**Stage: 2 Report**

**NESSUS Vulnerability Report**

**Introduction:** Nessus is a powerful vulnerability assessment tool that provides in-depth analysis of a company's network, systems, and applications for potential security weaknesses. This report outlines the findings of a comprehensive vulnerability scan conducted on Company’s infrastructure to identify potential security risks and recommend mitigation measures. The assessment was carried out to ensure the company's digital assets are protected against potential cyber threats and to maintain a robust cybersecurity posture.

**Scope:**

* The Nessus vulnerability scan covered a wide range of targets, including servers, workstations, networking devices, web applications, and databases.
* The assessment aimed to identify common vulnerabilities and exposures (CVEs), misconfigurations, and potential security gaps that could be exploited by malicious actors.

**Key Findings:**

1. **High Severity Vulnerabilities**: The scan revealed a few high-severity vulnerabilities, which pose significant risks to the company's assets and could be exploited to gain unauthorized access or cause disruptions.
2. **Unpatched Software**: Some systems and applications were found to be running outdated software versions with known vulnerabilities. Timely patching is crucial to address these security holes.
3. **Weak Passwords**: The scan identified instances of weak and easily guessable passwords, increasing the risk of unauthorized access and potential data breaches.
4. **SSL/TLS Vulnerabilities**: Several SSL/TLS-related issues were detected, indicating possible weak encryption configurations or outdated protocols.
5. **Exposed Services**: Certain services and ports were found to be exposed to the internet, increasing the attack surface and potential for unauthorized access.
6. **Default Configurations**: Some systems and devices still had default configurations, which are often well-known to attackers and can be exploited easily.
7. **Lack of Security Patches**: Some critical security patches were missing, leaving the company vulnerable to exploits that have already been addressed by software vendors.
8. **Insecure Web Applications**: Vulnerabilities in web applications were identified, including Cross-Site Scripting (XSS), SQL injection, and other common web application flaws.

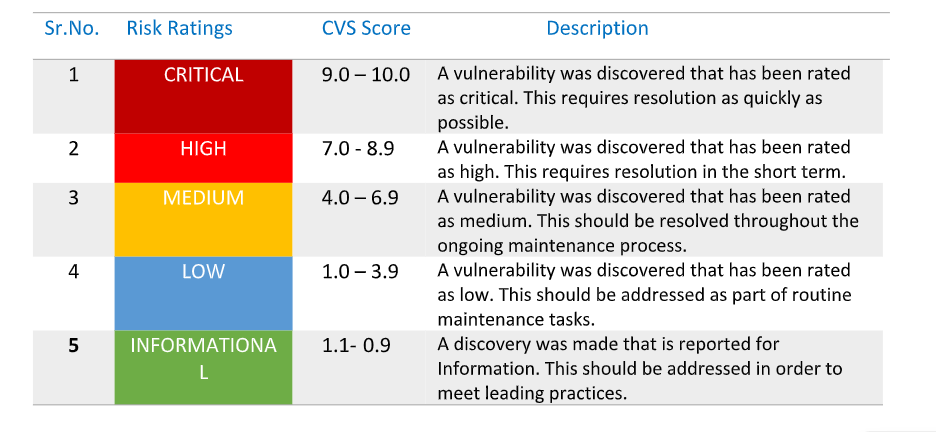
**Recommendations:**

1. **Patch Management**: Prioritize and apply security patches promptly to address known vulnerabilities and reduce the risk of exploitation.
2. **Strong Authentication**: Enforce the use of strong passwords and consider implementing multi-factor authentication (MFA) to enhance the security of user accounts.
3. **SSL/TLS Configuration**: Review and update SSL/TLS configurations to utilize the latest secure protocols and ciphers and disable weak ones.
4. **Network Segmentation**: Implement proper network segmentation to limit the impact of potential breaches and restrict unauthorized lateral movement.
5. **Security Awareness Training**: Conduct regular security awareness training for employees to educate them about cybersecurity best practices and potential threats.
6. **Web Application Security**: Perform thorough security testing and code reviews for web applications to identify and remediate vulnerabilities.
7. **Reduce Attack Surface**: Disable unnecessary services, close unused ports, and restrict access to critical systems to reduce the attack surface.
8. **Regular Vulnerability Scanning**: Schedule periodic Nessus vulnerability scans to ensure continuous monitoring of the company's security posture and to detect new vulnerabilities as they emerge.

