



Nessus Meta Scan Basic With Credentials

Report generated by Nessus™

Wed, 02 Oct 2019 00:19:07 CDT

TABLE OF CONTENTS

Hosts Executive Summary

| | |
|----------------------|---|
| • 192.168.1.154..... | 4 |
|----------------------|---|

Nessus Essentials

Hosts Executive Summary

192.168.1.154



Vulnerabilities

Total: 92

| SEVERITY | CVSS | PLUGIN | NAME |
|----------|------|--------|---|
| CRITICAL | 10.0 | 51988 | Bind Shell Backdoor Detection |
| CRITICAL | 10.0 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0 | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0 | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0 | 61708 | VNC Server 'password' Password |
| HIGH | 7.1 | 20007 | SSL Version 2 and 3 Protocol Detection |
| MEDIUM | 6.8 | 90509 | Samba Badlock Vulnerability |
| MEDIUM | 6.4 | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.4 | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 5.0 | 11213 | HTTP TRACE / TRACK Methods Allowed |
| MEDIUM | 5.0 | 42256 | NFS Shares World Readable |
| MEDIUM | 5.0 | 57608 | SMB Signing not required |
| MEDIUM | 5.0 | 15901 | SSL Certificate Expiry |
| MEDIUM | 5.0 | 45411 | SSL Certificate with Wrong Hostname |
| MEDIUM | 5.0 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| MEDIUM | 4.3 | 90317 | SSH Weak Algorithms Supported |
| MEDIUM | 4.3 | 78479 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |

| | | | |
|------|-----|------------------------|--|
| LOW | 2.6 | 70658 | SSH Server CBC Mode Ciphers Enabled |
| LOW | 2.6 | 71049 | SSH Weak MAC Algorithms Enabled |
| LOW | 2.6 | 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| LOW | 2.6 | 10407 | X Server Detection |
| INFO | N/A | 21186 | AJP Connector Detection |
| INFO | N/A | 18261 | Apache Banner Linux Distribution Disclosure |
| INFO | N/A | 48204 | Apache HTTP Server Version |
| INFO | N/A | 21745 | Authentication Failure - Local Checks Not Run |
| INFO | N/A | 110095 | Authentication Success |
| INFO | N/A | 84574 | Backported Security Patch Detection (PHP) |
| INFO | N/A | 39520 | Backported Security Patch Detection (SSH) |
| INFO | N/A | 39521 | Backported Security Patch Detection (WWW) |
| INFO | N/A | 45590 | Common Platform Enumeration (CPE) |
| INFO | N/A | 10028 | DNS Server BIND version Directive Remote Version Detection |
| INFO | N/A | 11002 | DNS Server Detection |
| INFO | N/A | 72779 | DNS Server Version Detection |
| INFO | N/A | 35371 | DNS Server hostname.bind Map Hostname Disclosure |
| INFO | N/A | 54615 | Device Type |
| INFO | N/A | 117530 | Errors in nessusd.dump |
| INFO | N/A | 35716 | Ethernet Card Manufacturer Detection |
| INFO | N/A | 86420 | Ethernet MAC Addresses |
| INFO | N/A | 10092 | FTP Server Detection |
| INFO | N/A | 10107 | HTTP Server Type and Version |
| INFO | N/A | 24260 | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | 10114 | ICMP Timestamp Request Remote Date Disclosure |

| | | | |
|------|-----|------------------------|--|
| INFO | N/A | 10397 | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure |
| INFO | N/A | 10394 | Microsoft Windows SMB Log In Possible |
| INFO | N/A | 10785 | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
| INFO | N/A | 11011 | Microsoft Windows SMB Service Detection |
| INFO | N/A | 100871 | Microsoft Windows SMB Versions Supported (remote check) |
| INFO | N/A | 106716 | Microsoft Windows SMB2 Dialects Supported (remote check) |
| INFO | N/A | 10437 | NFS Share Export List |
| INFO | N/A | 11219 | Nessus SYN scanner |
| INFO | N/A | 19506 | Nessus Scan Information |
| INFO | N/A | 11936 | OS Identification |
| INFO | N/A | 97993 | OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library) |
| INFO | N/A | 50845 | OpenSSL Detection |
| INFO | N/A | 48243 | PHP Version Detection |
| INFO | N/A | 66334 | Patch Report |
| INFO | N/A | 118224 | PostgreSQL STARTTLS Support |
| INFO | N/A | 26024 | PostgreSQL Server Detection |
| INFO | N/A | 11111 | RPC Services Enumeration |
| INFO | N/A | 53335 | RPC portmapper (TCP) |
| INFO | N/A | 10223 | RPC portmapper Service Detection |
| INFO | N/A | 25221 | Remote listeners enumeration (Linux / AIX) |
| INFO | N/A | 10263 | SMTP Server Detection |
| INFO | N/A | 70657 | SSH Algorithms and Languages Supported |
| INFO | N/A | 10881 | SSH Protocol Versions Supported |
| INFO | N/A | 10267 | SSH Server Type and Version Information |

| | | | |
|------|-----|------------------------|--|
| INFO | N/A | 56984 | SSL / TLS Versions Supported |
| INFO | N/A | 45410 | SSL Certificate 'commonName' Mismatch |
| INFO | N/A | 10863 | SSL Certificate Information |
| INFO | N/A | 70544 | SSL Cipher Block Chaining Cipher Suites Supported |
| INFO | N/A | 21643 | SSL Cipher Suites Supported |
| INFO | N/A | 62563 | SSL Compression Methods Supported |
| INFO | N/A | 57041 | SSL Perfect Forward Secrecy Cipher Suites Supported |
| INFO | N/A | 25240 | Samba Server Detection |
| INFO | N/A | 104887 | Samba Version |
| INFO | N/A | 96982 | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) |
| INFO | N/A | 22964 | Service Detection |
| INFO | N/A | 17975 | Service Detection (GET request) |
| INFO | N/A | 11153 | Service Detection (HELP Request) |
| INFO | N/A | 25220 | TCP/IP Timestamps Supported |
| INFO | N/A | 11819 | TFTP Daemon Detection |
| INFO | N/A | 104743 | TLS Version 1.0 Protocol Detection |
| INFO | N/A | 10287 | Traceroute Information |
| INFO | N/A | 11154 | Unknown Service Detection: Banner Retrieval |
| INFO | N/A | 20094 | VMware Virtual Machine Detection |
| INFO | N/A | 19288 | VNC Server Security Type Detection |
| INFO | N/A | 65792 | VNC Server Unencrypted Communication Detection |
| INFO | N/A | 10342 | VNC Software Detection |
| INFO | N/A | 11424 | WebDAV Detection |
| INFO | N/A | 10150 | Windows NetBIOS / SMB Remote Host Information Disclosure |
| INFO | N/A | 52703 | vsftpd Detection |