Progetto 27-10 Alessandro Moscetti

Link scansione iniziale

https://github.com/AlessandroMoscetti/Progetto_Epicode_27-10/blob/main/ScansioneInizio.pdf

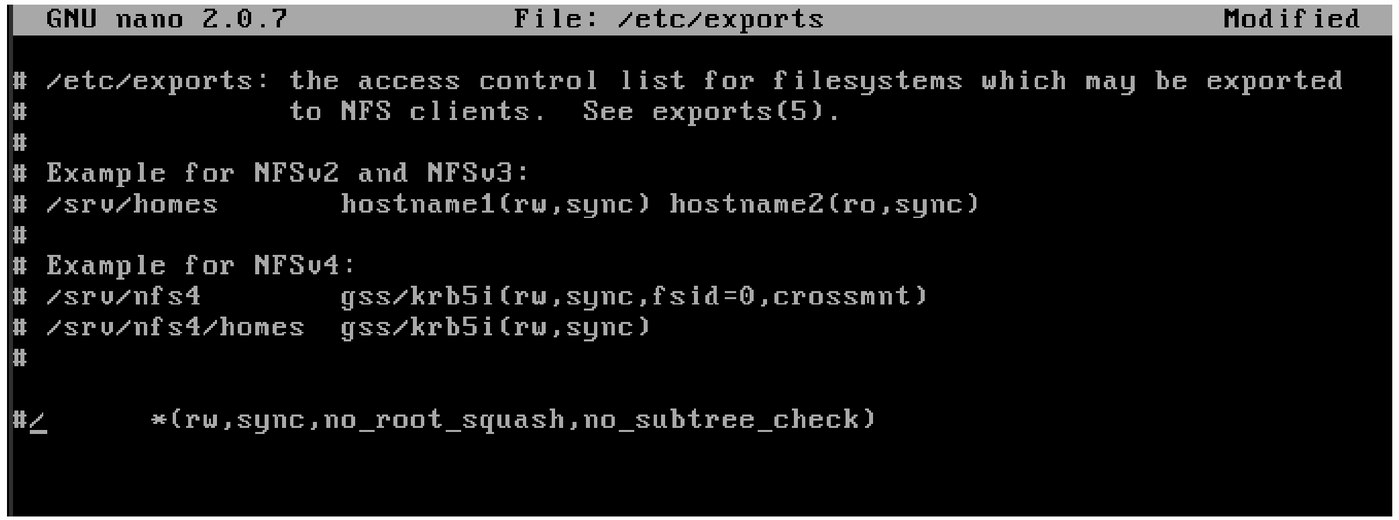
Prima vulnerabilità critica

CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure

Questa vulnerabilità riguarda il server NFS della nostra macchina sulla porta 2049.
NFS sta per Network File System ed è un protocollo di rete consente la condivisione di file su una rete.
Si basa su un client-server, in cui il server fornisce l'accesso alle risorse di file e il client utilizza il protocollo NFS per accedere e manipolare questi file e directory condivisi.
La vulnerabilità riguarda dei file condivisi che un utente malintenzionato potrebbe sfruttare per leggere (ed eventualmente scrivere) file sull'host remoto.

Soluzione

Per risolvere questa vulnerabilità sono andato a vedere con il comando “sudo nano /etc/exports” quali fossero le cartelle condivise dal server.
Come vediamo dall’immagine la cartella di root era in condivisione esponendoci alla vulnerabilità.
Commentando l’ultima riga come nell’immagine e salvando il file, al riavvio del server la cartella non sarà più condivisa.



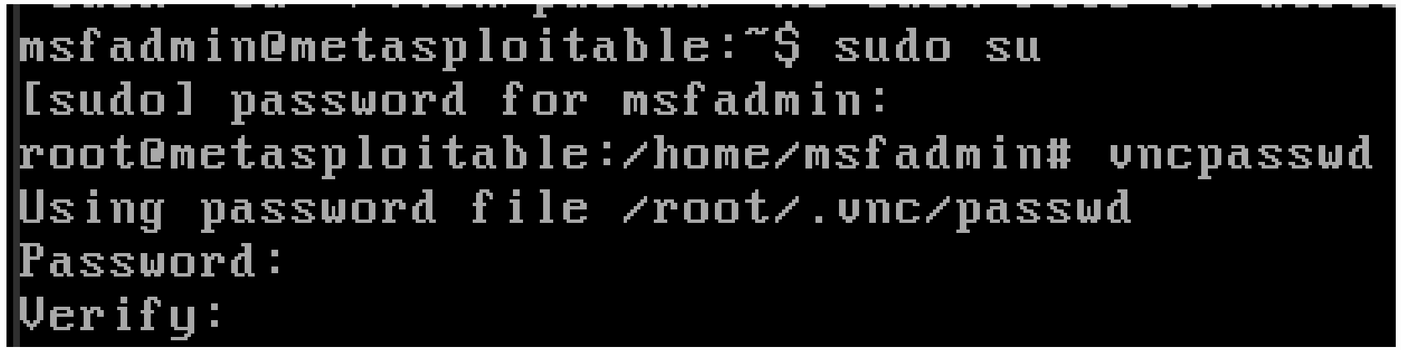
Seconda vulnerabilità critica

CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Questa vulnerabilità riguarda il server VNC della nostra macchina sulla porta 5900.
Un VNC (Virtual Network Computing) server è un'applicazione software che consente di controllare e interagire con un computer desktop da remoto.
Questa vulnerabilità riguarda la password del server settata con “password”.

Soluzione

Per risolvere questa vulnerabilità sono andato a modificare la password del nostro server VNC con il comando “vncpasswd” (con privilegi di amministratore).
Importante modificare la password periodicamente ed utilizzare password sicure.



Terza vulnerabilità critica

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection

Questa vulnerabilità riguarda una backdoor sulla porta 1524. Questa backdoor consente a un malintenzionato di stabilire una connessione remota non autenticata con una shell interattiva sul sistema bersaglio, così facendo può inviare comandi direttamente alla macchina bersaglio senza richiedere autenticazione

Soluzione

Per risolvere questa vulnerabilità sono andato ad inserire una regola nel firewall (iptables) della nostra macchina (fig.1).
Trattandosi di una backdoor in ascolto, sono andato a bloccare le connessioni in input su quella determinata porta.
Il comando nella fig. 2 serve per rendere la modifica nel firewall permanente.
Come possiamo vedere nella fig. 3 scannerizzando con nmap la porta 1524 della nostra macchina Metasploitable, dopo le modifiche effettuate, lo stato appare come “filtered” confermandoci l’effettivo funzionamento della regola del firewall.

1

```
root@metasploitable:/home/msfadmin# iptables -I INPUT -p tcp --dport 1524 -j DRO
P
```

2

```
msfadmin@metasploitable:~$ sudo iptables-save > /etc/iptables/rules.v4
```

3

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -p 1524 192.168.0.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 11:47 CEST
Nmap scan report for 192.168.0.101
Host is up (0.0022s latency).

PORT     STATE    SERVICE
1524/tcp filtered ingreslock

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

Link scansione finale

https://github.com/AlessandroMoscetti/Progetto_Epicode_27-10/blob/main/ScansioneFine.pdf

Grazie per l’attenzione.