W12D4 – Second Scan –-> Metasploitable

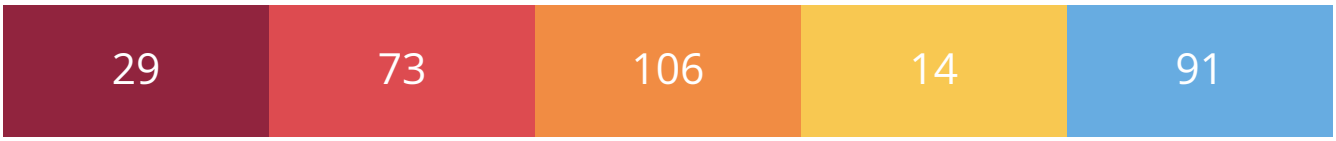
Report generated by Tenable Nessus™ Mon, 10 Feb 2025 04:26:34 CET

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

Epic-Metasploitable.epicode



Vulnerabilities Total: 313

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.1124	57603	Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow
CRITICAL	9.8	9.0	0.9713	45004	Apache 2.2.x < 2.2.15 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.4667	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabiliti
CRITICAL	9.8	6.7	0.4667	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.1741	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0094	193421	Apache 2.4.x < 2.4.54 Authentication Bypass
CRITICAL	9.8	6.7	0.01	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0114	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	9.0	0.9569	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	7.4	0.013	94403	Default Password 'service' for 'service' Account
CRITICAL	9.8	-	-	86072	ISC BIND Unsupported Version Detection
CRITICAL	9.8	-	-	57558	MySQL Unsupported Version Detection
CRITICAL	9.8	6.7	0.0078	90022	OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security By
CRITICAL	9.8	6.7	0.0399	178910	OpenSSH < 9.3p2 Vulnerability
CRITICAL	9.8	7.4	0.0185	169505	Samba < 4.15.13 / 4.16.x < 4.16.8 / 4.17.x < 4.17.4 Multiple Vulnerabilities
CRITICAL	9.8	5.9	0.0081	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	9.1	5.2	0.0132	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.0	6.5	0.0318	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

CRITICAL	9.0	8.1	0.9651	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	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	-	58987	PHP Unsupported Version Detection
CRITICAL	10.0	-	-	63347	PostgreSQL Unsupported Version Detection
CRITICAL	10.0	-	-	76314	Samba Unsupported Version Detection
CRITICAL	10.0*	5.1	0.2056	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.2056	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	7.4	0.8334	50544	ProFTPD < 1.3.3c Multiple Vulnerabilities
CRITICAL	10.0*	7.4	0.881	58662	Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflo
CRITICAL	10.0*	7.4	0.9359	25217	Samba < 3.0.25 Multiple Vulnerabilities
HIGH	8.8	5.9	0.0058	63349	PostgreSQL 7.4 < 7.4.29 / 8.0 < 8.0.25 / 8.1 < 8.1.21 / 8.2 < 8.2.1 8.3 < 8.3.11 / 8.4 < 8.4.4 Multiple Vulnerabilities
HIGH	8.8	7.3	0.0116	63353	PostgreSQL 8.3 < 8.3.19 / 8.4 < 8.4.12 / 9.0 < 9.0.8 / 9.1 < 9.1.4 Multiple Vulnerabilities
HIGH	8.8	5.9	0.9339	122058	Samba < 3.4.0 Remote Code Execution Vulnerability
HIGH	8.8	6.7	0.0171	168018	Samba < 4.15.12, 4.16.x < 4.16.7, and 4.17.x < 4.17.3 32-Bit Sys Buffer Overflow
HIGH	8.8	7.4	0.9517	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	4.4	0.8396	89999	ISC BIND 9 Multiple DoS
HIGH	8.6	5.2	0.0053	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	8.3	-	-	42424	CGI Generic SQL Injection (blind)
HIGH	8.2	6.4	0.358	40467	Apache 2.2.x < 2.2.12 Multiple Vulnerabilities
HIGH	8.1	6.7	0.5563	96450	Apache 2.2.x < 2.2.32 Multiple Vulnerabilities (httpoxy)
HIGH	7.8	6.7	0.1177	100996	ISC BIND 9.x.x < 9.9.10-P1 / 9.10.x < 9.10.5-P1 / 9.11.x < 9.11.1 Multiple Vulnerabilities

