# Cats company vulnerabilities

**By: Mahad Mohamood**

## Executive Summary

This vulnerability assessment was conducted to identify and evaluate security weaknesses in critical devices within the organization's network, specifically targeting a Windows 11 machine and a Linux Server.

The assessment was performed using OpenVAS/GVM to uncover potential vulnerabilities that could be exploited to compromise system integrity.

The scan revealed two main issues:

- TCP Timestamps Information Disclosure
- ICMP Timestamp Reply Information Disclosure.

These vulnerabilities can potentially expose system uptime and timestamp data that could be leveraged by attackers for further profiling or exploitation.

To mitigate these risks, we recommend :

- Disabling TCP timestamps on both Windows and Linux systems because this will prevent the leakage of system uptime information.
- Turning off ICMP timestamp responses on the Linux server because this will reduce the risk of exploiting potential weaknesses in time-based random number generators.

Implementing these recommendations will enhance the security of the network by addressing information disclosure vulnerabilities and improving the overall security posture of the organization.

## Scan Results

*Detailed Explanation of the Results*

The vulnerability scan conducted on the Windows 11 machine (IP: 10.0.2.55) and the Linux Server (IP: 10.0.2.15) using OpenVAS/GVM identified several key vulnerabilities related to TCP and ICMP timestamps. We will now discuss these vulnerabilities :

1. TCP Timestamps Information Disclosure:

- Windows 11:
    - Issue : TCP timestamp packets reveal system uptime, potentially exposing reboot patterns and last restart times.
    - Potential danger :An attacker might use uptime data to predict system maintenance schedules or plan attacks when the system is less monitored.
- Linux Server:
    - Issue : TCP timestamp packets reveal system uptime, potentially exposing operational duration and stability patterns.
    - Potential danger: An attacker could use uptime data to assess system stability or plan attacks based on reboot patterns

Significance: TCP timestamps are typically used for round-trip time measurements and other performance-related metrics. According to Science Direct, “Round-trip time refers to the time it takes for a packet of data to travel from a source to a destination and back again. It is a critical factor in determining the wait time for an acknowledgment (ACK) before retransmitting a segment. The round-trip time estimation is crucial for ensuring reliable and efficient communication in protocols like TCP.”

However, they also inadvertently expose uptime information that could be exploited by attackers to conduct timing-based attacks or profile the target system’s operational behavior. For instance, the National Institute of Standards and Technology (NIST, CVE-2005-0356) highlights that “timestamps option enabled allow remote attackers to cause a denial of service (connection loss) via a spoofed packet with a large timer value, which causes the host to discard later packets because they appear to be too old.”

2. ICMP Timestamp Reply Information Disclosure:

- Linux Server:
    - Issue : The Linux server’s response to ICMP timestamp requests includes detailed replies, including the originating timestamp, receive timestamp,

and transmit timestamp, exposing the server's internal clock settings and current time.

- Potential danger : An attacker might use the exposed timestamps to synchronize attacks with the server's clock or exploit timing discrepancies in time-sensitive applications.

Significance: ICMP timestamp responses are generally used for network diagnostics and can provide detailed timing information. According to CAPEC (CAPEC-295), "this pattern of attack leverages standard requests to learn the exact time associated with a target system. An adversary may be able to use the timestamp returned from the target to attack time-based security algorithms, such as random number generators, or time-based authentication mechanisms."

*Categorization of Results*

The vulnerabilities detected have been categorized as follows:

1. TCP Timestamps Information Disclosure:
    - Severity: Low (CVSS Base Score: 2.6 for Windows and 2.6 for Linux)
    - Reason for Categorization:
        - TCP timestamp vulnerabilities aid attackers in profiling the target.
        - This aligns with the Reconnaissance stage of the Lockheed Martin Cyber Kill Chain, which "includes activities such as researching potential targets, determining vulnerabilities, and exploring potential entry points." (*What is the cyber kill chain?* 2024)
        - As it mainly risks enhanced profiling rather than direct access or immediate exploitation, it is classified as low severity.
2. ICMP Timestamp Reply Information Disclosure:
    - Severity: Low (CVSS Base Score: 2.1)
    - Reason for Categorization:

- ICMP timestamp replies could potentially reveal timing information that might be used to exploit timing-based weaknesses.

