



# metasploit

---

Report generated by Tenable Nessus™

Fri, 02 Jan 2026 17:39:07 IST

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

|                       |    |
|-----------------------|----|
| • 192.168.86.1.....   | 4  |
| • 192.168.86.2.....   | 5  |
| • 192.168.86.131..... | 6  |
| • 192.168.86.133..... | 12 |
| • 192.168.86.254..... | 16 |

---

## Vulnerabilities by Host

---

# 192.168.86.1



## Vulnerabilities

Total: 11

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME   |
|----------|-----------|-----------|------------|--------|--|
| INFO     | N/A       | -         | -          | 45590  | Common Platform Enumeration (CPE)                      |
| INFO     | N/A       | -         | -          | 54615  | Device Type  |
| INFO     | N/A       | -         | -          | 53513  | Link-Local Multicast Name Resolution (LLMNR) Detection |
| INFO     | N/A       | -         | -          | 11219  | Nessus SYN scanner                                     |
| INFO     | N/A       | -         | -          | 19506  | Nessus Scan Information                                |
| INFO     | N/A       | -         | -          | 209654 | OS Fingerprints Detected                               |
| INFO     | N/A       | -         | -          | 11936  | OS Identification                                      |
| INFO     | N/A       | -         | -          | 22964  | Service Detection                                      |
| INFO     | N/A       | -         | -          | 25220  | TCP/IP Timestamps Supported                            |
| INFO     | N/A       | -         | -          | 10287  | Traceroute Information                                 |
| INFO     | N/A       | -         | -          | 20301  | VMware ESX/GSX Server Authentication Daemon Detection  |

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

## 192.168.86.2



### Vulnerabilities

Total: 14

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN                 | NAME  |
|----------|-----------|-----------|------------|------------------------|---|
| MEDIUM   | 6.5       | 4.0       | 0.0596     | <a href="#">50686</a>  | IP Forwarding Enabled                                   |
| MEDIUM   | 5.3       | -         | -          | <a href="#">12217</a>  | DNS Server Cache Snooping Remote Information Disclosure |
| INFO     | N/A       | -         | -          | <a href="#">45590</a>  | Common Platform Enumeration (CPE)                       |
| INFO     | N/A       | -         | -          | <a href="#">11002</a>  | DNS Server Detection                                    |
| INFO     | N/A       | -         | -          | <a href="#">72779</a>  | DNS Server Version Detection                            |
| INFO     | N/A       | -         | -          | <a href="#">54615</a>  | Device Type   |
| INFO     | N/A       | -         | -          | <a href="#">35716</a>  | Ethernet Card Manufacturer Detection                    |
| INFO     | N/A       | -         | -          | <a href="#">86420</a>  | Ethernet MAC Addresses                                  |
| INFO     | N/A       | -         | -          | <a href="#">11219</a>  | Nessus SYN scanner                                      |
| INFO     | N/A       | -         | -          | <a href="#">19506</a>  | Nessus Scan Information                                 |
| INFO     | N/A       | -         | -          | <a href="#">209654</a> | OS Fingerprints Detected                                |
| INFO     | N/A       | -         | -          | <a href="#">11936</a>  | OS Identification                                       |
| INFO     | N/A       | -         | -          | <a href="#">10287</a>  | Traceroute Information                                  |
| INFO     | N/A       | -         | -          | <a href="#">20094</a>  | VMware Virtual Machine Detection                        |

