**Stage 2**

**Overview :-**

Nessus is a widely used and trusted vulnerability assessment tool that plays a critical role in ensuring the security of computer systems and networks. Developed by Tenable Network Security, Nessus provides organizations with the capability to identify and assess vulnerabilities in their IT infrastructure.

Nessus employs a client-server architecture and relies on a database of known vulnerabilities, which it uses to compare and analyze the configuration and behavior of the scanned systems. Here's a simplified breakdown of how Nessus works:

1. Preparation: The user configures Nessus by specifying the target hosts or IP addresses to scan, the type of scan (e.g., full scan, web application scan), and other relevant settings.
2. Scan Initiation: The Nessus server sends scan requests to the target hosts. It leverages various scanning techniques, such as port scanning, vulnerability scanning, and compliance checks, to gather information about the target systems.
3. Vulnerability Assessment: Nessus compares the collected data with its extensive database of known vulnerabilities and security checks. It identifies and categorizes vulnerabilities based on severity levels.
4. Reporting: After the scan is complete, Nessus generates comprehensive reports that highlight the vulnerabilities discovered during the scan. These reports include detailed information about each vulnerability, including its description, severity, and potential impact.
5. Remediation: Armed with the scan results, organizations can prioritize and address the identified vulnerabilities, applying patches, configuration changes, or other mitigation measures as needed.

**Target website ➖ https://www.tnpgndec.com/**

**Target ip address:- 104.248.232.212**

**List of vulnerability ➖**

|  |  |  |  |
| --- | --- | --- | --- |
| [**S.No**](http://s.no/) | **Vulnerability name** | **Severity** | **Plugins** |
| 1 | SSL Certificate Cannot Be Trusted | MEDIUM | [51192](https://www.tenable.com/plugins/nessus/51192) |
| 2 | web.config File Information Disclosure | MEDIUM | [121479](https://www.tenable.com/plugins/nessus/121479) |
| 3 | ICMP Timestamp Request Remote Date Disclosure | INFO | [10114](https://www.tenable.com/plugins/nessus/10114) |
| 4 | Additional DNS Hostnames | INFO | [46180](https://www.tenable.com/plugins/nessus/46180) |
| 5 | Common Platform Enumeration (CPE) | INFO | [45590](https://www.tenable.com/plugins/nessus/45590) |
| 6 | Device Type | INFO | [54615](https://www.tenable.com/plugins/nessus/54615) |
| 7 | HSTS Missing From HTTPS Server | INFO | [84502](https://www.tenable.com/plugins/nessus/84502) |
| 8 | HTTP Server Type and Version | INFO | [10107](https://www.tenable.com/plugins/nessus/10107) |
| 9 | HyperText Transfer Protocol (HTTP) Information | INFO | [24260](https://www.tenable.com/plugins/nessus/24260) |
