

Version 10.3.0-debian9\_amd64

METASPLOITABLE

**IN QUESTO REPORT ELENCHEREMO LE VULNERABILITA’ SCANSIONATE E LE LORO REMEDIATION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **192.168.50.101** | | | | |
| 8 | 5 | 16 | 5 | 74 |

CRITICAL HIGH MEDIUM LOW INFO

Vulnerabilities Total: 108

|  |  |  |
| --- | --- | --- |
| **SEVERITY** | **CVSS V3.0** | **NAME** |
|  |  |  |
| CRITICAL | 9.8 | Apache Tomcat A JP Connector Request Injection (Ghostcat) |
|  |  |  |
|  |  |  |
| CRITICAL | 9.8 | Bind Shell Backdoor Detection |
|  |  |  |
|  |  |  |
| CRITICAL | 9.8 | SSL Version 2 and 3 Protocol Detection |
|  |  |  |
|  |  |  |
| CRITICAL | 10.0 | Unix Operating System Unsupported Version Detection |
|  |  |  |
|  |  |  |
| CRITICAL | 10.0\* | Debian OpenSSH/OpenSSL Package Random Number Generator |
|  |  | Weakness |
|  |  |  |
| CRITICAL | 10.0\* | Debian OpenSSH/OpenSSL Package Random Number Generator |
|  |  | Weakness (SSL check) |
|  |  |  |
| CRITICAL | 10.0\* | NFS Exported Share Information Disclosure |
|  |  |  |
|  |  |  |
| CRITICAL | 10.0\* | VNC Server 'password' Password |
|  |  |  |
|  |  |  |
| HIGH | 8.6 | ISC BIND Service Downgrade / Reflected DoS |
|  |  |  |
|  |  |  |
| HIGH | 7.5 | ISC BIND Denial of Service |
|  |  |  |
|  |  |  |
| HIGH | 7.5 | NFS Shares World Readable |
|  |  |  |
|  |  |  |
| HIGH | 7.5 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
|  |  |  |
|  |  |  |
| HIGH | 7.5 | Samba Badlock Vulnerability |
|  |  |  |
|  |  |  |
| MEDIUM | 6.8 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability |
|  |  | (POODLE) |
|  |  |  |
| MEDIUM | 6.5 | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS |
|  |  |  |
|  |  |  |
| MEDIUM | 6.5 | SSL Certificate Cannot Be Trusted |
|  |  |  |
|  |  |  |
| MEDIUM | 6.5 | SSL Self-Signed Certificate |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MEDIUM | | 6.5 | [104743](http://www.nessus.org/plugins/index.php?view=single&id=104743) | TLS Version 1.0 Protocol Detection |
| MEDIUM | | 5.9 | [31705](http://www.nessus.org/plugins/index.php?view=single&id=31705) | SSL Anonymous Cipher Suites Supported |
|  | |  |  |  |
| MEDIUM | | 5.9 | [89058](http://www.nessus.org/plugins/index.php?view=single&id=89058) | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| MEDIUM | | 5.9 | [65821](http://www.nessus.org/plugins/index.php?view=single&id=65821) | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
|  | |  |  |  |
|  | MEDIUM | 5.3 | [11213](http://www.nessus.org/plugins/index.php?view=single&id=11213) | HTTP TRACE / TRACK Methods Allowed |
|  | MEDIUM | 5.3 | [57608](http://www.nessus.org/plugins/index.php?view=single&id=57608) | SMB Signing not required |
|  | MEDIUM | 5.3 | [15901](http://www.nessus.org/plugins/index.php?view=single&id=15901) | SSL Certificate Expiry |
|  | MEDIUM | 5.3 | [45411](http://www.nessus.org/plugins/index.php?view=single&id=45411) | SSL Certificate with Wrong Hostname |
|  | | | | |
|  | MEDIUM | 5.3 | [26928](http://www.nessus.org/plugins/index.php?view=single&id=26928) | SSL Weak Cipher Suites Supported |
|  |  |  |  |  |
|  | MEDIUM | 4.0\* | [52611](http://www.nessus.org/plugins/index.php?view=single&id=52611) | SMTP Service STARTTLS Plaintext Command Injection |
|  |  |  |  |  |
|  | MEDIUM | 4.3\* | [90317](http://www.nessus.org/plugins/index.php?view=single&id=90317) | SSH Weak Algorithms Supported |
|  |  |  |  |  |
|  | MEDIUM | 4.3\* | [81606](http://www.nessus.org/plugins/index.php?view=single&id=81606) | SSL/TLS EXPORT\_RSA <= 512-bit Cipher Suites Supported (FREAK) |
|  |  |  |  |  |