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

# 192.168.86.131



## Vulnerabilities

Total: 119

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN                 | NAME  |
|----------|-----------|-----------|------------|------------------------|---|
| CRITICAL | 9.8       | 8.9       | 0.9447     | <a href="#">134862</a> | Apache Tomcat AJP Connector Request Injection (Ghostcat)                    |
| CRITICAL | 9.8       | -         | -          | <a href="#">51988</a>  | Bind Shell Backdoor Detection   |
| CRITICAL | 9.8       | -         | -          | <a href="#">20007</a>  | SSL Version 2 and 3 Protocol Detection                                      |
| CRITICAL | 10.0      | -         | -          | <a href="#">171340</a> | Apache Tomcat SEoL (<= 5.5.x)   |
| CRITICAL | 10.0      | -         | -          | <a href="#">201352</a> | Canonical Ubuntu Linux SEoL (8.04.x)  |
| CRITICAL | 10.0*     | 5.1       | 0.0165     | <a href="#">32314</a>  | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness             |
| CRITICAL | 10.0*     | 5.1       | 0.0165     | <a href="#">32321</a>  | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0*     | 7.4       | 0.8622     | <a href="#">46882</a>  | UnrealIRCd Backdoor Detection   |
| CRITICAL | 10.0*     | -         | -          | <a href="#">61708</a>  | VNC Server 'password' Password  |
| HIGH     | 8.6       | 5.2       | 0.1988     | <a href="#">136769</a> | ISC BIND Service Downgrade / Reflected DoS                                  |
| HIGH     | 7.5       | -         | -          | <a href="#">42256</a>  | NFS Shares World Readable   |
| HIGH     | 7.5       | 6.1       | 0.5535     | <a href="#">42873</a>  | SSL Medium Strength Cipher Suites Supported (SWEET32)                       |
| HIGH     | 7.5       | 5.9       | 0.7714     | <a href="#">90509</a>  | Samba Badlock Vulnerability   |
| HIGH     | 7.5*      | 6.7       | 0.5006     | <a href="#">10205</a>  | rlogin Service Detection  |
| HIGH     | 7.5*      | 6.7       | 0.5006     | <a href="#">10245</a>  | rsh Service Detection   |
| MEDIUM   | 6.5       | 4.4       | 0.0067     | <a href="#">139915</a> | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS                |
| MEDIUM   | 6.5       | -         | -          | <a href="#">51192</a>  | SSL Certificate Cannot Be Trusted   |
| MEDIUM   | 6.5       | -         | -          | <a href="#">57582</a>  | SSL Self-Signed Certificate   |

|        |      |     |        |                        |   |
|--------|------|-----|--------|------------------------|---|
| MEDIUM | 6.5  | -   | -      | <a href="#">104743</a> | TLS Version 1.0 Protocol Detection  |
| MEDIUM | 6.5  | -   | -      | <a href="#">42263</a>  | Unencrypted Telnet Server   |
| MEDIUM | 5.9  | 4.4 | 0.8974 | <a href="#">136808</a> | ISC BIND Denial of Service  |
| MEDIUM | 5.9  | 4.4 | 0.027  | <a href="#">31705</a>  | SSL Anonymous Cipher Suites Supported   |
| MEDIUM | 5.9  | 3.6 | 0.8838 | <a href="#">89058</a>  | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| MEDIUM | 5.9  | 7.3 | 0.8448 | <a href="#">65821</a>  | SSL RC4 Cipher Suites Supported (Bar Mitzvah)   |
| MEDIUM | 5.3  | -   | -      | <a href="#">12085</a>  | Apache Tomcat Default Files   |
| MEDIUM | 5.3  | -   | -      | <a href="#">12217</a>  | DNS Server Cache Snooping Remote Information Disclosure                               |
| MEDIUM | 5.3  | 4.0 | 0.6899 | <a href="#">11213</a>  | HTTP TRACE / TRACK Methods Allowed  |
| MEDIUM | 5.3  | -   | -      | <a href="#">57608</a>  | SMB Signing not required  |
| MEDIUM | 5.3  | -   | -      | <a href="#">15901</a>  | SSL Certificate Expiry  |
| MEDIUM | 5.3  | -   | -      | <a href="#">45411</a>  | SSL Certificate with Wrong Hostname   |
| MEDIUM | 5.3  | -   | -      | <a href="#">26928</a>  | SSL Weak Cipher Suites Supported  |
| MEDIUM | 4.0* | 7.3 | 0.2959 | <a href="#">52611</a>  | SMTP Service STARTTLS Plaintext Command Injection                                     |
| MEDIUM | 4.3* | 1.4 | 0.8962 | <a href="#">81606</a>  | SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FRE                            |
| LOW    | 3.7  | -   | -      | <a href="#">153953</a> | SSH Weak Key Exchange Algorithms Enabled  |
| LOW    | 3.7  | 3.9 | 0.9364 | <a href="#">83875</a>  | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)                                  |
| LOW    | 3.7  | 3.9 | 0.9364 | <a href="#">83738</a>  | SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam)                   |
| LOW    | 3.4  | 5.1 | 0.9402 | <a href="#">78479</a>  | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)           |
| LOW    | 2.1* | 2.2 | 0.0037 | <a href="#">10114</a>  | ICMP Timestamp Request Remote Date Disclosure   |
| LOW    | 2.6* | -   | -      | <a href="#">71049</a>  | SSH Weak MAC Algorithms Enabled   |
| LOW    | 2.6* | -   | -      | <a href="#">10407</a>  | X Server Detection  |
| INFO   | N/A  | -   | -      | <a href="#">10223</a>  | RPC portmapper Service Detection  |
| INFO   | N/A  | -   | -      | <a href="#">21186</a>  | AJP Connector Detection   |

