Manuel Di Gangi

S5_L4

Vulnerability Assessment

22 febbraio 2024

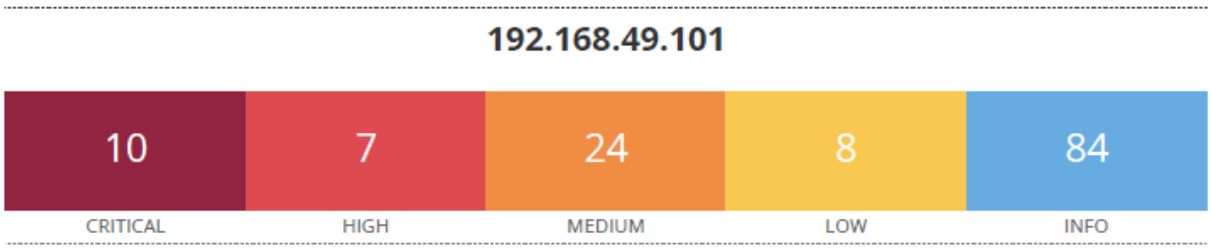
Traccia

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo). A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web. Gli obiettivi dell'esercizio sono:

- Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.
- Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

Risultati della scansione

A seguito della scansione effettuata sulla macchina di Metasploit mediante il programma Nessus, quest'ultimo ha generato il report allegato in fondo alla relazione, di seguito riporto i risultati ottenuti



Analisi - Vulnerabilità critiche

70728 - Apache PHP-CGI Remote Code Execution

Descrizione: L'installazione di PHP sul server web remoto contiene un difetto che potrebbe consentire il passaggio di un utente malintenzionato remoto, inviando argomenti di riga di comando come parte di una query al programma PHP-CGI. Si potrebbe abusare di questo codice eseguito arbitrariamente, rivelare codice sorgente PHP, causare un arresto anomalo del sistema, ecc.

Soluzione: aggiornare PHP alla versione 5.3.13, 5.4.3 o più recenti

134862 - Apache Tomcat A JP Connector Request Injection (Ghostcat)

Descrizione: È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere file di applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile

consenta il caricamento di file, un utente malintenzionato potrebbe caricare al suo interno codice dannoso JavaServer Pages (JSP) codice con una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione: Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat alla versine 7.0.100, 8.5.51,9.0.31 o successiva.

51988 - Bind Shell Backdoor Detection

Descrizione: Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può collegarsi alla porta remota ed inviare comandi direttamente.

Soluzione: Verifica se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

20007 - SSL Version 2 and 3 Protocol Detection

Descrizione: Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

- Uno schema di riempimento non sicuro con cifrari CBC.
- Schemi di rinegoziazione e ripresa delle sessioni non sicuri.

Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i clienti.

Sebbene SSL/TLS disponga di un mezzo sicuro per scegliere la versione più alta supportata del protocollo queste versioni verranno utilizzate solo se il client o il server non supportano niente di meglio), molti browser web potrebbero implementarlo in un modo non sicuro che consenta a un utente malintenzionato di eseguire il downgrade di una connessione.

Soluzione:

- Consultare la documentazione dell'applicazione per disattivare SSL 2.0 e 3.0.
- Utilizza invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.

125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

Descrizione: Secondo il numero di versione riportato, l'applicazione phpMyAdmin ospitata sul web server remoto, è precedente alla versione 4.8.6. È pertanto interessato da una vulnerabilità SQL injection (SQLi) presente nella funzionalità Designer di phpMyAdmin. Un utente malintenzionato remoto non autenticato può sfruttare questa situazione per iniettare o manipolare query SQL nel database back-end, con conseguente divulgazione o manipolazione di dati arbitrari.

Soluzione:

- Aggiornare a phpMyAdmin alla versione 4.8.6 o successiva.
- In alternativa, applicare le patch indicate negli avvisi del fornitore.

33850 - Unix Operating System Unsupported Version Detection

Descrizione: Secondo il numero di versione riportato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.

La mancanza di supporto implica che il fornitore non rilascerà alcuna nuova patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione: Esegui l'upgrade a una versione del sistema operativo Unix attualmente supportata.

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Descrizione: La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel file generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per configurare la decifrazione della sessione remota o impostare un attacco man in the middle.

Soluzione: Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutti gli SSH, SSL e Il materiale delle chiavi OpenVPN deve essere rigenerato.

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Descrizione: Il certificato x509 sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto al fatto che Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per configurare la decifrazione della sessione remota o impostare un attacco man in the middle.

Soluzione: Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutti gli SSH, SSL e Il materiale delle chiavi OpenVPN deve essere rigenerato.

11356 - NFS Exported Share Information Disclosure

Descrizione: Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere controllate dalla un host in scansione. L'attaccante potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto

Soluzione: Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

61708 - VNC Server 'password' Password

Descrizione: Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per prendere il controllo del sistema.

Soluzione: Proteggi il servizio VNC con una password complessa.

Valutazioni finali

In base all'analisi completa condotta sulla sicurezza informatica del sistema, si presentano di seguito le valutazioni finali insieme alle raccomandazioni per migliorare la robustezza complessiva della sicurezza:

Sommario delle Vulnerabilità:

Sono state identificate diverse vulnerabilità, suddivise in quattro categorie principali: critiche, elevate, moderate e basse. Le vulnerabilità critiche rappresentano un rischio significativo per la sicurezza del sistema e richiedono azioni immediate

Valutazione del Rischio:

Il rischio associato alle vulnerabilità è stato valutato considerando l'impatto sulla riservatezza, integrità e disponibilità dei dati. Le vulnerabilità critiche presentano un rischio elevato, mentre quelle di livello moderato richiedono attenzione per prevenire l'aggravamento.

Conclusione:

L'implementazione delle raccomandazioni fornite contribuirà in modo significativo a rafforzare la sicurezza del sistema, riducendo il rischio di violazioni e proteggendo l'integrità delle informazioni. L'impegno continuo verso le migliori pratiche di sicurezza informatica è essenziale per affrontare le minacce in evoluzione.

Report scansione allegato:

Prima_Scansione

Report generated by Nessus™ Thu, 22 Feb 2024 09:07:26 EST

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.49.101.....4

Vulnerabilities by Host

192.168.49.101

10	7	24	8	84
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 133

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	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	6.7	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)

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	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	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	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	-	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	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
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	-	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	-	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	-	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	-	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