\* indicates the v3.0 score was not available; the v2.0 score is shown

# 



VULNERABILITA’ CRITICHE

|  |  |
| --- | --- |
| Bind Shell Backdoor Detection | Una shell sta ascoltando sulla porta remota senza alcuna autenticazione richiesta. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi. |
| VNC Server 'password' Password | Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di 'password'. Un attaccante remoto e non autenticato potrebbe sfruttarlo per prendere il controllo del sistema. |

Sono state scelte due vulnerabilità tra le più critiche descritte nella seguente tabella in cui si procederà alla risoluzione delle seguenti falle:

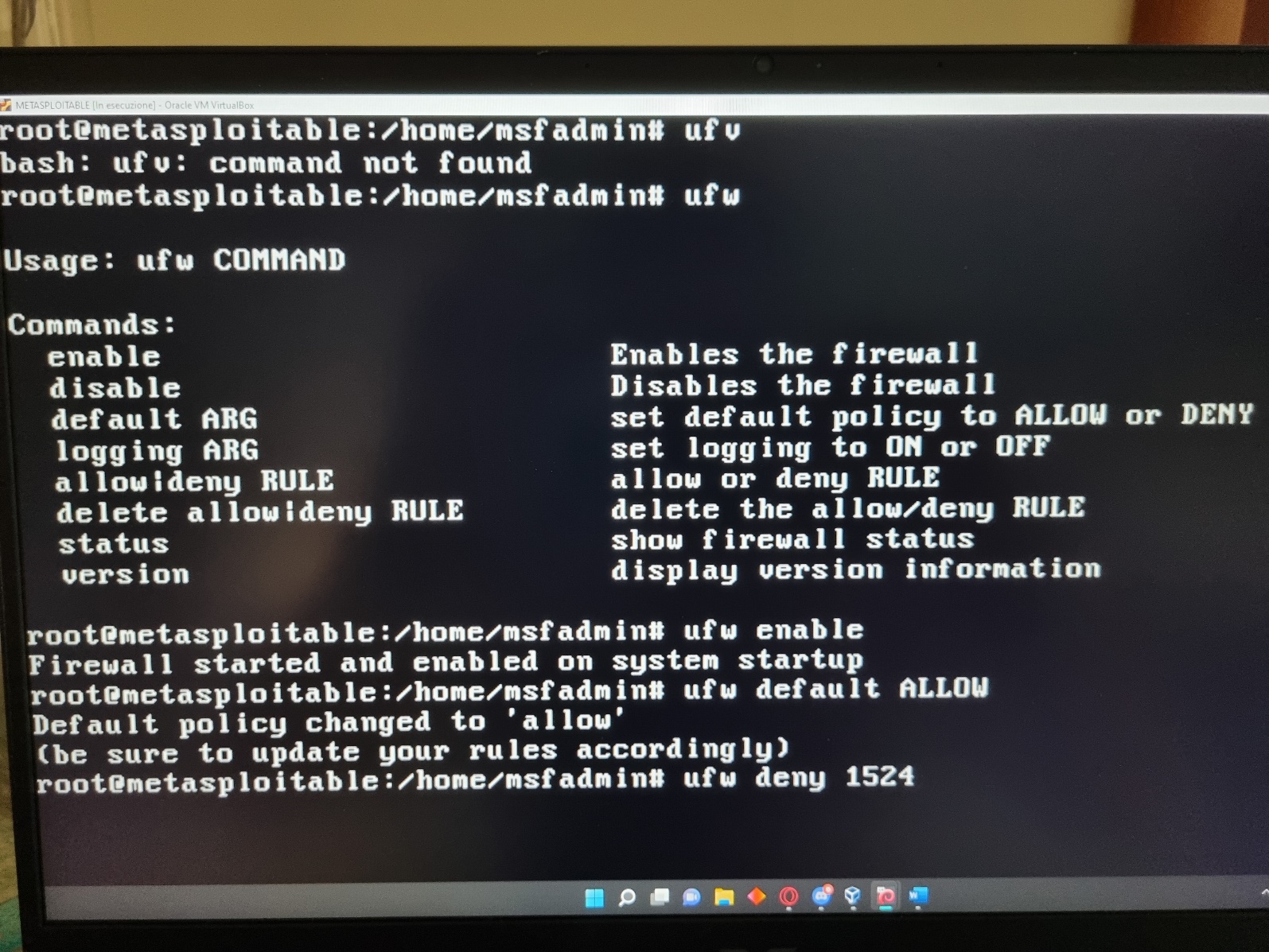
Le soluzioni per le vulnerabilità elencati sono le seguenti:

