TEAM 2.5

CyberSpectrum

STAGE 2

Overview:

Nessus scanning is a cybersecurity practice and a network vulnerability scanner that plays a crucial role in identifying and assessing vulnerabilities within computer systems, networks, and infrastructure. Nessus is developed by Tenable, Inc. and is widely used by security professionals and organizations to enhance their network security.

At its core, Nessus scanning is a systematic and automated process that involves the following key elements:

1. Vulnerability Detection: Nessus scanning actively seeks out vulnerabilities within a target system or network. These vulnerabilities can include software flaws, misconfigurations, weak passwords, and other security issues that could be exploited by malicious actors. The scanner relies on a comprehensive database of known vulnerabilities, continuously updated to include the latest threats.
2. Network Discovery: Before scanning for vulnerabilities, Nessus identifies and maps the target network or system. This initial discovery phase helps the scanner understand the topology of the network and determine what devices and services are present.
3. Scanning and Assessment: Once the network is discovered, Nessus conducts a series of tests and assessments. These include port scanning to identify open ports, services running on those ports, and attempts to identify vulnerabilities related to these services. The scanner may also test for weak or default passwords, misconfigured settings, and other common security issues.
4. Risk Assessment: After scanning, Nessus provides a detailed report that includes a list of identified vulnerabilities, their severity levels, potential

impacts, and recommendations for remediation. Each vulnerability is typically assigned a Common Vulnerability Scoring System (CVSS) score to help organizations prioritize their response.

5. Customization and Reporting: Nessus is highly customizable, allowing users to define scan policies, specify targets, and tailor scans to their specific needs. It generates comprehensive reports, often with detailed information about the vulnerabilities found and suggested remediation steps.
6. Continuous Monitoring: Nessus can be configured to perform regular, automated scans, helping organizations to continuously monitor their network security posture. This proactive approach allows for the identification of new vulnerabilities as they emerge.
7. Compliance and Configuration Auditing: Beyond vulnerability scanning, Nessus can perform compliance checks and configuration audits to ensure that systems and networks adhere to industry-specific standards and best practices.

The significance of Nessus scanning cannot be overstated in today's cybersecurity landscape. With a rapidly evolving threat landscape and ever-increasing network complexities, identifying and addressing vulnerabilities promptly is critical to safeguarding sensitive data and maintaining the integrity and availability of systems. Nessus not only provides valuable insights into existing weaknesses but also aids in compliance efforts, thereby helping organizations avoid potential breaches and data loss while remaining compliant with regulatory requirements.

Target Website: www.testfire.net

Target IP Address: 65.61.137.117

List of Vulnerabilities:

S. No.	Vulnerability	Severity	Plugins
1.	TLS Version 1.0 Protocol Detection	Medium	104743
2.	TLS Version 1.1 Protocol Deprecated	Medium	157288
3.	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Low	83875

4.	ICMP Timestamp Request Remote Date Disclosure	Info	10114
5.	Additional DNS Hostnames	Info	46180
6.	Apache Tomcat Detection	Info	39446
7.	Common Platform Enumeration (CPE	Info	45590
8.	Device Type	Info	54615
9.	HSTS Missing From HTTPS Server	Info	84502
10.	HTTP Server Type and Version	Info	10107
11.	HyperText Transfer Protocol (HTTP) Information	Info	24260
12.	Nessus SYN scanner	Info	11219
13.	Nessus Scan Information	Info	19506
14.	OS Identification	Info	11936
15.	SSL / TLS Versions Supported	Info	56984
16.	SSL Certificate Information	Info	10863
17.	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	Info	95631
18.	SSL Cipher Block Chaining Cipher Suites Supported	Info	70544
19.	SSL Cipher Suites Supported	Info	21643
20.	SSL Perfect Forward Secrecy Cipher Suites Supported	Info	57041
21.	SSL Root Certification Authority Certificate Information	Info	94761
22.	SSL/TLS Recommended Cipher Suites	Info	156899
23.	Service Detection	Info	22964
24.	TCP/IP Timestamps Supported	Info	25220
25.	TLS Version 1.1 Protocol Detection	Info	121010
26.	TLS Version 1.2 Protocol Detection	Info	136318
27.	Traceroute Information	Info	10287

REPORT

1. Vulnerability: TLS Version 1.0 Protocol Detection

Severity: Medium

Plugin: 104743

Port: HTTP 443

Description: This vulnerability indicates that the server supports the TLS 1.0 protocol, which is considered outdated and insecure due to known vulnerabilities.

