**Project Report: Vulnerability Assessment for Cat’s Company**

James Kuzhilaparambil

23 Sept 2024

Contents

[Executive Summary 3](#_heading=h.gjdgxs)

[Scan Results 3](#_heading=h.30j0zll)

[Methodology 3](#_heading=h.1fob9te)

[Findings 4](#_heading=h.3znysh7)

[Risk Assessment 4](#_heading=h.2et92p0)

[Recommendations 9](#_heading=h.tyjcwt)

[Conclusion: 10](#_heading=h.3dy6vkm)

[Appendices: 10](#_heading=h.1t3h5sf)

[References: 24](#_heading=h.4d34og8)

## Executive Summary

This report presents the findings from a comprehensive vulnerability assessment conducted on Cat’s Company’s network. The assessment aimed to identify potential security weaknesses and provide actionable recommendations to enhance the organization’s security posture. The scan revealed several vulnerabilities, categorized by severity, with detailed mitigation strategies. The top six vulnerabilities have been prioritized for immediate attention to reduce the risk of exploitation.

## Scan Results

The vulnerability scan was conducted using OpenVAS, a widely recognized open-source vulnerability scanner. The results were categorized based on severity: Critical, High, Medium, and Low. The vulnerabilities were then ordered by their potential impact on the network.

**Top Six Vulnerabilities:**

1. TCP Timestamps Information Disclosure (Host: 10.0.2.6)
2. TCP Timestamps Information Disclosure (Host: 10.0.2.15)
3. Services (Host: 10.0.2.6, Port: 80/tcp)
4. Services (Host: 10.0.2.15, Port: 80/tcp)
5. Services (Host: 10.0.2.15, Port: 3306/tcp)
6. Response Time / No 404 Error Code Check (Host: 10.0.2.6)

## Methodology

**Tools and Tests Used:**

* OpenVAS: Used for comprehensive vulnerability scanning.

**Purpose of Each Scan, Tool, and Test:**

* OpenVAS: To identify known vulnerabilities in the network.

**Environment:**

* The scans were conducted in a controlled environment within Cat’s Company’s internal network. The target systems included servers, workstations, and network devices.

## 

## Findings

**Systems Scanned Successfully:**

* 10.0.2.6: Successfully scanned, revealing multiple vulnerabilities.
* 10.0.2.15: Successfully scanned, revealing multiple vulnerabilities.

**Systems Not Scanned Successfully:**

* All targeted systems were scanned successfully.

## Risk Assessment

**Index of All Vulnerabilities Found:**

* Critical: None
* High: None
* Medium: None
* Low: Multiple (detailed below)

**Explanation of Risk Categories:**

* Critical: Immediate action required to prevent severe impact.
* High: Significant risk that should be addressed promptly.
* Medium: Moderate risk that should be mitigated in a reasonable timeframe.
* Low: Minor risk that should be addressed as resources permit.

**List of All Vulnerabilities:**

1. **TCP Timestamps Information Disclosure (Host: 10.0.2.6)**
   * **Severity**: 2.6 (Low)
   * **Description**: Allows computation of system uptime.
   * **Solution**: Disable TCP timestamps on Windows.
   * **Rationale**: Although low severity, this vulnerability can reveal system uptime, which could be useful information for attackers.
   * **Affected**: 1 host
   * **QoD**: 80%
   * **Location**: general/tcp

**Summary**: The remote host implements TCP timestamps, allowing the computation of the system’s uptime.

**Detection Result**: The host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 second in between:

* Packet 1: 2209349
* Packet 2: 2210441

**Insight**: The remote host implements TCP timestamps as defined by RFC1323/RFC7323.

**Detection Method**: Special IP packets are forged and sent with a slight delay between them to the target IP. The responses are searched for timestamps. If found, the timestamps are reported.

**Details**:

* **OID**: 1.3.6.1.4.1.25623.1.0.80091
* **Version Used**: 2023-12-15T16:10:08Z

**Affected Software/OS**: TCP implementations that implement RFC1323/RFC7323.

**Impact**: A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**Solution**:

* **Windows**: Execute netsh int tcp set global timestamps=disabled. Note that starting with Windows Server 2008 and Vista, the timestamp cannot be completely disabled. The default behavior of the TCP/IP stack on these systems is to not use the Timestamp options when initiating TCP connections but to use them if the TCP peer initiating communication includes them in their synchronize (SYN) segment.

**References**:

* RFC1323
* RFC7323
* Microsoft Download
* Fortiguard

1. **TCP Timestamps Information Disclosure (Host: 10.0.2.15)**
   * **Severity**: 2.6 (Low)
   * **Description**: Allows computation of system uptime.
   * **Solution**: Disable TCP timestamps on Linux.
   * **Rationale**: Same as above, addressing this on both hosts is important for consistency.
   * **Affected**: 1 host
   * **QoD**: 80%
   * **Location**: general/tcp

**Summary**: The remote host implements TCP timestamps, allowing the computation of the system’s uptime.

**Detection Result**: The host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 second in between:

* Packet 1: 592180588
* Packet 2: 592181671

**Insight**: The remote host implements TCP timestamps as defined by RFC1323/RFC7323.

**Detection Method**: Special IP packets are forged and sent with a slight delay between them to the target IP. The responses are searched for timestamps. If found, the timestamps are reported.

