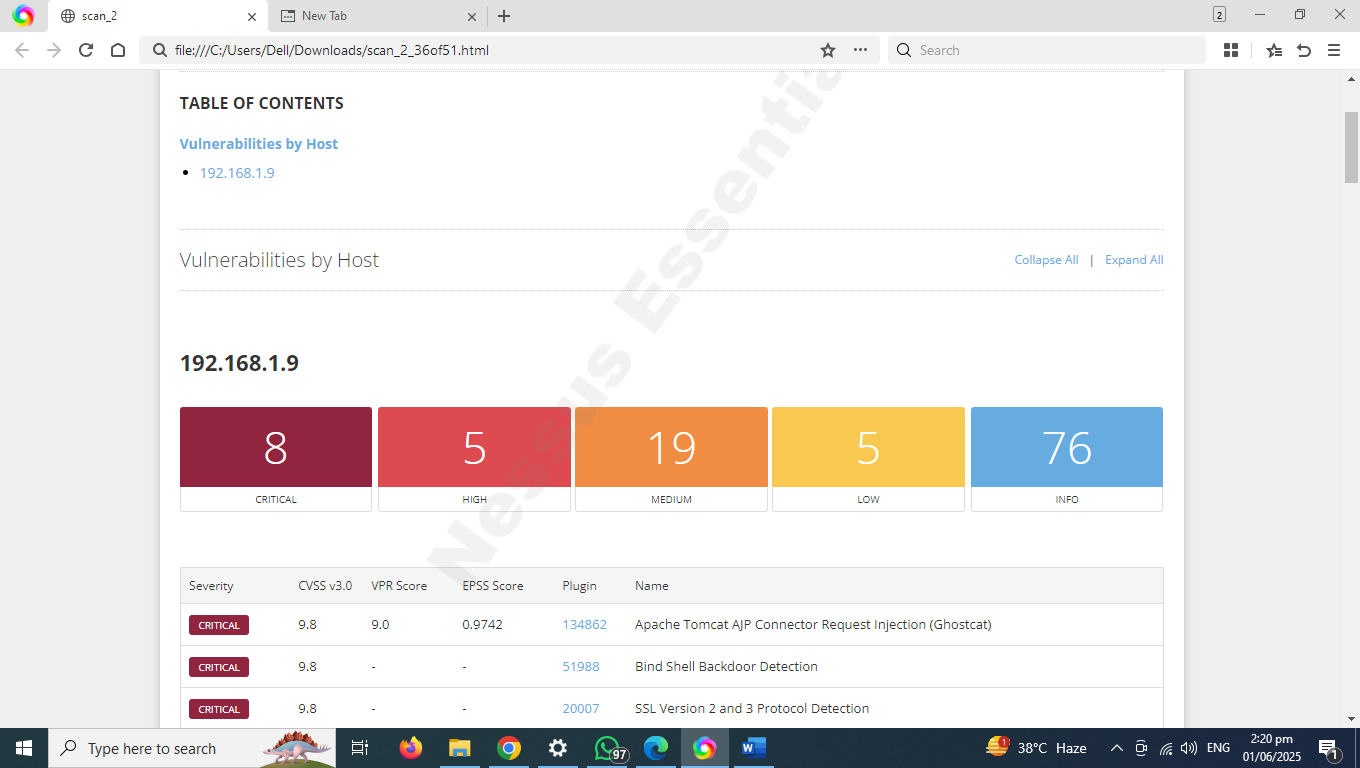
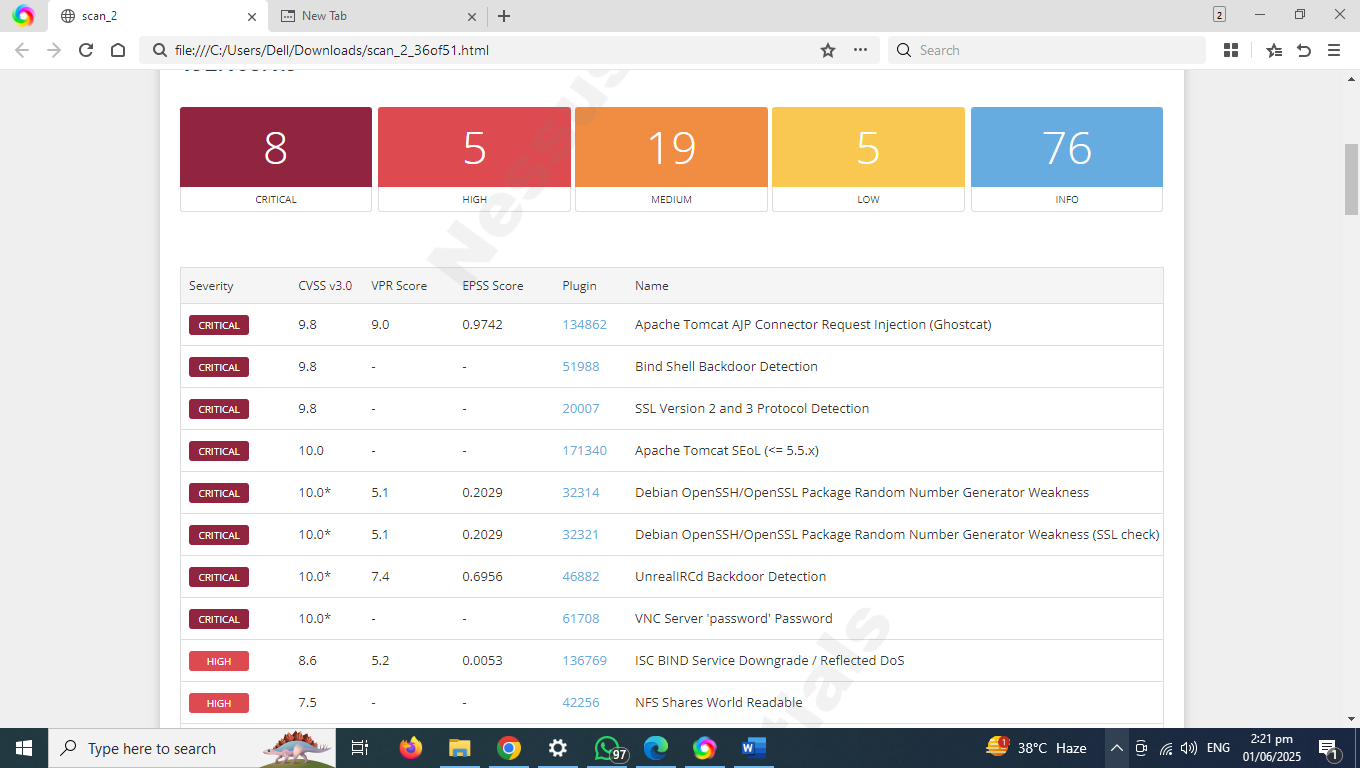