- However, the actual impact is minimal and the risk is more theoretical than practical.

- As such, it is classified as low severity.

The vulnerabilities are categorized as low severity because they are useful for profiling but do not lead to direct system compromise or access to sensitive data.

*Ordering of Vulnerabilities*

The vulnerabilities are ordered based on their potential impact and the likelihood of exploitation:

1. TCP Timestamps Information Disclosure:

2. ICMP Timestamp Reply Information Disclosure:

This ordering is based on the fact that TCP timestamps can be used to infer system behavior more concretely compared to ICMP timestamps. Therefore, the TCP timestamp disclosure presents a clearer path to potential misuse in terms of system profiling and timing attacks, making it a higher priority for mitigation. Here are few reasons to justify this rational :

- “The accuracy of connectivity measured using TCP is 20–30% higher than that measured using ICMP.”(Li Wenwei b et al., 2006)

- “ICMP is not designed for data transmitting, and it can be easily imposed by network attack activities such as Smurf, Ping of Death, etc.”(Li Wenwei b et al., 2006)

- “Many routers and end hosts have rate limited or even blocked ICMP packets, which may lead to obtain wrong measuring results or the measurement cannot be conducted at all.”(Li Wenwei b et al., 2006)

## Methodology

The methodology used OpenVAS with Nmap in a controlled Kali Linux environment for a comprehensive vulnerability assessment, enabling identification of security weaknesses, for Windows and Linux machines. The OpenVAS tool was able to access the system and gather detailed information from both the windows and linux machines.

Tools Used :

- OpenVAS is “a comprehensive vulnerability scanning and management solution designed to detect and assess security Vulnerabilities in computer systems, networks, and applications. It provides a framework for vulnerability scanning, vulnerability management, and vulnerability assessment. ”(OpenVAS explained, 2023)

- Kali Linux “is an open-source, Debian-based Linux distribution which allows users to perform advanced penetration testing and security auditing.”(What is Kali Linux?: Kali linux documentation, 2024)

- Nmap is “short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. ”(Shivanandhan, 2020) OpenVAS utilizes Nmap as part of its network scanning process to perform host discovery and port scanning.

Environments Used :

- Kali Linux was configured in VirtualBox to run vulnerability scans with OpenVAS. This setup offers isolation, preventing impact on production systems. Kali’s built-in tools and configurations are optimized for effective security testing.

- Ubuntu Linux Environment (IP: 10.0.2.15) served as the target for the vulnerability scan. This Ubuntu environment mirrors typical Linux distributions used in organizations, helping identify vulnerabilities relevant to similar systems.

- Windows 11 Environment  (IP: 10.0.2.55) was used as a target for the assessment. This setup helps identify vulnerabilities affecting current Windows platforms, ensuring the organization's security measures are current.

## Risk assessment

*List of Vulnerabilities :*

1. TCP Timestamps Information Disclosure
    - Description: This vulnerability arises because the TCP stack on the system implements timestamps as defined by RFC1323/RFC7323. This allows an attacker to infer the system's uptime based on timestamp values.
    - Target/System Affected: Linux Server and Windows 11
    - Affected Software/Service: TCP implementation adhering to RFC1323/RFC7323
2. ICMP Timestamp Reply Information Disclosure
    - Description: This vulnerability allows the system to respond to ICMP timestamp requests, disclosing timestamps that include the originating, receive, and transmit times.
    - Target/System Affected: Linux Server
    - Affected Software/Service: ICMP protocol

Impact and Risk Analysis

1. TCP Timestamps Information Disclosure
    - Exposure: Reveals system uptime, which may help infer other operational details.
    - Cost of Exploitation: Minimal direct cost, but may provide useful context for other attacks.

- Extent of Impact: Limited to uptime exposure; no direct impact on functionality or security.

- Likelihood of Exploitation: Low; provides limited advantage to attackers.

- Indicators of Compromise (IoCs): TCP timestamps in network traffic may signal this vulnerability.

2. ICMP Timestamp Reply Information Disclosure

    - Exposure: Reveals time-based information that could aid in exploiting time-based weaknesses.

    - Cost of Exploitation: Minimal direct impact, but may help an attacker understand system patterns.

    - Extent of Impact: Affects confidentiality of timestamp data; limited direct impact on security.

