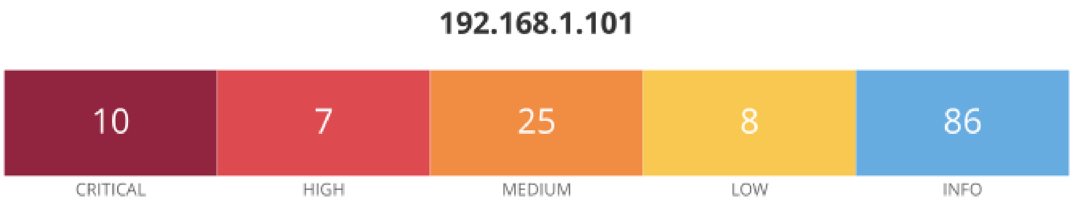
VULNERABILITA’

Dopo aver effettuato una scansione da voi richiesta sul sistema operativo Metasploitable per individuarne le vulnerabilità, i risultati sono:



192.168.1.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
10	7	25	8	86

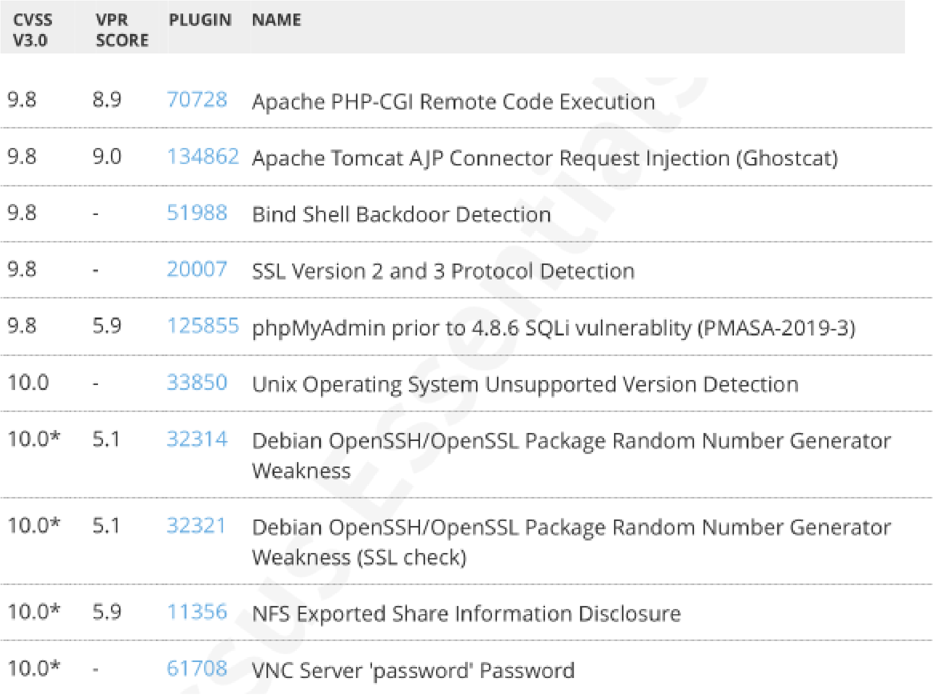
Di seguito, una spiegazione sui vari livelli di criticità:

- **CRITICAL**: Le vulnerabilità critiche sono quelle che rappresentano un rischio elevato e possono essere sfruttate facilmente.
- **HIGH**: Le vulnerabilità con un livello alto indicano rischi significativi, sebbene potrebbero avere una complessità di sfruttamento maggiore rispetto a quelle critiche.
- **MEDIUM**: Le vulnerabilità di livello medio sono considerate di minore gravità rispetto a quelle di livello critico o alto, ma possono ancora rappresentare una minaccia significativa per la sicurezza se sfruttate.
- LOW: Le vulnerabilità di livello basso sono considerate meno critiche e hanno un impatto limitato sulla sicurezza.
- INFO: Questo livello è assegnato a problemi che non rappresentano una vera vulnerabilità, ma forniscono informazioni utili sull'ambiente, come dettagli sul sistema operativo o sulle configurazioni di rete.