HIGH	7.8	5.9	0.0688	93194	OpenSSH < 7.3 Multiple Vulnerabilities
HIGH	7.7	6.6	0.9696	55976	Apache HTTP Server Byte Range DoS
HIGH	7.5	3.6	0.004	193422	Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability
HIGH	7.5	3.6	0.1578	193423	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
HIGH	7.5	3.6	0.02	193424	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)
HIGH	7.5	4.4	0.0013	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	3.6	0.0574	193419	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)
HIGH	7.5	4.4	0.0019	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	3.6	0.7753	96625	ISC BIND 9 < 9.9.9-P5 / 9.9.9-S7 / 9.10.4-P5 / 9.11.0-P2 Multiple
HIGH	7.5	3.6	0.9292	94577	ISC BIND 9 Recursive Response DNAME Record Handling DoS
HIGH	7.5	5.1	0.0465	190444	ISC BIND 9.0.0 < 9.16.48 / 9.9.3-S1 < 9.16.48-S1 / 9.18.0 < 9.18.24 / 9.18.11-S1 < 9.18.24-S1 / 9.19.0 < 9.19.21 Vulnerabilit (cve-2023-50387)
HIGH	7.5	4.4	0.0005	190462	ISC BIND 9.0.0 < 9.16.48 / 9.9.3-S1 < 9.16.48-S1 / 9.18.0 < 9.18.24 / 9.18.11-S1 < 9.18.24-S1 / 9.19.0 < 9.19.21 Vulnerabilit (cve-2023-50868)
HIGH	7.5	4.4	0.0005	181670	ISC BIND 9.2.0 < 9.16.44 / 9.9.3-S1 < 9.16.44-S1 / 9.18.0 < 9.18.19 / 9.18.0-S1 < 9.18.19-S1 / 9.19.0 < 9.19.17 Vulnerability (cve-2023-3341)
HIGH	7.5	4.4	0.0004	190463	ISC BIND 9.9.3-S1 < 9.16.48-S1 / 9.0.0 < 9.16.48 / 9.16.8-S1 < 9.16.48-S1 / 9.18.0 < 9.18.24 / 9.18.11-S1 < 9.18.24-S1 / 9.19.0 9.19.21 Vulnerability (cve-2023-4408)
HIGH	7.5	3.6	0.9518	87502	ISC BIND 9.x < 9.9.8-P2 / 9.10.x < 9.10.3-P2 Response Parsing Attribute Handling DoS
HIGH	7.5	3.6	0.1441	94611	ISC BIND 9.x < 9.9.9-P3 Options Sections DoS
HIGH	7.5	3.6	0.0208	149211	ISC BIND DNAME Recursion DoS (CVE-2021-25215)
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	-	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	3.6	0.005	106755	ProFTPD < 1.3.5b / 1.3.6x < 1.3.6rc2 weak Diffie-Hellman key

HIGH	7.5	5.9	0.0489	90508	Samba 3.x < 4.2.10 / 4.2.x < 4.2.10 / 4.3.x < 4.3.7 / 4.4.x < 4.4.1 Multiple Vulnerabilities (Badlock)
HIGH	7.5	5.9	0.0489	90509	Samba Badlock Vulnerability
HIGH	7.3	6.7	0.499	42052	Apache 2.2.x < 2.2.14 Multiple Vulnerabilities
HIGH	7.3	6.7	0.9575	77531	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
HIGH	7.3	6.7	0.1089	96151	OpenSSH < 7.4 Multiple Vulnerabilities
HIGH	7.3	5.9	0.0099	63355	PostgreSQL 8.3 < 8.3.18 Multiple Vulnerabilities
HIGH	7.3	4.2	0.0034	106750	ProFTPD 1.3.1 SQL injection protection bypass
HIGH	7.0	5.9	0.0038	62101	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities
HIGH	7.0	4.7	0.9608	88385	ISC BIND 9.3.0 < 9.9.8-P3 / 9.9.x-Sx < 9.9.8-S4 / 9.10.x < 9.10.3- Multiple DoS
HIGH	7.5*	-	-	39465	CGI Generic Command Execution
HIGH	7.5*	-	-	39469	CGI Generic Remote File Inclusion
HIGH	7.8*	3.6	0.1022	62562	ISC BIND 9 DNS RDATA Handling DoS
HIGH	7.8*	3.6	0.0949	60120	ISC BIND 9 Multiple Denial of Service Vulnerabilities
HIGH	7.8*	3.6	0.7196	79861	ISC BIND 9 Multiple DoS Vulnerabilities
HIGH	8.5*	3.6	0.9038	59446	ISC BIND 9 Zero-Length RDATA Section Denial of Service / Information Disclosure
HIGH	7.8*	3.7	0.9641	85896	ISC BIND 9.0.x < 9.9.7-P3 / 9.10.x < 9.10.2-P4 Multiple DoS
HIGH	7.8*	8.1	0.9669	85241	ISC BIND 9.7.x < 9.9.7-P2 / 9.10.x < 9.10.2-P3 TKEY Query Hanc Remote DoS
HIGH	7.8*	5.9	0.3322	62119	ISC BIND Assertion Error Resource Record RDATA Query Parsi Remote DoS
HIGH	8.5*	6.7	0.1739	17804	MySQL < 5.0.83 Denial of Service
HIGH	7.5*	7.4	0.9577	17835	MySQL < 5.0.90 / 5.1.43 / 5.5.0-m2 Multiple Buffer Overflows
HIGH	7.5*	7.3	0.9741	34159	MySQL Community Server 5.0 < 5.0.67 Multiple Vulnerabilities
HIGH	7.5*	6.3	0.0157	44081	OpenSSH < 5.7 Multiple Vulnerabilities

