Course 6 Project:
Cat’s Company Vulnerabilities

By Evelyn Wolfe

Table of Contents

Executive Summary

The recent vulnerability assessment identified three areas of concern within the organization's network systems. While none of these vulnerabilities pose an immediate critical threat, addressing them will enhance the organization's overall security posture and reduce potential risks. The first vulnerability involves a risk of service disruption due to how the system handles secure communications, which could allow an attacker to temporarily overload system resources. The second issue relates to specific services that unintentionally reveal internal system details, potentially giving attackers the information they need to target more sensitive areas. Lastly, a minor vulnerability was detected that reveals how long certain systems have been active, which, while low in severity, could provide helpful reconnaissance data for attackers planning a more significant breach.

To mitigate these risks, immediate steps include applying security updates provided by software vendors, restricting access to exposed systems, and disabling certain unnecessary features to prevent exploitation. These actions will limit opportunities for attackers to gather sensitive information or disrupt critical services. Although the vulnerabilities identified are not severe, addressing them promptly is a proactive measure to maintain the organization's resilience against potential threats and safeguard operational integrity.

Scan Results

On January 5, 2025, at 15:27:45 UTC, a vulnerability assessment scan was conducted on the organization's primary servers. The servers under review included a Windows 11 machine configured as a server, identified by IP address 10.0.2.6, and an Ubuntu-Linux machine identified by IP address 10.0.2.15. This scan, performed using Greenbone's "OpenVAS" software, aimed to identify and document vulnerabilities within the network infrastructure.

Results of the scan

While the vulnerabilities identified in this summary are limited in number, the company’s overall security posture and the effectiveness of its defensive measures are commendable. The scan identified the following vulnerabilities:

Finding One: A Denial of Service (DoS) vulnerability with a severity level of Medium (CVSS 5.0) was detected. This vulnerability is associated with the SSL/TLS Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) and was identified on the Windows 11 Server. This issue could potentially disrupt service availability if exploited, emphasizing the importance of maintaining secure communication protocols.
CVE website. (2012, June). https://www.cve.org/CVERecord?id=CVE-2011-1473
CVE website. (2012, June). https://www.cve.org/CVERecord?id=CVE-2011-5094

Finding Two: A Distributed Computing Environment/Remote Procedure Call (DCE/RPC) vulnerability, also involving MSRPC services, was discovered. This vulnerability, rated as Medium severity (CVSS 5.0), was detailed in the DCE/RPC and MSRPC Service Enumeration Report and is associated with the Windows 11 Server. The presence of this vulnerability highlights the need to monitor and secure inter-process communications to prevent unauthorized access or information leakage.

Finding Three: A TCP Timestamps Information Disclosure vulnerability with a severity level of Low (CVSS 2.6) was also identified. This issue, detailed in the TCP Timestamp Information Disclosure report, affects both the Ubuntu-Linux Server and the Windows 11 Server. While considered low risk, it represents an information leakage vector that could be leveraged during reconnaissance phases of an attack.

For references to the scan report and its finding OpenVAS Scan 05-01-2025

Categorized

The vulnerability scan conducted on January 5, 2025, was categorized as a comprehensive network security assessment, focusing on identifying potential weakness across critical systems. The scan targeted both the Windows 11 Server and the Ubuntu-Linux Server. Any other servers or machines online during the scan would have been included in the assessment. While the scan categorized vulnerabilities into four severities - Critical, High, Medium and Low - our findings only identified two serverities: Medium and Low.

The Medium-severity vulnerabilities identified include the SSL/TLS Renegotiation Denial of Service (DoS) vulnerability (CVE-2011-1473, CVE-2011-5094) and the DCE/RPC MSRPC Service Enumeration vulnerability. These findings underscore the importance of securing inter-process communication services and ensuring encryption processes to mitigate potential service disruption.

The Low-severity vulnerability, TCP Timestamps Information Disclosure, was detected on both the Windows 11 and Ubuntu-Linux servers. While it poses minimal direct risk, this finding highlights an information leakage issue that could aid threat actors during reconnaissance efforts.

Methodology

Our scan was conducted using OpenVAS, an open-source, community supported vulnerability assessment tool developed by the company Greenbone. OpenVAS performs a comprehensive thorough evaluation of the systems by assessing the vulnerabilities against an extensive database of known CVEs(Common Vulnerabilities and Exposures) and NVTs (Network Vulnerabilities Tests). This tool provides detailed insight into identifying vulnerabilities, including their severity score (CVSS or Common Vulnerability Scoring System) associated risk, and potential remediation steps. This makes OpenVAS an essential tool for enabling robust and actionable security assessment.

The primary purpose of the vulnerability scan was to identify potential weaknesses and security gaps across the organization, with a focus on our critical systems, ensuring that the company remains resilient against emerging threats. While numerous tools can perform similar assessments, the open-source nature and comprehensive capabilities of OpenVAS made it a practical choice for the evaluation. OpenVAS effectively delivered the initial insight necessary to assess vulnerabilities, helping to prioritize remediation efforts and strengthen the overall security posture for the organization.