A seguire nel report, sono indicate le vulnerabilità, divise in quattro colonne:

- **CSVV v3.0:** Il CVSS (Common Vulnerability Scoring System) è uno standard industriale per valutare e assegnare un punteggio numerico alle vulnerabilità delle informazioni. La versione 3.0 fornisce un modello migliorato e più accurato per valutare il rischio associato alle vulnerabilità.
- **VPR SCORE:** indica la probabilità di sfruttamento di una vulnerabilità.
- **PLUGIN:** componenti software specializzati che ampliano le funzionalità di uno strumento di sicurezza, consentendo di identificare e valutare le potenziali minacce alla sicurezza all'interno di un sistema.
- **NAME:** nome della vulnerabilità

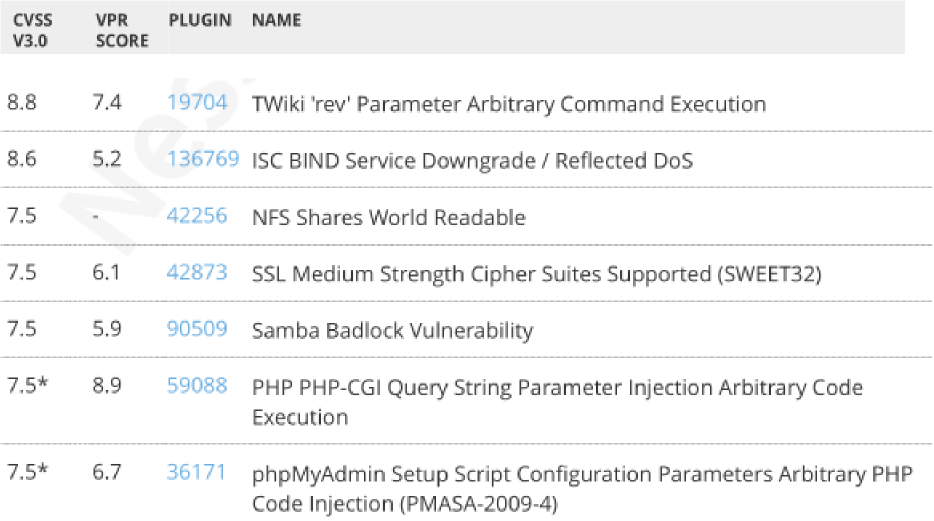
LIVELLO CRITICAL



CVSS V3.0	VPR SCORE	PLUGIN	NAME
9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
9.8	-	51988	Bind Shell Backdoor Detection
9.8	-	20007	SSL Version 2 and 3 Protocol Detection
9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
10.0	-	33850	Unix Operating System Unsupported Version Detection
10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
10.0*	5.9	11356	NFS Exported Share Information Disclosure
10.0*	-	61708	VNC Server 'password' Password

*indica che il punteggio v3.0 non era disponibile; viene mostrato il punteggio v2.0.

LIVELLO HIGH

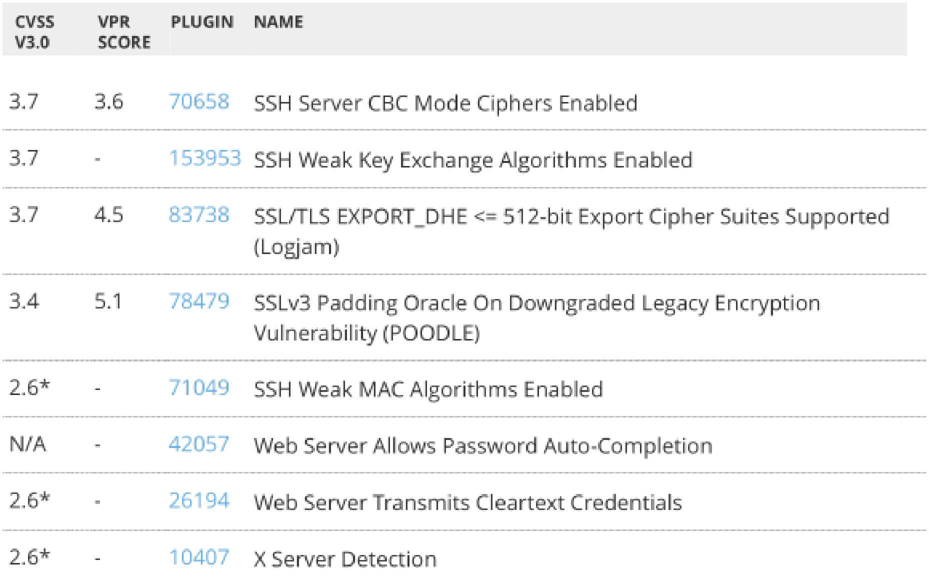


CVSS V3.0	VPR SCORE	PLUGIN	NAME
8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
7.5	-	42256	NFS Shares World Readable
7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
7.5	5.9	90509	Samba Badlock Vulnerability
7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
7.5*	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