HIGH	7.5*	5.3	0.0364	73079	OpenSSH < 6.6 Multiple Vulnerabilities
HIGH	8.5*	3.4	0.0092	84638	OpenSSH < 6.9 Multiple Vulnerabilities
HIGH	7.5*	6.7	0.162	35043	PHP 5 < 5.2.7 Multiple Vulnerabilities
HIGH	7.5*	6.7	0.0368	48244	PHP 5.2 < 5.2.14 Multiple Vulnerabilities
HIGH	7.5*	6.7	0.0218	41014	PHP < 5.2.11 Multiple Vulnerabilities
HIGH	7.5*	7.4	0.7069	32123	PHP < 5.2.6 Multiple Vulnerabilities
HIGH	7.5*	6.3	0.0032	35067	PHP < 5.2.8 Multiple Vulnerabilities
HIGH	7.5*	9.0	0.9569	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	6.3	0.8473	57537	PHP < 5.3.9 Multiple Vulnerabilities
HIGH	7.5*	9.0	0.9569	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	9.0*	6.7	0.0176	56956	ProFTPD < 1.3.3g / 1.3.4 Response Pool Use-After-Free Code Execution
HIGH	7.5*	7.4	0.9706	47036	Samba 3.x < 3.3.13 SMB1 Packet Chaining Memory Corruption
HIGH	7.5*	5.9	0.8775	49228	Samba 3.x < 3.5.5 / 3.4.9 / 3.3.14 sid_parse Buffer Overflow
HIGH	7.5*	5.8	0.0304	24685	Samba < 3.0.24 Multiple Flaws
HIGH	9.3*	6.7	0.9617	28228	Samba < 3.0.27 Multiple Vulnerabilities
HIGH	9.3*	6.7	0.9718	29253	Samba < 3.0.28 send_mailslot Function Remote Buffer Overflo
HIGH	7.5*	6.0	0.9599	32476	Samba < 3.0.30 receive_smb_raw Function Remote Buffer Ove
HIGH	7.5*	6.1	0.0351	17210	TWiki ImageGalleryPlugin Shell Command Injection
HIGH	7.5*	6.7	0.0294	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary Code Injection (PMASA-2009-4)
HIGH	7.5*	7.3	0.9741	17814	yaSSL 1.7.5 Buffer Overflow
MEDIUM	6.8	5.2	0.8396	89998	ISC BIND 9 Multiple DoS
MEDIUM	6.8	6.1	0.004	159491	OpenSSH < 8.0
MEDIUM	6.5	4.4	0.004	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