    - Likelihood of Exploitation: Low; ICMP timestamps are less commonly targeted.

    - Indicators of Compromise (IoCs): ICMP timestamp requests and replies may indicate the vulnerability.

## Recommendations

Full List of Actions in Prioritized Order

1. Disable TCP Timestamps on Affected Systems
    - Explanation: Prevents the exposure of system uptime, reducing the risk of attackers gaining potentially useful operational information.
    - Actions:
        - Linux: Add net.ipv4.tcp_timestamps = 0 to /etc/sysctl.conf and run sysctl -p to apply the changes.
        - Windows: Execute netsh int tcp set global timestamps=disabled. Note that this setting may not fully disable timestamps on newer Windows versions.
2. Disable ICMP Timestamp Replies
    - Explanation: Prevents the leakage of time-based information, reducing the risk of exploiting time-based weaknesses.
    - Action: Configure the Linux Server to disable ICMP timestamp replies, either through system settings or firewall rules to block ICMP packets related to timestamps.
3. Update and Patch Systems Regularly
    - Explanation: This is a general best practice that supports the mitigation of both the specific vulnerabilities found and other potential security issues.
    - Action: Implement a routine schedule for applying updates and patches to all systems, including both the Linux Server and Windows 11.

4. Monitor Network Traffic for Indicators of Compromise (IoCs)

    - Explanation: Regular network monitoring for specific IoCs related to the identified vulnerabilities, such as unusual ICMP or TCP traffic patterns, can enhance your organization's ability to respond promptly to any emerging threats.

    - Action: Set up network monitoring tools to detect and alert on suspicious traffic patterns associated with TCP timestamps and ICMP timestamps.

5. Review and Strengthen Firewall Rules

    - Explanation: Ensuring that firewall rules are correctly configured can prevent unwanted or suspicious network traffic from reaching critical systems.

    - Actions:

        - Review and update firewall configurations to block ICMP timestamp requests and unnecessary TCP traffic.

        - Ensure that the firewall rules are aligned with the organization's security policies.

Why This Order?

- Immediate Impact: Disabling TCP and ICMP timestamp replies directly mitigates the identified vulnerabilities.

- Long-term Security: Regular updates and patching ensure ongoing security.

- Proactive Monitoring and Prevention: Monitoring network traffic and reviewing firewall rules help detect and prevent exploits.

By implementing these recommendations, you will address the identified vulnerabilities effectively while also strengthening the overall security posture of the organization.

## Conclusion

The assessment of Linux Server and Windows 11 identified low-severity vulnerabilities: TCP Timestamps and ICMP Timestamp Replies. While not an immediate threat, they can provide useful information for attackers. Recommended actions include disabling these timestamps and implementing regular updates, proactive monitoring, and firewall enhancements. These steps will improve security and resilience against potential threats.

## References


1. Round-trip time. Round-Trip Time - an overview | ScienceDirect Topics. (n.d.). https://www.sciencedirect.com/topics/computer-science/round-trip-time

2. National Institute of Standards and Technology. (n.d.). CVE-2005-0356 (vulnerability details). National Vulnerability Database. Retrieved August 12, 2024, from https://nvd.nist.gov/vuln/detail/CVE-2005-0356

3. MITRE. (n.d.). CAPEC-295: ICMP timestamp response attack. Common Attack Pattern Enumeration and Classification. Retrieved August 12, 2024, from https://capec.mitre.org/data/definitions/295.html

4. What is the cyber kill chain?. SentinelOne. (2024, August 8). https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-kill-chain/

5. Wenwei, L., Dafang, Z., Jinmin, Y., & Gaogang, X. (2006, October 20). On evaluating the differences of TCP and ICMP in network measurement. Computer Communications. https://www.sciencedirect.com/science/article/abs/pii/S0140366406003719

6. OpenVAS explained. isecjobs.com. (2023, December 6). https://isecjobs.com/insights/openvas-explained/

7. What is Kali Linux?: Kali linux documentation. Kali Linux. (2024, May 6). https://www.kali.org/docs/introduction/what-is-kali-linux/

8. Shivanandhan, M. (2020, October 2). What is nmap and how to use it – a tutorial for the greatest scanning tool of all time. freeCodeCamp.org. https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/