LIVELLO MEDIUM

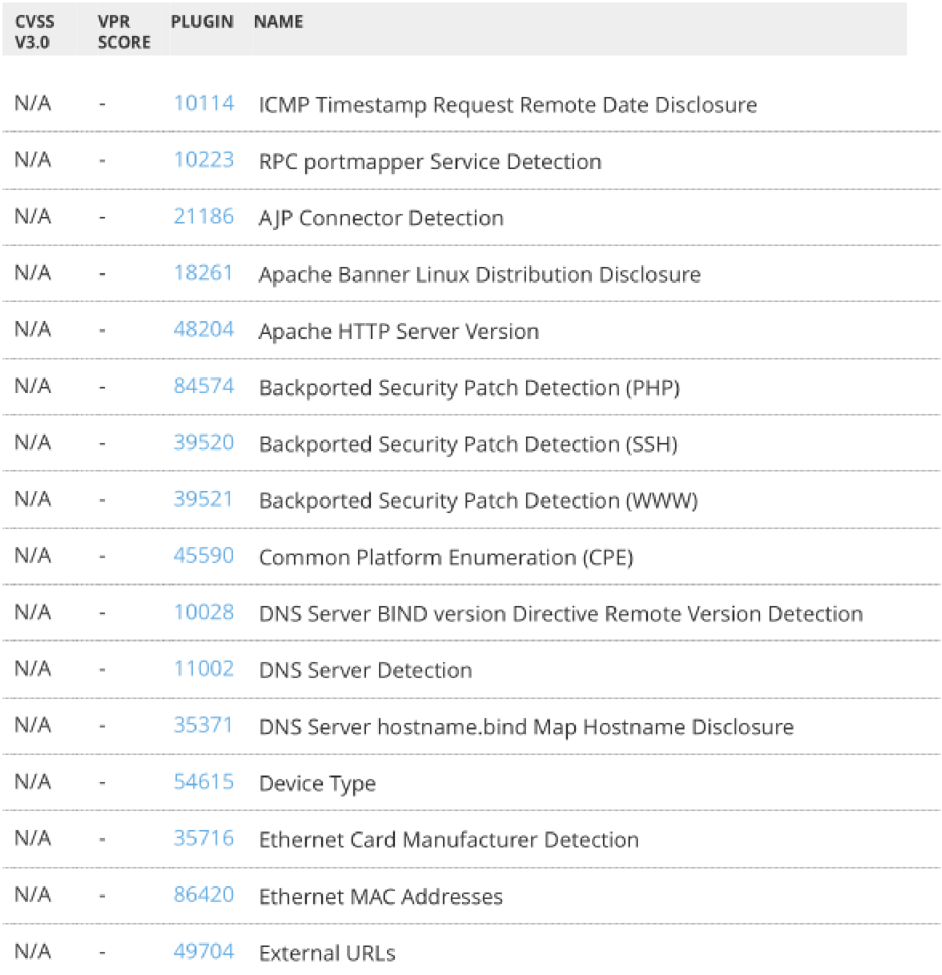
CVSS V3.0	VPR SCORE	PLUGIN	NAME
6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
6.5	-	51192	SSL Certificate Cannot Be Trusted
6.5	-	57582	SSL Self-Signed Certificate
6.5	-	104743	TLS Version 1.0 Protocol Detection
5.9	4.4	136808	ISC BIND Denial of Service
5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
5.3	-	40984	Browsable Web Directories
5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
5.3	-	57608	SMB Signing not required
5.3	-	15901	SSL Certificate Expiry
5.3	-	45411	SSL Certificate with Wrong Hostname
5.3	-	26928	SSL Weak Cipher Suites Supported
5.3	-	11229	Web Server info.php / phpinfo.php Detection
5.0*	-	11411	Backup Files Disclosure
5.0*	-	46803	PHP expose_php Information Disclosure
4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
4.3*	-	90317	SSH Weak Algorithms Supported
4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
4.3*	3.8	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
5.0*	-	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
4.3*	3.0	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)

