PROGETTO S5/L5

Scansione di Metasploitable per la rilevazione delle vulnerabilità presenti

VULNERABILITÀ DA ANALIZZARE

Da Kali Linux è stata effettuata la scansione su Metasploitable e verranno prese in analisi 3 diverse vulnerabilità secondo la traccia dettata.

Traccia:

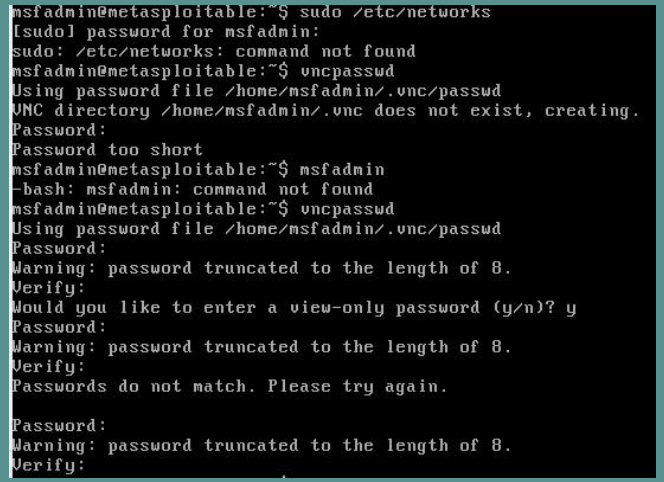
Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

VNC SERVER

CRITICAL	10.0*	-	61708	VNC Server 'password' Password

La prima vulnerabilità da fixare è la password del VNC server. Per risolvere questo problema è necessario inserire una password di almeno 8 caratteri. L'immagine sottostante mostrerà i passaggi. Su Metasploitable digitiamo vncpasswd, poi inseriamo la password e premiamo enter. Dopo aver confermato riavviamo la macchina per salvare le nuove modifiche.



NFS Exported Share Information Disclosure

CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure

La seconda vulnerabilità riguarda NFS. Per risolvere questa vulnerabilità nell'ultima riga scritta del codice è stato sostituito il segno asterisco (*) con l' IP di Metasploitable in modo da far accedere solo quello specifico indirizzo.

Bind Shell Backdoor Detection

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection

L’ultima vulnerabilità da fixare è la backdoor aperta sulla porta 1524.
In questo caso ci sono due possibili soluzioni:

- La prima consiste nell'interruzione del processo tramite il comando “sudo kill” e il numero del processo.
- La seconda possibile soluzione consiste nella configurazione del firewall impostato su block e l’ IP di Metasploitable sulla destinazione

```
msfadmin@metasploitable:/etc$ sudo netstat -tulpn | grep 1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
4623/xinetd
msfadmin@metasploitable:/etc$ sudo kill 4623
msfadmin@metasploitable:/etc$ _
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sS -p 1524 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 08:48 EST
Nmap scan report for 192.168.49.101
Host is up (0.00073s latency).

PORT     STATE  SERVICE
1524/tcp closed ingreslock

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓ 1/274 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
☐	✗ 0/144 B	IPv4 TCP	*	*	192.168.49.101	1524	*	none			⚓ ✎ ⧉ ⊘ 🗑
☐	✓ 0/0 B	IPv6 *	*	*	*	*	*	none		Default allow to any rule	⚓ ✎ ⧉ ⊘ 🗑 ✗
☐	✓ 191/60.07 MiB	IPv4 *	192.168.50.0/24	*	192.168.49.0/24	*	*	none		Default allow LAN to any rule	⚓ ✎ ⧉ ⊘ 🗑 ✗
☐	✗ 0/0 B	IPv4 TCP	192.168.50.100/24	*	192.168.49.101/24	80 (HTTP)	*	none			⚓ ✎ ⧉ ☑ 🗑

SCANSIONE FINALE

192.168.49.101

Vulnerabilities Total: 112

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	-	90509	Samba Badlock Vulnerability
HIGH	7.5*	-	10205	rlogin Service Detection