



# Scan\_Metasploitable\_SameNetwork

---

Report generated by Tenable Nessus™

Mon, 19 May 2025 19:02:33 CEST

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

- 192.168.1.5..... 4

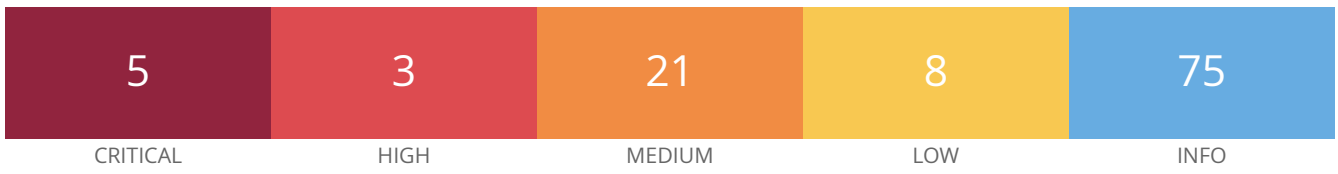
Nessus Essentials

---

## Vulnerabilities by Host

---

# 192.168.1.5



## Vulnerabilities

Total: 112

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	-	201352	Canonical Ubuntu Linux SEoL (8.04.x)
CRITICAL	10.0*	5.1	0.0165	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0165	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
HIGH	8.6	5.2	0.0334	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.1	0.406	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.7992	90509	Samba Badlock Vulnerability
MEDIUM	6.8	6.0	0.9211	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisonin
MEDIUM	6.5	4.4	0.0045	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	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	0.9234	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.027	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	3.6	0.8991	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

MEDIUM	5.9	7.3	0.9303	<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	0.8269	<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	5.0*	4.4	0.8222	<a href="#">10595</a>	DNS Server Zone Transfer Information Disclosure (AXFR)
MEDIUM	4.0*	7.3	0.6945	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3*	1.4	0.9243	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREEBIE)
LOW	3.7	1.4	0.0307	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	0.9403	<a href="#">83875</a>	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	4.5	0.9403	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam)
LOW	3.4	5.1	0.942	<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="#">42255</a>	NFS Server Superfluous
INFO	N/A	-	-	<a href="#">10223</a>	RPC portmapper Service 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="#">39519</a>	Backported Security Patch Detection (FTP)
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="#">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="#">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="#">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="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
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	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
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 (unauthenticated check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10281	Telnet Server Detection
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
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	-	-	135860	WMI Not Available
INFO	N/A	-	-	20108	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