**Stage 2**

**Overview of Nessus :-**

|  |  |
| --- | --- |
|  | |
| [**Developer(s)**](https://en.wikipedia.org/wiki/Programmer) | [Tenable, Inc.](https://en.wikipedia.org/wiki/Tenable,_Inc.) |
| [**Stable release**](https://en.wikipedia.org/wiki/Software_release_life_cycle) | 8.15.8 / January 18, 2023[[1]](https://en.wikipedia.org/wiki/Nessus_(software)#cite_note-1) |
| [**Operating system**](https://en.wikipedia.org/wiki/Operating_system) | [Linux](https://en.wikipedia.org/wiki/Linux), [macOS](https://en.wikipedia.org/wiki/MacOS) and [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) |
| [**Type**](https://en.wikipedia.org/wiki/Software_categories#Categorization_approaches) | [Vulnerability scanner](https://en.wikipedia.org/wiki/Vulnerability_scanner) |
| [**License**](https://en.wikipedia.org/wiki/Software_license) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software); [GPL](https://en.wikipedia.org/wiki/GNU_Public_License) (2.2.11 and earlier) |
| **Website** | [https://www.tenable.com](https://www.tenable.com/) |

* **Nessus** is a [proprietary](https://en.wikipedia.org/wiki/Proprietary_software) [vulnerability scanner](https://en.wikipedia.org/wiki/Vulnerability_scanner) developed by [Tenable, Inc.](https://en.wikipedia.org/wiki/Tenable,_Inc.)
* **By nessus ,we can analyse the weakness and to take some corrective action to provide security.**
* Vulnerability assessment is a process that identifies and evaluates network vulnerabilities by constantly scanning and monitoring your organization's entire attack surface for risks. It is the first step in defending your network against vulnerabilities that may threaten your organization.
* Unfortunately, almost [60% of cybersecurity professionals](https://www.tenable.com/ponemon-report/cyber-risk) say they don’t have a set schedule to scan for vulnerabilities and many don’t scan for publicly disclosed vulnerabilities at all. Don’t become one of these statistics. Tenable can help you adopt best practices for vulnerability assessment, including recommendations about how to make your program stronger.
* Once downloaded the nessus software from website, activation code sent through mail was provided to activate the vulnerability software.

**Target website ➖www.sonatech.ac.in**

**Target ip address:-162.215.219.65**

**List of vulnerability ➖**

|  |  |  |  |
| --- | --- | --- | --- |
| **s.no** | **Vulnerability name** | **Severity** | **Plugins** |
| **1** | **Service Detection** | **info** | **Plugin ID:22964** |
| **2** | **Nessus SYN scanner** | **info** | **Plugin ID:11219** |
| **3** | **SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)** | **medium** | **Plugin ID:18375** |
| **4** | **SSH Server CBC Mode Ciphers Enabled** | **low** | **Plugin ID:70658** |
| **5** | **SSH Weak Key Exchange Algorithms Enabled** | **low** | **Plugin ID:153973** |

**REPORT:-**

**Vulnerability Name:- Service Detection**

**severity : -info**

**Plugin:- Plugin ID:22964**

**Port :-** 21 / tcp / ftp

**Description:-** Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

**solution:-**

Review the detailed findings in the vulnerability scan report for specific information about the service detection vulnerability.

Follow the recommended steps provided by the scanning tool for addressing and mitigating the identified issues.

Apply necessary patches, updates, or configuration changes to secure the detected services.

**Business Impact:**

The impact of the vulnerability depends on the specific findings. Potential consequences may include unauthorized access to misconfigured services, exposure to known vulnerabilities, or other security risks. Addressing and remediating the identified vulnerabilities promptly is essential to reduce potential security threats.

**Recommendations:**

Thoroughly review the vulnerability scan report to understand the nature of the service detection vulnerability.

Implement the recommended changes to secure the identified services, including applying patches or updating configurations.

Regularly conduct vulnerability scans to proactively identify and address potential security issues

**Vulnerability Name:- Nessus SYN scanner**

**severity : -info**

**Plugin:- Plugin ID:11219**

**Port :-** 21 / tcp / ftp

**Description:-** This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.   
  
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

**solution:-** Protect your target with an IP filter.

**Business Impact**::-

The impact of the vulnerability depends on the specific findings. Potential consequences may include unauthorized access to open ports, increased exposure to network attacks, or other security risks. It is crucial to address and remediate the identified vulnerabilities promptly to mitigate potential security threats.

**Recommendations:**

Review the Nessus scan report thoroughly to understand the nature of the vulnerability.

Apply the recommended patches or configuration changes to address the identified issues.

Regularly perform network scans and security assessments to proactively identify and mitigate potential vulnerabilities

**Vulnerability Name:- SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)**

**severity : -medium**

**Plugin:- Plugin ID:18375**

**Port :-** 1243/ tcp / ssh

**Description:-** he remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.  
  
Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions

**solution:-** Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

**Business Impact**::-

This vulnerability poses a significant risk to the security of SSH communications. Successful exploitation could lead to unauthorized access to sensitive information, data manipulation, or disruption of critical business operations. It is crucial to promptly address and remediate this vulnerability to mitigate potential security threats.

**Recommendations:**

Implement the vendor-recommended patches or updates for the SSH server.

Review and adjust SSH server configurations to adhere to best security practices.

Conduct thorough security assessments and audits to identify and address any additional vulnerabilities.

**Vulnerability Name:- SSH Server CBC Mode Ciphers Enabled**

**severity : -low**

**Plugin:- Plugin ID:70658**

**Port :-** 1243/ tcp / ssh

**Description:-** The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.   
  
Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions

**solution:-** Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

**Business Impact**::-

Exploiting this vulnerability could result in unauthorized access to sensitive information, data tampering, or even potential disruption of business operations. It is crucial to address this issue promptly to enhance the security of SSH communications and protect against potential security breaches.

**Recommendations:**

Conduct a thorough review of the SSH server configuration to identify and disable CBC mode ciphers.

Regularly update and patch the SSH server software to ensure the latest security enhancements are applied.

Monitor SSH server logs for any suspicious activities and conduct regular security audits.

**Vulnerability Name:- SSH Weak Key Exchange Algorithms Enabled**

**severity : -low**

**Plugin:- Plugin ID:153973**

**Port :-** 1243/ tcp / ssh

**Description:-** The remote SSH server is configured to allow key exchange algorithms which are considered weak.  
  
This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:  
  
diffie-hellman-group-exchange-sha1  
  
diffie-hellman-group1-sha1  
  
gss-gex-sha1-\*  
  
gss-group1-sha1-\*  
  
gss-group14-sha1-\*  
  
rsa1024-sha1  
  
Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

**Solution:** Contact the vendor or consult product documentation to disable the weak algorithms.

**Business Impact**::- If exploited, this vulnerability could lead to unauthorized access to sensitive information, loss of data confidentiality, and potential disruption of business operations. It is crucial to address this issue promptly to mitigate the risk of security breaches and protect the integrity of the organization's data and systems.

**Recommendations:**

Conduct a thorough review of the SSH server configuration to identify and disable weak key exchange algorithms.

Regularly update and patch the SSH server software to ensure the latest security enhancements are applied.

Monitor SSH server logs for any suspicious activities and conduct regular security audits

**Prepared by**

**S.Padmavathy, AP/CSE, Sona College of Technology,Salem-636005**