



## metasploitable2

---

Report generated by Nessus™

Thu, 01 Jun 2023 10:18:57 EDT

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.34.100.....	4
-----------------------	---

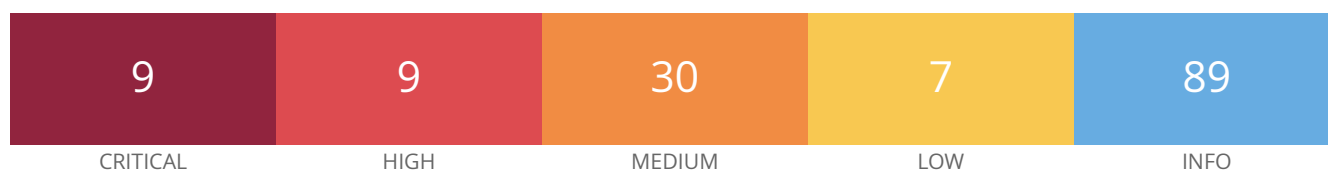
Nessus Essentials

---

## **Vulnerabilities by Host**

---

192.168.34.100



## Vulnerabilities

Total: 144

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
CRITICAL	10.0	-	171340	Apache Tomcat Web Server SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	8.3	-	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	-	39465	CGI Generic Command Execution
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution

HIGH	7.5*	6.7	<a href="#">36171</a>	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
MEDIUM	6.5	3.6	<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	6.1	3.8	<a href="#">10815</a>	Web Server Generic XSS
MEDIUM	5.9	5.1	<a href="#">136808</a>	ISC BIND Denial of Service
MEDIUM	5.3	-	<a href="#">12085</a>	Apache Tomcat Default Files
MEDIUM	5.3	-	<a href="#">40984</a>	Browsable Web Directories
MEDIUM	5.3	-	<a href="#">39467</a>	CGI Generic Path Traversal
MEDIUM	5.3	4.0	<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	2.9	<a href="#">58751</a>	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
MEDIUM	5.3	-	<a href="#">11229</a>	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0*	-	<a href="#">11411</a>	Backup Files Disclosure
MEDIUM	4.3*	-	<a href="#">44136</a>	CGI Generic Cookie Injection Scripting
MEDIUM	4.3*	-	<a href="#">49067</a>	CGI Generic HTML Injections (quick test)
MEDIUM	6.8*	-	<a href="#">42872</a>	CGI Generic Local File Inclusion (2nd pass)
MEDIUM	5.0*	-	<a href="#">46195</a>	CGI Generic Path Traversal (extended test)
MEDIUM	4.3*	-	<a href="#">47831</a>	CGI Generic XSS (comprehensive test)
MEDIUM	4.3*	-	<a href="#">55903</a>	CGI Generic XSS (extended patterns)
MEDIUM	4.3*	-	<a href="#">39466</a>	CGI Generic XSS (quick test)
MEDIUM	5.0*	-	<a href="#">46803</a>	PHP expose_php Information Disclosure

MEDIUM	4.0*	6.3	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	5.0*	-	<a href="#">57640</a>	Web Application Information Disclosure
MEDIUM	4.3*	-	<a href="#">85582</a>	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3*	3.8	<a href="#">51425</a>	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	5.0*	-	<a href="#">36083</a>	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
MEDIUM	4.3*	3.0	<a href="#">49142</a>	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
LOW	3.7	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	<a href="#">70658</a>	SSH Server CBC Mode Ciphers 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
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="#">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="#">47830</a>	CGI Generic Injectable Parameter
INFO	N/A	-	<a href="#">33817</a>	CGI Generic Tests Load Estimation (all tests)

INFO	N/A	-	<a href="#">39470</a>	CGI Generic Tests Timeout
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="#">132634</a>	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	<a href="#">49704</a>	External URLs
INFO	N/A	-	<a href="#">10092</a>	FTP Server Detection
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="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
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="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects 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="#">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="#">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="#">40665</a>	Protected Web Page 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="#">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="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	<a href="#">11819</a>	TFTP Daemon Detection
INFO	N/A	-	<a href="#">19941</a>	TWiki 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="#">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="#">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="#">40405</a>	Web Server Detection (HTTP/1.1)
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="#">11419</a>	Web Server Office File Inventory
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
INFO	N/A	-	<a href="#">17219</a>	phpMyAdmin Detection
INFO	N/A	-	<a href="#">52703</a>	vsftpd Detection

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