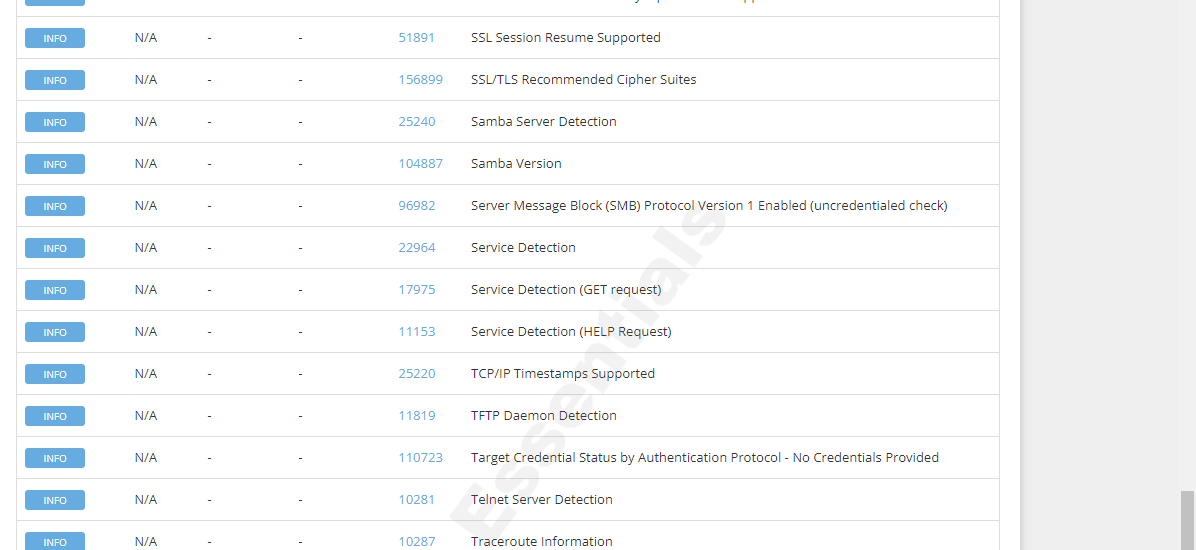
Full Vulnerability Scan