|      |     |   |   |                        |   |
|------|-----|---|---|------------------------|---|
| INFO | N/A | - | - | <a href="#">18261</a>  | Apache Banner Linux Distribution Disclosure                                 |
| INFO | N/A | - | - | <a href="#">48204</a>  | Apache HTTP Server Version  |
| INFO | N/A | - | - | <a href="#">39446</a>  | Apache Tomcat Detection   |
| INFO | N/A | - | - | <a href="#">84574</a>  | Backported Security Patch Detection (PHP)                                   |
| INFO | N/A | - | - | <a href="#">39520</a>  | Backported Security Patch Detection (SSH)                                   |
| INFO | N/A | - | - | <a href="#">39521</a>  | Backported Security Patch Detection (WWW)                                   |
| INFO | N/A | - | - | <a href="#">45590</a>  | Common Platform Enumeration (CPE)   |
| INFO | N/A | - | - | <a href="#">10028</a>  | DNS Server BIND version Directive Remote Version Detection                  |
| INFO | N/A | - | - | <a href="#">11002</a>  | DNS Server Detection  |
| INFO | N/A | - | - | <a href="#">72779</a>  | DNS Server Version Detection  |
| INFO | N/A | - | - | <a href="#">35371</a>  | DNS Server hostname.bind Map Hostname Disclosure                            |
| INFO | N/A | - | - | <a href="#">54615</a>  | Device Type   |
| INFO | N/A | - | - | <a href="#">35716</a>  | Ethernet Card Manufacturer Detection  |
| INFO | N/A | - | - | <a href="#">86420</a>  | Ethernet MAC Addresses  |
| INFO | N/A | - | - | <a href="#">10092</a>  | FTP Server Detection  |
| INFO | N/A | - | - | <a href="#">10107</a>  | HTTP Server Type and Version  |
| INFO | N/A | - | - | <a href="#">24260</a>  | HyperText Transfer Protocol (HTTP) Information                              |
| INFO | N/A | - | - | <a href="#">11156</a>  | IRC Daemon Version Detection  |
| INFO | N/A | - | - | <a href="#">10397</a>  | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure                 |
| INFO | N/A | - | - | <a href="#">10785</a>  | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
| INFO | N/A | - | - | <a href="#">11011</a>  | Microsoft Windows SMB Service Detection                                     |
| INFO | N/A | - | - | <a href="#">100871</a> | Microsoft Windows SMB Versions Supported (remote check)                     |
| INFO | N/A | - | - | <a href="#">106716</a> | Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)           |
| INFO | N/A | - | - | <a href="#">10719</a>  | MySQL Server Detection  |