**Details**:

* **OID**: 1.3.6.1.4.1.25623.1.0.80091
* **Version Used**: 2023-12-15T16:10:08Z

**Affected Software/OS**: TCP implementations that implement RFC1323/RFC7323.

**Impact**: A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**Solution**:

* **Linux**: Add the line net.ipv4.tcp\_timestamps = 0 to /etc/sysctl.conf and execute sysctl -p to apply the settings at runtime.

**References**:

* RFC1323
* RFC7323
* Microsoft Download
* Fortiguard

1. **Services (Host: 10.0.2.6, Port: 80/tcp)**
   * **Severity**: 0.0 (Log)
   * **Description**: Web server running on this port.
   * **Solution**: Ensure proper configuration and monitoring of the web server.
   * **Rationale**: Identifying running services helps in understanding the attack surface.
   * **Affected**: 1 host
   * **QoD**: 80%
   * **Location**: 80/tcp

**Summary**: This plugin performs service detection to identify which services are running on the remote port(s).

**Detection Result**: A web server is running on this port.

**Insight**: This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server that could be listening on another port than 80 or 443 and makes this information available for other check routines.

**Detection Method**: The plugin uses various techniques to identify the services running on the specified ports.

**Details**:

* **OID**: 1.3.6.1.4.1.25623.1.0.10330
* **Version Used**: 2023-06-14T05:05:19Z

**Mitigation**: Ensure proper configuration and monitoring of the web server.

1. **Services (Host: 10.0.2.15, Port: 80/tcp)**
   * **Severity**: 0.0 (Log)
   * **Description**: Web server running on this port.
   * **Solution**: Ensure proper configuration and monitoring of the web server.
   * **Rationale**: Same as above, ensuring consistency across hosts.
   * **Affected**: 1 host
   * **QoD**: 80%
   * **Location**: 80/tcp

**Summary**: This plugin performs service detection to identify which services are running on the remote port(s).

**Detection Result**: A web server is running on this port.

**Insight**: This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server that could be listening on another port than 80 or 443 and makes this information available for other check routines.

**Detection Method**: The plugin uses various techniques to identify the services running on the specified ports.

**Details**:

* **OID**: 1.3.6.1.4.1.25623.1.0.10330
* **Version Used**: 2023-06-14T05:05:19Z

**Mitigation**: Ensure proper configuration and monitoring of the web server.

1. **Services (Host: 10.0.2.15, Port: 3306/tcp)**
   * **Severity**: 0.0 (Log)
   * **Description**: Unknown service running, usually reserved for MySQL.
   * **Solution**: Verify the service running on this port and ensure it is properly secured.
   * **Rationale**: Unknown services can pose a risk if not properly managed.
   * **Affected**: 1 host
   * **QoD**: 80%
   * **Location**: 3306/tcp

**Summary**: This plugin performs service detection to identify which services are running on the remote port(s).

**Detection Result**: An unknown service is running on this port. It is usually reserved for MySQL.

**Insight**: This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server that could be listening on another port than 80 or 443 and makes this information available for other check routines.

**Detection Method**: The plugin uses various techniques to identify the services running on the specified ports.

**Details**:

* **OID**: 1.3.6.1.4.1.25623.1.0.10330
* **Version Used**: 2023-06-14T05:05:19Z

**Mitigation**: Verify the service running on this port and ensure it is properly secured.

1. **Response Time / No 404 Error Code Check (Host: 10.0.2.6)**
   * **Severity**: 0.0 (Log)
   * **Description**: Web server does not return proper 404 error codes.
   * **Solution**: Configure the web server to return proper 404 error codes and ensure it responds in a reasonable time.
   * **Rationale**: Proper error handling and response times are crucial for security and performance.
   * **Affected**: 1 host
   * **QoD**: 80%
   * **Location**: 80/tcp

**Summary**: This vulnerability test (VT) checks if the remote web server does not reply with a 404 error code and verifies if it responds to the scanner’s requests in a reasonable amount of time.

**Detection Result**: The host returns a 30x (e.g., 301) error code when a non-existent file is requested. Some HTTP-related checks have been disabled.

**Insight**: This web server might show the following issues:

* It is misconfigured in that it does not return ‘404 Not Found’ error codes when a non-existent file is requested, possibly returning a site map, search page, authentication page, or redirect instead.
* The scanner might enable some countermeasures for this, but they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
* It doesn’t respond in a reasonable amount of time to various HTTP requests sent by this VT.

To keep the scan time reasonable, the remote web server might not be tested. If the remote server should be tested, it needs to be fixed to reply to the scanner’s requests in a reasonable amount of time. Alternatively, the ‘Maximum response time (in seconds)’ preference could be raised to a higher value if longer scan times are acceptable.