Solution: Disable TLS 1.0 and upgrade to a more secure TLS version, such as TLS 1.2 or TLS 1.3.

Business Impact: Using TLS 1.0 poses a risk of data interception and exploitation, potentially leading to data breaches and loss of trust among users.

2. Vulnerability: TLS Version 1.1 Protocol Deprecated

Severity: Medium

Plugin: 157288

Port: 443

Description: TLS 1.1 is deprecated due to known vulnerabilities. This finding suggests that the server supports TLS 1.1.

Solution: Disable TLS 1.1 and upgrade to a more secure TLS version, such as TLS 1.2 or TLS 1.3.

Business Impact: Continuing to use TLS 1.1 increases the risk of security incidents and impacts the organization's reputation.

3. Vulnerability: SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Severity: Low

Plugin: 83875

Port: 443

Description: The server employs weak Diffie-Hellman key exchange, making it vulnerable to the Logjam attack.

Solution: Generate a strong Diffie-Hellman key with a key length greater than 1024 bits.

Business Impact: Weak key exchange may lead to eavesdropping and the compromise of sensitive data.

4. Vulnerability: ICMP Timestamp Request Remote Date Disclosure

Severity: Info

Plugin: 10114

Port: NA

Description: This vulnerability allows remote attackers to determine the system's time and date.

Solution: Disable or filter ICMP timestamp requests.

Business Impact: Attackers can use this information to plan coordinated attacks, impacting the organization's security.

5. Vulnerability: Additional DNS Hostnames

Severity: Info

Plugin: 46180

Port: NA

Description: Multiple DNS hostnames are associated with the target, which may indicate misconfigurations or multiple entry points.

Solution: Review DNS configurations and consolidate hostnames if necessary.

Business Impact: Misconfigured DNS records can lead to routing and security issues.

6. Vulnerability: Apache Tomcat Detection

Severity: Info

Plugin: 39446

Port: 8080

Description: The scan detected the presence of an Apache Tomcat web server.

Solution: Ensure the Apache Tomcat server is up to date and securely configured.

Business Impact: Unsecured Apache Tomcat servers may be exploited, leading to data breaches or service disruptions.

7. Vulnerability: Common Platform Enumeration (CPE)

Severity: Info

Plugin: 45590

Port: NA

Description: This identifies the Common Platform Enumeration (CPE) entries associated with the target.

Solution: Ensure the CPE entries are accurate and up to date.

Business Impact: Inaccurate CPE entries can affect system management and software inventory.

8. Vulnerability: Device Type

Severity: Info

Plugin: 54615

Port: NA

Description: The scan detects and categorizes the type of devices present.

Solution: Review device categorization for accuracy.

Business Impact: Accurate device classification aids in network management and security.

9. Vulnerability: HSTS Missing from HTTPS Server

Severity: Info

Plugin: 84502

Port: 443

Description: HTTP Strict Transport Security (HSTS) is not implemented on the HTTPS server.

Solution: Enable HSTS to enhance security by ensuring secure connections.

Business Impact: Without HSTS, users may be vulnerable to man-in-the-middle attacks.

10. Vulnerability: HTTP Server Type and Version

Severity: Info

Plugin: 10107

Port: 80

Description: The scan identifies the type and version of the HTTP server.

Solution: Review the server type and version for security updates.

Business Impact: Server type and version disclosure can be exploited to target known vulnerabilities.