|      |     |   |   |                        |  |
|------|-----|---|---|------------------------|--|
| INFO | N/A | - | - | <a href="#">10437</a>  | NFS Share Export List                          |
| INFO | N/A | - | - | <a href="#">11219</a>  | Nessus SYN scanner                             |
| INFO | N/A | - | - | <a href="#">19506</a>  | Nessus Scan Information                        |
| INFO | N/A | - | - | <a href="#">209654</a> | OS Fingerprints Detected                       |
| INFO | N/A | - | - | <a href="#">11936</a>  | OS Identification                              |
| INFO | N/A | - | - | <a href="#">117886</a> | OS Security Patch Assessment Not Available     |
| INFO | N/A | - | - | <a href="#">181418</a> | OpenSSH Detection                              |
| INFO | N/A | - | - | <a href="#">50845</a>  | OpenSSL Detection                              |
| INFO | N/A | - | - | <a href="#">48243</a>  | PHP Version Detection                          |
| INFO | N/A | - | - | <a href="#">66334</a>  | Patch Report                                   |
| INFO | N/A | - | - | <a href="#">118224</a> | PostgreSQL STARTTLS Support                    |
| INFO | N/A | - | - | <a href="#">26024</a>  | PostgreSQL Server Detection                    |
| INFO | N/A | - | - | <a href="#">22227</a>  | RMI Registry Detection                         |
| INFO | N/A | - | - | <a href="#">11111</a>  | RPC Services Enumeration                       |
| INFO | N/A | - | - | <a href="#">53335</a>  | RPC portmapper (TCP)                           |
| INFO | N/A | - | - | <a href="#">277650</a> | Remote Services Not Using Post-Quantum Ciphers |
| INFO | N/A | - | - | <a href="#">10263</a>  | SMTP Server Detection                          |
| INFO | N/A | - | - | <a href="#">42088</a>  | SMTP Service STARTTLS Command Support          |
| INFO | N/A | - | - | <a href="#">70657</a>  | SSH Algorithms and Languages Supported         |
| INFO | N/A | - | - | <a href="#">149334</a> | SSH Password Authentication Accepted           |
| INFO | N/A | - | - | <a href="#">10881</a>  | SSH Protocol Versions Supported                |
| INFO | N/A | - | - | <a href="#">10267</a>  | SSH Server Type and Version Information        |
| INFO | N/A | - | - | <a href="#">56984</a>  | SSL / TLS Versions Supported                   |
| INFO | N/A | - | - | <a href="#">45410</a>  | SSL Certificate 'commonName' Mismatch          |
| INFO | N/A | - | - | <a href="#">10863</a>  | SSL Certificate Information                    |