MEDIUM	6.5	3.6	0.0056	119264	ISC BIND 9.x.x < 9.11.5 / 9.12.x < 9.12.3 Policy-Bypass Record Update Vulnerability
MEDIUM	6.5	4.4	0.0179	106679	ISC BIND Zone Data Denial of Service
MEDIUM	6.5	6.1	0.9548	187201	OpenSSH < 9.6 Multiple Vulnerabilities
MEDIUM	6.5	6.5	0.0021	63354	PostgreSQL 8.3 < 8.3.20 / 8.4 < 8.4.13 / 9.0 < 9.0.9 / 9.1 < 9.1.5 Multiple Vulnerabilities
MEDIUM	6.5	2.5	0.005	106752	ProFTPD < 1.3.2b / 1.3.3x < 1.3.3rc2 client-hostname restrictio bypass
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	4.4	0.0015	183023	Samba < 4.17.12 / 4.18.x < 4.18.8 / 4.19.x < 4.19.1 Incorrect Permissions Handling
MEDIUM	6.5	4.4	0.8069	129696	phpMyAdmin <= 4.9.1 Cross-Site Request Forgery Vulnerabilit
MEDIUM	6.4	3.8	0.0121	90023	OpenSSH < 7.2p2 X11Forwarding xauth Command Injection
MEDIUM	6.3	5.9	0.0384	63348	PostgreSQL 7.4 < 7.4.27 / 8.0 < 8.0.23 / 8.1 < 8.1.19 / 8.2 < 8.2. 8.3 < 8.3.9 / 8.4 < 8.4.2 Multiple Vulnerabilities
MEDIUM	6.3	3.4	0.0353	63350	PostgreSQL 7.4 < 7.4.30 / 8.0 < 8.0.26 / 8.1 < 8.1.22 / 8.2 < 8.2. 8.3 < 8.3.12 / 8.4 < 8.4.5 / 9.0 < 9.0.1
MEDIUM	6.3	6.5	0.0183	63351	PostgreSQL 8.2 < 8.2.20 / 8.3 < 8.3.14 / 8.4 < 8.4.7 / 9.0 < 9.0.3 Buffer Overflow Vulnerability
MEDIUM	6.3	4.9	0.9359	82580	Samba 3.0.0 'SamrChangePassword' RCE
MEDIUM	6.1	6.7	0.3465	85382	OpenSSH < 7.0 Multiple Vulnerabilities
MEDIUM	6.1	3.8	0.025	10815	Web Server Generic XSS
MEDIUM	6.1	3.0	0.0019	117334	phpMyAdmin < 4.8.3 Vulnerability (PMASA-2018-5)
MEDIUM	5.9	3.6	0.8997	92493	ISC BIND 9.x < 9.9.9-P2 / 9.10.x < 9.10.4-P2 / 9.11.0a3 < 9.11.0 lwres Query DoS
MEDIUM	5.9	4.4	0.9724	136808	ISC BIND Denial of Service
MEDIUM	5.9	-	-	99359	OpenSSH < 7.5
MEDIUM	5.6	4.4	0.5048	68915	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities

MEDIUM	5.6	-	-	58681	PHP 5.2.x filter_globals Subsequence Request Parsing Remote Code Execution
MEDIUM	5.5	3.6	0.0004	106756	ProFTPD < 1.3.5e / 1.3.6x < 1.3.6rc5 AllowChrootSymlinks bypa
MEDIUM	5.3	-	-	83346	.bash_history Files Disclosed via Web Server
MEDIUM	5.3	3.6	0.2873	48205	Apache 2.2.x < 2.2.16 Multiple Vulnerabilities
MEDIUM	5.3	4.4	0.8276	50070	Apache 2.2.x < 2.2.17 Multiple Vulnerabilities
MEDIUM	5.3	4.4	0.9667	53896	Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS
MEDIUM	5.3	2.2	0.494	56216	Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS
MEDIUM	5.3	6.6	0.9702	57791	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities
MEDIUM	5.3	3.0	0.1707	64912	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
MEDIUM	5.3	1.4	0.3357	73405	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
MEDIUM	5.3	4.2	0.221	33477	Apache 2.2.x < 2.2.9 Multiple Vulnerabilities (DoS, XSS)
MEDIUM	5.3	1.4	0.0027	193420	Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)
MEDIUM	5.3	2.2	0.5744	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
MEDIUM	5.3	-	-	106232	Apache ServerTokens Information Disclosure
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	5.3	-	-	39467	CGI Generic Path Traversal
MEDIUM	5.3	4.0	0.0225	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	1.4	0.006	154662	ISC BIND 9.3.0 < 9.11.36 / 9.9.3-S1 < 9.11.36-S1 / 9.12.0 < 9.16.22 / 9.16.8-S1 < 9.16.22-S1 / 9.17.0 < 9.17.19 Vulnerability (CVE-2021-25219)
MEDIUM	5.3	1.4	0.0035	165312	ISC BIND 9.9.3-S1 < 9.16.33-S1 / 9.0.0 < 9.16.33 / 9.16.8-S1 < 9.16.33-S1 / 9.18.0 < 9.18.7 / 9.19.0 < 9.19.5 Vulnerability (cve-2022-2795)
MEDIUM	5.3	1.4	0.0036	103781	OpenSSH < 7.6
MEDIUM	5.3	4.9	0.0331	159490	OpenSSH < 7.8

