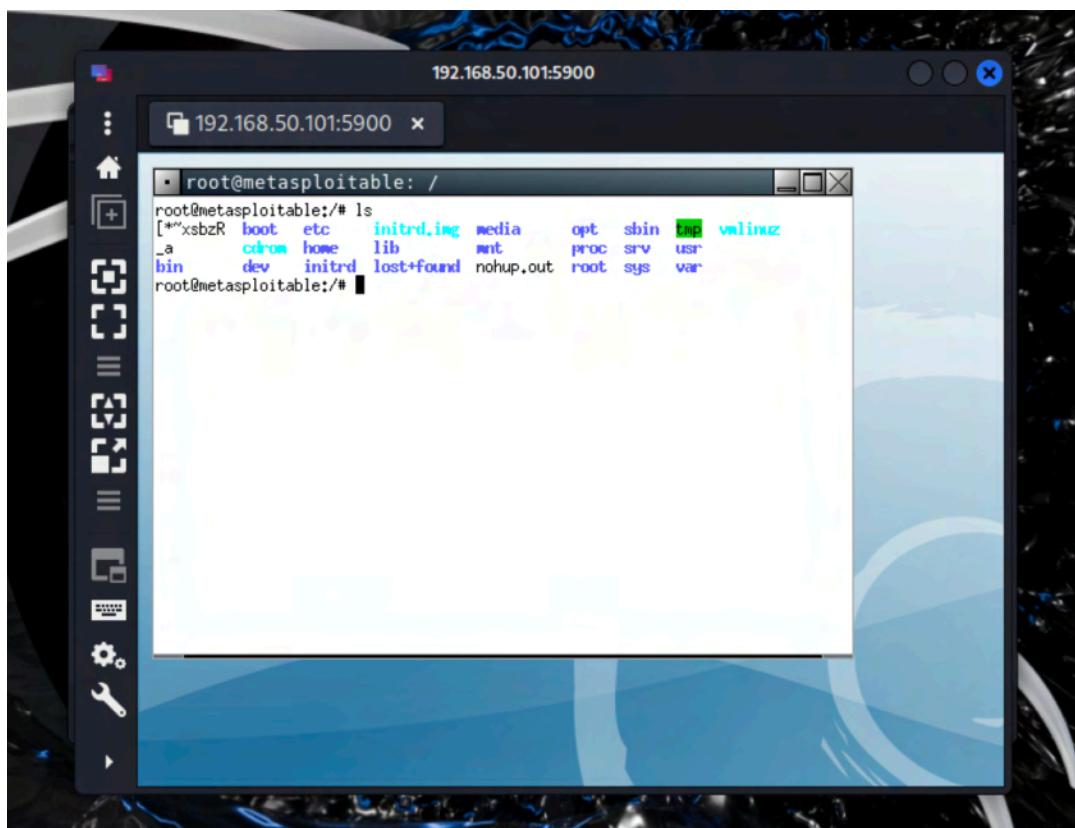


W12D4 - Scansione Nessus

Nella scorsa consegna abbiamo verificato la presenza di numerose vulnerabilità della macchina target Metasploitable2.
L'esercizio di oggi prevede di mitigare queste vulnerabilità , nello specifico quattro vulnerabilità riscontrate.

1. Accesso vnc con ‘password’ come password



Come detto nel report precedente la vulnerabilità riscontrata permette l'accesso tramite porta 5900 in VCN usando la password come credenziale di password.

Il mio obiettivo per mitigare tale vulnerabilità sarà quello di fornire un'altra password e verificarne la correzione.

Innanzitutto voglio scoprire quale processo è in esecuzione su quella porta e lo termino con kill e riavvio il server con la nuova password configurata in precedenza.