|      |     |   |   |                        |   |
|------|-----|---|---|------------------------|---|
| INFO | N/A | - | - | <a href="#">70544</a>  | SSL Cipher Block Chaining Cipher Suites Supported                             |
| INFO | N/A | - | - | <a href="#">21643</a>  | SSL Cipher Suites Supported   |
| INFO | N/A | - | - | <a href="#">62563</a>  | SSL Compression Methods Supported   |
| INFO | N/A | - | - | <a href="#">57041</a>  | SSL Perfect Forward Secrecy Cipher Suites Supported                           |
| INFO | N/A | - | - | <a href="#">51891</a>  | SSL Session Resume Supported  |
| INFO | N/A | - | - | <a href="#">156899</a> | SSL/TLS Recommended Cipher Suites   |
| INFO | N/A | - | - | <a href="#">25240</a>  | Samba Server Detection  |
| INFO | N/A | - | - | <a href="#">104887</a> | Samba Version   |
| INFO | N/A | - | - | <a href="#">96982</a>  | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)  |
| INFO | N/A | - | - | <a href="#">22964</a>  | Service Detection   |
| INFO | N/A | - | - | <a href="#">17975</a>  | Service Detection (GET request)   |
| INFO | N/A | - | - | <a href="#">11153</a>  | Service Detection (HELP Request)  |
| INFO | N/A | - | - | <a href="#">278501</a> | Smartbedded Meteobridge Web Detection   |
| INFO | N/A | - | - | <a href="#">25220</a>  | TCP/IP Timestamps Supported   |
| INFO | N/A | - | - | <a href="#">11819</a>  | TFTP Daemon Detection   |
| INFO | N/A | - | - | <a href="#">110723</a> | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | - | <a href="#">10281</a>  | Telnet Server Detection   |
| INFO | N/A | - | - | <a href="#">10287</a>  | Traceroute Information  |
| INFO | N/A | - | - | <a href="#">11154</a>  | Unknown Service Detection: Banner Retrieval                                   |
| INFO | N/A | - | - | <a href="#">20094</a>  | VMware Virtual Machine Detection  |
| INFO | N/A | - | - | <a href="#">19288</a>  | VNC Server Security Type Detection  |
| INFO | N/A | - | - | <a href="#">65792</a>  | VNC Server Unencrypted Communication Detection                                |
| INFO | N/A | - | - | <a href="#">10342</a>  | VNC Software Detection  |
| INFO | N/A | - | - | <a href="#">20108</a>  | Web Server / Application favicon.ico Vendor Fingerprinting                    |

|      |     |   |   |       |  |
|------|-----|---|---|-------|--|
| INFO | N/A | - | - | 11422 | Web Server Unconfigured - Default Install Page Present   |
| INFO | N/A | - | - | 11424 | WebDAV Detection   |
| INFO | N/A | - | - | 10150 | Windows NetBIOS / SMB Remote Host Information Disclosure |
| INFO | N/A | - | - | 52703 | vsftpd Detection   |

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

# 192.168.86.133



## Vulnerabilities

Total: 77

| Severity | CVSS V3.0 | VPR Score | EPSS Score | Plugin                 | Name  |
|----------|-----------|-----------|------------|------------------------|---|
| HIGH     | 7.5       | 3.6       | 0.0004     | <a href="#">274433</a> | Python Library Brotli <= 1.1.0 DoS                    |
| MEDIUM   | 6.5       | -         | -          | <a href="#">51192</a>  | SSL Certificate Cannot Be Trusted                     |
| MEDIUM   | 5.3       | 1.4       | 0.0001     | <a href="#">265895</a> | Ruby REXML 3.3.3 < 3.4.2 DoS vulnerability            |
| INFO     | N/A       | -         | -          | <a href="#">196906</a> | AI/LLM Software Report                                |
| INFO     | N/A       | -         | -          | <a href="#">141394</a> | Apache HTTP Server Installed (Linux)                  |
| INFO     | N/A       | -         | -          | <a href="#">142640</a> | Apache HTTP Server Site Enumeration                   |
| INFO     | N/A       | -         | -          | <a href="#">45590</a>  | Common Platform Enumeration (CPE)                     |
| INFO     | N/A       | -         | -          | <a href="#">182774</a> | Curl Installed (Linux / Unix)                         |
| INFO     | N/A       | -         | -          | <a href="#">55472</a>  | Device Hostname                                       |
| INFO     | N/A       | -         | -          | <a href="#">54615</a>  | Device Type   |
| INFO     | N/A       | -         | -          | <a href="#">25203</a>  | Enumerate IPv4 Interfaces via SSH                     |
| INFO     | N/A       | -         | -          | <a href="#">25202</a>  | Enumerate IPv6 Interfaces via SSH                     |
| INFO     | N/A       | -         | -          | <a href="#">33276</a>  | Enumerate MAC Addresses via SSH                       |
| INFO     | N/A       | -         | -          | <a href="#">170170</a> | Enumerate the Network Interface configuration via SSH |
| INFO     | N/A       | -         | -          | <a href="#">179200</a> | Enumerate the Network Routing configuration via SSH   |
| INFO     | N/A       | -         | -          | <a href="#">168980</a> | Enumerate the PATH Variables                          |
| INFO     | N/A       | -         | -          | <a href="#">35716</a>  | Ethernet Card Manufacturer Detection                  |
| INFO     | N/A       | -         | -          | <a href="#">86420</a>  | Ethernet MAC Addresses                                |
| INFO     | N/A       | -         | -          | <a href="#">204827</a> | Exiv2 Installed (Linux / Unix)                        |