VNC Server 'password' Password : Mettere in sicurezza il servizio VNC con una password più efficace e complessa.

Bind Shell Backdoor Detection: Verificare se l’host remote è stato compromesso e reinstalla il Sistema se necessario.

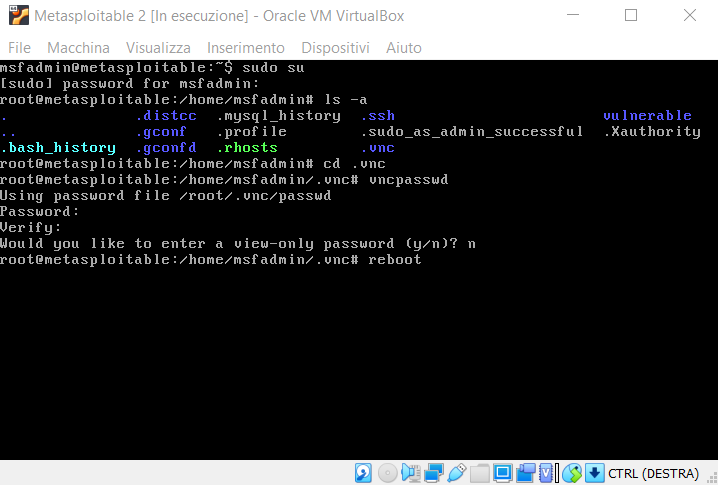
REMEDIATION

RIMEDIO VULNERABILITA’

Bind Shell Backdoor Detection

E’ stata risolta la vulnerabilità di sicurezza della backdoor

Tramite configurazione firewall negando la connessione alla porta 1524 ovvero chiudendola.



VNC Server 'password' Password.

La vulnerabilità di tale processo è stata rimediata impostando una password di sola lettura oltre ad essere stata cambiata con un’altra più sofisticata

REPORT SCAN DOPO REMEDIATION VULNERABILITA’

Da come si evince dal report post remediation, le vulnerabilità sono state sistemate.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **192.168.1.9** | | | | |
| 9 | 7 | 19 | 5 | 77 |

