ESERCIZIO DI FINE MODULO M3

port scansione completa con Nessus su Metasploitable 2:

Prima di tutto dobbiamo far partire dalla Nostra macchina Kali (192.168.50.100) il servizio Nessus tramite la shell con il comando ***systemctl start nessusd*.** Dopodiché immettiamo questo indirizzo nel nostro browser: https://kali:8834/#/ in modo da iniziare la nostra scansione. Nel frattempo ho fatto ping sulla macchina target **192.168.50.101** per vedere se comunica, ed il risultato è stato **positivo.**

Iniziamo la scansione su Nessus eseguendo le seguenti fasi di ingaggio.

- Nome della scansione
- Indirizzo ip target 192.168.50.101
- Discovery:Port scan: All ports
- Port scanner
- Assesment: Scan type scan for known web vulnerabilities
- Avvio scansione

tenable® Nessus

Scan 1

Report generated by Tenable Nessus™ Mon, 17 Feb 2025 19:35:51 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.50.101

5	23	33	8	92
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 161

SEVERITY	CVSS V2.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	-	51988	Bind Shell Backdoor 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	-	-	61708	VNC Server 'password' Password
HIGH	9.3	8.1	0.9667	156164	Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execu
HIGH	9.3	10.0	0.971	156016	Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)
HIGH	9.3	10.0	0.971	156056	Apache Log4Shell RCE detection via Raw Socket Logging (Direc Check)
HIGH	9.3	10.0	0.971	156115	Apache Log4Shell RCE detection via callback correlation (Direc Check FTP)
HIGH	9.3	10.0	0.971	156014	Apache Log4Shell RCE detection via callback correlation (Direc Check HTTP)
HIGH	9.3	10.0	0.971	156669	Apache Log4Shell RCE detection via callback correlation (Direc Check MSRPC)
HIGH	9.3	10.0	0.971	156197	Apache Log4Shell RCE detection via callback correlation (Direc Check NetBIOS)
HIGH	9.3	10.0	0.971	156559	Apache Log4Shell RCE detection via callback correlation (Direc Check RPCBIND)

HIGH	9.3	10.0	0.971	156232	Apache Log4Shell RCE detection via callback correlation (Direc Check SMB)
HIGH	9.3	10.0	0.971	156132	Apache Log4Shell RCE detection via callback correlation (Direc Check SMTP)
HIGH	9.3	10.0	0.971	156166	Apache Log4Shell RCE detection via callback correlation (Direc Check SSH)
HIGH	9.3	10.0	0.971	156162	Apache Log4Shell RCE detection via callback correlation (Direc Check Telnet)
HIGH	7.5	9.0	0.9569	70728	Apache PHP-CGI Remote Code Execution
HIGH	7.5	8.9	0.974	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
HIGH	7.5	-	-	39465	CGI Generic Command Execution
HIGH	7.5	-	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5	-	-	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	7.4	0.9714	164017	NodeJS System Information Library Command Injection (CVE-2021-21315)
HIGH	7.5	9.0	0.9569	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5	9.5	0.975	159375	Spring Cloud Function SPEL Expression Injection (direct check
HIGH	7.5	7.4	0.9517	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	7.5	6.7	0.0294	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary Code Injection (PMASA-2009-4)
HIGH	7.5	5.9	0.0081	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
MEDIUM	6.8	-	-	42872	CGI Generic Local File Inclusion (2nd pass)
MEDIUM	6.8	5.9	0.0489	90509	Samba Badlock Vulnerability
MEDIUM	6.4	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	-	-	57582	SSL Self-Signed Certificate
MEDIUM	5.0	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.0	-	-	11411	Backup Files Disclosure

MEDIUM	5.0	-	-	40984	Browsable Web Directories
MEDIUM	5.0	-	-	39467	CGI Generic Path Traversal
MEDIUM	5.0	-	-	46195	CGI Generic Path Traversal (extended test)
MEDIUM	5.0	4.0	0.0225	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	5.2	0.0053	136769	ISC BIND Service Downgrade / Reflected DoS
MEDIUM	5.0	-	-	42256	NFS Shares World Readable
MEDIUM	5.0	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	5.0	-	-	57608	SMB Signing not required
MEDIUM	5.0	-	-	15901	SSL Certificate Expiry
MEDIUM	5.0	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	-	-	57640	Web Application Information Disclosure
MEDIUM	5.0	-	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0	-	-	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-200
MEDIUM	4.3	-	-	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3	-	-	49067	CGI Generic HTML Injections (quick test)
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	4.3	4.4	0.9724	136808	ISC BIND Denial of Service
MEDIUM	4.3	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	2.9	0.0143	58751	SSL/TLS Protocol Initialization Vector Implementation Informa Disclosure Vulnerability (BEAST)
MEDIUM	4.3	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3	3.8	0.025	10815	Web Server Generic XSS
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

MEDIUM	4.0	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	4.0	7.3	0.0135	52611	SMTP Service STARTTLS Plaintext Command Injection
LOW	2.6	6.5	0.6016	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6	-	-	71049	SSH Weak MAC Algorithms Enabled
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
LOW	2.1	2.2	0.8939	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	N/A	-	-	42057	Web Server Allows Password Auto-Completion
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	21186	AJP Connector Detection
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39446	Apache Tomcat Detection
INFO	N/A	-	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
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	-	-	72779	DNS Server Version Detection

INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
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	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	14788	IP Protocols Scan
INFO	N/A	-	-	11156	IRC Daemon Version Detection
INFO	N/A	-	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosur
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	-	-	10437	NFS Share Export List
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
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	-	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	-	26024	PostgreSQL Server 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	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	11153	Service Detection (HELP Request)

INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
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	-	-	40405	Web Server Detection (HTTP/1.1)
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	-	-	52703	vsftpd Detection