**Cat’s Company Vulnerability Assessment**

**—----------------------------------------------------------------------------------------------------------------------------**

**Executive Summary:**

Upon completion of a comprehensive vulnerability assessment utilizing the Greenbone OpenVAS platform, our cybersecurity team has identified 57 vulnerabilities within the network infrastructure of Cat’s Company. Of these findings, three high-severity vulnerabilities demand immediate attention due to their potential to compromise system integrity and provide unauthorized access to sensitive data.

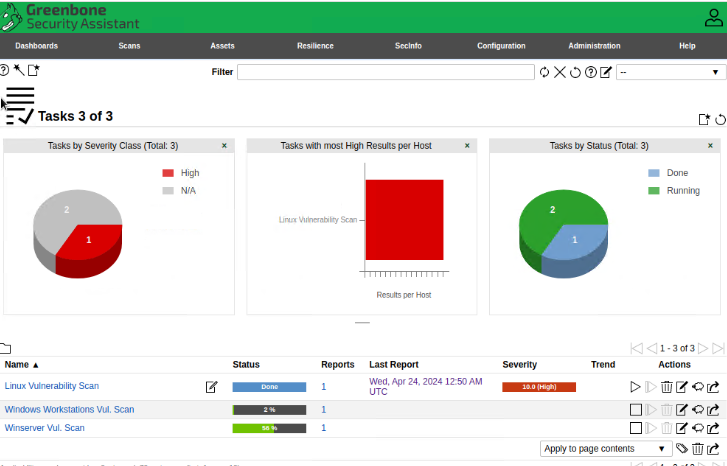
The primary concern is the discovery of an outdated vulnerability scanning engine, which could result in undetected exposures and undermines our security efforts. Additionally, the presence of default credentials in critical HTTP services, alongside unprotected authentication mechanisms in our intrusion detection system, represents a significant security oversight.

Less urgent but equally important for our sustained security are the medium-severity vulnerabilities related to SSL/TLS configurations and expired certificates. These weaknesses, if unaddressed, could leave our company susceptible to data interception and loss of trust in our digital communications.

In response to these findings, this report outlines a series of prioritized remediation steps, beginning with the imperative upgrade of our scanning engine and the immediate securing of affected service credentials. It is imperative that Cat’s Company responds decisively to these vulnerabilities to maintain the integrity of our operations and uphold our commitment to security excellence.

The recommended course of action, detailed herein, aligns with industry best practices and reinforces our proactive stance on cybersecurity management.

**Scan Results**:

****

**Detailed Scan Results**

The vulnerability assessment executed using the Greenbone OpenVAS tool yielded precise and actionable intelligence on the security status of Cat’s Company’s IT infrastructure. The scanning process was meticulous in its approach, uncovering a spectrum of vulnerabilities that have been rigorously classified according to their severity, as determined by the Common Vulnerability Scoring System (CVSS).

**Scans included: Linux Systems, Windows Workstations, and windows server.**

**Classification of Identified Vulnerabilities:**

- **High Severity (3 Identified)**: These vulnerabilities are characterized by their potential to significantly compromise the network and data integrity. The issues in this category, which include an outdated scan engine and insecure authentication practices, are acute and require immediate resolution to avert possible exploitation.

- **Medium Severity (4 Identified)**: Although not as immediately critical as the high-severity vulnerabilities, this group includes encryption weaknesses and expired certificates that pose risks to the confidentiality and trustworthiness of our secure communications. These medium-severity vulnerabilities could be leveraged as a foothold by adversaries to escalate their attacks.

- **Low Severity (28 Identified)**: These vulnerabilities represent minimal immediate risk but require acknowledgement and eventual remediation to enhance overall security posture and prevent cumulative risk over time.

- **Informational (22 Identified):** Entries classified under 'Log' or informational are not vulnerabilities per se but are valuable for understanding the security environment and for detailed logging purposes.

**Quantitative and Qualitative Data Overview:**

The quantitative data obtained points to a significant volume of medium to low-severity issues that, while not urgent, suggest a pattern of small but pervasive neglect that could lead to larger security gaps if not methodically addressed. Qualtatively, the vulnerabilities range from potentially crippling to minor, painting a picture of a network that, while fundamentally robust, shows areas of weakness that could be shored up to forestall security breaches.

**Interpretation for Strategic Planning:**

The results of this scan form the backbone of a strategic plan to rectify existing vulnerabilities and bolster our network defenses. The insights gathered have been instrumental in prioritizing the response to these vulnerabilities and provide a clear roadmap for action.

**Methodology**:

To comprehensively evaluate the security posture of Cat’s Company’s network infrastructure, the following structured and systematic approach was adopted:

**1. Tool Selection and Configuration:**

- **Greenbone's OpenVAS**: Chosen for its robust scanning capabilities and wide recognition in the industry, OpenVAS was configured for an in-depth examination of the company's network. It was selected due to its comprehensive vulnerability tests and its alignment with industry standards.

- **Scanning Profiles**: Various scanning profiles were configured to ensure a tailored approach to different network segments and device types, optimizing the scan for efficiency and effectiveness.