11. Vulnerability: HyperText Transfer Protocol (HTTP) Information

Severity: Info

Plugin: 24260

Port: 80

Description: HTTP information is provided, which may include headers, methods, and other details about the HTTP service.

Solution: Ensure that HTTP headers and configurations align with security best practices.

Business Impact: Incorrect or insecure HTTP configurations may lead to security vulnerabilities and data exposure.

12. Vulnerability: Nessus SYN scanner

Severity: Info

Plugin: 11219

Port: NA

Description: Nessus employs SYN scanning to discover open ports on the target.

Solution: Ensure that SYN scanning is conducted responsibly and with appropriate permissions.

Business Impact: SYN scanning helps identify potential entry points for attacks, making it a valuable security tool.

13. Vulnerability: Nessus Scan Information

Severity: Info

Plugin: 19506

Port: NA

Description: Nessus provides information about the scan configuration and settings.

Solution: Review and adjust scan configurations to meet security objectives.

Business Impact: Proper scan configurations ensure comprehensive and accurate vulnerability assessments.

14. Vulnerability: OS Identification

Severity: Info

Plugin: 11936

Port: NA

Description: The scan identifies the target's operating system.

Solution: Validate the accuracy of the OS identification and take necessary security measures.

Business Impact: Accurate OS identification aids in security policy enforcement and patch management.

15. Vulnerability: SSL / TLS Versions Supported

Severity: Info

Plugin: 56984

Port: 443

Description: The scan identifies the SSL/TLS versions supported by the server.

Solution: Disable outdated and insecure SSL/TLS versions.

Business Impact: Supporting insecure SSL/TLS versions can lead to data exposure and breaches.

16. Vulnerability: SSL Certificate Information

Severity: Info

Plugin: 10863

Port: 443

Description: SSL certificate details, including expiration date and issuer, are provided.

Solution: Regularly update SSL certificates to maintain secure connections.

Business Impact: Expired or misconfigured certificates can lead to security warnings and disruptions.

17. Vulnerability: SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Severity: Info

Plugin: 95631

Port: 443

Description: The SSL certificate is signed using a weak hashing algorithm from a known certificate authority.

Solution: Obtain a new certificate signed with a stronger hashing algorithm.

Business Impact: Weakly signed certificates can be exploited, impacting the trustworthiness of secure connections.

18. Vulnerability: SSL Cipher Block Chaining Cipher Suites Supported

Severity: Info

Plugin: 70544

Port: 443

Description: The scan identifies SSL cipher suites that use Cipher Block Chaining (CBC).

Solution: Disable insecure CBC cipher suites and prioritize secure options.

Business Impact: Insecure cipher suites can lead to attacks like "Padding Oracle" and data leaks.

19. Vulnerability: SSL Cipher Suites Supported

Severity: Info

Plugin: 21643

Port: 443

Description: The scan lists the supported SSL cipher suites.

Solution: Disable insecure cipher suites and prioritize strong encryption.

Business Impact: Weak cipher suites can lead to data exposure and attacks.

20. Vulnerability: SSL Perfect Forward Secrecy Cipher Suites Supported

Severity: Info

Plugin: 57041

Port: 443

Description: The scan identifies SSL cipher suites that support Perfect Forward Secrecy (PFS).

Solution: Enable PFS cipher suites to enhance security.

Business Impact: PFS ensures that past communications remain secure even if encryption keys are compromised.

21. Vulnerability: SSL Root Certification Authority Certificate Information

Severity: Info

Plugin: 94761

Port: 443

Description: Information about the SSL root certification authority certificate is provided.

Solution: Ensure the root certificate is trusted and up to date.

Business Impact: Expired or untrusted root certificates can lead to security warnings.

22. Vulnerability: SSL/TLS Recommended Cipher Suites

Severity: Info

Plugin: 156899

Port: 443

Description: The scan provides information about recommended SSL/TLS cipher suites.

Solution: Configure the server to use recommended and secure cipher suites.

Business Impact: Properly configured cipher suites enhance data security.