|      |     |   |   |                        |   |
|------|-----|---|---|------------------------|---|
| INFO | N/A | - | - | <a href="#">168982</a> | Filepaths contain Dangerous characters (Linux)  |
| INFO | N/A | - | - | <a href="#">10107</a>  | HTTP Server Type and Version  |
| INFO | N/A | - | - | <a href="#">202721</a> | Hierarchical Data Format HDF5 File Detection for Linux/UNIX                           |
| INFO | N/A | - | - | <a href="#">24260</a>  | HyperText Transfer Protocol (HTTP) Information  |
| INFO | N/A | - | - | <a href="#">171410</a> | IP Assignment Method Detection  |
| INFO | N/A | - | - | <a href="#">147817</a> | Java Detection and Identification (Linux / Unix)                                      |
| INFO | N/A | - | - | <a href="#">189990</a> | Jmcnamara Spreadsheet-ParseExcel Installed (Unix)                                     |
| INFO | N/A | - | - | <a href="#">151883</a> | Libgcrypt Installed (Linux/UNIX)  |
| INFO | N/A | - | - | <a href="#">200214</a> | Libndp Installed (Linux / Unix)   |
| INFO | N/A | - | - | <a href="#">157358</a> | Linux Mounted Devices   |
| INFO | N/A | - | - | <a href="#">193143</a> | Linux Time Zone Information   |
| INFO | N/A | - | - | <a href="#">95928</a>  | Linux User List Enumeration   |
| INFO | N/A | - | - | <a href="#">19506</a>  | Nessus Scan Information   |
| INFO | N/A | - | - | <a href="#">10147</a>  | Nessus Server Detection   |
| INFO | N/A | - | - | <a href="#">64582</a>  | Netstat Connection Information  |
| INFO | N/A | - | - | <a href="#">14272</a>  | Netstat Portscanner (SSH)   |
| INFO | N/A | - | - | <a href="#">178771</a> | Node.js Installed (Linux / UNIX)  |
| INFO | N/A | - | - | <a href="#">178772</a> | Node.js Modules Installed (Linux)   |
| INFO | N/A | - | - | <a href="#">201190</a> | NumPy Detection   |
| INFO | N/A | - | - | <a href="#">209654</a> | OS Fingerprints Detected  |
| INFO | N/A | - | - | <a href="#">11936</a>  | OS Identification   |
| INFO | N/A | - | - | <a href="#">97993</a>  | OS Identification and Installed Software Enumeration over SSH (Using New SSH Library) |
| INFO | N/A | - | - | <a href="#">117887</a> | OS Security Patch Assessment Available  |
| INFO | N/A | - | - | <a href="#">148373</a> | OpenJDK Java Detection (Linux / Unix)   |
| INFO | N/A | - | - | <a href="#">168007</a> | OpenSSL Installed (Linux)   |