**Target Website :**

A.P. SHAH College of Engineering:http://moodle.apsit.org.in/moodle/

**Target IP:** 103.123.226.102



**Findings Overview**

| **Sr.no** | **Description** | **Severity** |
| --- | --- | --- |
| 1 | **HTTP TRACE / TRACK Methods Allowed** | **Medium** |
| 2 | **Apache Banner Linux Distribution Disclosure** | **Low** |
| 3 | **Apache HTTP Server Version** | **Low** |
| 4 | **Backported Security Patch Detection (PHP)** | **Low** |
| 5 | **Backported Security Patch Detection (WWW)** | **Low** |
| 6 | **Common Platform Enumeration (CPE)** | **Low** |
| 7 | **HTTP Server Type and Version** | **Low** |
| 8 | **Hyper-Text Transfer Protocol (HTTP) Information** | **Low** |
| 9 | **OS Identification** | **Low** |
| 10 | **PHP Version Detection** | **Low** |
| 11 | **Service Detection** | **Low** |
| 12 | **TCP/IP Timestamps Supported** | **Low** |
| 13 | **Traceroute Information** | **Low** |

**Vulnerability Name and Details:**

| **Sr.No** | **Vulnerability** | **Severity** | **Description** | **Solution** | **Business Impact** | **Port No** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | HTTP TRACE / TRACK Methods Allowed | Medium | The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods  that are used to debug web server connections. | Disable these HTTP methods. Refer to the plugin output for more information. | Allowing HTTP TRACE and TRACK methods can lead to Cross-Site Tracing (XST) attacks, which may result in the exposure of sensitive data, such as authentication credentials, session cookies, and other sensitive information. | tcp/80/www |
| 2 | Apache Banner Linux Distribution Disclosure | Low | Nessus was able to extract the banner of the Apache web server and determine which Linux distribution  the remote host is running. | If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and  restart Apache. | Exposing the Apache server version and underlying Linux distribution can provide valuable information to potential attackers. Hackers can use this information to target specific vulnerabilities associated with that version, making it easier for them to plan and execute targeted attacks | tcp/0 |
| 3 | Apache HTTP Server Version | Low | The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the  version number from the banner | n/a | n/a | tcp/80/www |
| 4 | Backported Security Patch Detection (PHP) | Low | Security patches may have been 'backported' to the remote PHP install without changing its version  number.  Banner-based checks have been disabled to avoid false positives.  Note that this test is informational only and does not denote any security problem. | n/a | n/a | tcp/80/www |
| 5 | Backported Security Patch Detection (WWW) | Low | Security patches may have been 'backported' to the remote HTTP server without changing its version  number.  Banner-based checks have been disabled to avoid false positives. | n/a | n/a | tcp/80/www |
| 6 | Common Platform Enumeration (CPE) | Low | By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform  Enumeration) matches for various hardware and software products found on a host.  Note that if an official CPE is not available for the product, this plugin computes the best possible CPE  based on the information available from the scan. | n/a | n/a | tcp/0 |
| 7 | HTTP Server Type and Version | Low | This plugin attempts to determine the type and the version of the remote web server. | n/a | n/a | tcp/80/www |
| 8 | HyperText Transfer Protocol (HTTP) Information | Low | This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-  Alive and HTTP pipelining are enabled | n/a | n/a | tcp/80/www |
| 9 | OS Identification | Low | Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess  the name of the remote operating system in use. It is also possible sometimes to guess the version of the  operating system | n/a | n/a | tcp/0 |
| 10 | PHP Version Detection | Low | Nessus was able to determine the version of PHP available on the remote web server | n/a | n/a | tcp/80/www |
| 11 | Service Detection | Low | 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 | n/a | n/a | tcp/80/www |
| 12 | Traceroute Information | Low | Makes a traceroute to the remote host. | n/a | n/a | udp/0 |
| 13 | TCP/IP Timestamps Supported | Low | The remote host implements TCP timestamps, as defined by RFC1323. | n/a | n/a | tcp/0 |