CRITICAL HIGH MEDIUM LOW INFO

Vulnerabilities Total: 119

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **SEVERITY** | **CVSS V3.0** | **PLUGIN** | **NAME** |
|  |  |  |  |  |
|  | CRITICAL | 9.8 | [134862](http://www.nessus.org/plugins/index.php?view=single&id=134862) | Apache Tomcat A JP Connector Request Injection (Ghostcat) |
|  |  |  |  |  |
|  |  |  |  |  |
|  | CRITICAL | 9.8 | [20007](http://www.nessus.org/plugins/index.php?view=single&id=20007) | SSL Version 2 and 3 Protocol Detection |
|  |  |  |  |  |
|  |  |  |  |  |
|  | CRITICAL | 9.1 | [33447](http://www.nessus.org/plugins/index.php?view=single&id=33447) | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning |
|  |  |  |  |  |
|  |  |  |  |  |
|  | CRITICAL | 10.0 | [33850](http://www.nessus.org/plugins/index.php?view=single&id=33850) | Unix Operating System Unsupported Version Detection |
|  |  |  |  |  |
|  |  |  |  |  |
|  | CRITICAL | 10.0 | [34460](http://www.nessus.org/plugins/index.php?view=single&id=34460) | Unsupported Web Server Detection |
|  |  |  |  |  |
|  |  |  |  |  |
|  | CRITICAL | 10.0\* | [32314](http://www.nessus.org/plugins/index.php?view=single&id=32314) | Debian OpenSSH/OpenSSL Package Random Number Generator |
|  |  |  |  | Weakness |
|  |  |  |  |  |
|  | CRITICAL | 10.0\* | [32321](http://www.nessus.org/plugins/index.php?view=single&id=32321) | Debian OpenSSH/OpenSSL Package Random Number Generator |
|  |  |  |  | Weakness (SSL check) |
|  |  |  |  |  |
|  | CRITICAL | 10.0\* | [11356](http://www.nessus.org/plugins/index.php?view=single&id=11356) | NFS Exported Share Information Disclosure |
|  |  |  |  |  |
|  |  |  |  |  |
|  | CRITICAL | 10.0\* | [46882](http://www.nessus.org/plugins/index.php?view=single&id=46882) | UnrealIRCd Backdoor Detection |
|  |  |  |  |  |
|  |  |  |  |  |
|  | HIGH | 8.6 | [136769](http://www.nessus.org/plugins/index.php?view=single&id=136769) | ISC BIND Service Downgrade / Reflected DoS |
|  |  |  |  |  |
|  |  |  |  |  |
|  | HIGH | 7.5 | [136808](http://www.nessus.org/plugins/index.php?view=single&id=136808) | ISC BIND Denial of Service |
|  |  |  |  |  |
|  |  |  |  |  |
|  | HIGH | 7.5 | [42256](http://www.nessus.org/plugins/index.php?view=single&id=42256) | NFS Shares World Readable |
|  |  |  |  |  |
|  |  |  |  |  |
|  | HIGH | 7.5 | [42873](http://www.nessus.org/plugins/index.php?view=single&id=42873) | SSL Medium Strength Cipher Suites Supported (SWEET32) |
|  |  |  |  |  |
|  |  |  |  |  |
|  | HIGH | 7.5 | [90509](http://www.nessus.org/plugins/index.php?view=single&id=90509) | Samba Badlock Vulnerability |
|  |  |  |  |  |
|  |  |  |  |  |
|  | HIGH | 7.5\* | [10205](http://www.nessus.org/plugins/index.php?view=single&id=10205) | rlogin Service Detection |
|  |  |  |  |  |
|  |  |  |  |  |
|  | HIGH | 7.5\* | [10245](http://www.nessus.org/plugins/index.php?view=single&id=10245) | rsh Service Detection |

6.8 [78479](http://www.nessus.org/plugins/index.php?view=single&id=78479) SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

MEDIUM

MEDIUM

6.5 [139915](http://www.nessus.org/plugins/index.php?view=single&id=139915) ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

6.5 [51192](http://www.nessus.org/plugins/index.php?view=single&id=51192) SSL Certificate Cannot Be Trusted

MEDIUM

MEDIUM

6.5 [57582](http://www.nessus.org/plugins/index.php?view=single&id=57582) SSL Self-Signed Certificate

6.5 [104743](http://www.nessus.org/plugins/index.php?view=single&id=104743) TLS Version 1.0 Protocol Detection

MEDIUM

MEDIUM

6.5 [42263](http://www.nessus.org/plugins/index.php?view=single&id=42263) Unencrypted Telnet Server

5.9 [31705](http://www.nessus.org/plugins/index.php?view=single&id=31705) SSL Anonymous Cipher Suites Supported

MEDIUM

MEDIUM

5.9 [89058](http://www.nessus.org/plugins/index.php?view=single&id=89058) SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

5.9 [65821](http://www.nessus.org/plugins/index.php?view=single&id=65821) SSL RC4 Cipher Suites Supported (Bar Mitzvah)