LIVELLO LOW



CVSS V3.0	VPR SCORE	PLUGIN	NAME
3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
3.7	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
2.6*	-	71049	SSH Weak MAC Algorithms Enabled
N/A	-	42057	Web Server Allows Password Auto-Completion
2.6*	-	26194	Web Server Transmits Cleartext Credentials
2.6*	-	10407	X Server Detection

LIVELLO INFO

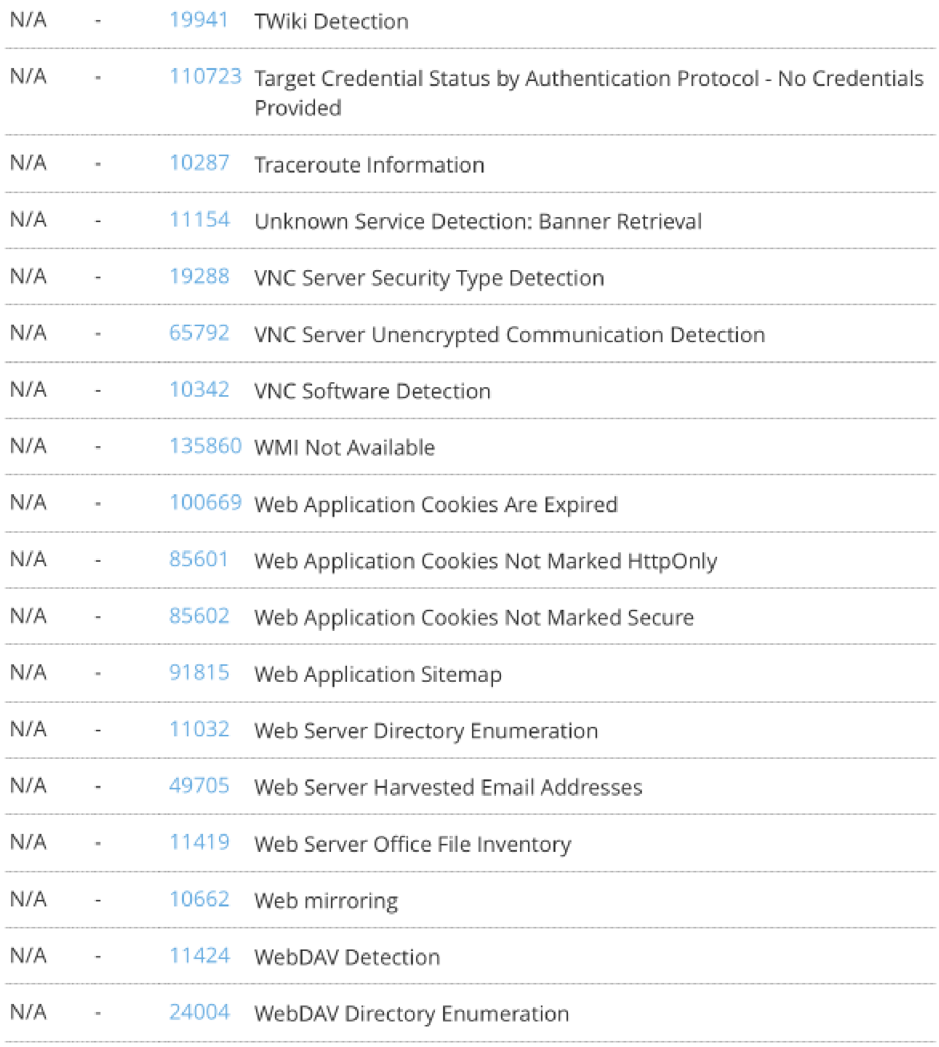


CVSS V3.0	VPR SCORE	PLUGIN	NAME
N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
N/A	-	10223	RPC portmapper Service Detection
N/A	-	21186	AJP Connector Detection
N/A	-	18261	Apache Banner Linux Distribution Disclosure
N/A	-	48204	Apache HTTP Server Version
N/A	-	84574	Backported Security Patch Detection (PHP)
N/A	-	39520	Backported Security Patch Detection (SSH)
N/A	-	39521	Backported Security Patch Detection (WWW)
N/A	-	45590	Common Platform Enumeration (CPE)
N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
N/A	-	11002	DNS Server Detection
N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
N/A	-	54615	Device Type
N/A	-	35716	Ethernet Card Manufacturer Detection
N/A	-	86420	Ethernet MAC Addresses
N/A	-	49704	External URLs