|      |     |   |   |                        |  |
|------|-----|---|---|------------------------|--|
| INFO | N/A | - | - | <a href="#">232856</a> | OpenVPN Installed (Linux)  |
| INFO | N/A | - | - | <a href="#">216936</a> | PHP Scripting Language Installed (Unix)  |
| INFO | N/A | - | - | <a href="#">179139</a> | Package Manager Packages Report (nix)  |
| INFO | N/A | - | - | <a href="#">66334</a>  | Patch Report   |
| INFO | N/A | - | - | <a href="#">130024</a> | PostgreSQL Client/Server Installed (Linux)                                       |
| INFO | N/A | - | - | <a href="#">277650</a> | Remote Services Not Using Post-Quantum Ciphers                                   |
| INFO | N/A | - | - | <a href="#">207584</a> | Ruby Gem Modules Installed (Linux)   |
| INFO | N/A | - | - | <a href="#">202184</a> | Ruby Programming Language Installed (Linux)                                      |
| INFO | N/A | - | - | <a href="#">174788</a> | SQLite Local Detection (Linux / Unix)  |
| INFO | N/A | - | - | <a href="#">56984</a>  | SSL / TLS Versions Supported   |
| INFO | N/A | - | - | <a href="#">10863</a>  | SSL Certificate Information  |
| INFO | N/A | - | - | <a href="#">21643</a>  | SSL Cipher Suites Supported  |
| INFO | N/A | - | - | <a href="#">57041</a>  | SSL Perfect Forward Secrecy Cipher Suites Supported                              |
| INFO | N/A | - | - | <a href="#">22964</a>  | Service Detection  |
| INFO | N/A | - | - | <a href="#">278501</a> | Smartbedded Meteobridge Web Detection  |
| INFO | N/A | - | - | <a href="#">22869</a>  | Software Enumeration (SSH)   |
| INFO | N/A | - | - | <a href="#">42822</a>  | Strict Transport Security (STS) Detection  |
| INFO | N/A | - | - | <a href="#">277654</a> | TLS Supported Groups   |
| INFO | N/A | - | - | <a href="#">136318</a> | TLS Version 1.2 Protocol Detection   |
| INFO | N/A | - | - | <a href="#">138330</a> | TLS Version 1.3 Protocol Detection   |
| INFO | N/A | - | - | <a href="#">110095</a> | Target Credential Issues by Authentication Protocol - No Issues Found            |
| INFO | N/A | - | - | <a href="#">141118</a> | Target Credential Status by Authentication Protocol - Valid Credentials Provided |
| INFO | N/A | - | - | <a href="#">163326</a> | Tenable Nessus Installed (Linux)   |
| INFO | N/A | - | - | <a href="#">237200</a> | Tornado Detection  |

|      |     |   |   |                        |   |
|------|-----|---|---|------------------------|---|
| INFO | N/A | - | - | <a href="#">192709</a> | Tukaani XZ Utils Installed (Linux / Unix)       |
| INFO | N/A | - | - | <a href="#">110483</a> | Unix / Linux Running Processes Information      |
| INFO | N/A | - | - | <a href="#">152742</a> | Unix Software Discovery Commands Available      |
| INFO | N/A | - | - | <a href="#">186361</a> | VMWare Tools or Open VM Tools Installed (Linux) |
| INFO | N/A | - | - | <a href="#">20094</a>  | VMware Virtual Machine Detection                |
| INFO | N/A | - | - | <a href="#">189731</a> | Vim Installed (Linux)                           |
| INFO | N/A | - | - | <a href="#">182848</a> | libcurl Installed (Linux / Unix)                |
| INFO | N/A | - | - | <a href="#">204828</a> | libexiv2 Installed (Linux / Unix)               |
| INFO | N/A | - | - | <a href="#">136340</a> | nginx Installed (Linux/UNIX)                    |

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

## 192.168.86.254



### Vulnerabilities

Total: 6

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME                                 |
|----------|-----------|-----------|------------|--------|--------------------------------------|
| LOW      | 3.3*      | -         | -          | 10663  | DHCP Server Detection                |
| INFO     | N/A       | -         | -          | 35716  | Ethernet Card Manufacturer Detection |
| INFO     | N/A       | -         | -          | 86420  | Ethernet MAC Addresses               |
| INFO     | N/A       | -         | -          | 19506  | Nessus Scan Information              |
| INFO     | N/A       | -         | -          | 10287  | Traceroute Information               |
| INFO     | N/A       | -         | -          | 20094  | VMware Virtual Machine Detection     |

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