|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Severity |  | CVSS v3.0 |  | VPR Score |  | EPSS Score |  | Plugin | Name |
|  | CRITICAL |  | 9.8 |  | 9.0 |  | 0.9742 |  | [134862](https://www.tenable.com/plugins/nessus/134862) | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
|  | CRITICAL |  | 9.8 |  | - |  | - |  | [51988](https://www.tenable.com/plugins/nessus/51988) | Bind Shell Backdoor Detection |
|  | CRITICAL |  | 9.8 |  | - |  | - |  | [20007](https://www.tenable.com/plugins/nessus/20007) | SSL Version 2 and 3 Protocol Detection |
|  | CRITICAL |  | 10.0 |  | - |  | - |  | [171340](https://www.tenable.com/plugins/nessus/171340) | Apache Tomcat SEoL (<= 5.5.x) |
|  | CRITICAL |  | 10.0\* |  | 5.1 |  | 0.2029 |  | [32314](https://www.tenable.com/plugins/nessus/32314) | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
|  | CRITICAL |  | 10.0\* |  | 5.1 |  | 0.2029 |  | [32321](https://www.tenable.com/plugins/nessus/32321) | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
|  | CRITICAL |  | 10.0\* |  | 7.4 |  | 0.6956 |  | [46882](https://www.tenable.com/plugins/nessus/46882) | UnrealIRCd Backdoor Detection |
|  | CRITICAL |  | 10.0\* |  | - |  | - |  | [61708](https://www.tenable.com/plugins/nessus/61708) | VNC Server 'password' Password |
|  | HIGH |  | 8.6 |  | 5.2 |  | 0.0053 |  | [136769](https://www.tenable.com/plugins/nessus/136769) | ISC BIND Service Downgrade / Reflected DoS |
|  | HIGH |  | 7.5 |  | - |  | - |  | [42256](https://www.tenable.com/plugins/nessus/42256) | NFS Shares World Readable |
|  | HIGH |  | 7.5 |  | 5.1 |  | 0.0398 |  | [42873](https://www.tenable.com/plugins/nessus/42873) | SSL Medium Strength Cipher Suites Supported (SWEET32) |
|  | HIGH |  | 7.5 |  | 5.9 |  | 0.0489 |  | [90509](https://www.tenable.com/plugins/nessus/90509) | Samba Badlock Vulnerability |
|  | HIGH |  | 7.5\* |  | 7.4 |  | 0.015 |  | [10205](https://www.tenable.com/plugins/nessus/10205) | rlogin Service Detection |
|  | MEDIUM |  | 6.8 |  | 6.0 |  | 0.2471 |  | [33447](https://www.tenable.com/plugins/nessus/33447) | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning |
|  | MEDIUM |  | 6.5 |  | 4.4 |  | 0.004 |  | [139915](https://www.tenable.com/plugins/nessus/139915) | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS |
|  | MEDIUM |  | 6.5 |  | - |  | - |  | [51192](https://www.tenable.com/plugins/nessus/51192) | SSL Certificate Cannot Be Trusted |
|  | MEDIUM |  | 6.5 |  | - |  | - |  | [57582](https://www.tenable.com/plugins/nessus/57582) | SSL Self-Signed Certificate |
|  | MEDIUM |  | 6.5 |  | - |  | - |  | [104743](https://www.tenable.com/plugins/nessus/104743) | TLS Version 1.0 Protocol Detection |
|  | MEDIUM |  | 6.5 |  | - |  | - |  | [42263](https://www.tenable.com/plugins/nessus/42263) | Unencrypted Telnet Server |
|  | MEDIUM |  | 5.9 |  | 4.4 |  | 0.9728 |  | [136808](https://www.tenable.com/plugins/nessus/136808) | ISC BIND Denial of Service |
|  | MEDIUM |  | 5.9 |  | 4.4 |  | 0.003 |  | [31705](https://www.tenable.com/plugins/nessus/31705) | SSL Anonymous Cipher Suites Supported |
|  | MEDIUM |  | 5.9 |  | 3.6 |  | 0.935 |  | [89058](https://www.tenable.com/plugins/nessus/89058) | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
|  | MEDIUM |  | 5.9 |  | 4.4 |  | 0.0079 |  | [65821](https://www.tenable.com/plugins/nessus/65821) | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
|  | MEDIUM |  | 5.3 |  | - |  | - |  | [12085](https://www.tenable.com/plugins/nessus/12085) | Apache Tomcat Default Files |
|  | MEDIUM |  | 5.3 |  | - |  | - |  | [12217](https://www.tenable.com/plugins/nessus/12217) | DNS Server Cache Snooping Remote Information Disclosure |
|  | MEDIUM |  | 5.3 |  | 4.0 |  | 0.0225 |  | [11213](https://www.tenable.com/plugins/nessus/11213) | HTTP TRACE / TRACK Methods Allowed |