23. Vulnerability: Service Detection

Severity: Info

Plugin: 22964

Port: NA

Description: The scan identifies the services and ports exposed by the target.

Solution: Review and secure exposed services and ports.

Business Impact: Accurate service detection is essential for security policy enforcement.

24. Vulnerability: TCP/IP Timestamps Supported

Severity: Info

Plugin: 25220

Port: NA

Description: The server supports TCP/IP timestamps.

Solution: Evaluate the necessity of TCP/IP timestamps and disable if not needed.

Business Impact: Enabling unnecessary timestamps can expose the system to certain attacks.

25. Vulnerability: TLS Version 1.1 Protocol Detection

Severity: Info

Plugin: 121010

Port: 443

Description: The scan detects the support for TLS 1.1 protocol.

Solution: Disable TLS 1.1 and upgrade to a more secure TLS version.

Business Impact: Continuing to support TLS 1.1 increases security risks and vulnerabilities.

26. Vulnerability: TLS Version 1.2 Protocol Detection

Severity: Info

Plugin: 136318

Port: NA

Description: The scan detects the support for TLS 1.2 protocol.

Solution: Maintain support for TLS 1.2, which is a secure protocol.

Business Impact: Supporting TLS 1.2 is a best practice for secure communication.

27. Vulnerability: Traceroute Information

Severity: Info

Plugin: 10287

Port: NA

Description: Traceroute information is provided, revealing the network path between the scanner and the target.

Solution: Ensure that sensitive network path information is not disclosed.

Business Impact: Disclosing network paths may expose infrastructure details, aiding potential attackers.

Target Website: www.vtop.vitbhopal.ac.in

Target IP Address 1: 182.73.197.23

List of Vulnerabilities:

S. No.	Vulnerability	Severity	Plugins
1.	Nessus SYN scanner	Info	11219
2.	Nessus Scan Information	Info	19506
3.	OS Identification Failed	Info	50350
4.	Open Port Re-check	Info	10919
5.	Service Detection	Info	22964
6.	Traceroute Information	Info	10287
7.	Web Server No 404 Error Code Check	Info	10386

REPORT

1. Vulnerability: Nessus SYN Scanner

Severity: Info

Plugin: 11219

Port: NA

Description: Detection of the use of the Nessus SYN scanner tool. This indicates that the scan is being conducted using Nessus's SYN scanning methodology.

Solution: No specific action is required for this detection as it is an indication of the scanning tool being used.

Business Impact: The Nessus SYN scanner is an essential tool for conducting network and vulnerability assessments. It is not a vulnerability, but a tool used for improving security.

2. Vulnerability: Nessus Scan Information

Severity: Info

Plugin: 19506

Port: NA

Description: Detection of general information related to the Nessus scan, such as scan settings, policy, and timestamps. This information is part of the scan report.

Solution: No specific action is required for this detection as it is a report of the scan information.

Business Impact: Nessus scan information is crucial for assessing the security posture of a network and identifying vulnerabilities.

3. Vulnerability: OS Identification Failed

Severity: Info

Plugin: 50350

Port: NA

Description: Detection that the scan failed to identify the target's operating system. This may indicate difficulty in accurately determining the OS.

Solution: Review and validate the OS identification results and consider alternative methods if OS identification is essential.

Business Impact: Accurate OS identification is important for maintaining and securing the target's infrastructure.

4. Vulnerability: Open Port Re-check

Severity: Info

Plugin: 10919

Port: NA

Description: Detection of a re-check for open ports. This indicates a secondary check for previously identified open ports to confirm their status.

Solution: No specific action is required for this detection as it is a part of the scan process.

Business Impact: Open port re-checks are a part of ensuring the accuracy of open port identification.

5. Vulnerability: Service Detection

Severity: Info

Plugin: 22964

Port: NA

Description: Detection of services running on the target system. This information helps identify the services available on the target.

Solution: No specific action is required for this detection as it is a part of the scan process.

Business Impact: Accurate service detection aids in network management and security.

