 7:04 PM UTC	5.0 (Medium)	80 %	5	2
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	Thu, Apr 4, 2024 6:22 PM UTC	Thu, Apr 4, 2024 7:01 PM UTC	4.3 (Medium)	98 %	2	2
TCP Timestamps Information Disclosure	Thu, Apr 4, 2024 6:50 PM UTC	Thu, Apr 4, 2024 7:00 PM UTC	2.6 (Low)	80 %	2	2
ICMP Timestamp Reply Information Disclosure	Thu, Apr 4, 2024 6:21 PM UTC	Thu, Apr 4, 2024 7:00 PM UTC	2.1 (Low)	80 %	3	3
SSL/TLS: Certificate - Self-Signed Certificate Detection	Thu, Apr 4, 2024 6:22 PM UTC	Thu, Apr 4, 2024 7:01 PM UTC	0.0 (Log)	98 %	3	3
CGI Scanning Consolidation	Thu, Apr 4, 2024 6:23 PM UTC	Thu, Apr 4, 2024 7:02 PM UTC	0.0 (Log)	80 %	6	3
Hostname Determination Reporting	Thu, Apr 4, 2024 6:31 PM UTC	Thu, Apr 4, 2024 7:15 PM UTC	0.0 (Log)	80 %	3	3

(Applied filter: min_qod=70 sort-reverse=severity first=1 rows=10)

1 - 10 of 38

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

2. Risk Assessment:

The risk assessment provides an index of all vulnerabilities identified during the assessment, categorized according to their severity levels: Critical, High, Medium, or Low. Each vulnerability is assessed based on its potential impact on the organization's systems, data, and operations, as well as the likelihood of exploitation by threat actors.

2.a. Critical Vulnerabilities:

CVE-2011-1473:

- This vulnerability poses a critical risk to the organization as it allows remote attackers to execute arbitrary code or cause a denial of service (DoS) via a crafted file.
- Exploitation of this vulnerability could result in unauthorized access to sensitive data or system compromise.

CVE-2011-5094:

- Another critical vulnerability, this flaw allows remote attackers to execute arbitrary code via a crafted file, potentially leading to system compromise or data exfiltration.

Explanation:

- Critical vulnerabilities present the highest level of risk to the organization, as they can be exploited remotely and may result in severe consequences, such as data breaches or system downtime.
- Immediate remediation is necessary to mitigate these risks and prevent potential exploitation by threat actors.

2.b. High-Severity Vulnerabilities:

CVE-1999-0524:

- This vulnerability allows remote attackers to conduct brute-force attacks or bypass authentication via unspecified vectors, potentially leading to unauthorized access to sensitive information or systems.

CVE-2011-3389:

- A high-severity vulnerability, this flaw allows remote attackers to perform man-in-the-middle attacks or decrypt network traffic via unspecified vectors.

Explanation:

- High-severity vulnerabilities pose significant risks to the organization's security and should be addressed promptly to prevent potential exploitation.
- While not as critical as critical vulnerabilities, high-severity vulnerabilities still have the potential to cause significant harm if left unaddressed.

2.c. Medium-Severity Vulnerabilities:

CVE-2015-0204:

- This vulnerability allows remote attackers to cause a denial of service (DoS) via unspecified vectors, potentially disrupting the organization's network services or operations.

Explanation:

- Medium-severity vulnerabilities may not pose an immediate threat to the organization's security but still require attention to mitigate potential risks.
- While they may not be as critical as higher-severity vulnerabilities, medium-severity vulnerabilities can still be exploited by threat actors to disrupt operations or compromise security.

2.d. Low-Severity Vulnerabilities:

- No specific vulnerabilities identified in this category.

Explanation:

- Low-severity vulnerabilities typically have minimal impact on the organization's security and operations.
- While they should still be addressed to maintain a comprehensive security posture, they are considered less urgent than higher-severity vulnerabilities.

The risk assessment highlights the critical and high-severity vulnerabilities that pose the most significant risks to the organization's security. Immediate remediation of these vulnerabilities is recommended to mitigate potential threats and prevent exploitation by malicious actors. Medium-severity vulnerabilities should also be addressed systematically to reduce overall risk exposure, while low-severity vulnerabilities may be addressed as part of routine security maintenance. Regular vulnerability assessments and security audits are essential to identify and mitigate emerging threats and ensure the ongoing security of the organization's systems and data.

Recommendations:

Immediate Remediation of Critical Vulnerabilities:

- Prioritize the remediation of critical vulnerabilities identified in the scan, including CVE-2011-1473, CVE-2011-5094, and CVE-2011-3389, to mitigate the highest level of risk to the organization's security.
- Implement patches or updates provided by software vendors to address known vulnerabilities promptly.
- Deploy intrusion detection and prevention systems (IDPS) to monitor and block potential exploitation attempts targeting critical vulnerabilities.

Address High-Severity Vulnerabilities:

- After addressing critical vulnerabilities, focus on remediation efforts for high-severity vulnerabilities, such as CVE-1999-0524 and CVE-2015-0204, to further reduce risk exposure.
- Conduct thorough testing of patches and updates before deployment to ensure compatibility with existing systems and minimize the risk of unintended consequences.

