



# Scansione finale

---

Report generated by Nessus™

Sat, 27 Jul 2024 18:15:36 EDT

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.50.100.....	4
-----------------------	---

Nessus Essentials

---

## **Vulnerabilities by Host**

---

192.168.50.100



## Vulnerabilities

Total: 66

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection
INFO	N/A	-	10223	RPC portmapper Service 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	-	<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="#">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="#">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="#">181418</a>	OpenSSH Detection

INFO	N/A	-	<a href="#">66334</a>	Patch Report
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="#">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="#">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 (unauthenticated 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="#">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="#">10287</a>	Traceroute Information
INFO	N/A	-	<a href="#">11154</a>	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	<a href="#">11424</a>	WebDAV Detection
INFO	N/A	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	<a href="#">52703</a>	vsftpd Detection

---

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