**2. Target Environment:**

- **EVE Lab Environment**: The assessments were carried out within a controlled EVE network simulation environment, which provided an isolated and secure platform for vulnerability scanning without impacting live systems.

- **System Targets:** A Linux system, a Windows server, and several workstations were included to ensure broad coverage across various operating environments within the company.

**3. Scan Execution:**

- **Pre-Scan Network Enumeration**: A preliminary sweep of the network was performed to map out the live systems and services in operation, aiding in the customization of subsequent vulnerability scans.

- **Vulnerability Scanning:** Using OpenVAS, vulnerability scans were executed against the identified targets. The scans were comprehensive, covering thousands of known vulnerabilities and checking for updates prior to execution to include the latest vulnerability definitions.

- **Credential and Non-Credential Scans:** Both types of scans were employed—credential scans for deep inspection of systems where appropriate access was provided, and non-credential scans to simulate an attacker's perspective from outside the network.

**4. Results Collection and Analysis:**

- **Automated Analysis:** OpenVAS provided an automated initial analysis of vulnerabilities based on their severity, utilizing its built-in database and the latest threat intelligence.

- **Manual Review**: A manual review followed to contextualize the findings within the specific operational environment of Cat’s Company, accounting for any custom configurations and mitigating controls in place.

**5. Reporting and Documentation**:

- **Raw Data Handling:** All raw scan data was securely collected and stored for in depth analysis and for maintaining an audit trail.

- **Report Generation:** Standardized reporting templates were used to document the findings, ensuring consistency and ease of interpretation.

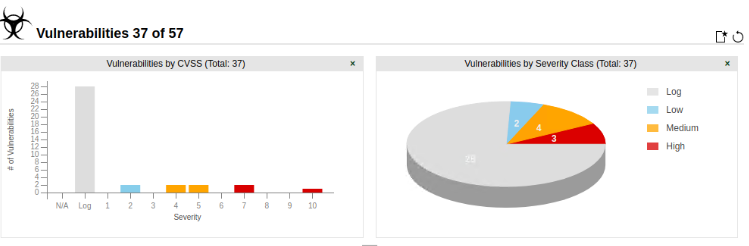
6. **Quality Assurance:**

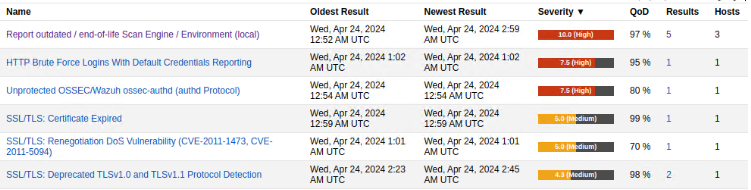
- **Peer Review**: Scan configurations and findings were peer reviewed by the security team to ensure accuracy and completeness.

- **Verification**: A subset of identified vulnerabilities was randomly selected for verification to confirm the presence of the reported vulnerabilities and to avoid false positives.

**Risk Assessment**:

The risk assessment was meticulously formulated following the categorization of vulnerabilities into Critical, High, Medium, or Low severity. The vulnerabilities were analyzed based on the potential impact on Cat’s Company’s assets, with a keen focus on the operational significance of the affected targets, services, or software. Here is an assessment of the six most significant vulnerabilities, arranged by severity:





**1. Critical Severity:**

- *Not Applicable* - No vulnerabilities in the scan were classified as 'Critical' severity.

2. **High Severity**:

- **Outdated/End-of-Life Scan Engine**:

- **Description**: The company's security system relies on an outdated vulnerability scanning engine, leading to a significant risk of missing new threats.

- **Solution**: Upgrade to the most recent version of the scanning software.

- **Systems Affected**: The entire network infrastructure.

- **HTTP Brute Force Logins With Default Credentials**:

- **Description**: Certain HTTP services were discovered to be using default credentials, posing a substantial risk of unauthorized access.

- **Solution**: Enforce strong, unique passwords and consider multifactor authentication where possible.

- **Systems Affected**: 1 known service point, potentially more if default credentials are used network-wide.

- **Unprotected OSSEC/Wazuh ossec-authd**:

- **Description**: The intrusion detection system's authentication service is unprotected, risking system integrity.

- **Solution**: Secure the authentication service and update the intrusion detection system.

- **Systems Affected**: 1 core security system.

3. **Medium Severity**:

- **SSL/TLS Certificate Expired**:

- **Description**: Expired SSL/TLS certificates could lead to compromised secure communications.

- **Solution**: Renew the certificates and manage their lifecycle.

- **Systems Affected**: At least 1 server, with potential widespread effects on all secure communications.

- **SSL/TLS Renegotiation DoS Vulnerability**:

- **Description**: Vulnerabilities in the SSL/TLS renegotiation process may allow denial-of-service attacks.

- **Solution**: Disable renegotiation or update the SSL/TLS protocols.

- **Systems Affected**: Multiple servers utilizing SSL/TLS renegotiation.

