**PROJECT 6**

**Title: Cat’s Company Vulnerability Assessment Report**

***By Titobiloluwa (Tito) Ilori***

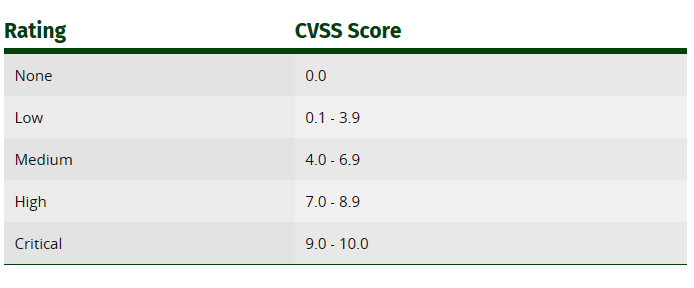
1. **Executive Summary**

A credentialled vulnerability assessment scan was conducted on the computer devices and servers that are within the CAT IT Infrastructure using OpenVAS, to collect and prioritize based on all the information that was found from highest risk to lowest and determine what information would be necessary for the executive team to make decisions and preparations to have them mitigated. The scan was successfully carried out on 2 servers (Linux and Windows) and 2 Windows workstations with 46 unique vulnerabilities detected with the network.

Four vulnerabilities are recommended to be mitigated early, based on their severity as corroborated by known vulnerabilities on NIST National Vulnerability Database. The actions will protect the company’s assets and improve its security posture. The web server on the Linux server is vulnerable to loss of data confidentiality, integrity and server availability which will cost the company so much loss. Therefore, it is crucial to change the default password on the web server and disable renegotiation capabilities from the affected SSL/TLS service as soon as possible. It is also important to note that the workstations have an outdated Operation System as the vendor does not support or provide security updates for it anymore. It is recommended to upgrade to a version which is still supported. These and more in this report will ensure the company improves its security posture. See this [5-7 minute](https://docs.google.com/presentation/d/15bwL7nHGPyukyzEuexu3Ag1e4Jh_nCMG/edit?usp=sharing&ouid=115416687649530778723&rtpof=true&sd=true) briefing summarizing the report and recommendations.

**2. Scan Result**

Within the OpenVAS, there are 4 categorizations of severity, High severity (7 – 10), medium severity (4 – 6.9), low severity (0 – 3.9) and none/logs. This tool also provides the relevant CVE ID on the NIST NVD. Below is the severity rating compared to the CVSS score.



*Table 1: CVSS v3.0 Qualitative severity rating scale [1]*

Recommendations to improve Cat’s company security posture will be determined based on the severity rating. The more the score, the more severity it poses on the security posture and the more its recommendation will be prioritized.

In this report, the four target devices that were successfully scanned will be tabulated, and recommendations will be given as per priority and scope.

**3. Methodology**

For this vulnerability assessment, we used the Greenbone Security Assistant (web-based) of an open-source vulnerability scanner called Open Vulnerability Assessment Scanner (OpenVAS). This tool can search for known vulnerabilities in host devices within a local network. The web-based user interface runs a current version updated on 2023-07-27.

**Host-Based Scan**: OpenVAS was used to run full and fast vulnerability scans on all the hosts within the local network. The target devices included a Windows Server 2016 (IP: 172.16.14.53), Linux – Ubuntu (IP: 172.16.14.52), Kali Linux Machine (IP: 172.16.14.51) and two Windows workstations (IPs: 172.16.14.50/54).

**Authenticated scanning: The** credentials for each host was registered on the OpenVAS tool, allowing the tool to scan the host thoroughly for any vulnerabilities present.

The OpenVAS tool was installed on the Kali Linux machine.

**4. Findings**

Of the Five (4) hosts identified as within the local network, 4 hosts were successfully scanned. The Kali Linux machine vulnerability scan was not successful.

**5 Risk Assessment**

This report identifies 46 unique security vulnerabilities across the devices that could have a significant impact on applications used for day-to-day business operations.

A screenshot of a computer

Description automatically generated

| **High Severity** | **Medium Severity** | **Low Severity** | **Logs** |
| --- | --- | --- | --- |
| **4** | **5** | **2** | **35** |

*Table 5.0: Summary of the vulnerability detected during the scan in OpenVAS*

**5.1 High Severity Vulnerability**

4 were unique high-severity vulnerabilities. The table below highlights 2 high severity vulnerabilities.

| **Host IP Address(es)** | **Description** | **CVE ID(s)** | **Solution** |
| --- | --- | --- | --- |
| Windows Workstations  172.16.14.50  172.16.14.54 | An EOL (End of Life) version of OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of the host. [2] | - | Upgrade the OS on the host to a version which is still supported and receiving security updates by the vendor. |
| Linux server  172.16.14.52 | HTTP Brute Force logins with Default credentials. This issue may be exploited by a remote attacker to – for instance, gain access to sensitive information or modify system configuration. [3] | **CVE-1999-0502 [3]** | Change the default password as soon as possible. [4] |

*Table 5.1: Table highlights 2 of the 4 unique high-severity vulnerabilities.*

**5.2 Medium Severity Vulnerability**

5 was the unique medium severity vulnerability across the 4 target devices. These vulnerabilities often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner but are not as urgent as the other vulnerabilities.