6. Vulnerability: Traceroute Information

Severity: Info

Plugin: 10287

Port: NA

Description: Detection of traceroute information, which is used to identify the network path to the target. Traceroute helps understand the route that packets take between the source and destination.

Solution: No specific action is required for this detection as it is a part of the scan process.

Business Impact: Accurate traceroute information aids in network troubleshooting and management.

7. Vulnerability: Web Server No 404 Error Code Check

Severity: Info

Plugin: 10386

Port: 80

Description: Detection of a check for 404 error codes from the web server. This indicates that the scanner is assessing how the web server handles missing or nonexistent pages (404 errors).

Solution: Review and validate the handling of 404 errors on the web server. Ensure that sensitive information is not disclosed in error messages.

Business Impact: Proper handling of 404 errors is important for user experience and security, as it can prevent the disclosure of sensitive information.

Target Website: www.vtop.vitbhopal.ac.in

Target IP Address 2: 14.99.16.249

List of Vulnerabilities:

S. No.	Vulnerabilities	Severity	Plugins
1.	Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability	High	166906
2.	Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities	High	138591
3.	Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities	High	147164
4.	Apache Tomcat 9.0.0.M1 < 9.0.71	High	171657
5.	Apache Tomcat 9.0.13 < 9.0.63 vulnerability	High	160894
6.	Apache Tomcat 9.x < 9.0.40 Information Disclosure	High	144050
7.	Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability	Medium	151502
8.	Apache Tomcat 9.0.0.M1 < 9.0.80	Medium	180194
9.	Apache Tomcat 9.0.30 < 9.0.65 vulnerability	Medium	162498
10.	Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability	Medium	152182
11.	Apache Tomcat 9.0.0.M1 < 9.0.81 multiple vulnerabilities	Medium	182809
12.	Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up	Medium	141446
13.	Apache Tomcat 9.0.0.M1 < 9.0.72	Medium	173251

14.	Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations	Low	159464
15.	Apache Tomcat Detection	Info	39446
16.	Common Platform Enumeration (CPE)	Info	45590
17.	Host Fully Qualified Domain Name (FQDN) Resolution	Info	12053
18.	Inconsistent Hostname and IP Address	Info	46215
19.	Nessus SYN scanner	Info	11219
20.	Nessus Scan Information	Info	19506
21.	OS Identification Failed	Info	50350
22.	Open Port Re-check	Info	10919
23.	Patch Report	Info	66334
24.	Service Detection	Info	22964
25.	Traceroute Information	Info	10287
26.	Web Server No 404 Error Code Check	Info	10386

REPORT

1. Vulnerability: Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability

Severity: High

Plugin: 166906

Port: 8080

Description: Vulnerability in Apache Tomcat versions that can allow request smuggling attacks.

Solution: Update Apache Tomcat to a version that is not affected by this vulnerability.

Business Impact: Failure to address this vulnerability could lead to request smuggling attacks, potentially causing data manipulation or security breaches.

2. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities

Port: 8080

Severity: High

Plugin: 138591

Description: Detection of multiple vulnerabilities in the specified Apache Tomcat version range.

Solution: Upgrade Apache Tomcat to a version that addresses these vulnerabilities.

Business Impact: Failure to address these vulnerabilities can lead to various security risks, including potential data breaches.

3. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities

Severity: High

Plugin: 147164

Port: 8080

Description: Detection of multiple vulnerabilities in the specified Apache Tomcat version range.

Solution: Upgrade Apache Tomcat to a version that fixes these vulnerabilities.

Business Impact: Ignoring these vulnerabilities can expose the system to various security threats.

4. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.71

Severity: High

Plugin: 171657

Port: 8080

Description: Detection of the use of an Apache Tomcat version within the specified range.

Solution: Consider upgrading to a more recent, secure version of Apache Tomcat.

Business Impact: Using older versions of Apache Tomcat can expose systems to known vulnerabilities and security issues.

5. Vulnerability: Apache Tomcat 9.0.13 < 9.0.63 Vulnerability

Severity: High

Plugin: 160894

Port: 8080

Description: Detection of a vulnerability within the specified Apache Tomcat version range.