|  | MEDIUM |  | 5.3 |  | - |  | - |  | [57608](https://www.tenable.com/plugins/nessus/57608) | SMB Signing not required |
|  | MEDIUM |  | 5.3 |  | - |  | - |  | [15901](https://www.tenable.com/plugins/nessus/15901) | SSL Certificate Expiry |
|  | MEDIUM |  | 5.3 |  | - |  | - |  | [45411](https://www.tenable.com/plugins/nessus/45411) | SSL Certificate with Wrong Hostname |
|  | MEDIUM |  | 5.3 |  | - |  | - |  | [26928](https://www.tenable.com/plugins/nessus/26928) | SSL Weak Cipher Suites Supported |
|  | MEDIUM |  | 4.0\* |  | 7.3 |  | 0.0135 |  | [52611](https://www.tenable.com/plugins/nessus/52611) | SMTP Service STARTTLS Plaintext Command Injection |
|  | MEDIUM |  | 4.3\* |  | 3.7 |  | 0.9488 |  | [81606](https://www.tenable.com/plugins/nessus/81606) | SSL/TLS EXPORT\_RSA <= 512-bit Cipher Suites Supported (FREAK) |
|  | LOW |  | 3.7 |  | 4.5 |  | 0.9698 |  | [83875](https://www.tenable.com/plugins/nessus/83875) | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) |
|  | LOW |  | 3.7 |  | 4.5 |  | 0.9698 |  | [83738](https://www.tenable.com/plugins/nessus/83738) | SSL/TLS EXPORT\_DHE <= 512-bit Export Cipher Suites Supported (Logjam) |
|  | LOW |  | 3.4 |  | 5.1 |  | 0.9746 |  | [78479](https://www.tenable.com/plugins/nessus/78479) | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
|  | LOW |  | 2.1\* |  | 2.2 |  | 0.8939 |  | [10114](https://www.tenable.com/plugins/nessus/10114) | ICMP Timestamp Request Remote Date Disclosure |
|  | LOW |  | 2.6\* |  | - |  | - |  | [10407](https://www.tenable.com/plugins/nessus/10407) | X Server Detection |
|  | INFO |  | N/A |  | - |  | - |  | [10223](https://www.tenable.com/plugins/nessus/10223) | RPC portmapper Service Detection |
|  | INFO |  | N/A |  | - |  | - |  | [21186](https://www.tenable.com/plugins/nessus/21186) | AJP Connector Detection |
|  | INFO |  | N/A |  | - |  | - |  | [18261](https://www.tenable.com/plugins/nessus/18261) | Apache Banner Linux Distribution Disclosure |
|  | INFO |  | N/A |  | - |  | - |  | [48204](https://www.tenable.com/plugins/nessus/48204) | Apache HTTP Server Version |
|  | INFO |  | N/A |  | - |  | - |  | [39446](https://www.tenable.com/plugins/nessus/39446) | Apache Tomcat Detection |
|  | INFO |  | N/A |  | - |  | - |  | [84574](https://www.tenable.com/plugins/nessus/84574) | Backported Security Patch Detection (PHP) |
|  | INFO |  | N/A |  | - |  | - |  | [39520](https://www.tenable.com/plugins/nessus/39520) | Backported Security Patch Detection (SSH) |
|  | INFO |  | N/A |  | - |  | - |  | [39521](https://www.tenable.com/plugins/nessus/39521) | Backported Security Patch Detection (WWW) |
|  | INFO |  | N/A |  | - |  | - |  | [45590](https://www.tenable.com/plugins/nessus/45590) | Common Platform Enumeration (CPE) |
|  | INFO |  | N/A |  | - |  | - |  | [10028](https://www.tenable.com/plugins/nessus/10028) | DNS Server BIND version Directive Remote Version Detection |
|  | INFO |  | N/A |  | - |  | - |  | [35373](https://www.tenable.com/plugins/nessus/35373) | DNS Server DNSSEC Aware Resolver |
|  | INFO |  | N/A |  | - |  | - |  | [11002](https://www.tenable.com/plugins/nessus/11002) | DNS Server Detection |
|  | INFO |  | N/A |  | - |  | - |  | [72779](https://www.tenable.com/plugins/nessus/72779) | DNS Server Version Detection |
|  | INFO |  | N/A |  | - |  | - |  | [35371](https://www.tenable.com/plugins/nessus/35371) | DNS Server hostname.bind Map Hostname Disclosure |
|  | INFO |  | N/A |  | - |  | - |  | [54615](https://www.tenable.com/plugins/nessus/54615) | Device Type |
|  | INFO |  | N/A |  | - |  | - |  | [35716](https://www.tenable.com/plugins/nessus/35716) | Ethernet Card Manufacturer Detection |
|  | INFO |  | N/A |  | - |  | - |  | [86420](https://www.tenable.com/plugins/nessus/86420) | Ethernet MAC Addresses |
