### Vulnerabilities Information

The below Table 5 show the output result of vulnerabilities discovered on the target host system i.e. 172.19.3.92 after scanning and are classified based on their CVSS scores, impact, risk level. However, suggestion on how to mitigate or eradicate these vulnerabilities is discussed.

Table 5: Overall OpenVAS Scan Overview

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S/N | NAME | Service (Port) | Threat Level | CVSS Scores |
| 1. | FTP | 21/TCP | Medium | 6.4 |
| 2. | HTTP | 80/TCP | Medium | 4.8 |
| 3. | TELNET | 23/TCP | Medium | 4.8 |

### 2.1.1 FTP (File Transfer Protocol) – Port 21/TCP

The file transfer protocol (FTP) is for downloading and uploading files over the years; however, FTP is one of the most extensively utilized network services. This, on the other hand, sends passwords and files in plaintext since it lacks an adequate identity authentication method and a secure transmission mechanism. As a result, a study into the security of FTP systems is critical. Because there is no way given for sending data in an encrypted form, the original FTP protocol is inherently unsafe. Table 6 below shows the CVSS scores, risk level, impacts, and mitigation process to prevent FTP from being vulnerable to attack according to the vulnerability assessment scanning (OpenVAS) report run on the provided target host system.

Table 6: FTP Report Overview

|  |  |  |
| --- | --- | --- |
| **Risk Level: Medium** | | **CVSS Score:** 6.4 |
| **Vulnerability** | Users are not required to have an account on the supplied target host system; nevertheless, when requested for a login, users can commonly enter 'anonymous' FTP'. Although users are frequently requested to enter their email address as their password, no verification of the given data is conducted. | |
| **Vulnerability Detection** | The distant FTP server may be accessed using anonymous identities anonymous@example.com and “FTP: anonymous@example.com”. | |
| **Impact** | An attacker may be able to gain access to sensitive files and upload or remove files based on the files available via this anonymous FTP login and the permissions of this account. | |
| **Solution** | If you don't wish to share files, turn off the anonymous login. | |
| **Solution Type** | Mitigation | |

According to NIST (2022), This common vulnerabilities and exposures item is related to configuration rather than a software defect according to CVSS, this CVE entry has no impact as a software fault. The CIA triad of the FTP vulnerability listed below:

* **Confidentiality:** The vulnerability could affect the confidentiality of the data to be constantly jeopardized. If an attacker potentially takes sensitive data by using a man-in-the-middle attack to intercept a communication or hacking directly into a server.
* **Integrity:** Referential integrity is extremely important for business transactions as illegal modifications to information can turns to challenges, report misrepresentations, and financial difficulties if the FTP services are compromised.
* **Availability:** A denial of service (DoS) could be caused with the FTP service which can prevent data from being accessible.

### 2.1.2 HTTP (Hypertext Transfer Protocol) – Port 80/TCP

As reported by (Patni et al., 2017), The HyperText Transfer Protocol Latest release (HTTP/2) is an improvement to the widely used HTTP/1.1. This protocol was designed to improve current applications and services based on the previous standard with minor adjustments and rebuilding. As a result, new weaknesses, and attacks on them have emerged. HTTP/2's protection is ensured via Transport Layer Security (TLS). The HTTP port 80 of the given target host system is vulnerable to the following vulnerabilities:

* CSRF(Cross-SiteRequest Forgery)HTTP-Enum (Directory Enumeration)
* Slowloris DOS Attack
* HTTP-Sqli-Injection (SQL Injection)

Table 7 shows the CVSS scores, risk level, impacts, and mitigation process to prevent the target from being vulnerable to attack according to the vulnerability assessment scanning (OpenVAS) report run on the provided target host system.

Table 7: HTTP Report Overview

|  |  |  |
| --- | --- | --- |
| **Risk Level: Medium** | | **CVSS Score:** 4.8 |
| **Vulnerability** | Examine previously gathered data to see if the host/application is not requiring the transfer of sensitive data through an encrypted SSL/TLS connection. The following are now being checked by the script:  - HTTP Simple Authentication (Basic Auth)  - HTTP Forms (e.g. Login) with 'password' input fields  Details: HTTP Cleartext Transmission of Sensitive Information | |
| **Vulnerability Detection** | The following input fields (url:input name) were identified:  <http://172.19.3.92/login.html>:password  <http://172.19.3.92/phpmyadmin/>:pma password | |
| **Impact** | An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords. | |
| **Solution** | Enforce the use of an encrypted SSL/TLS connection for the delivery of sensitive data. Additionally, ensure that the host / application redirects all users to the secure SSL/TLS connection before enabling sensitive data to be entered into the aforementioned functionalities. | |
| **Solution Type** | Workaround | |

According to CWE (2022), the flaw is created by the absence of a security technique throughout the architecture design phases which the likelihood of exploits is on a high side. The common CIA triad consequence is **Integrity** and **Confidentiality** which means Anyone with access to the channel of communication can read the information.

### 2.1.3 TELNET (Terminal Network) – Port 23/TCP

Telnet protocol is the normal procedure for Internet remote login service and the first remote management protocol supported by network equipment which can be used in almost all types of network operating systems for remote management and configuration of network equipment such as routers and switches (YaYuan Yang, 2020). Table 8 below shows the CVSS scores, risk level, impacts, and mitigation process to prevent Telnet for being vulnerable to attack according to the vulnerable assessment scanning (OpenVAS) report run on the provided target host system.

Table 8: TELNET Report Overview

|  |  |  |
| --- | --- | --- |
| **Risk Level: Medium** | | **CVSS Score:** 4.8 |
| **Vulnerability** | Telnet Unencrypted Cleartext Login | |
| **Vulnerability Detection** | The vulnerability was discovered using the Vulnerability Detection Method. | |
| **Impact** | By sniffing Telnet communications, an attacker can get login names and passwords. | |
| **Solution** | Replace Telnet with a protocol that provides encrypted connections, such as SSH. | |
| **Solution Type** | Mitigation | |

The CIA triad of the TELNET vulnerability are list below:

* **Confidentiality:** The vulnerability could affect the confidentiality of the data to be constantly jeopardized. If an attacker potentially takes sensitive data by using a man-in-the-middle attack to intercept a communication.
* **Integrity:** Login credential could be obtained
* **Availability:** A denial of service (DoS) could be caused.