Solution: Update Apache Tomcat to a version that addresses this vulnerability.

Business Impact: Neglecting this vulnerability can result in potential security breaches and system compromise.

6. Vulnerability: Apache Tomcat 9.x < 9.0.40 Information Disclosure

Severity: High

Plugin: 144050

Port: 8080

Description: Detection of an information disclosure vulnerability in Apache Tomcat.

Solution: Update Apache Tomcat to a version that patches this vulnerability.

Business Impact: Exploiting this vulnerability can lead to unauthorized access to sensitive information, potentially causing data leaks.

7. Vulnerability: Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 Vulnerability

Severity: Medium

Plugin: 151502

Port: 8080

Description: Detection of vulnerabilities in specific versions of Apache Tomcat.

Solution: Upgrade Apache Tomcat to a version that addresses these vulnerabilities.

Business Impact: Neglecting these vulnerabilities can lead to security risks, including potential data breaches.

8. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.80

Severity: Medium

Plugin: 180194

Port: 8080

Description: Detection of the use of an Apache Tomcat version within the specified range.

Solution: Consider upgrading to a more recent, secure version of Apache Tomcat.

Business Impact: Using older versions of Apache Tomcat can expose systems to known vulnerabilities and security issues.

9. Vulnerability: Apache Tomcat 9.0.30 < 9.0.65 Vulnerability

Severity: Medium

Plugin: 162498

Port: 8080

Description: Detection of a vulnerability within the specified Apache Tomcat version range.

Solution: Update Apache Tomcat to a version that addresses this vulnerability.

Business Impact: Neglecting this vulnerability can result in potential security breaches and system compromise.

10. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.48 Vulnerability

Severity: Medium

Plugin: 152182

Port: 8080

Description: Detection of a vulnerability within the specified Apache Tomcat version range.

Solution: Update Apache Tomcat to a version that patches this vulnerability.

Business Impact: Exploiting this vulnerability can lead to unauthorized access to the system and potential data leaks.

11. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.81 Multiple Vulnerabilities

Severity: Medium

Plugin: 182809

Port: 8080

Description: Detection of multiple vulnerabilities in the specified Apache Tomcat version range.

Solution: Upgrade Apache Tomcat to a version that fixes these vulnerabilities.

Business Impact: Ignoring these vulnerabilities can expose the system to various security threats, including potential data breaches.

12. Vulnerability: Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up

Severity: Medium

Plugin: 141446

Port: 8080

Description: Detection of a vulnerability related to HTTP/2 request mix-up in specific Apache Tomcat versions.

Solution: Update Apache Tomcat to a version that addresses this vulnerability.

Business Impact: Exploiting this vulnerability can lead to unauthorized access and potential data manipulation.

13. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.72

Severity: Medium

Plugin: 173251

Port: 8080

Description: Detection of the use of an Apache Tomcat version within the specified range.

Solution: Consider upgrading to a more recent, secure version of Apache Tomcat.

Business Impact: Using older versions of Apache Tomcat can expose systems to known vulnerabilities and security issues.

14. Vulnerability: Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations

Severity: Low

Plugin: 159464

Port: 8080

Description: Detection of mitigations related to the Spring4Shell vulnerability (CVE-2022-22965) in specified Apache Tomcat versions.

Solution: Implement the necessary mitigations as recommended to protect against the Spring4Shell vulnerability.

Business Impact: Neglecting these mitigations can expose the system to the Spring4Shell vulnerability, potentially leading to unauthorized access and data breaches.

15. Vulnerability: Apache Tomcat Detection

Severity: Info

Plugin: 39446

Port: 8080

Description: Detection of an Apache Tomcat server, an open-source web application server.

Solution: Keep the Apache Tomcat server and its components updated to mitigate known vulnerabilities.

Business Impact: Running outdated Apache Tomcat versions can expose the system to security vulnerabilities and potential attacks.