|  | INFO |  | N/A |  | - |  | - |  | [10092](https://www.tenable.com/plugins/nessus/10092) | FTP Server Detection |
|  | INFO |  | N/A |  | - |  | - |  | [10107](https://www.tenable.com/plugins/nessus/10107) | HTTP Server Type and Version |
|  | INFO |  | N/A |  | - |  | - |  | [24260](https://www.tenable.com/plugins/nessus/24260) | HyperText Transfer Protocol (HTTP) Information |
|  | INFO |  | N/A |  | - |  | - |  | [11156](https://www.tenable.com/plugins/nessus/11156) | IRC Daemon Version Detection |
|  | INFO |  | N/A |  | - |  | - |  | [10397](https://www.tenable.com/plugins/nessus/10397) | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure |
|  | INFO |  | N/A |  | - |  | - |  | [10785](https://www.tenable.com/plugins/nessus/10785) | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
|  | INFO |  | N/A |  | - |  | - |  | [11011](https://www.tenable.com/plugins/nessus/11011) | Microsoft Windows SMB Service Detection |
|  | INFO |  | N/A |  | - |  | - |  | [100871](https://www.tenable.com/plugins/nessus/100871) | Microsoft Windows SMB Versions Supported (remote check) |
|  | INFO |  | N/A |  | - |  | - |  | [106716](https://www.tenable.com/plugins/nessus/106716) | Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) |
|  | INFO |  | N/A |  | - |  | - |  | [10719](https://www.tenable.com/plugins/nessus/10719) | MySQL Server Detection |
|  | INFO |  | N/A |  | - |  | - |  | [10437](https://www.tenable.com/plugins/nessus/10437) | NFS Share Export List |
|  | INFO |  | N/A |  | - |  | - |  | [11219](https://www.tenable.com/plugins/nessus/11219) | Nessus SYN scanner |
|  | INFO |  | N/A |  | - |  | - |  | [19506](https://www.tenable.com/plugins/nessus/19506) | Nessus Scan Information |
|  | INFO |  | N/A |  | - |  | - |  | [11936](https://www.tenable.com/plugins/nessus/11936) | OS Identification |
|  | INFO |  | N/A |  | - |  | - |  | [117886](https://www.tenable.com/plugins/nessus/117886) | OS Security Patch Assessment Not Available |
|  | INFO |  | N/A |  | - |  | - |  | [181418](https://www.tenable.com/plugins/nessus/181418) | OpenSSH Detection |
|  | INFO |  | N/A |  | - |  | - |  | [50845](https://www.tenable.com/plugins/nessus/50845) | OpenSSL Detection |
|  | INFO |  | N/A |  | - |  | - |  | [48243](https://www.tenable.com/plugins/nessus/48243) | PHP Version Detection |
|  | INFO |  | N/A |  | - |  | - |  | [66334](https://www.tenable.com/plugins/nessus/66334) | Patch Report |
|  | INFO |  | N/A |  | - |  | - |  | [118224](https://www.tenable.com/plugins/nessus/118224) | PostgreSQL STARTTLS Support |
|  | INFO |  | N/A |  | - |  | - |  | [26024](https://www.tenable.com/plugins/nessus/26024) | PostgreSQL Server Detection |
|  | INFO |  | N/A |  | - |  | - |  | [22227](https://www.tenable.com/plugins/nessus/22227) | RMI Registry Detection |
|  | INFO |  | N/A |  | - |  | - |  | [11111](https://www.tenable.com/plugins/nessus/11111) | RPC Services Enumeration |
|  | INFO |  | N/A |  | - |  | - |  | [53335](https://www.tenable.com/plugins/nessus/53335) | RPC portmapper (TCP) |
|  | INFO |  | N/A |  | - |  | - |  | [10263](https://www.tenable.com/plugins/nessus/10263) | SMTP Server Detection |
|  | INFO |  | N/A |  | - |  | - |  | [42088](https://www.tenable.com/plugins/nessus/42088) | SMTP Service STARTTLS Command Support |
|  | INFO |  | N/A |  | - |  | - |  | [149334](https://www.tenable.com/plugins/nessus/149334) | SSH Password Authentication Accepted |
|  | INFO |  | N/A |  | - |  | - |  | [10881](https://www.tenable.com/plugins/nessus/10881) | SSH Protocol Versions Supported |
|  | INFO |  | N/A |  | - |  | - |  | [10267](https://www.tenable.com/plugins/nessus/10267) | SSH Server Type and Version Information |
|  | INFO |  | N/A |  | - |  | - |  | [56984](https://www.tenable.com/plugins/nessus/56984) | SSL / TLS Versions Supported |