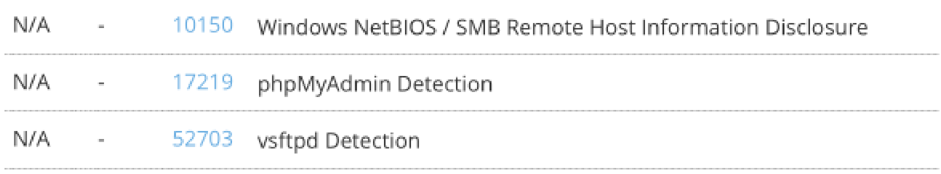
N/A	-	10092	FTP Server Detection
N/A	-	43111	HTTP Methods Allowed (per directory)
N/A	-	10107	HTTP Server Type and Version
N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
N/A	-	11156	IRC Daemon Version Detection
N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
N/A	-	11011	Microsoft Windows SMB Service Detection
N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
N/A	-	10437	NFS Share Export List
N/A	-	19506	Nessus Scan Information
N/A	-	10335	Nessus TCP scanner
N/A	-	11936	OS Identification
N/A	-	117886	OS Security Patch Assessment Not Available
N/A	-	181418	OpenSSH Detection
N/A	-	50845	OpenSSL Detection
N/A	-	48243	PHP Version Detection
N/A	-	66334	Patch Report
N/A	-	118224	PostgreSQL STARTTLS Support
N/A	-	26024	PostgreSQL Server Detection
N/A	-	22227	RMI Registry Detection

N/A	-	11111	RPC Services Enumeration
N/A	-	53335	RPC portmapper (TCP)
N/A	-	10263	SMTP Server Detection
N/A	-	42088	SMTP Service STARTTLS Command Support
N/A	-	70657	SSH Algorithms and Languages Supported
N/A	-	149334	SSH Password Authentication Accepted
N/A	-	10881	SSH Protocol Versions Supported
N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
N/A	-	10267	SSH Server Type and Version Information
N/A	-	56984	SSL / TLS Versions Supported
N/A	-	45410	SSL Certificate 'commonName' Mismatch
N/A	-	10863	SSL Certificate Information
N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
N/A	-	21643	SSL Cipher Suites Supported
N/A	-	62563	SSL Compression Methods Supported
N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
N/A	-	51891	SSL Session Resume Supported

N/A	-	62563	SSL Compression Methods Supported
N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
N/A	-	51891	SSL Session Resume Supported
N/A	-	156899	SSL/TLS Recommended Cipher Suites
N/A	-	25240	Samba Server Detection
N/A	-	104887	Samba Version
N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
N/A	-	22964	Service Detection
N/A	-	11153	Service Detection (HELP Request)
N/A	-	25220	TCP/IP Timestamps Supported
N/A	-	11819	TFTP Daemon Detection



N/A	-	19941	TWiki Detection
N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
N/A	-	10287	Traceroute Information
N/A	-	11154	Unknown Service Detection: Banner Retrieval
N/A	-	19288	VNC Server Security Type Detection
N/A	-	65792	VNC Server Unencrypted Communication Detection
N/A	-	10342	VNC Software Detection
N/A	-	135860	WMI Not Available
N/A	-	100669	Web Application Cookies Are Expired
N/A	-	85601	Web Application Cookies Not Marked HttpOnly
N/A	-	85602	Web Application Cookies Not Marked Secure
N/A	-	91815	Web Application Sitemap
N/A	-	11032	Web Server Directory Enumeration
N/A	-	49705	Web Server Harvested Email Addresses
N/A	-	11419	Web Server Office File Inventory
N/A	-	10662	Web mirroring
N/A	-	11424	WebDAV Detection
N/A	-	24004	WebDAV Directory Enumeration



N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
N/A	-	17219	phpMyAdmin Detection
N/A	-	52703	vsftpd Detection

Di seguito, un link per andare più nello specifico sulle vulnerabilità:

https://kali:8834/#/scans/reports/5/vulnerabilities