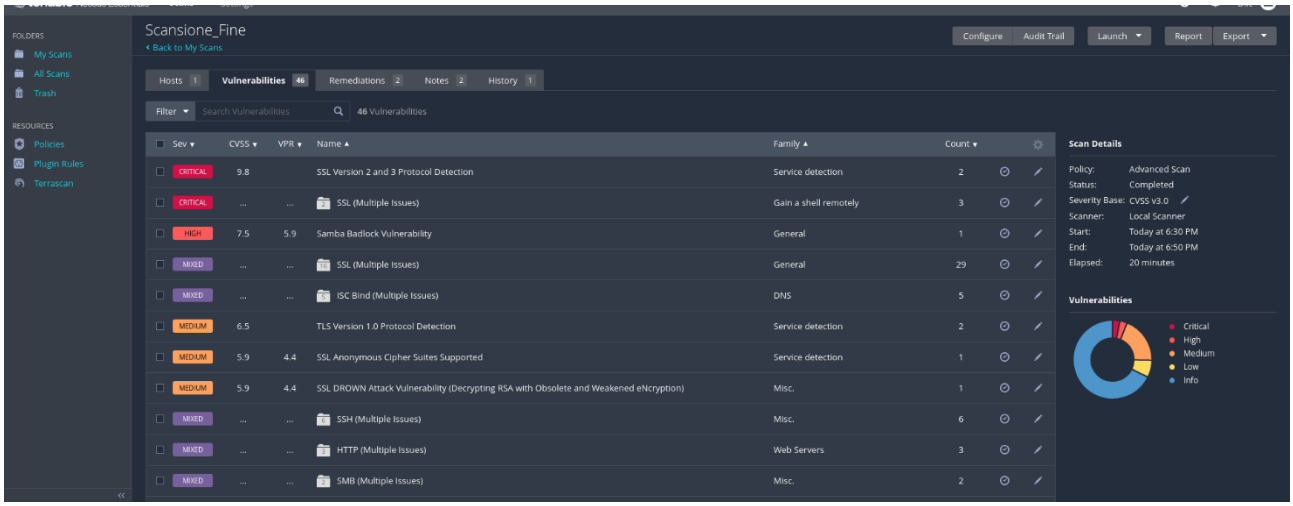
In questo terzo documento confronterò le vulnerabilità critiche individuate nella prima scansione con quelle rilevate nella scansione finale dopo aver effettuato le remediation necessarie.

Nota: la macchina Metasploitable non è connessa a Internet ma è situata su una rete interna. Di conseguenza, molti aggiornamenti non sono stati eseguiti, anche se alcune vulnerabilità potevano essere risolte con un aggiornamento ad una versione più nuova della stessa.



Apache Tomcat AJP Connector Request Injection (Ghostcat)

Stato nella scansione iniziale: presente.

Stato nella scansione finale: non presente.

La vulnerabilità Ghostcat è stata completamente mitigata. Questa azione ha rimosso una criticità significativa che permetteva a un attaccante remoto non autenticato di leggere file delle applicazioni web o eseguire codice remoto.

Bind Shell Backdoor Detection

Stato nella scansione iniziale: presente.

Stato nella scansione finale: non presente.

La backdoor della shell di bind è stata rimossa, indicando che il sistema compromesso è stato verificato e ripristinato correttamente. Questo rimuove un vettore di attacco che permetteva a un attaccante di inviare comandi direttamente al sistema.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Stato nella scansione iniziale: presente.

Stato nella scansione finale: presente.

Questa vulnerabilità rimane, poiché ho preferito non rigenerare che le chiavi SSH e altri materiali crittografici, in quanto si richiedeva un aggiornamento degli stessi. La debolezza nel generatore di numeri casuali di OpenSSL su sistemi Debian o Ubuntu può permettere a un attaccante di ottenere la chiave privata e decifrare le sessioni SSH. È cruciale rigenerare tutte le chiavi per mitigare questo rischio.

SSL Version 2 and 3 Protocol Detection

Stato nella scansione iniziale: presente.

Stato nella scansione finale: presente.

Il servizio continua ad accettare connessioni SSL 2.0 e/o SSL 3.0. Sono a conoscenza che questi protocolli sono affetti da diversi difetti crittografici che possono essere sfruttati per condurre attacchi di tipo man-in-the-middle o per decrittare le comunicazioni. È necessario disabilitare SSL 2.0 e 3.0 e utilizzare TLS 1.2 o versioni superiori per migliorare la sicurezza, ma, anche in questo caso, ho preferito non aggiornare le versioni.

VNC Server 'password' Password

Stato nella scansione iniziale: presente.

Stato nella scansione finale: non presente.

La password debole del server VNC è stata cambiata con una più sicura. Questo rimuove un rischio critico che permetteva l'accesso remoto non autenticato utilizzando la password "password".

NFS Exported Share Information Disclosure

Stato nella scansione iniziale: presente.

Stato nella scansione finale: non presente.

Le condivisioni NFS sono state configurate con le giuste restrizioni per evitare accessi non autorizzati. Questo elimina totalmente la vulnerabilità che permetteva a un attaccante di montare le condivisioni e leggere o scrivere file senza restrizioni.

Considerazioni personali:

Le azioni di remediation intraprese hanno avuto successo nella mitigazione di diverse vulnerabilità critiche, come l'iniezione di richieste nel connettore AJP di Apache Tomcat, la backdoor della shell di bind, la password debole del server VNC e la configurazione delle condivisioni NFS. Tuttavia, rimangono alcune vulnerabilità critiche che richiedono ulteriori interventi:

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness: È essenziale rigenerare tutto il materiale crittografico per assicurare la sicurezza delle comunicazioni SSH e SSL.

SSL Version 2 and 3 Protocol Detection: La disabilitazione dei protocolli SSL 2.0 e 3.0 è cruciale per prevenire attacchi crittografici.

L'analisi delle vulnerabilità rimaste suggerisce che il sistema necessita di ulteriori aggiornamenti e verifiche per assicurare una sicurezza ottimale. È raccomandato continuare a monitorare il sistema con scansioni regolari e aggiornare costantemente le configurazioni di sicurezza.

In conclusione, sicuramente la maggior parte delle vulnerabilità critiche iniziali sono state risolte con successo, indicando un miglioramento significativo nella sicurezza del sistema. Restano però alcune aree di criticità che richiedono attenzione immediata. È importante continuare con le pratiche di sicurezza e gli aggiornamenti regolari per mantenere la sicurezza del sistema a un livello elevato.

In allegato metto il report completo della scansione finale su Nessus, con la lista delle vulnerabilità rilevate, descrizioni dettagliate, rischi associati, soluzioni possibili.

Scansione_Fine

Report generated by Nessus™ Sun, 28 Jul 2024 18:50:34 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.50.101

3	3	16	6	58
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 86

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol 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)
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
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	4.4	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	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
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	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
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	2.9	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	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
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	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses

INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
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	-	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	-	66334	Patch Report
INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server 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	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

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