



Metasploitable Scan

Report generated by Tenable Nessus™

Sun, 30 Mar 2025 18:55:42 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

• 192.168.100.100.....	4
------------------------	---

Nessus Essentials

Vulnerabilities by Host

192.168.100.100



Vulnerabilities

Total: 140

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.7044	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.7044	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.71	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0004	193421	Apache 2.4.x < 2.4.54 Authentication Bypass
CRITICAL	9.8	6.7	0.9002	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.4003	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	7.4	0.9404	197839	Apache Tomcat 8.0.0.RC1 < 8.0.39 multiple vulnerabilities
CRITICAL	9.8	6.7	0.5303	111067	Apache Tomcat 8.0.0.RC1 < 8.0.53 multiple vulnerabilities
CRITICAL	9.8	8.9	0.9447	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	9.5	0.9447	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check)
CRITICAL	9.1	5.2	0.0054	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.1	6.0	0.0105	197850	Apache Tomcat 8.0.0.RC1 < 8.0.37 multiple vulnerabilities
CRITICAL	9.1	5.2	0.2176	197857	Apache Tomcat 8.0.0.RC1 < 8.0.42
CRITICAL	9.0	6.5	0.2314	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	0.9443	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	-	171356	Apache HTTP Server SEoL (2.1.x <= x <= 2.2.x)
CRITICAL	10.0	-	-	171342	Apache Tomcat SEoL (8.0.x)
CRITICAL	10.0	-	-	58987	PHP Unsupported Version Detection

CRITICAL	10.0	-	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	5.9	0.505	60085	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities
HIGH	8.1	8.9	0.9439	103697	Apache Tomcat 8.0.0.RC1 < 8.0.47
HIGH	8.1	9.8	0.9443	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)
HIGH	7.5	3.6	0.5469	193422	Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability
HIGH	7.5	3.6	0.1508	193423	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
HIGH	7.5	3.6	0.0139	193424	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)
HIGH	7.5	4.4	0.8196	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	4.4	0.0035	193419	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)
HIGH	7.5	4.4	0.8849	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	4.4	0.4296	197829	Apache Tomcat 8.0.0.RC1 < 8.0.36
HIGH	7.5	3.6	0.0892	197846	Apache Tomcat 8.0.0.RC1 < 8.0.41
HIGH	7.5	3.6	0.0268	99367	Apache Tomcat 8.0.0.RC1 < 8.0.43
HIGH	7.5	4.4	0.0957	197837	Apache Tomcat 8.0.0.RC1 < 8.0.44
HIGH	7.5	3.6	0.1244	121124	Apache Tomcat 8.0.0.RC1 < 8.0.52
HIGH	7.5	-	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	4.2	0.0815	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	5.1	0.3833	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	7.3	0.9113	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
HIGH	7.3	6.7	0.8915	77531	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
HIGH	7.3	3.4	0.04	10547	Microsoft Windows LAN Manager SNMP LanMan Services Disclosure
HIGH	7.3	5.9	0.0333	66584	PHP 5.3.x < 5.3.23 Multiple Vulnerabilities
HIGH	7.3	4.2	0.4829	71426	PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities

HIGH	7.3	6.0	0.5625	77285	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities
HIGH	7.0	5.9	0.0732	62101	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities
HIGH	9.3*	9.6	0.8839	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	7.5*	7.4	0.926	59056	PHP 5.3.x < 5.3.13 CGI Query String Code Execution
HIGH	7.5*	7.3	0.1383	59529	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities
HIGH	7.5*	5.9	0.0333	64992	PHP 5.3.x < 5.3.22 Multiple Vulnerabilities
HIGH	7.5*	8.9	0.9442	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	6.0	0.9233	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.8	6.0	0.1658	90510	MS16-047: Security Update for SAM and LSAD Remote Protocol (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	4.4	0.1958	106976	Apache Tomcat 8.0.0.RC1 < 8.0.50 multiple vulnerabilities
MEDIUM	6.5	2.5	0.0427	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
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	5.9	6.1	0.7957	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.6	5.9	0.4044	68915	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
MEDIUM	5.3	6.7	0.9023	57791	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities
MEDIUM	5.3	3.0	0.6143	64912	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
MEDIUM	5.3	1.4	0.3783	73405	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
MEDIUM	5.3	1.4	0.0019	193420	Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	4.0	0.8269	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	3.4	0.04	10546	Microsoft Windows LAN Manager SNMP LanMan Users Disclosure
MEDIUM	5.3	-	-	152853	PHP < 7.3.28 Email Header Injection

MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	4.3	1.4	0.0539	102588	Apache Tomcat 8.0.0.RC1 < 8.0.45
MEDIUM	4.0	-	-	58453	Terminal Services Doesn't Use Network Level Authentication (Only)
MEDIUM	5.0*	3.6	0.2356	66842	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities
MEDIUM	6.8*	5.9	0.2032	67259	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	0.1605	58966	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	5.0*	3.4	0.0016	73289	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	4.3*	-	-	57690	Terminal Services Encryption Level is Medium or Low
LOW	3.7	1.4	0.0009	159462	Apache Tomcat 8.x < 8.5.78 Spring4Shell CVE-2021-43980
LOW	2.1*	2.9	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	-	-	21186	AJP Connector Detection
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39446	Apache Tomcat Detection
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection

INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	14274	Nessus SNMP Scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	66173	RDP Screenshot
INFO	N/A	-	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	-	35296	SNMP Protocol Version Detection
INFO	N/A	-	-	19763	SNMP Query Installed Software Disclosure
INFO	N/A	-	-	34022	SNMP Query Routing Information Disclosure
INFO	N/A	-	-	10550	SNMP Query Running Process List Disclosure
INFO	N/A	-	-	10800	SNMP Query System Information Disclosure
INFO	N/A	-	-	10551	SNMP Request Network Interfaces Enumeration
INFO	N/A	-	-	185519	SNMP Server Detection
INFO	N/A	-	-	40448	SNMP Supported Protocols Detection

INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	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	-	-	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	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	20094	VMware Virtual Machine 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

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