



## meta-Basic-scan

---

Report generated by Nessus™

Thu, 04 Aug 2022 08:25:56 EDT

---

---

TABLE OF CONTENTS

---

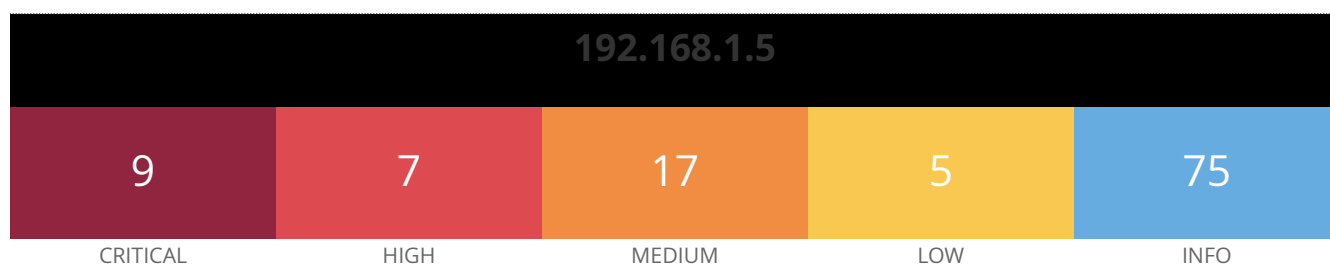
**Vulnerabilities by Host**

- 192.168.1.5..... 4

---

## **Vulnerabilities by Host**

---



## Vulnerabilities

Total: 113

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	<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="#">33850</a>	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	<a href="#">32314</a>	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	<a href="#">32321</a>	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	<a href="#">11356</a>	NFS Exported Share Information Disclosure
CRITICAL	10.0*	<a href="#">46882</a>	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	<a href="#">61708</a>	VNC Server 'password' Password
HIGH	8.6	<a href="#">136769</a>	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	<a href="#">136808</a>	ISC BIND Denial of Service
HIGH	7.5	<a href="#">42256</a>	NFS Shares World Readable
HIGH	7.5	<a href="#">42873</a>	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	<a href="#">90509</a>	Samba Badlock Vulnerability
HIGH	7.5*	<a href="#">10205</a>	rlogin Service Detection
HIGH	7.5*	<a href="#">10245</a>	rsh Service Detection
MEDIUM	6.8	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

MEDIUM	6.5	<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	<a href="#">31705</a>	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	<a href="#">89058</a>	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	<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*	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3*	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6*	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
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="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
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="#">46180</a>	Additional DNS Hostnames

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="#">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="#">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="#">12053</a>	Host Fully Qualified Domain Name (FQDN) Resolution
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="#">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="#">11936</a>	OS Identification
INFO	N/A	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	<a href="#">10919</a>	Open Port Re-check
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	57041	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	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