MEDIUM

MEDIUM

5.3 [12085](http://www.nessus.org/plugins/index.php?view=single&id=12085) Apache Tomcat Default Files

5.3 [12217](http://www.nessus.org/plugins/index.php?view=single&id=12217) DNS Server Cache Snooping Remote Information Disclosure

MEDIUM

MEDIUM

5.3 [11213](http://www.nessus.org/plugins/index.php?view=single&id=11213) HTTP TRACE / TRACK Methods Allowed

5.3 [57608](http://www.nessus.org/plugins/index.php?view=single&id=57608) SMB Signing not required

MEDIUM

MEDIUM

5.3 [15901](http://www.nessus.org/plugins/index.php?view=single&id=15901) SSL Certificate Expiry

5.3 [45411](http://www.nessus.org/plugins/index.php?view=single&id=45411) SSL Certificate with Wrong Hostname

MEDIUM

MEDIUM

5.3 [26928](http://www.nessus.org/plugins/index.php?view=single&id=26928) SSL Weak Cipher Suites Supported

4.0\* [52611](http://www.nessus.org/plugins/index.php?view=single&id=52611) SMTP Service STARTTLS Plaintext Command Injection 4.3\* [90317](http://www.nessus.org/plugins/index.php?view=single&id=90317) SSH Weak Algorithms Supported

MEDIUM

MEDIUM

MEDIUM

4.3\* [81606](http://www.nessus.org/plugins/index.php?view=single&id=81606) SSL/TLS EXPORT\_RSA <= 512-bit Cipher Suites Supported (FREAK)

LOW

3.7 [153953](http://www.nessus.org/plugins/index.php?view=single&id=153953) SSH Weak Key Exchange Algorithms Enabled

3.7 [83738](http://www.nessus.org/plugins/index.php?view=single&id=83738) SSL/TLS EXPORT\_DHE <= 512-bit Export Cipher Suites Supported (Logjam) 2.6\* [70658](http://www.nessus.org/plugins/index.php?view=single&id=70658) SSH Server CBC Mode Ciphers Enabled

LOW

LOW

LOW

2.6\* [71049](http://www.nessus.org/plugins/index.php?view=single&id=71049) SSH Weak MAC Algorithms Enabled 2.6\* [10407](http://www.nessus.org/plugins/index.php?view=single&id=10407) X Server Detection

LOW

N/A [10114](http://www.nessus.org/plugins/index.php?view=single&id=10114) ICMP Timestamp Request Remote Date Disclosure N/A [10223](http://www.nessus.org/plugins/index.php?view=single&id=10223) RPC portmapper Service Detection

INFO

INFO

INFO

N/A [21186](http://www.nessus.org/plugins/index.php?view=single&id=21186) A JP Connector Detection

INFO

N/A [18261](http://www.nessus.org/plugins/index.php?view=single&id=18261) Apache Banner Linux Distribution Disclosure N/A [48204](http://www.nessus.org/plugins/index.php?view=single&id=48204) Apache HTTP Server Version

N/A [39446](http://www.nessus.org/plugins/index.php?view=single&id=39446) Apache Tomcat Detection

INFO

INFO

INFO

INFO

INFO

N/A [39519](http://www.nessus.org/plugins/index.php?view=single&id=39519) Backported Security Patch Detection (FTP) N/A [84574](http://www.nessus.org/plugins/index.php?view=single&id=84574) Backported Security Patch Detection (PHP) N/A [39520](http://www.nessus.org/plugins/index.php?view=single&id=39520) Backported Security Patch Detection (SSH) N/A [39521](http://www.nessus.org/plugins/index.php?view=single&id=39521) Backported Security Patch Detection (WWW) N/A [45590](http://www.nessus.org/plugins/index.php?view=single&id=45590) Common Platform Enumeration (CPE)

N/A [10028](http://www.nessus.org/plugins/index.php?view=single&id=10028) DNS Server BIND version Directive Remote Version Detection N/A [35373](http://www.nessus.org/plugins/index.php?view=single&id=35373) DNS Server DNSSEC Aware Resolver