| 10 | Nessus SYN scanner | INFO | [11219](https://www.tenable.com/plugins/nessus/11219) |
| 11 | Nessus Scan Information | INFO | [19506](https://www.tenable.com/plugins/nessus/19506) |
| 12 | OS Identification | INFO | [11936](https://www.tenable.com/plugins/nessus/11936) |
| 13 | OS Security Patch Assessment Not Available | INFO | [117886](https://www.tenable.com/plugins/nessus/117886) |
| 14 | SSH Algorithms and Languages Supported | INFO | [70657](https://www.tenable.com/plugins/nessus/70657) |
| 15 | SSH Password Authentication Accepted | INFO | [149334](https://www.tenable.com/plugins/nessus/149334) |
| 16 | SSH Protocol Versions Supported | INFO | [10881](https://www.tenable.com/plugins/nessus/10881) |
| 17 | SSH SHA-1 HMAC Algorithms Enabled | INFO | [153588](https://www.tenable.com/plugins/nessus/153588) |
| 18 | SSH Server Type and Version Information | INFO | [10267](https://www.tenable.com/plugins/nessus/10267) |
| 19 | SSL / TLS Versions Supported | INFO | [56984](https://www.tenable.com/plugins/nessus/56984) |
| 20 | SSL Certificate Information | INFO | [10863](https://www.tenable.com/plugins/nessus/10863) |
| 21 | SSL Certificate Signed Using Weak Hashing Algorithm (Known CA) | INFO | [95631](https://www.tenable.com/plugins/nessus/95631) |
| 22 | SSL Cipher Block Chaining Cipher Suites Supported | INFO | [70544](https://www.tenable.com/plugins/nessus/70544) |
| 23 | SSL Cipher Suites Supported | INFO | [21643](https://www.tenable.com/plugins/nessus/21643) |
| 24 | SSL Perfect Forward Secrecy Cipher Suites Supported | INFO | [57041](https://www.tenable.com/plugins/nessus/57041) |
| 25 | SSL Root Certification Authority Certificate Information | INFO | [94761](https://www.tenable.com/plugins/nessus/94761) |
| 26 | SSL/TLS Recommended Cipher Suites | INFO | [156899](https://www.tenable.com/plugins/nessus/156899) |
| 27 | Service Detection | INFO | [22964](https://www.tenable.com/plugins/nessus/22964) |
| 28 | TCP/IP Timestamps Supported | INFO | [25220](https://www.tenable.com/plugins/nessus/25220) |
| 29 | TLS Next Protocols Supported | INFO | [62564](https://www.tenable.com/plugins/nessus/62564) |
| 30 | TLS Version 1.2 Protocol Detection | INFO | [136318](https://www.tenable.com/plugins/nessus/136318) |
| 31 | Target Credential Status by Authentication Protocol - No Credentials Provided | INFO | [110723](https://www.tenable.com/plugins/nessus/110723) |
| 32 | Traceroute Information | INFO | [10287](https://www.tenable.com/plugins/nessus/10287) |
| 33 | Web Application Cookies Are Expired | INFO | [100669](https://www.tenable.com/plugins/nessus/100669) |
| 34 | Web Server No 404 Error Code Check | INFO | [10386](https://www.tenable.com/plugins/nessus/10386) |
| 35 | nginx HTTP Server Detection | INFO | [106375](https://www.tenable.com/plugins/nessus/106375) |