## Recommendations

**Full List of Actions in Prioritized Order:**

1. **Disable TCP Timestamps on Hosts 10.0.2.6 and 10.0.2.15**
   * **Reason**: Prevents attackers from computing system uptime.
   * **Action**:
     + **Linux**: Add net.ipv4.tcp\_timestamps = 0 to /etc/sysctl.conf and execute sysctl -p.
     + **Windows**: Execute netsh int tcp set global timestamps=disabled.
2. **Ensure Proper Configuration and Monitoring of Web Servers (Hosts: 10.0.2.6 and 10.0.2.15)**
   * **Reason**: Identifies running services and ensures they are properly configured.
   * **Action**: Regularly review and update web server configurations.
3. **Verify and Secure the Service Running on Port 3306/tcp (Host: 10.0.2.15)**
   * **Reason**: Unknown services can pose a risk if not properly managed.
   * **Action**: Confirm the service and apply necessary security measures.
4. **Configure Web Server to Return Proper 404 Error Codes (Host: 10.0.2.6)**
   * **Reason**: Proper error handling is crucial for security and performance.
   * **Action**: Update web server configuration to return 404 error codes for non-existent files.

**Recommendations on Security Policies and Configurations:**

* **Patch Management**: Implement a robust patch management process to ensure timely updates.
* **Immediate Actions**: Focus on disabling TCP timestamps on both hosts and ensuring proper configuration of identified services.
* **Security Awareness Training**: Educate staff on security best practices and threat recognition and response.
* **Security Policies**: Update security policies to include regular vulnerability assessments to identify and mitigate new vulnerabilities.
* **Continuous Monitoring**: Use monitoring tools to detect and respond to new vulnerabilities and security incidents in real-time.

Conclusion:

This comprehensive report aims to provide Cat’s Company with actionable insights, mitigations and recommendations to enhance its security posture. By addressing the prioritized vulnerabilities and implementing the suggested security measures, the organization can significantly reduce its risk of exploitation and protect against potential threats.

Appendices: **( Scan screenshots )**

**Dashboard**

A screenshot of a computer

Description automatically generated

Windows 11 immediate scan

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Windows 11 Discovery scan – with credentials

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

After remove all filter settings for QoD

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Windows 11 NVT scan – with credentials

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Ubuntu Linux Immediate scan

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Ubuntu Discovery scan – with credentials

A screenshot of a computer

Description automatically generated

After remove all filter settings for QoD

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Ubuntu Linux NVT scan – with credentials

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## References:

* *OWASP Vulnerability Management Guide | OWASP Foundation*. (n.d.). https://owasp.org/www-project-vulnerability-management-guide/
* OWASP Foundation, Inc. (2020). *OWASP Vulnerability Management Guide (OVMG)*. https://owasp.org/www-project-vulnerability-management-guide/OWASP-Vuln-Mgm-Guide-Jul23-2020.pdf
* *CISA releases SSVC methodology to prioritize vulnerabilities | CISA*. (2022, November 10). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/alerts/2022/11/10/cisa-releases-ssvc-methodology-prioritize-vulnerabilities
* Schaffer, K. B., Mell, P., Trinh, H., & Van Wyk, I. (2023). *Recommendations for federal vulnerability disclosure guidelines*. https://doi.org/10.6028/nist.sp.800-216
* Moussouris, K. & Luta Security. (2021). *Guidelines for Enhancing Software Supply Chain Security Vulnerability Disclosure Programs: Available standards & Best practices*. Luta Security, Inc. https://www.nist.gov/system/files/documents/2021/11/19/09-Final%20-%20Moussouris-%20EO%2014028%20VDP%20Best%20Practices.pdf
* *Vulnerability prioritization: tutorial & best practices*. (n.d.). https://www.silk.security/vulnerability-management-lifecycle/vulnerability-prioritization
* Leadership, S. C. (2024, March 1). *Vulnerability Management Metrics: 5 metrics to start measuring in your vulnerability management program | Part 1 of 2 | SANS Institute | Jonathan Risto*. https://www.sans.org/blog/5-metrics-start-measuring-vulnerability-management-program/
* Scarfone, K. A., Souppaya, M. P., Cody, A., & Orebaugh, A. D. (2008). *Technical guide to information security testing and assessment.* https://doi.org/10.6028/nist.sp.800-115
* Sahoo, P. K. (2023, October 25). *A complete guide on vulnerability scanning explained*. Qualysec | Penetration Testing Services and Solutions. https://qualysec.com/vulnerability-scanning-explained-a-comprehensive-overview/
* *How to conduct a vulnerability assessment | PDQ*. (n.d.). https://www.pdq.com/blog/how-to-conduct-vulnerability-assessment/
* Pham, C. (2023, August 29). Vulnerability Scanning: What It Is & Why It’s Important for Security and Compliance. *Secureframe*. https://secureframe.com/blog/vulnerability-scanning
* Chen, S. (n.d.). *Security tools benchmarking*. https://sectooladdict.blogspot.com/