INFO

INFO

INFO

INFO

INFO

N/A [11002](http://www.nessus.org/plugins/index.php?view=single&id=11002) DNS Server Detection

INFO

N/A [72779](http://www.nessus.org/plugins/index.php?view=single&id=72779) DNS Server Version Detection

N/A [35371](http://www.nessus.org/plugins/index.php?view=single&id=35371) DNS Server hostname.bind Map Hostname Disclosure N/A [54615](http://www.nessus.org/plugins/index.php?view=single&id=54615) Device Type

INFO

INFO

INFO

N/A [35716](http://www.nessus.org/plugins/index.php?view=single&id=35716) Ethernet Card Manufacturer Detection N/A [86420](http://www.nessus.org/plugins/index.php?view=single&id=86420) Ethernet MAC Addresses

INFO

INFO

N/A [10092](http://www.nessus.org/plugins/index.php?view=single&id=10092) FTP Server Detection

INFO

N/A [10107](http://www.nessus.org/plugins/index.php?view=single&id=10107) HTTP Server Type and Version

N/A [24260](http://www.nessus.org/plugins/index.php?view=single&id=24260) HyperText Transfer Protocol (HTTP) Information N/A [11156](http://www.nessus.org/plugins/index.php?view=single&id=11156) IRC Daemon Version Detection

INFO

INFO

INFO

N/A [10397](http://www.nessus.org/plugins/index.php?view=single&id=10397) Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

INFO

N/A [10785](http://www.nessus.org/plugins/index.php?view=single&id=10785) Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

N/A [11011](http://www.nessus.org/plugins/index.php?view=single&id=11011) Microsoft Windows SMB Service Detection

INFO

INFO

N/A [100871](http://www.nessus.org/plugins/index.php?view=single&id=100871) Microsoft Windows SMB Versions Supported (remote check)

N/A [106716](http://www.nessus.org/plugins/index.php?view=single&id=106716) Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) N/A [10437](http://www.nessus.org/plugins/index.php?view=single&id=10437) NFS Share Export List

INFO

INFO

INFO

N/A [11219](http://www.nessus.org/plugins/index.php?view=single&id=11219) Nessus SYN scanner

INFO

N/A [19506](http://www.nessus.org/plugins/index.php?view=single&id=19506) Nessus Scan Information N/A [11936](http://www.nessus.org/plugins/index.php?view=single&id=11936) OS Identification

N/A [117886](http://www.nessus.org/plugins/index.php?view=single&id=117886) OS Security Patch Assessment Not Available N/A [10919](http://www.nessus.org/plugins/index.php?view=single&id=10919) Open Port Re-check

INFO

INFO

INFO

INFO

N/A [50845](http://www.nessus.org/plugins/index.php?view=single&id=50845) OpenSSL Detection N/A [48243](http://www.nessus.org/plugins/index.php?view=single&id=48243) PHP Version Detection N/A [66334](http://www.nessus.org/plugins/index.php?view=single&id=66334) Patch Report

INFO

INFO

INFO

N/A [118224](http://www.nessus.org/plugins/index.php?view=single&id=118224) PostgreSQL STARTTLS Support N/A [26024](http://www.nessus.org/plugins/index.php?view=single&id=26024) PostgreSQL Server Detection N/A [22227](http://www.nessus.org/plugins/index.php?view=single&id=22227) RMI Registry Detection

INFO

INFO

INFO

N/A [11111](http://www.nessus.org/plugins/index.php?view=single&id=11111) RPC Services Enumeration N/A [53335](http://www.nessus.org/plugins/index.php?view=single&id=53335) RPC portmapper (TCP) N/A [10263](http://www.nessus.org/plugins/index.php?view=single&id=10263) SMTP Server Detection

INFO

INFO

INFO

N/A [42088](http://www.nessus.org/plugins/index.php?view=single&id=42088) SMTP Service STARTTLS Command Support N/A [70657](http://www.nessus.org/plugins/index.php?view=single&id=70657) SSH Algorithms and Languages Supported N/A [149334](http://www.nessus.org/plugins/index.php?view=single&id=149334) SSH Password Authentication Accepted N/A [10881](http://www.nessus.org/plugins/index.php?view=single&id=10881) SSH Protocol Versions Supported