**REPORT:-**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **severity** | **Plugin ID** | **Port** | **Description** | **Solution** | **Risk** | **Business Impact** |
| HTTP Server Type and Version | Info | 10107 | 80 | This plugin attempts to determine the type and the version of the  remote web server. | n/a | None | Information Leakage |
| HTTP Server Type and Version | Info | 10107 | 443 | This plugin attempts to determine the type and the version of the  remote web server. | n/a | None | Information Leakage |
| ICMP Timestamp Request Remote Date Disclosure | Info | 10114 | 0 | The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.  Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time. | Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). | None | Information Leakage |
| SSH Server Type and Version Information | Info | 10267 | 22 | It is possible to obtain information about the remote SSH server by sending an empty authentication request. | n/a | None | Information Leakage |
| Traceroute Information | Info | 10287 | 0 | Makes a traceroute to the remote host. | n/a | None | Information Leakage |
| Web Server No 404 Error Code Check | Info | 10386 | 443 | The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.  Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. | n/a | None | Information Leakage |
| SSL Certificate Information | Info | 10863 | 443 | This plugin connects to every SSL-related port and attempts to  extract and dump the X.509 certificate. | n/a | None | Information Leakage |
| SSH Protocol Versions Supported | Info | 10881 | 22 | This plugin determines the versions of the SSH protocol supported by the remote SSH daemon. | n/a | None | Information Leakage |
| Nessus SYN scanner | Info | 11219 | 22 | 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. | Protect your target with an IP filter. | None | Information Leakage |
| Nessus SYN scanner | Info | 11219 | 80 | 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. | Protect your target with an IP filter. | None | Information Leakage |
| Nessus SYN scanner | Info | 11219 | 443 | 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. | Protect your target with an IP filter. | None | Information Leakage |
| OS Identification | Info | 11936 | 0 | 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 | None | Information Leakage |
| Nessus Scan Information | Info | 19506 | 0 | This plugin displays, for each tested host, information about the scan itself :   - The version of the plugin set.  - The type of scanner (Nessus or Nessus Home).  - The version of the Nessus Engine.  - The port scanner(s) used.  - The port range scanned.  - The ping round trip time   - Whether credentialed or third-party patch management  checks are possible.  - Whether the display of superseded patches is enabled  - The date of the scan.  - The duration of the scan.  - The number of hosts scanned in parallel.  - The number of checks done in parallel. | n/a | None | Information Leakage |
| SSL Cipher Suites Supported | Info | 21643 | 443 | This plugin detects which SSL ciphers are supported by the remote service for encrypting communications. | n/a | None | Information Leakage |
| Service Detection | Info | 22964 | 22 | 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 | None | Information Leakage |
| Service Detection | Info | 22964 | 80 | 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 | None | Information Leakage |
| Service Detection | Info | 22964 | 443 | 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 | None | Trust and Security Risk |
| Service Detection | Info | 22964 | 443 | 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 | None | Information Leakage |
| HyperText Transfer Protocol (HTTP) Information | Info | 24260 | 80 | This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...   This test is informational only and does not denote any security problem. | n/a | None | Information Leakage |
| HyperText Transfer Protocol (HTTP) Information | Info | 24260 | 443 | This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...   This test is informational only and does not denote any security problem. | n/a | None | Information Leakage |
| TCP/IP Timestamps Supported | Info | 25220 | 0 | The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed. | n/a | None | Information Leakage |
| Common Platform Enumeration (CPE) | Info | 45590 | 0 | 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 | None | Information Leakage |
| Additional DNS Hostnames | Info | 46180 | 0 | Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.  Different web servers may be hosted on name-based virtual hosts. | If you want to test them, re-scan using the special vhost syntax, such as :  www.example.com[192.0.32.10] | None | Information Leakage |
| SSL Certificate Cannot Be Trusted | Medium | 51192 | 443 | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the  server might not be descended from a known public  certificate authority. This can occur either when the  top of the chain is an unrecognized, self-signed  certificate, or when intermediate certificates are  missing that would connect the top of the certificate  chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate  that is not valid at the time of the scan. This can  occur either when the scan occurs before one of the  certificate's 'notBefore' dates, or after one of the  certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature  that either didn't match the certificate's information  or could not be verified. Bad signatures can be fixed by  getting the certificate with the bad signature to be  re-signed by its issuer. Signatures that could not be  verified are the result of the certificate's issuer  using a signing algorithm that Nessus either does not  support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and  identity of the web server. This could make it easier to carry out  man-in-the-middle attacks against the remote host. | Purchase or generate a proper SSL certificate for this service. | Medium | Security Enhancement Opportunity |
| Device Type | Info | 54615 | 0 | Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc). | n/a | None | Trust and Security Risk |
| SSL / TLS Versions Supported | Info | 56984 | 443 | This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications. | n/a | None | Trust and Security Risk |
