



# Metasploitable2

Report generated by Nessus™

Thu, 28 Mar 2024 14:22:16 CET

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.159.136.....	4
------------------------	---

Nessus Essentials

---

## Vulnerabilities by Host

---

192.168.159.136



## Vulnerabilities

Total: 83

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	10245	rsh Service Detection
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	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
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
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking

LOW	3.7	3.6	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	-	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	<a href="#">42057</a>	Web Server Allows Password Auto-Completion
LOW	2.6*	-	<a href="#">26194</a>	Web Server Transmits Cleartext Credentials
LOW	2.6*	-	<a href="#">34850</a>	Web Server Uses Basic Authentication Without HTTPS
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="#">39446</a>	Apache Tomcat Detection
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="#">49704</a>	External URLs
INFO	N/A	-	<a href="#">43111</a>	HTTP Methods Allowed (per directory)
INFO	N/A	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	<a href="#">14788</a>	IP Protocols Scan
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="#">50344</a>	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	<a href="#">50345</a>	Missing or Permissive X-Frame-Options HTTP Response Header
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="#">181418</a>	OpenSSH Detection
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="#">40665</a>	Protected Web Page 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="#">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="#">11819</a>	TFTP Daemon Detection
INFO	N/A	-	<a href="#">19941</a>	TWiki Detection
INFO	N/A	-	<a href="#">10281</a>	Telnet Server 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="#">135860</a>	WMI Not Available
INFO	N/A	-	<a href="#">72771</a>	Web Accessible Backups
INFO	N/A	-	<a href="#">100669</a>	Web Application Cookies Are Expired
INFO	N/A	-	<a href="#">85601</a>	Web Application Cookies Not Marked HttpOnly
INFO	N/A	-	<a href="#">85602</a>	Web Application Cookies Not Marked Secure
INFO	N/A	-	<a href="#">40773</a>	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	-	<a href="#">91815</a>	Web Application Sitemap
INFO	N/A	-	<a href="#">20108</a>	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	<a href="#">11032</a>	Web Server Directory Enumeration
INFO	N/A	-	<a href="#">49705</a>	Web Server Harvested Email Addresses
INFO	N/A	-	<a href="#">11422</a>	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	<a href="#">10662</a>	Web mirroring
INFO	N/A	-	<a href="#">11424</a>	WebDAV Detection
INFO	N/A	-	<a href="#">24004</a>	WebDAV Directory Enumeration
INFO	N/A	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure

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