In questi tre report, condurrò una valutazione completa delle vulnerabilità sul sistema target Metasploitable. L'obiettivo di questo esercizio è identificare le vulnerabilità critiche, implementare azioni di rimedio e successivamente verificare l'efficacia di queste azioni tramite una scansione di controllo. Metasploitable è una macchina virtuale intenzionalmente vulnerabile, comunemente utilizzata per testare strumenti e pratiche di sicurezza.

Il mio approccio si articolerà nei seguenti passaggi:

Scansione iniziale delle vulnerabilità: Eseguirò una scansione esaustiva per identificare tutte le vulnerabilità presenti sul sistema target. Questo comporterà l'uso di strumenti avanzati di scansione per generare un report dettagliato delle debolezze di sicurezza.

Selezione delle vulnerabilità critiche: Dai risultati della scansione iniziale, mi concentrerò su 2 a 4 vulnerabilità critiche. Queste vulnerabilità saranno evidenziate per la loro gravità e il potenziale impatto sul sistema.

Azioni di rimedio: Per ciascuna vulnerabilità critica identificata, implementerò misure di rimedio appropriate. Questo potrebbe includere l'applicazione di patch software, la riconfigurazione dei servizi o l'implementazione di regole firewall per mitigare il rischio. In particolare, dimostrerò l'uso di regole firewall per una delle vulnerabilità per mostrare un approccio di mitigazione a livello di rete.

Scansione di verifica: Dopo aver implementato le azioni di rimedio, eseguirò una scansione di controllo per verificare l'efficacia delle soluzioni adottate. L'obiettivo è confermare che le vulnerabilità precedentemente identificate siano state risolte o mitigate.

Analisi comparativa: Confronterò i risultati delle scansioni iniziale e di controllo per dimostrare i miglioramenti nella postura di sicurezza del sistema. Questo fornirà un'indicazione chiara del successo delle azioni di rimedio.

Le scoperte e i passaggi di rimedio saranno documentati nelle sezioni seguenti, insieme a screenshot e spiegazioni di ciascuna fase del processo. L'obiettivo è non solo migliorare la sicurezza del sistema Metasploitable, ma anche fornire una guida completa su come affrontare vulnerabilità critiche in ambienti simili.

REPORT SCANSIONE INIZIALE

In questo primo documento presento i risultati della scansione iniziale delle vulnerabilità sul sistema target Metasploitable. L'obiettivo principale di questa scansione è identificare tutte le vulnerabilità presenti sul sistema per poi selezionare le vulnerabilità critiche su cui intervenire con azioni di rimedio mirate.

Per eseguire questa scansione ho utilizzato Nessus, uno strumento avanzato di valutazione delle vulnerabilità, su una macchina Kali Linux. La macchina Kali e la macchina target Metasploitable sono poste sulla stessa rete interna, il che consente una comunicazione diretta e senza interferenze esterne, garantendo la precisione e la completezza della scansione.

Ho avviato la scansione completa per rilevare tutte le vulnerabilità note sul sistema Metasploitable. La scansione ha analizzato vari aspetti del sistema, inclusi i servizi in esecuzione, le versioni dei software installati e le configurazioni di sicurezza.

Al termine della scansione, Nessus ha generato un report dettagliato che include tutte le vulnerabilità trovate, classificate per gravità (critica, alta, media, bassa e informativa).

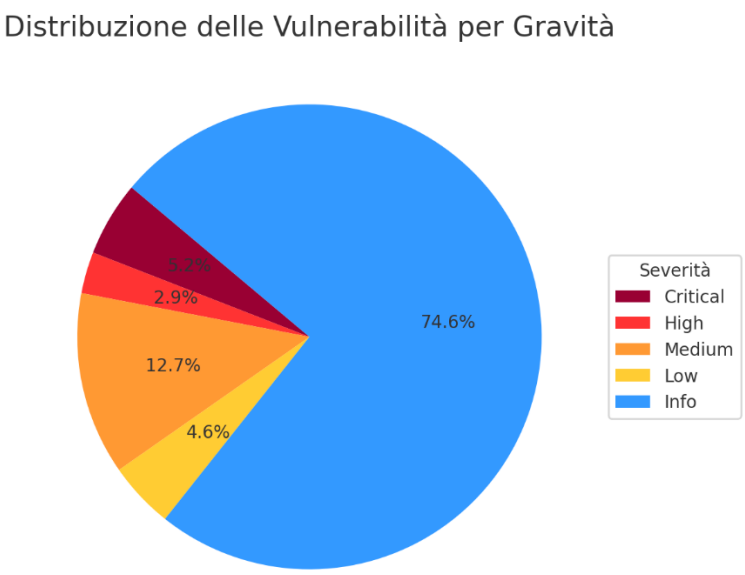
Ho analizzato il report per identificare le vulnerabilità critiche che necessitano di interventi immediati.

Il report generato da Nessus ha rilevato diverse vulnerabilità presenti sul sistema Metasploitable. Di seguito una sintesi delle vulnerabilità individuate:

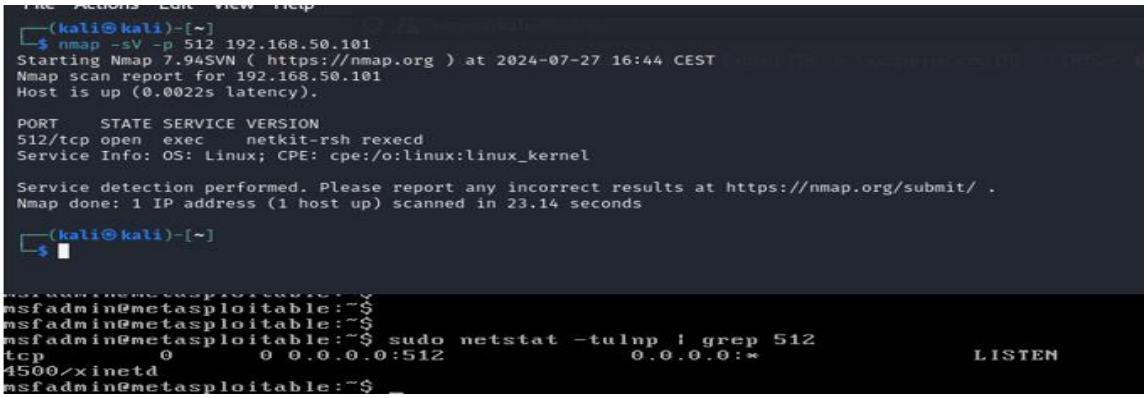
Vulnerabilità Critiche: Include falle di sicurezza che possono essere sfruttate facilmente da attaccanti remoti e che hanno un impatto severo sulla sicurezza del sistema.

Vulnerabilità Alte: Include vulnerabilità con un elevato rischio di exploit che potrebbero compromettere l'integrità, la riservatezza o la disponibilità del sistema.

Vulnerabilità Medie e Basse: Include vulnerabilità che presentano rischi moderati o bassi e che potrebbero richiedere ulteriori condizioni per essere sfruttate.



Nella scansione iniziale, le vulnerabilità critiche identificate sono queste che specificherò di seguito (includono anche quelle evidenziate nell'esercizio, eccetto per la vulnerabilità rexecd Service Detection, che, anche se attiva e con la porta 512 aperta su Metasploite, non viene individuata con lo scan):



NFS Exported Share Information Disclosure (CVE-1999-0170, CVE-1999-0211, CVE-1999-0554): almeno una delle condivisioni NFS esportate dal server remoto può essere montata dall'host di scansione. Un attaccante potrebbe sfruttare questa vulnerabilità per leggere e, possibilmente, scrivere file sul server remoto, esponendo dati sensibili e permettendo la modifica non autorizzata dei file.

VNC Server 'password' Password: un server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad autenticarsi utilizzando la password 'password', permettendo a un attaccante remoto di prendere il controllo del sistema, compromettendo integrità e sicurezza.

Bind Shell Backdoor Detection: una shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un attaccante può utilizzare questa vulnerabilità connettendosi alla porta remota e inviando comandi direttamente, permettendone l'esecuzione sul sitema.

Apache Tomcat AJP Connector Request Injection (Ghostcat) (CVE-2020-1938, CVE-2020-1745): una vulnerabilità nel connettore AJP di Apache Tomcat permette a un attaccante remoto non autenticato di leggere file di applicazioni web da un server vulnerabile e, in alcuni casi, di ottenere l'esecuzione di codice remoto (RCE). Anche in questo caso possono essere letti file sensibili e, potenzialmente, ci può essere l'esecuzione di codice non autorizzato sul server.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (CVE-2008-0166): le chiavi SSH generate su un sistema Debian o Ubuntu affetto da un bug nel generatore di numeri casuali della libreria OpenSSL sono deboli e facilmente compromettibili. Un attaccante può ottenere facilmente la parte privata della chiave remota e utilizzarla per decifrare le sessioni o eseguire

attacchi man-in-the-middle, compromettendo la riservatezza delle comunicazioni.

SSL Version 2 and 3 Protocol Detection (CVE-2014-3566): il servizio remoto accetta connessioni criptate utilizzando SSL 2.0 e/o SSL 3.0, versioni del protocollo SSL affette da diverse vulnerabilità crittografiche note. Un attaccante può sfruttare queste debolezze per condurre attacchi man-in-the-middle o per decifrare le comunicazioni tra il servizio e i client.

Unix Operating System Unsupported Version Detection: il sistema operativo Unix in uso è una versione non supportata. Ciò significa che non riceve più aggiornamenti di sicurezza, esponendo il sistema a potenziali vulnerabilità non risolte.

SSH Server Weak Algorithms Supported: il server SSH remoto è configurato per utilizzare algoritmi di cifratura deboli o nessun algoritmo di cifratura. Questo rende il servizio vulnerabile ad attacchi crittografici, compromettendo la sicurezza delle comunicazioni SSH.

TABELLA RIASSUNTIVA DELLE CRITICITÀ

Vulnerabilità	Descrizione	Gravità
NFS Exported Share Information Disclosure	Esportazione di condivisioni NFS non autorizzate	Critica
VNC Server 'password' Password	Password debole su server VNC	Critica
Bind Shell Backdoor Detection	Shell in ascolto senza autenticazione	Critica
Apache Tomcat AJP Connector Request Injection	Iniezione di richieste nel connettore AJP	Critica
Debian OpenSSH/OpenSSL Package RNG Weakness	Debolezza nel generatore di numeri casuali OpenSSL	Critica
SSL Version 2 and 3 Protocol Detection	Utilizzo di protocolli SSL obsoleti	Critica
Unix OS Unsupported Version Detection	Sistema operativo non supportato	Critica
SSH Server Weak Algorithms Supported	Algoritmi di cifratura deboli o non cifrati	Critica

Allegato

In allegato a questo documento includerò il report riassuntivo delle criticità generato da Nessus, che fornisce una visione dettagliata di tutte le vulnerabilità individuate e classificate per severità. Questo report servirà come base per le azioni di rimedio descritte nei documenti successivi.

SCAN META

Report generated by Nessus™ Sat, 27 Jul 2024 15:52:50 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.50.101

Vulnerabilities Total: 103

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
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	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	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
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
LOW	2.6*	-	10407	X Server Detection
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	-	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	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10092	FTP Server Detection
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	-	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	-	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	-	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	-	11424	WebDAV Detection
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	52703	vsftpd Detection

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