- **Deprecated TLSv1.0 and TLSv1.1 Protocols**:

- **Description**: The continued use of deprecated TLS protocols makes the network susceptible to newer cryptographic attacks.

- **Solution**: Transition to TLSv1.2 or TLSv1.3 and disable deprecated protocols.

- **Systems Affected**: Various network endpoints using older encryption protocols.

4. **Low Severity:**

- *Not detailed in the provided information* - Additional low-severity vulnerabilities should be addressed after the higher-severity issues.

Each vulnerability's risk level is determined by its impact on the confidentiality, integrity, and availability (CIA) of the company’s data and systems. The critical and high-severity vulnerabilities directly threaten business operations and should be addressed immediately. Medium-severity vulnerabilities require timely remediation to prevent any future security incidents. The index of vulnerabilities provides a clear view of the current risk landscape and underpins the urgent need for the recommendations outlined in this report.

**Recommendations:**

The risk assessment illuminates several areas where immediate improvements are required. Based on the vulnerabilities identified, the following actions are recommended to bolster the security posture of Cat’s Company:

1. **Upgrade Security Scanning Tools:**

- **Priority**: Urgent

- **Justification:** The current scanning tools are outdated, potentially missing new vulnerabilities and exposures.

- **Action Steps**: Procure the latest version of the scanning software, update the systems, and perform a full re-scan to ensure all vulnerabilities are identified.

2. **Enforce Strong Authentication Measures**:

- **Priority**: Urgent

- **Justification**: Default credentials present a high risk of unauthorized access, one of the most common attack vectors.

- **Action Steps**: Immediately replace all default passwords with strong, unique passwords, enforce password complexity requirements, and implement account lockout policies to prevent brute force attempts. Where applicable, enable multi-factor authentication.

3. **Secure OSSEC/Wazuh Authentication Protocol**:

- **Priority**: Urgent

- **Justification**: Intrusion detection systems are critical; unprotected authentication could lead to system compromise and loss of sensitive data.

- **Action Steps**: Update and configure OSSEC/Wazuh with secure authentication protocols, ensuring the service is properly hardened against attacks.

4. **Renew and Manage SSL/TLS Certificates**:

- **Priority**: High

- **Justification**: Expired certificates can lead to a loss of trust and allow man-in-the-middle attacks.

- **Action Steps**: Immediately renew any expired certificates. Implement an automated certificate management system to track and renew certificates before they expire.

5. **Update SSL/TLS Protocols**:

- **Priority**: High

- **Justification**: Older versions of SSL/TLS are vulnerable to exploits that compromise secure communications.

- **Action Steps**: Disable outdated SSL/TLS protocols such as TLSv1.0 and TLSv1.1 across all systems. Ensure all systems use TLSv1.2 or higher, with a preference for TLSv1.3 where supported. Review and disable any weak ciphers.

6. **Continual Security Awareness Training**:

- **Priority**: Moderate

- **Justification**: Human error remains a significant risk factor in cybersecurity.

- **Action Steps:** Develop an ongoing security training program for all employees, focusing on recognizing and responding to security threats, the importance of strong passwords, and adherence to security policies.

7. **Regular Patch Management and System Updates**:

- **Priority**: Moderate

- **Justification**: Many vulnerabilities arise from outdated systems and software.

- **Action Steps**: Establish a regular schedule for patch management and system updates. Automate the update processes where possible and ensure a procedure is in place for emergency patches in response to critical threats.

8. **Incident Response Plan Revision**:

- **Priority**: Moderate

- **Justification**: A comprehensive incident response plan is essential for minimizing the impact of any security breach.

- **Action Steps**: Review and update the incident response plan to incorporate the latest best practices. Conduct regular drills to ensure the team's readiness.

9. **Network Segmentation and Monitoring Enhancement**:

- **Priority:** Moderate

- **Justification**: Segmentation can limit the spread of an attack within the network, and enhanced monitoring can detect anomalies sooner.

- **Action Steps**: Evaluate current network segmentation and implement improvements to isolate sensitive data and systems. Enhance monitoring capabilities to detect and respond to unusual network traffic patterns.

These recommendations are intended to provide a clear and actionable path to strengthening Cat’s Company’s cybersecurity infrastructure. By systematically addressing the vulnerabilities in order of priority, thhis company can effectively mitigate the identified risks, safeguarding against potential security breaches and ensuring the continuity of its operations.

**Citations**

1. Greenbone Networks (2023). OpenVAS. [Software documentation and usage guidelines]/

2. First.org. (2023). \*Common Vulnerability Scoring System (CVSS)\*. Retrieved from <https://www.first.org/cvss/>

3. Cybersecurity & Infrastructure Security Agency (CISA). (2023). \*Best Practices for Public Key Infrastructure (PKI) Management\*.

<https://www.cisa.gov/topics/cybersecurity-best-practices>

**POWERPOINT FOR CAT**

<https://docs.google.com/presentation/d/1vDjBHI5owoVbkPDmu9PCNm7O6Br7UTGU/edit#slide=id.p1>