MEDIUM	5.3	-	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	1.4	0.0172	64669	PostgreSQL 8.3 < 8.3.23 / 8.4 < 8.4.16 / 9.0 < 9.0.12 / 9.1 < 9.1.8 9.2 < 9.2.3 Denial of Service
MEDIUM	5.3	2.2	0.0802	106753	ProFTPD < 1.3.4rc2 client-hostname restriction bypass
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	2.9	0.0143	58751	SSL/TLS Protocol Initialization Vector Implementation Informa Disclosure Vulnerability (BEAST)
MEDIUM	5.3	-	-	121041	Sensitive File Disclosure
MEDIUM	5.3	-	-	88490	Web Server Error Page Information Disclosure
MEDIUM	5.3	-	-	88099	Web Server HTTP Header Information Disclosure
MEDIUM	5.3	-	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	4.3	1.4	0.0015	106751	ProFTPD < 1.3.2rc3 ABOR Denial of Service
MEDIUM	5.0*	-	-	11411	Backup Files Disclosure
MEDIUM	4.3*	-	-	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3*	-	-	49067	CGI Generic HTML Injections (quick test)
MEDIUM	6.8*	-	-	42872	CGI Generic Local File Inclusion (2nd pass)
MEDIUM	5.0*	-	-	46195	CGI Generic Path Traversal (extended test)
MEDIUM	6.4*	-	-	46194	CGI Generic Path Traversal (write test)
MEDIUM	6.8*	-	-	46196	CGI Generic XML Injection
MEDIUM	4.3*	-	-	47831	CGI Generic XSS (comprehensive test)
MEDIUM	4.3*	-	-	55903	CGI Generic XSS (extended patterns)
MEDIUM	4.3*	-	-	39466	CGI Generic XSS (quick test)
MEDIUM	5.0*	3.4	0.0205	62355	ISC BIND Cache Update Policy Deleted Domain Name Resolvir Weakness
MEDIUM	5.0*	5.1	0.955	40422	ISC BIND Dynamic Update Message Handling Remote DoS

MEDIUM	6.8*	5.2	0.0096	56283	Linux Kernel TCP Sequence Number Generation Security Weal
MEDIUM	5.8*	6.7	0.1	42899	MySQL 5.0 < 5.0.88 Multiple Vulnerabilities
MEDIUM	4.0*	3.6	0.0096	57604	MySQL 5.0 < 5.0.95 Multiple Vulnerabilities
MEDIUM	4.0*	4.4	0.0974	17833	MySQL < 5.0.54 / 5.1.23 / 6.0.4 Denial of Service
MEDIUM	4.6*	5.5	0.0008	17812	MySQL < 5.0.88 / 5.1.42 / 5.5.0 / 6.0.14 MyISAM CREATE TABLE Privilege Check Bypass
MEDIUM	5.0*	3.6	0.0798	17834	MySQL < 5.0.92 Multiple Denial of Service
MEDIUM	6.5*	5.9	0.0015	64503	MySQL Binary Log SQL Injection
MEDIUM	6.5*	7.4	0.8863	46702	MySQL Community Server < 5.1.47 / 5.0.91 Multiple Vulnerabi
MEDIUM	6.5*	6.1	0.0521	44079	OpenSSH < 4.9 'ForceCommand' Directive Bypass
MEDIUM	4.0*	6.5	0.6016	44065	OpenSSH < 5.2 CBC Plaintext Disclosure
MEDIUM	5.0*	3.6	0.0787	67140	OpenSSH LoginGraceTime / MaxStartups DoS
MEDIUM	6.9*	6.0	0.0099	31737	OpenSSH X11 Forwarding Session Hijacking
MEDIUM	6.8*	7.7	0.9754	74326	OpenSSL 'ChangeCipherSpec' MiTM Potential Vulnerability
MEDIUM	6.8*	5.8	0.0237	51139	PHP 5.2 < 5.2.15 Multiple Vulnerabilities
MEDIUM	5.0*	4.4	0.0163	51439	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS
MEDIUM	5.1*	4.4	0.0177	39480	PHP < 5.2.10 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	0.0905	43351	PHP < 5.2.12 Multiple Vulnerabilities
MEDIUM	4.4*	6.7	0.0565	28181	PHP < 5.2.5 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	0.0973	35750	PHP < 5.2.9 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	0.0257	58966	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	6.4*	5.3	0.0176	44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
MEDIUM	5.0*	3.4	0.0029	73289	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	5.0*	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	6.8*	6.7	0.1596	51366	ProFTPD < 1.3.3d 'mod_sql' Buffer Overflow
MEDIUM	4.0*	7.3	0.0135	52611	SMTP Service STARTTLS Plaintext Command Injection

MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	5.0*	3.6	0.0324	52503	Samba 3.x < 3.3.15 / 3.4.12 / 3.5.7 'FD_SET' Memory Corruptio
MEDIUM	6.8*	6.7	0.0343	55733	Samba 3.x < 3.3.16 / 3.4.14 / 3.5.10 Multiple Vulnerabilities
MEDIUM	5.0*	4.4	0.9683	69276	Samba 3.x < 3.5.22 / 3.6.x < 3.6.17 / 4.0.x < 4.0.8 read_nttrans_ea_lis DoS
MEDIUM	6.0*	6.6	0.016	41970	Samba < 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 Multiple Vulnerabilities
MEDIUM	5.1*	5.9	0.0425	64459	Samba < 3.5.21 / 3.6.12 / 4.0.2 SWAT Multiple Vulnerabilities
MEDIUM	6.5*	5.9	0.0059	20068	TWiki %INCLUDE Parameter Arbitrary Command Injection
MEDIUM	5.0*	-	-	57640	Web Application Information Disclosure
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3*	3.8	0.2301	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	4.3*	3.0	0.0022	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-20
LOW	3.7	4.5	0.9689	86328	SSH Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	6.5	0.6016	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.1*	2.2	0.8939	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	5.9	0.2545	42983	ISC BIND 9 DNSSEC Cache Poisoning
LOW	2.6*	3.8	0.1054	17811	MySQL < 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 Client XSS
LOW	1.2*	3.6	0.0004	44080	OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
LOW	2.1*	3.4	0.0004	53841	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure
LOW	1.2*	3.6	0.0004	66970	ProFTPD FTP Command Handling Symlink Arbitrary File Overw
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	-	26194	Web Server Transmits Cleartext Credentials
LOW	2.6*	-	-	34850	Web Server Uses Basic Authentication Without HTTPS

LOW	2.6*	-	-	10407	X Server Detection
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	111465	Apache HTTP Server Error Page Detection
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39446	Apache Tomcat Detection
INFO	N/A	-	-	42799	Broken Web Servers
INFO	N/A	-	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	-	39470	CGI Generic Tests Timeout
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	11951	DNS Server Fingerprinting
INFO	N/A	-	-	72779	DNS Server Version Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
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	-	-	14788	IP Protocols Scan

INFO	N/A	-	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosur
INFO	N/A	-	-	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
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 (remo check)
INFO	N/A	-	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	-	50345	Missing or Permissive X-Frame-Options HTTP Response Heade
INFO	N/A	-	-	10719	MySQL Server Detection
INFO	N/A	-	-	10437	NFS Share Export List
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10335	Nessus TCP scanner
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	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	10180	Ping the remote host
INFO	N/A	-	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	110976	PostgreSQL Unauthenticated Version Detection
INFO	N/A	-	-	40665	Protected Web Page Detection
INFO	N/A	-	-	22227	RMI Registry Detection

INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support
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	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
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 (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	19941	TWiki Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
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	-	-	72771	Web Accessible Backups
INFO	N/A	-	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	-	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	-	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	-	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	-	-	91815	Web Application Sitemap
INFO	N/A	-	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	11032	Web Server Directory Enumeration
INFO	N/A	-	-	49705	Web Server Harvested Email Addresses
INFO	N/A	-	-	11419	Web Server Office File Inventory
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	-	10662	Web mirroring
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	17219	phpMyAdmin Detection
INFO	N/A	-	-	11421	smtpscan SMTP Fingerprinting

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