REPORT VULNERABILITA’ TROVATE SU METASPLOITABLE CON SCANSIONE SU NESSUS

Gentili Dirigenti,

Con il presente rapporto, desidero portare alla vostra attenzione le vulnerabilità critiche e le relative raccomandazioni di mitigazione identificate nel nostro ambiente IT durante una recente analisi di sicurezza condotta con il software Nessus. Questo report fornisce una panoramica delle principali aree di rischio e delle azioni necessarie per proteggere l'azienda da potenziali minacce informatiche.

Nell'ambito della scansione effettuata, sono state identificate un totale di:

11 vulnerabilità critiche

9 vulnerabilità alte

26 vulnerabilità medie

9 vulnerabilità basse

91 informazioni

Ogni categoria di vulnerabilità rappresenta un potenziale punto di ingresso per attacchi informatici che potrebbero compromettere la sicurezza dei nostri sistemi e delle nostre informazioni sensibili. È fondamentale affrontare queste vulnerabilità con urgenza e adottare le misure di sicurezza appropriate per mitigare i rischi associati.

Vulnerability Assessment su Metasploitable

Report generated by Nessus™ Mon, 26 Feb 2024 14:54:05 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.0.108

11	9	26	9	91
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 146

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	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	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
HIGH	7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution

HIGH	7.5*	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection
MEDIUM	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
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	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
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	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	5.3	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0*	-	11411	Backup Files Disclosure
MEDIUM	5.0*	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported

MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3*	3.8	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	5.0*	-	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
MEDIUM	4.3*	3.0	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
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*	-	10407	X Server Detection
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
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	-	39519	Backported Security Patch Detection (FTP)
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	-	45590	Common Platform Enumeration (CPE)

INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	35373	DNS Server DNSSEC Aware Resolver
INFO	N/A	-	11002	DNS Server 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	-	11156	IRC Daemon Version Detection
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
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 (remote 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 Header
INFO	N/A	-	10719	MySQL Server Detection
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	-	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	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	62563	SSL Compression Methods 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	-	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	-	10281	Telnet Server Detection
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	-	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	-	91815	Web Application Sitemap
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	-	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

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

Nel seguito di questo rapporto, verranno presentate le principali vulnerabilità critiche identificate, insieme alle relative soluzioni raccomandate. Si prega di prestare particolare attenzione alle raccomandazioni fornite e di collaborare con il team IT per implementare le misure di sicurezza necessarie.

Vulnerabilità Principali:

Apache PHP-CGI Remote Code Execution (CVE-2012-1823):

Severità: **Critica**

Descrizione: Vulnerabilità di esecuzione remota del codice che potrebbe consentire a un attaccante di eseguire codice malevolo sul server.

Misure correttive: Aggiornare Apache e PHP alla versione più recente. Applicare patch di sicurezza rilasciate dagli sviluppatori.

Apache Tomcat AJP Connector Request Injection (Ghostcat) (CVE-2020-1938):

Severità: **Critica**

Descrizione: Vulnerabilità che potrebbe consentire a un attaccante di leggere o scrivere file sensibili sul server Tomcat.

Misure correttive: Aggiornare Tomcat alla versione più recente. Limitare l'accesso al connettore AJP o disabilitarlo se non è necessario.

Bind Shell Backdoor Detection:

Severità: **Critica**

Descrizione: Rilevata la presenza di una backdoor di shell Bind che potrebbe consentire a un attaccante l'accesso non autorizzato.

Misure correttive: Identificare e rimuovere la backdoor. Rivedere e rafforzare la configurazione di sicurezza.

phpMyAdmin SQL Injection (PMASA-2019-3):

Severità: **Critica**

Descrizione: Vulnerabilità SQL injection in phpMyAdmin che potrebbe consentire a un attaccante di eseguire comandi SQL malevoli.

Misure correttive: Aggiornare phpMyAdmin alla versione più recente. Applicare le patch di sicurezza disponibili.

Misure di Sicurezza Consigliate:

Aggiornamento del Sistema Operativo:

Mantenere il sistema operativo (Debian) e tutti i software aggiornati con le ultime patch di sicurezza.

Aggiornamento dei Software Web:

Mantenere Apache, PHP, Tomcat e altri software web aggiornati per mitigare le vulnerabilità note.

Configurazione Sicura:

Configurare in modo sicuro i servizi e disabilitare quelli non necessari.

Impostare correttamente le autorizzazioni sui file e le directory.

Monitoraggio Attività di Rete:

Implementare un sistema di monitoraggio delle attività di rete per rilevare comportamenti anomali.

Gestione delle Credenziali:

Utilizzare password forti e crittografare le comunicazioni sensibili.

Backup Regolari:

Eseguire backup regolari dei dati importanti per facilitare il ripristino in caso di incidenti.

Conclusione:

Il presente report di valutazione delle vulnerabilità ha evidenziato diverse criticità all'interno dell'infrastruttura, mettendo in luce rischi significativi per la sicurezza dei dati e la stabilità operativa dell'ambiente aziendale. Le vulnerabilità identificate, che spaziano da gravi problemi di sicurezza

informatica a questioni di configurazione errata e versioni obsolete di software, richiedono un'azione immediata per mitigare i rischi e proteggere l'azienda da potenziali minacce esterne e interne.

Affrontare queste vulnerabilità richiederà un impegno completo e coordinato da parte del team IT, in collaborazione con gli stakeholder aziendali pertinenti. È fondamentale stabilire una roadmap chiara e prioritaria per l'applicazione delle misure correttive, con un'attenzione particolare alle vulnerabilità di criticità elevata e ai rischi che potrebbero avere un impatto immediato sulla sicurezza e sulla continuità operativa.

Inoltre, è essenziale implementare una rigorosa politica di gestione delle patch e delle configurazioni, garantendo che tutti i sistemi e le applicazioni siano mantenuti aggiornati e configurati in conformità con le best practice di sicurezza. L'educazione e la formazione del personale sull'importanza della sicurezza informatica e sulle pratiche migliori sono altresì cruciali per mitigare i rischi associati a comportamenti non sicuri e per garantire una cultura aziendale consapevole della sicurezza.

In conclusione, affrontare le vulnerabilità identificate richiede un impegno proattivo e continuo per proteggere l'azienda, i suoi dati e i suoi stakeholder da minacce potenzialmente dannose. Con una pianificazione strategica e un'azione tempestiva, l'azienda può rafforzare significativamente la sua postura di sicurezza informatica e affrontare con successo le sfide della sicurezza nell'era digitale in continua evoluzione.