| SSL Perfect Forward Secrecy Cipher Suites Supported | Info | 57041 | 443 | The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised. | n/a | None | User Experience Impact |
| TLS Next Protocols Supported | Info | 62564 | 443 | This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.  Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols. | n/a | None | Information Leakage |
| SSL Cipher Block Chaining Cipher Suites Supported | Info | 70544 | 443 | The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly. | n/a | None | Access Control Risk |
| SSH Algorithms and Languages Supported | Info | 70657 | 22 | This script detects which algorithms and languages are supported by the remote service for encrypting communications. | n/a | None | Security Assessment Limitation |
| HSTS Missing From HTTPS Server | Info | 84502 | 443 | The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS).  HSTS is an optional response header that can be configured on the server to instruct  the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. | Configure the remote web server to use HSTS. | None | Information Leakage |
| SSL Root Certification Authority Certificate Information | Info | 94761 | 443 | The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain. | Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies. | None | Information Leakage |
| SSL Certificate Signed Using Weak Hashing Algorithm (Known CA) | Info | 95631 | 443 | The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a  cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be  vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another  certificate with the same digital signature, allowing the attacker to masquerade as the affected service.  Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as  vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.  Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable  Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.  Known certificate authority root certificates are inherently trusted and so any potential issues with the signature,  including it being signed using a weak hashing algorithm, are not considered security issues. | Contact the Certificate Authority to have the certificate reissued. | None | Authentication Security Risk |
| Web Application Cookies Are Expired | Info | 100669 | 80 | The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser. | Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.  If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie. | None | Authentication Security Risk |
| Web Application Cookies Are Expired | Info | 100669 | 443 | The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser. | Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.  If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie. | None | Security Enhancement Opportunity |
| nginx HTTP Server Detection | Info | 106375 | 80 | Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host. | n/a | None | Vulnerability to Attacks |
| nginx HTTP Server Detection | Info | 106375 | 443 | Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host. | n/a | None | Data Theft, User Privacy Violation |
| Target Credential Status by Authentication Protocol - No Credentials Provided | Info | 110723 | 0 | Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.  Please note the following :  - This plugin reports per protocol, so it is possible for  valid credentials to be provided for one protocol and not  another. For example, authentication may succeed via SSH  but fail via SMB, while no credentials were provided for  an available SNMP service.  - Providing valid credentials for all available  authentication protocols may improve scan coverage, but  the value of successful authentication for a given  protocol may vary from target to target depending upon  what data (if any) is gathered from the target via that  protocol. For example, successful authentication via SSH  is more valuable for Linux targets than for Windows  targets, and likewise successful authentication via SMB  is more valuable for Windows targets than for Linux  targets. | n/a | None | Unauthorized Actions |
| OS Security Patch Assessment Not Available | Info | 117886 | 0 | OS Security Patch Assessment is not available on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.  This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin. | n/a | None | Resource Exhaustion, Service Disruption |
| web.config File Information Disclosure | Medium | 121479 | 443 | An information disclosure vulnerability exists in the remote web server due to the disclosure of the web.config file. An unauthenticated, remote attacker can exploit this, via a simple GET request, to disclose potentially sensitive configuration information. | Ensure proper restrictions are in place, or remove the web.config file if the file is not required. | Medium | Data Integrity Compromise, Fraud |
| TLS Version 1.2 Protocol Detection | Info | 136318 | 443 | The remote service accepts connections encrypted using TLS 1.2. | N/A | None | Unauthorized Access, Data Leakage |
| SSH Password Authentication Accepted | Info | 149334 | 22 | The SSH server on the remote host accepts password authentication. | n/a | None | Data Breach, Data Manipulation |
| SSH SHA-1 HMAC Algorithms Enabled | Info | 153588 | 22 | The remote SSH server is configured to enable SHA-1 HMAC algorithms.  Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.  Note that this plugin only checks for the options of the remote SSH server. | n/a | None | Service Disruption, Revenue Loss |
| SSL/TLS Recommended Cipher Suites | Info | 156899 | 443 | The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:  TLSv1.3:  - 0x13,0x01 TLS13\_AES\_128\_GCM\_SHA256  - 0x13,0x02 TLS13\_AES\_256\_GCM\_SHA384  - 0x13,0x03 TLS13\_CHACHA20\_POLY1305\_SHA256  TLSv1.2:  - 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256  - 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256  - 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384  - 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384  - 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305  - 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305  - 0x00,0x9E DHE-RSA-AES128-GCM-SHA256  - 0x00,0x9F DHE-RSA-AES256-GCM-SHA384  This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years. | Only enable support for recommened cipher suites. | None | Data Exposure, Unauthorized Access |