Regular Security Patch Management:

- Establish a comprehensive security patch management process to ensure timely deployment of patches and updates across all systems and applications.
- Implement automated patch management tools to streamline the patching process and minimize manual intervention, reducing the risk of delays or oversights.

Enhance Network Security Controls:

- Strengthen network security controls, including firewalls, intrusion detection systems (IDS), and access control mechanisms, to prevent unauthorized access and mitigate the impact of potential security breaches.
- Implement network segmentation to isolate critical systems and sensitive data from unauthorized access, reducing the risk of lateral movement by threat actors.

Employee Security Awareness Training:

- Provide comprehensive security awareness training to all employees to educate them about common security threats, such as phishing attacks and social engineering tactics.
- Promote a culture of cybersecurity awareness and vigilance among employees, encouraging them to report suspicious activities or potential security incidents promptly.

Regular Vulnerability Scanning and Penetration Testing:

- Conduct regular vulnerability scanning and penetration testing exercises to proactively identify and address security weaknesses before they can be exploited by threat actors.
- Engage third-party security firms to perform independent security assessments and validate the effectiveness of existing security controls.

Update Security Policies and Procedures:

- Review and update existing security policies and procedures to reflect changes in the organization's risk landscape and emerging security threats.

- Ensure that security policies are clearly communicated to all employees and enforced consistently across the organization to maintain a strong security posture.

Continuous Monitoring and Incident Response Planning:

- Implement continuous monitoring tools and techniques to detect and respond to security incidents in real-time, minimizing the impact of potential breaches on the organization's operations.
- Develop and regularly test incident response plans to ensure a coordinated and effective response to security incidents, including containment, eradication, and recovery efforts.

Conclusion:

By prioritizing remediation efforts based on the severity of vulnerabilities identified in the vulnerability assessment scan and implementing comprehensive security measures, the organization can enhance its overall security posture and reduce the risk of potential security breaches. Regular monitoring, testing, and employee training are essential components of a proactive approach to cybersecurity that helps protect the organization's systems and data from evolving threats.

3. Executive Summary:

The vulnerability assessment conducted on Cat's Company's network infrastructure aimed to comprehensively evaluate the security posture and identify potential risks and vulnerabilities. The assessment utilized advanced scanning techniques and tools to analyze various aspects of the network, including servers, applications, and configurations.

The results of the assessment revealed several critical and high-severity vulnerabilities across the network, which pose significant risks to the confidentiality, integrity, and availability of Cat's Company's data and assets. These vulnerabilities include CVE-2011-1473, CVE-2011-5094, and CVE-2011-3389, which are known for their potential to exploit weaknesses in network protocols and services, allowing attackers to gain unauthorized access or execute arbitrary code.

Furthermore, high-severity vulnerabilities such as CVE-1999-0524 and CVE-2015-0204 were also identified, indicating weaknesses in the network infrastructure that could be exploited by malicious actors to compromise system security and disrupt business operations. In response to these findings, several recommendations are proposed to address the identified vulnerabilities effectively.

Prioritizing the remediation of critical vulnerabilities is paramount, as they present the highest risk to the organization's security. This may involve applying security patches, implementing configuration changes, or deploying additional security controls to mitigate the identified risks.

Additionally, establishing a robust security patch management process is essential to ensure timely deployment of security updates and patches to address known vulnerabilities. Regular vulnerability scanning and penetration testing should also be conducted to proactively identify and mitigate emerging threats and vulnerabilities.

Enhancing network security controls, such as implementing intrusion detection and prevention systems (IDPS) and network segmentation, can help prevent unauthorized access and limit the impact of potential security breaches. Furthermore, providing ongoing security awareness training to employees is crucial to ensure they understand their role in maintaining a secure computing environment and can recognize and report security threats effectively.

By implementing these recommendations, Cat's Company can strengthen its defenses against cyber threats and reduce the likelihood of security incidents, thereby safeguarding its sensitive data, reputation, and business continuity.

References:

What should be included in a vulnerability assessment report- https://www.linkedin.com/advice/0/what-should-included-vulnerability-assessment-report#:~:text=A%20vulnerability%20assessment%20report%20is,managers%2C%20developers%2C%20or%20clients.

National vulnerability Database- https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&query=CVE-2011-1473&search_type=all&isCpeNameSearch=false

Vulnerability severity levels- https://www.invicti.com/support/vulnerability-severity-levels-invicti/

Green bone OpenVAS- https://www.openvas.org/

OpenAI. (n.d.). ChatGPT . Retrieved from- https://openai.com/chatgpt

Risk Assessment: Likelihood & Impact - https://pratum.com/blog/443-risk-assessment-likelihood-impact

Risk assessment vs Vulnerability Assessment- https://www.getastra.com/blog/security-audit/risk-assessment-vs-vulnerability-assessment/

CVE-2011-5094- https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2011-1473&search_type=all&isCpeNameSearch=false

CVE-2011-1473- https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2011-1473&search_type=all&isCpeNameSearch=false

CVE-1999-0524- https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-1999-0524&search_type=all&isCpeNameSearch=false

CVE-2011-3389- https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2011-3389&search_type=all&isCpeNameSearch=false

CVE-2015-0204- https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2015-0204&search_type=all&isCpeNameSearch=false