|  | INFO |  | N/A |  | - |  | - |  | [45410](https://www.tenable.com/plugins/nessus/45410) | SSL Certificate 'commonName' Mismatch |
|  | INFO |  | N/A |  | - |  | - |  | [10863](https://www.tenable.com/plugins/nessus/10863) | SSL Certificate Information |
|  | INFO |  | N/A |  | - |  | - |  | [70544](https://www.tenable.com/plugins/nessus/70544) | SSL Cipher Block Chaining Cipher Suites Supported |
|  | INFO |  | N/A |  | - |  | - |  | [21643](https://www.tenable.com/plugins/nessus/21643) | SSL Cipher Suites Supported |
|  | INFO |  | N/A |  | - |  | - |  | [62563](https://www.tenable.com/plugins/nessus/62563) | SSL Compression Methods Supported |
|  | INFO |  | N/A |  | - |  | - |  | [57041](https://www.tenable.com/plugins/nessus/57041) | SSL Perfect Forward Secrecy Cipher Suites Supported |
|  | INFO |  | N/A |  | - |  | - |  | [51891](https://www.tenable.com/plugins/nessus/51891) | SSL Session Resume Supported |
|  | INFO |  | N/A |  | - |  | - |  | [156899](https://www.tenable.com/plugins/nessus/156899) | SSL/TLS Recommended Cipher Suites |
|  | INFO |  | N/A |  | - |  | - |  | [25240](https://www.tenable.com/plugins/nessus/25240) | Samba Server Detection |
|  | INFO |  | N/A |  | - |  | - |  | [104887](https://www.tenable.com/plugins/nessus/104887) | Samba Version |
|  | INFO |  | N/A |  | - |  | - |  | [96982](https://www.tenable.com/plugins/nessus/96982) | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) |
|  | INFO |  | N/A |  | - |  | - |  | [22964](https://www.tenable.com/plugins/nessus/22964) | Service Detection |
|  | INFO |  | N/A |  | - |  | - |  | [17975](https://www.tenable.com/plugins/nessus/17975) | Service Detection (GET request) |
|  | INFO |  | N/A |  | - |  | - |  | [11153](https://www.tenable.com/plugins/nessus/11153) | Service Detection (HELP Request) |
|  | INFO |  | N/A |  | - |  | - |  | [25220](https://www.tenable.com/plugins/nessus/25220) | TCP/IP Timestamps Supported |
|  | INFO |  | N/A |  | - |  | - |  | [11819](https://www.tenable.com/plugins/nessus/11819) | TFTP Daemon Detection |
|  | INFO |  | N/A |  | - |  | - |  | [110723](https://www.tenable.com/plugins/nessus/110723) | Target Credential Status by Authentication Protocol - No Credentials Provided |
|  | INFO |  | N/A |  | - |  | - |  | [10281](https://www.tenable.com/plugins/nessus/10281) | Telnet Server Detection |
|  | INFO |  | N/A |  | - |  | - |  | [10287](https://www.tenable.com/plugins/nessus/10287) | Traceroute Information |
|  | INFO |  | N/A |  | - |  | - |  | [11154](https://www.tenable.com/plugins/nessus/11154) | Unknown Service Detection: Banner Retrieval |
|  | INFO |  | N/A |  | - |  | - |  | [19288](https://www.tenable.com/plugins/nessus/19288) | VNC Server Security Type Detection |
|  | INFO |  | N/A |  | - |  | - |  | [65792](https://www.tenable.com/plugins/nessus/65792) | VNC Server Unencrypted Communication Detection |
|  | INFO |  | N/A |  | - |  | - |  | [10342](https://www.tenable.com/plugins/nessus/10342) | VNC Software Detection |
|  | INFO |  | N/A |  | - |  | - |  | [135860](https://www.tenable.com/plugins/nessus/135860) | WMI Not Available |
|  | INFO |  | N/A |  | - |  | - |  | [20108](https://www.tenable.com/plugins/nessus/20108) | Web Server / Application favicon.ico Vendor Fingerprinting |
|  | INFO |  | N/A |  | - |  | - |  | [11422](https://www.tenable.com/plugins/nessus/11422) | Web Server Unconfigured - Default Install Page Present |
|  | INFO |  | N/A |  | - |  | - |  | [11424](https://www.tenable.com/plugins/nessus/11424) | WebDAV Detection |
|  | INFO |  | N/A |  | - |  | - |  | [10150](https://www.tenable.com/plugins/nessus/10150) | Windows NetBIOS / SMB Remote Host Information Disclosure |
|  | INFO |  | N/A |  | - |  | - |  | [52703](https://www.tenable.com/plugins/nessus/52703) | vsftpd Detection |