Findings

Finding One: Denial of Service

The scans identified a Denial of Service (DoS) vulnerability in the SSL/TLS service of the Windows 11 server, and is treated as a Medium Severity with the CVSS score 5.0 out of 10. This issue, associated with the CVE-2011-1473, and CVE-2011-5094, arise from the server's failure to restrict client-initiated renegotiation within an established SSL/TLS connection. This flaw allows an attacker to perform multiple renegotiations. During the scan, the vulnerability was confirmed with 10 successful renegotiations detected under the TLSv1.2 protocol.
CVE website. (2012, June). https://www.cve.org/CVERecord?id=CVE-2011-1473
CVE website. (2012, June). https://www.cve.org/CVERecord?id=CVE-2011-5094

Finding Two: Distributed Computing Environment/Remote Procedures Call (DCE/RPC)

In addition, vulnerability at Medium-severity with a CVSS score of 5.0 out of 10. This vulnerability is associated with the Distributed Computing Environment/Remote Procedure Call (DCE/RPC) and MSRPC services running on the Windows 11 Server. It allows an attacker to enumerate active services by querying port 135 and associated high ports (such as 49664 to 49670), potentially exposing sensitive service and process information. Specific services that were identified include **lsass.exe** (SAM access), **spoolsv.exe** (Spooler service), and **Windows Event Log**. Furthermore, the scan reflected detailed annotations and endpoints provided in the scan results.

Finding Three: A TCP Timestamps Information Disclosure

The final vulnerability detected was classified as Low-severity, with a CVSS score of 2.6 out of 10. This vulnerability is related to **TCP Timestamps Information Disclosure.** The issue arises because the remote host implements TCP timestamps, as defined by Internet Engineering Task Force (IETF) documentation: RFC 1323 and RFC 7323. By analyzing timestamps in responses to specially crafted IP packets, a threat actor could potentially determine the system's uptime. During the scan, two timestamps were retrieved with a 1-second delay between packets: 991527481 and 991528558, confirming the presence of this feature.
Although this vulnerability does not pose a direct risk to the organization's integrity or data confidentiality, it can provide reconnaissance information to an attacker. This feature is commonly implemented in TCP across both Linux and Windows systems.
TCP Extensions for High Performance. (1992, May) IETF IETF - RFC1323
TCP Extensions for High Performance (2014, September) IETF IETF - RFC7323

Risk Assessment

Categorized of Vulnerability

While the vulnerabilities identified during the scan were categorized based on their severity levels using the **Common Vulnerability Scoring System (CVSS)**, which provides a standardized framework for assessing risk, the report reflected only two severities: **Medium** and **Low**. It is important to note that vulnerabilities categorized as **Critical** and **High** should be addressed immediately due to their significant impact. Medium-severity vulnerabilities, with a score of **5.0 out of 10**, represent moderate risks that could affect system availability or enable attackers to gather critical and sensitive information. In contrast, Low-severity vulnerabilities, with a score of **2.6 out of 10**, pose minimal risks to a system's confidentiality, integrity, and availability.

Although Low-severity vulnerabilities are less likely to cause immediate harm, a persistent attacker could still exploit them to gain insights into the system, which might be used to facilitate more advanced attacks. Addressing vulnerabilities based on their severity ensures that the organization's resources are effectively allocated to mitigate the most significant risks first, while also reducing overall exposure to potential threats.

Recommendations

Remedy for Denial of Service:

The recommended solution for the **SSL/TLS Renegotiation Denial of Service (DoS) vulnerability** involves implementing a vendor-specific fix or disabling renegotiation capabilities within the affected SSL/TLS service. Organizations should first contact the vendor of the affected service to determine if a security patch or update is available to address this issue. Applying the patch ensures secure handling of the renegotiation process. If a patch is not available, disabling renegotiation capabilities entirely within the service configuration is advised as a general mitigation strategy. This prevents attackers from exploiting the vulnerability by performing multiple renegotiations within a single connection, thereby mitigating the risk of CPU resource exhaustion. Additionally, monitoring network traffic for abnormal renegotiation patterns and implementing rate-limiting or network access controls can further reduce exposure. Upgrading cryptographic libraries, such as OpenSSL and Mozilla NSS, to their latest versions is also recommended to address related vulnerabilities and enhance overall system security. By taking these steps, organizations can protect their systems from potential denial of service attacks and ensure continued availability of critical services.

Remedy for DCE/RPC and MSRPC Service Enumeration Vulnerability:

After analyzing the report, the recommended remedy for the Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) or MSRPC Services is to filter incoming traffic to the affected ports. This can be achieved by configuring a firewall or network access control lists (ACLs) to restrict access. It is also advisable to limit communication with these ports to trusted systems or specific IP addresses. The identified affected ports include **port 135** and high ports such as **49664 to 49670**.

Remedy for TCP Timestamp Information Disclosure

The best recommendation provided from the scan is to disable the TCP Timestamp in order to mitigate the risk of an attacker collecting any information during reconnaissance. There is some information regarding disabling the TCP Timestamps.

- For Linux, a simple command within the terminal, please refer to the TCP Timestamp disable for Linux Document for more information.
- For Windows, please see TCP Timestamp disable for Windows Document

Citations and References

DOS:

[TLS] SSL renegotiation DOS. (2011, March 15). IEFT Mail Archive https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/

Bernat, V. (2011, November 1). *TLS computational DoS mitigation.* https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation

CVE Website (2012, June 16) *CVE-2011-1473* https://www.cve.org/CVERecord?id=CVE-2011-1473

CVE Website (2012, June 16) *CVE-2011-5094* https://www.cve.org/CVERecord?id=CVE-2011-5094

DCE/RPC and MSRPC Service

DCE/RPC - Wireshark Wiki. (n.d.). https://wiki.wireshark.org/DCE/RPC

Mitigating DCE/RPC/MSRPC enumeration vulnerabilities? (2022, October 20). Greenbone Community Forum. https://forum.greenbone.net/t/mitigating-dce-rpc-msrpc-enumeration-vulnerabilities/13310

TCP Timestamp

TCP Extensions for High Performance. (1992, May) IETF https://datatracker.ietf.org/doc/html/rfc1323

TCP Extensions for High Performance (2014, September) IETF https://datatracker.ietf.org/doc/html/rfc7323

PSIRT | FortiGuard Labs. (2019, June 24). FortiGuard Labs. https://www.fortiguard.com/psirt/FG-IR-16-090