16. Vulnerability: Common Platform Enumeration (CPE)

Severity: Info

Plugin: 45590

Port: NA

Description: Detection of Common Platform Enumeration (CPE) information related to the target.

Solution: Review and validate the CPE information for accuracy and relevance.

Business Impact: Accurate CPE information is essential for managing and securing the components of a system.

17. Vulnerability: Host Fully Qualified Domain Name (FQDN) Resolution

Severity: Info

Plugin: 12053

Port: NA

Description: Detection of the fully qualified domain name (FQDN) resolution for the target.

Solution: Review and validate the FQDN resolution for correctness.

Business Impact: Accurate FQDN resolution is crucial for system identification and security management.

18. Vulnerability: Inconsistent Hostname and IP Address

Severity: Info

Plugin: 46215

Port: NA

Description: Detection of inconsistencies between hostnames and IP addresses associated with the target.

Solution: Resolve inconsistencies to ensure accurate DNS configurations.

Business Impact: Inconsistent hostname and IP address configurations can lead to network and security issues.

19. Vulnerability: Nessus SYN Scanner

Severity: Info

Plugin: 11219

Port: NA

Description: Detection of the Nessus SYN scanner tool's use, indicating that the scanner is being used for the assessment.

Solution: No specific action is required for this detection as it is an indication of the scanning tool.

Business Impact: The Nessus SYN scanner is an important tool for network and vulnerability assessments, helping organizations identify and address security issues.

20. Vulnerability: Nessus Scan Information

Severity: Info

Plugin: 19506

Port: NA

Description: Detection of general information related to the Nessus scan, such as scan settings, policy, and timestamps.

Solution: No specific action is required for this detection as it is a reporting of the scan information.

Business Impact: Nessus scan information is important for assessing the security posture of a network and identifying vulnerabilities.

21. Vulnerability: OS Identification Failed

Severity: Info

Plugin: 50350

Port: NA

Description: Detection that the scan failed to identify the target's operating system. This may indicate difficulty in accurately determining the OS.

Solution: Review and validate the OS identification results and consider alternative methods if OS identification is essential.

Business Impact: Accurate OS identification is important for maintaining and securing the target's infrastructure.

22. Vulnerability: Open Port Re-check

Severity: Info

Plugin: 10919

Port: NA

Description: Detection of a re-check for open ports. This indicates a secondary check for previously identified open ports to confirm their status.

Solution: No specific action is required for this detection as it is a part of the scan process.

Business Impact: Open port re-checks are a part of ensuring the accuracy of open port identification.

23. Vulnerability: Patch Report

Severity: Info

Plugin: 66334

Port: NA

Description: Detection of patch report information, which may relate to the status of applied security patches.

Solution: Review the patch report information and take necessary actions to address any missing or critical patches.

Business Impact: Ensuring that systems have up-to-date patches is essential for mitigating known vulnerabilities and enhancing security.

24. Vulnerability: Service Detection

Severity: Info

Plugin: 22964

Port: NA

Description: Detection of services running on the target system. This information helps identify the services available on the target.

Solution: No specific action is required for this detection as it is a part of the scan process.

Business Impact: Accurate service detection aids in network management and security.

25. Vulnerability: Traceroute Information

Severity: Info

Plugin: 10287

Port: NA

Description: Detection of traceroute information, which is used to identify the network path to the target. Traceroute helps understand the route that packets take between the source and destination.

Solution: No specific action is required for this detection as it is a part of the scan process.

Business Impact: Accurate traceroute information aids in network troubleshooting and management.

26. Vulnerability: Web Server No 404 Error Code Check

Severity: Info

Plugin: 10386

Port: 80

Description: Detection of a check for 404 error codes from the web server. This indicates that the scanner is assessing how the web server handles missing or nonexistent pages (404 errors).

Solution: Review and validate the handling of 404 errors on the web server. Ensure that sensitive information is not disclosed in error messages.

Business Impact: Proper handling of 404 errors is important for user experience and security, as it can prevent the disclosure of sensitive information.