Vulnerability Assessment  
Report  
  
Created by: Harsh Patel

Date: January 20, 2025

**Table of Contents**

Executive Summary 3

Scan Results 3

Methodology 4

Findings 5

Risk Assessment 5

Recommendations 6

Conclusion 6

References 7

**EXECUTIVE SUMMARY**

This report provides an overview of the vulnerability assessment conducted for Cat’s Company to identify security weaknesses in its IT infrastructure. The purpose of the assessment was to safeguard critical assets and support informed decision-making by the executive team. The OpenVAS scan revealed six vulnerabilities, categorized based on their severity, ranging from Critical to Low. These vulnerabilities pose risks including potential unauthorized access, service disruption, and exposure of sensitive data.

Our prioritized recommendations address these vulnerabilities systematically to minimize risk and enhance the organization’s security posture. Immediate actions are advised for Critical and High-risk vulnerabilities, while Medium and Low-risk issues can be addressed subsequently as part of a strategic plan. This report includes detailed findings, risk assessments, and practical recommendations to mitigate identified threats effectively.

By implementing the proposed measures, Cat’s Company can significantly reduce its exposure to cyber threats and strengthen its overall resilience against potential attacks.

**SCAN RESULTS**

**Summary of Results:** The vulnerability scan was conducted using OpenVAS, targeting a Windows 11 machine and a Linux server within Cat’s network. The results were categorized based on industry-standard severity levels:

* **Critical:** 2 vulnerabilities
* **High:** 2 vulnerabilities
* **Medium:** 1 vulnerability
* **Low:** 1 vulnerability

**Critical Vulnerabilities:**

1. **Remote Code Execution in Outdated Software**: Found on the Linux server, this vulnerability allows attackers to execute arbitrary code.
2. **Unpatched Zero-Day Exploit**: Detected on the Windows 11 machine, leaving it susceptible to unauthorized access.

**High Vulnerabilities**:

1. **Weak Password Policies**: Affecting both systems, increasing the risk of brute force attacks.
2. **Default Configuration Settings**: Found on the Linux server, exposing sensitive services to attackers.

**Medium Vulnerability**:

1. **Unencrypted Network Traffic**: Detected between internal systems, making data interception possible.

**Low Vulnerability**:

1. **Unused Open Ports**: Identified on the Linux server, increasing the attack surface.

**METHODOLOGY**

The assessment utilized the following tools and procedures:

* **OpenVAS:** Conducted comprehensive scans for vulnerabilities across systems.
* **Environment:** Windows 11 workstation and Linux server in a simulated network.
* **Testing:** Authenticated scans were performed to uncover deeper vulnerabilities, ensuring the accuracy of results.

Tool’s purpose:

* **OpenVAS:** Detects known vulnerabilities and categorizes them based on severity.

Once test was over Cross-checked results against the NIST database and MITRE guidelines for validation.

**FINDINGS**

1. **Successful Scans:**
   * **Windows 11 machine**: All scheduled scans completed successfully.
   * **Linux server**: Majority of scans were successful; minor issues due to restrictive permissions.
2. **Unsuccessful Scans**: Firewall interruptions caused brief inconsistencies during initial scans but were resolved by reconfiguring firewall settings.

**RISK ASSESSMENT**

Severity Categories and Risk Index:

* **Critical:** Exploits with immediate business impact (e.g., data breaches).
* **High:** High probability of compromise if unaddressed.
* **Medium:** Moderate risk that requires timely attention.
* **Low:** Low probability of exploitation but still worth addressing.

Detailed Vulnerabilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Severity | Vulnerability | Description | Solution | Affected System |
| Critical | Remote code Execution | Arbitrary code execution via outdated software. | Patch/update software immediately. | Linux |
| Critical | Unpatched Zero-Day Exploit | Exploitation risk due to lack of patches. | Apply vendor provided patches. | Windows Machine |
| High | Weak Passwords and Policies | Susceptible to brute force attacks. | Enforcing strong password policies. | Both Systems |
| High | Default Configuration Settings | Exposure of sensitive services. | Disable default settings and reconfigure. | Linux |
| Medium | Unencrypted Network Traffic | Risk of data interception. | Implement network encryption (e.g., TLS). | Internal Network of Company |
| Low | Unused Open Ports | Increased attack surface. | Close all unnecessary ports. | Linux Server |

**RECOMMENDATIONS**

1. **Critical Priority:**
   * Apply immediate patches for remote code execution and zero-day exploits.
   * Conduct penetration testing post-remediation to validate fixes.
2. **High Priority:**
   * Implement strong password policies, including multi-factor authentication.
   * Reconfigure Linux server to disable default settings and minimize exposed services.
3. **Medium Priority:**
   * Enable encryption protocols like TLS for internal communications.
   * Educate employees on secure communication practices.
4. **Low Priority:**
   * Close unused ports to reduce the attack surface.
   * Conduct regular scans to identify and address new vulnerabilities.
5. **Policy Recommendations:**
   * Establish a patch management process.
   * Regularly audit configurations and update policies to align with best practices.

**CONCLUSION**

The assessment identified six vulnerabilities, two of which are critical and require immediate attention. By implementing the recommendations, Cat’s Company can significantly enhance its security posture, reduce exposure to risks, and ensure operational continuity. Regular assessments and adherence to best practices are essential for maintaining a secure environment.

**References**

Zbrog, B. M. (2024, March 14). *A guide to digital forensics and cybersecurity tools*. Forensics Colleges. <https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools>

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. In *NIST CSWP 29* [Report]. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

*CVE website*. (n.d.). <https://www.cve.org/ResourcesSupport/FAQs#pc_cve_list_basicscve_list_data_feeds>

*Active Scanning: Vulnerability scanning, sub-technique T1595.002 - Enterprise | MITRE ATT&CK®*. (n.d.). <https://attack.mitre.org/techniques/T1595/002/>