**Deliverable 1: Scanning and Reporting Using Nessus Vulnerability Scanner**

Hammaz Ahmed

Department of Professional Studies, Saint Louis University

CYBR-5220-21- Incident Response and Mitigation

Randy Sliva, Teacher.

November 11th, 2023

**Deliverable 1: Scanning and Reporting Using Nessus Vulnerability Scanner**

**Target Selection**

Sanofi is a multinational pharmaceutical company that deals with multiple aspects of healthcare and can include research, development, manufacturing, and distribution of pharmaceuticals. The primary reason for choosing this company is that pharmaceutical companies are among the most targeted industries out there because of their sensitive data, and valuable Personally identifiable information. This company belongs among the mid-sized companies and hence there are more chances of discovering vulnerabilities which will also be more common among smaller-sized companies. This report can also help other lower-level companies by matching the loopholes that are present in this project. A basic network scan was performed using Nessus Essentials and the report and a summary along with recommendations are provided below.

**Audience**

This report is for the CEO of our organization. It gives the higher-ups an overview of the current vulnerabilities presented in our website “<https://www.sanofi.com/en>”. The report also provides recommendations and steps to take to minimize or completely eradicate the vulnerabilities present.

**Figure 1**

Visual Analysis of Vulnerabilities Present

A diagram of a pie chart

Description automatically generated

**Figure 2**

Report From Nessus

A screenshot of a computer

Description automatically generated

**Table 1**

Top 5 Vulnerabilities Present

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CVE | CVSS/Severity | Vulnerability Name | Reason | Solution |
| CVE-2023-25690 | 9.8/ Critical | Apache 2.4.x < 2.4.56 Multiple Vulnerabilities | The version of Apache httpd installed on the remote host is prior to 2.4.56 | Upgrade to Apache version 2.4.56 or later. |
| CVE-2021-44224 | 9.8/Critical | Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF | A version of Apache httpd installed on the remote host is equal to or greater than 2.4.7 and prior to 2.4.52. | Upgrade to Apache version 2.4.52 or later. |
| CVE-2023-31122 | 7.5/High | Apache 2.4.x <2 .4.58 Multiple form of Vulnerabilities | The version of Apache httpd installed on the remote host is prior to 2.4.58. | Upgrade to Apache version 2.4.58 or later. |
| CVE-2021-36160 | 7.5/High | Apache >= 2.4.30 < 2.4.49 mod\_proxy\_uwsgi | The version of Apache httpd installed on the remote host is greater than 2.4.30 and is prior to 2.4.49. | Upgrade to Apache version 2.4.49 or later. |
| CVE-2016-6797 | 6.5/Medium | HSTS Missing From HTTPS Server (RFC 6797) | Remote web server is not enforcing HSTS, the lack of HSTS allows downgrade attacks, and SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. | Configure the remote web server to use HSTS. |

**Assessment**

The organization is at serious risk of security breaches due to the presence of critical vulnerabilities in its Apache HTTP Server software. These vulnerabilities could allow attackers to launch Denial of Service (DoS) attacks, which would overwhelm the server and make it unavailable to legitimate users, or Server-Side Request Forgery (SSRF) attacks, which could allow attackers to control the server and execute arbitrary commands. The organization's HTTPS server is also vulnerable to attack because it does not have HSTS (HTTP Strict Transport Security) enabled. HSTS instructs web browsers to always connect to the server over HTTPS, even if the user types in an HTTP URL. This helps to protect against attacks that downgrade security to HTTP, such as man-in-the-middle attacks. Without HSTS, sensitive data could be exposed to potential attackers.

**Figure 3**

Screenshot from Nessus Dashboard

A screenshot of a computer

Description automatically generated

**Recommendations**

1. **Apache HTTP Server:** Our organization should prioritize updating all Apache servers. This will automatically address critical vulnerabilities mentioned in table 1.
2. **HSTS Configuration:** Upgrading to HSTS (HyperText Strict Transport Security) will better the HTPPS connection, hence preventing man-in-the-middle attack and downgrade attacks.
3. **Regular Vulnerability Scanning:** Regular scans can help identify new security weaknesses as they arise and enable proactive measures to minimize risks.
4. **Patch Management:** Having and implementing robust patch management procedures and rules will reduce the chances of exposure to vulnerabilities.

**Remaining Vulnerabilities**

#### As shown in Figure 1 above there are other vulnerabilities as well which I haven’t mentioned in my table of top 5 vulnerabilities. For instance, “HTTP/2 Cleartext Detection”. This can be avoided by regulating and limiting incoming traffic coming to this port. As for all the other minor vulnerabilities present, as recommended if we update our systems and patch them now and, in the future, then these vulnerabilities will occur at a very low rate and won't pose any threat to our organization.

#### Conclusion

#### It is essential to address the critical vulnerabilities found in the Apache HTTP Server and implement HSTS in the organization's web servers to strengthen the security posture. Immediate action should be taken to update and patch vulnerable systems, and ongoing security measures should be implemented to prevent the emergence of new vulnerabilities. A proactive approach to security is crucial to protect the organization's digital assets and data.

#### Reference

*How To: Run Your First Vulnerability Scan with Nessus*. (2023, October 31). Tenable®. <https://www.tenable.com/blog/how-to-run-your-first-vulnerability-scan-with-nessus>

KtechHub. (2019, September 2). *How to do Vulnerability Scanning with Nessus* [Video]. YouTube. <https://www.youtube.com/watch?v=35a0VhzIO2Y>

Rangapur, A. (2021, December 16). Vulnerability scanning using Nessus Essentials - Security at your desk - Medium. *Medium*. https://medium.com/security-at-your-desk/vulnerability-scanning-using-nessus-essentials-c1a6b71c21f8