The table below highlights 2 of the 5 vulnerabilities.

| **Host IP Address(es)** | **Description** | **CVE ID(s)** | **Solution(s)** |
| --- | --- | --- | --- |
| Linux server  172.16.14.52 | SSL/TLS: Renegotiation DoS Vulnerability. The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability. | CVE-2011-1473  CVE-2011-5094  [5] | Remove/disable renegotiation capabilities from/in the affected SSL/TLS service [6] |
| Windows Server  172.16.14.53 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection. Contains known Cryptographic flaws like BEAST (Browser Exploit Against SSL/TLS) and FREAK (Factoring Attack on RSA-EXPORT Keys Padding Oracle on Downgraded Legacy Encryption) | CVE-2011-3389  [7]  CVE-2015-0204  [8] | It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favour of the TLSv1.2+ protocols. |

*Table 5.2: Table highlights 2 of the 5 unique medium severity vulnerabilities.*

**5.3 Low Severity Vulnerability**

2 unique low-severity vulnerabilities were found during this scan. The table below shows 1 of the 2.

| **Host IP Address(es)** | **Description** | **CVE ID(s)** | **Solution(s)** |
| --- | --- | --- | --- |
| All scanned devices | ICMP Timestamp Reply Information Disclosure. | CVE-1999-0524 [9] | Disable the support for ICMP timestamp on the hosts completely/protect the hosts by a firewall, and block ICMP packets passing through the firewall in either direction. |

*1Table 5.3: Table highlights 1 of the 2 unique low-severity vulnerabilities.*

**6. Recommendations**

The recommendations provided in this report are derived from the findings obtained during the credentialed vulnerability scan with OpenVAS. It is essential to acknowledge that vulnerability scanning is just one aspect of assessing the network's security posture. Therefore, the results should not be considered the sole and definitive measure of the Cat’s company’s security posture. To comprehensively evaluate the current security status, other factors like policy review, examination of internal security controls and procedures, or internal red teaming/penetration testing should also be considered.

**6.1 Remediation**

Taking the following actions across all hosts will strengthen the security posture of Cat’s company.

| Priority | Steps to Take | Effect to Security Posture |
| --- | --- | --- |
| 1 | Change the default password as soon as possible to prevent HTTP Brute Force logins with Default credentials. [3] | Strengthens the Confidentiality and Integrity of the web server. This will prevent (avoid) Cat’s company from all risks associated with the loss of Confidentiality and Integrity data. [4] |
| 2 | Upgrade the Windows Workstation Operating System on the host to a version which is still supported and receiving security updates by the vendor. | The risk associated with attackers exploiting the numerous vulnerabilities of the EOL version of OS to compromise the CIA triad will be controlled/avoided. |
| 3 | Remove/disable renegotiation capabilities from/in the affected SSL/TLS service on the Ubuntu (Linux) server [6] | This will prevent (Risk Avoidance) from Denial of Service (Availability) attack if exploited by an attack which will cost the business a lot if the web server goes down. |
| 4 | If applicable, educated the staff of Cat’s Company to ensure best password practices and the IT department to stay updated on security patches available for OSs and applications used in the company. | Strengthens the security posture. |
| 5 | Disable the support for ICMP timestamp on the hosts completely/protect the hosts by a firewall, and block ICMP packets passing through the firewall in either direction. [9] | This vulnerability should be accepted as it poses low exploitability/vulnerability to the infrastructure and it costs more to implement the controls. |

**APPENDIX A:** Display of Successful Vulnerability Scan in OpenVAS – Greenbone Security Assistant.

A screenshot of a computer

Description automatically generated

**APPENDIX B:**

1. Common Vulnerability Scoring System v3.0: Specification Document <https://www.first.org/cvss/v3.0/specification-document>

2. Lifecycle FAQ - Windows - <https://support.microsoft.com/en-US/help/13853/windows-lifecycle-fact-sheet>

3. CVE-1999-0502 Detail - NIST NVD (Aug 17, 2022) <https://nvd.nist.gov/vuln/detail/CVE-1999-0502>

4. Default Credentials - Mitre Att&ck (Mar 9, 2023) <https://attack.mitre.org/techniques/T0812/>

5. CVE-2011-5094 Detail - NIST NVD (June 18, 2012) <https://nvd.nist.gov/vuln/detail/CVE-2011-5094>

6. How to Secure Server- and Client-Initiated SSL Renegotiation - Borislav Kiprin (Apr 2, 2021) <https://crashtest-security.com/secure-client-initiated-ssl-renegotiation/>

7. CVE-2011-3389 Detail - NIST NVD (Nov 29, 2022) - <https://nvd.nist.gov/vuln/detail/CVE-2011-3389>

8. CVE-2015-0204 Detail - NIST NVD (July 18, 2018) - <https://nvd.nist.gov/vuln/detail/CVE-2015-0204>

9. CVE-1999-0524 Detail - NIST NVD (Oct 14, 2022) - <https://nvd.nist.gov/vuln/detail/CVE-1999-0524>