**Document the Most Critical Vulnerabilities**

Below are the most critical open ports and services found, with their associated risks and simple fixes/mitigations:

**1. Telnet (Port 23) – High Risk**

**Vulnerability:**  
Telnet transmits all data in plaintext, including usernames and passwords. Easily intercepted with packet sniffers.

**Fix / Mitigation:**

* Disable Telnet service.
* Use SSH (Port 22) for secure remote access instead.
* Block port 23 at firewall level.

**2. HTTP (Port 80) – High Risk**

**Vulnerability:**  
HTTP does not encrypt data, which can lead to:

* Credential theft
* Session hijacking
* Man-in-the-middle attacks

**Fix / Mitigation:**

* Redirect all HTTP traffic to HTTPS (Port 443).
* Use a valid SSL/TLS certificate (e.g., Let’s Encrypt).
* Use modern protocols (TLS 1.2 or 1.3).

**3. DNS (Port 53) – Medium Risk**

**Vulnerability:**

* Can be abused for DNS tunneling (data exfiltration).
* May be misconfigured (open recursion, zone transfer).

**Fix / Mitigation:**

* Restrict DNS service to internal IPs only.
* Use DNSSEC to secure domain resolutions.
* Disable open recursive DNS if not required.

**4. SSH (Port 22) – Medium Risk if Weak Auth**

**Vulnerability:**

* Can be brute-forced if using password authentication.
* Attackers target SSH via automated scripts.

**Fix / Mitigation:**

* Disable password authentication.
* Use key-based SSH login.
* Use tools like Fail2ban or a firewall to limit login attempts.
* Change the default SSH port.

**5. HTTPS (Port 443) – Low Risk**

**Vulnerability:**

* Low if configured correctly, but weak/old SSL protocols (like SSLv2/3, TLS 1.0) can be exploited.

**Fix / Mitigation:**

* Enforce TLS 1.2 or TLS 1.3 only.
* Disable weak ciphers and SSLv2/v3.
* Periodically scan with SSL Labs to verify configuration.