INFO

INFO

INFO

INFO

N/A [153588](http://www.nessus.org/plugins/index.php?view=single&id=153588) SSH SHA-1 HMAC Algorithms Enabled N/A [10267](http://www.nessus.org/plugins/index.php?view=single&id=10267) SSH Server Type and Version Information N/A [56984](http://www.nessus.org/plugins/index.php?view=single&id=56984) SSL / TLS Versions Supported

INFO

INFO

N/A [45410](http://www.nessus.org/plugins/index.php?view=single&id=45410) SSL Certificate 'commonName' Mismatch N/A [10863](http://www.nessus.org/plugins/index.php?view=single&id=10863) SSL Certificate Information

INFO

INFO

INFO

N/A [70544](http://www.nessus.org/plugins/index.php?view=single&id=70544) SSL Cipher Block Chaining Cipher Suites Supported N/A [21643](http://www.nessus.org/plugins/index.php?view=single&id=21643) SSL Cipher Suites Supported

INFO

INFO

N/A [57041](http://www.nessus.org/plugins/index.php?view=single&id=57041) SSL Perfect Forward Secrecy Cipher Suites Supported N/A [51891](http://www.nessus.org/plugins/index.php?view=single&id=51891) SSL Session Resume Supported

INFO

INFO

N/A [156899](http://www.nessus.org/plugins/index.php?view=single&id=156899) SSL/TLS Recommended Cipher Suites N/A [25240](http://www.nessus.org/plugins/index.php?view=single&id=25240) Samba Server Detection

INFO

INFO

N/A [104887](http://www.nessus.org/plugins/index.php?view=single&id=104887) Samba Version

INFO

N/A [96982](http://www.nessus.org/plugins/index.php?view=single&id=96982) Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

N/A [22964](http://www.nessus.org/plugins/index.php?view=single&id=22964) Service Detection

INFO

INFO

INFO

N/A [17975](http://www.nessus.org/plugins/index.php?view=single&id=17975) Service Detection (GET request) N/A [25220](http://www.nessus.org/plugins/index.php?view=single&id=25220) TCP/IP Timestamps Supported N/A [11819](http://www.nessus.org/plugins/index.php?view=single&id=11819) TFTP Daemon Detection

N/A [110723](http://www.nessus.org/plugins/index.php?view=single&id=110723) Target Credential Status by Authentication Protocol - No Credentials Provided

INFO

INFO

INFO

N/A [10281](http://www.nessus.org/plugins/index.php?view=single&id=10281) Telnet Server Detection N/A [10287](http://www.nessus.org/plugins/index.php?view=single&id=10287) Traceroute Information

N/A [11154](http://www.nessus.org/plugins/index.php?view=single&id=11154) Unknown Service Detection: Banner Retrieval N/A [19288](http://www.nessus.org/plugins/index.php?view=single&id=19288) VNC Server Security Type Detection

INFO

INFO

INFO

INFO

N/A [65792](http://www.nessus.org/plugins/index.php?view=single&id=65792) VNC Server Unencrypted Communication Detection N/A [10342](http://www.nessus.org/plugins/index.php?view=single&id=10342) VNC Software Detection

INFO

INFO

N/A [135860](http://www.nessus.org/plugins/index.php?view=single&id=135860) WMI Not Available

INFO

INFO

N/A [20108](http://www.nessus.org/plugins/index.php?view=single&id=20108) Web Server / Application favicon.ico Vendor Fingerprinting N/A [11422](http://www.nessus.org/plugins/index.php?view=single&id=11422) Web Server Unconfigured - Default Install Page Present

INFO N/A [11424](http://www.nessus.org/plugins/index.php?view=single&id=11424) WebDAV Detection

INFO N/A [10150](http://www.nessus.org/plugins/index.php?view=single&id=10150) Windows NetBIOS / SMB Remote Host Information Disclosure

INFO N/A [52703](http://www.nessus.org/plugins/index.php?view=single&id=52703) vsftpd Detection

\* indicates the v3.0 score was not available; the v2.0 score is shown