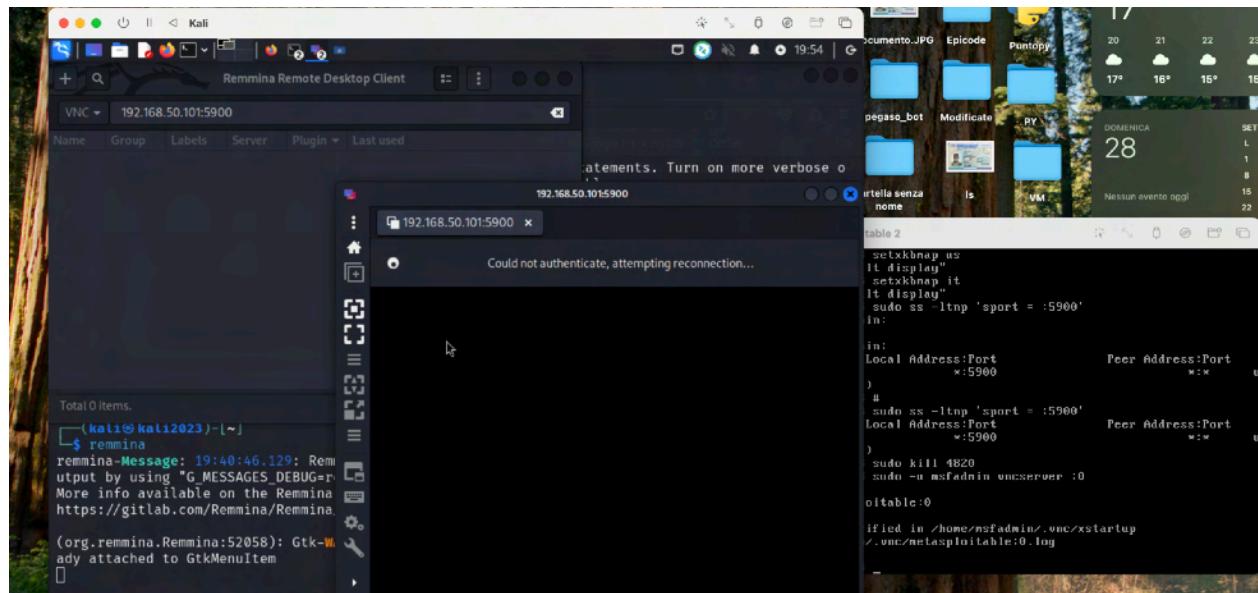
```
0      5                           *:5900          *:*
sers:((Xtightvnc",4820,3))
msfadmin@metasploitable:~$ #
msfadmin@metasploitable:~$ sudo ss -ltnp 'sport = :5900'
Recv-Q Send-Q          Local Address:Port          Peer Address:Por
0      5                           *:5900          *:*
sers:((Xtightvnc",4820,3))
msfadmin@metasploitable:~$ sudo kill 4820
msfadmin@metasploitable:~$ sudo -u msfadmin vncserver :0
```

Ho dovuto fare quest'ulteriore passaggio in quanto lanciando solo i comandi per cambiare password essa non sovrascriveva la vecchia consentendo comunque l'accesso con la vecchia credenziale.

Il comando che mi ha permesso di cambiare password è stato il seguente :

```
sudo: vncpassword: command not found
msfadmin@metasploitable:~$ sudo -u msfadmin vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
```

Infatti verificando nuovamente con remmina l'accesso mi viene negato quando inserisco la vecchia credenziale 'password' e non la nuova password da me impostata.



2. NFS attivo

Questa vulnerabilità sulla porta 2049 risulta aperto di default e procederemo quindi alla chiusura della stessa per evitare possibili attacchi.

Ci limiteremo a lanciare il comando che termini il servizio NFS:

```
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server stop
 * Stopping NFS kernel daemon                                         [ OK ]
 * Unexporting directories for NFS kernel daemon...                 [ OK ]
msfadmin@metasploitable:~$ #
msfadmin@metasploitable:~$
```

Verifico la chiusura della porta con un Nmap da kali verso la mia macchina e sulla quella specifica porta :

```
(kali㉿kali2023)~]$ nmap -sV 192.168.50.101 -p 2049
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 19:29 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0032s latency).

PORT      STATE SERVICE VERSION
2049/tcp   open  nfs      2-4 (RPC #100003)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.26 seconds

(kali㉿kali2023)~]$ nmap -sV 192.168.50.101 -p 2049
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-29 19:39 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0048s latency).

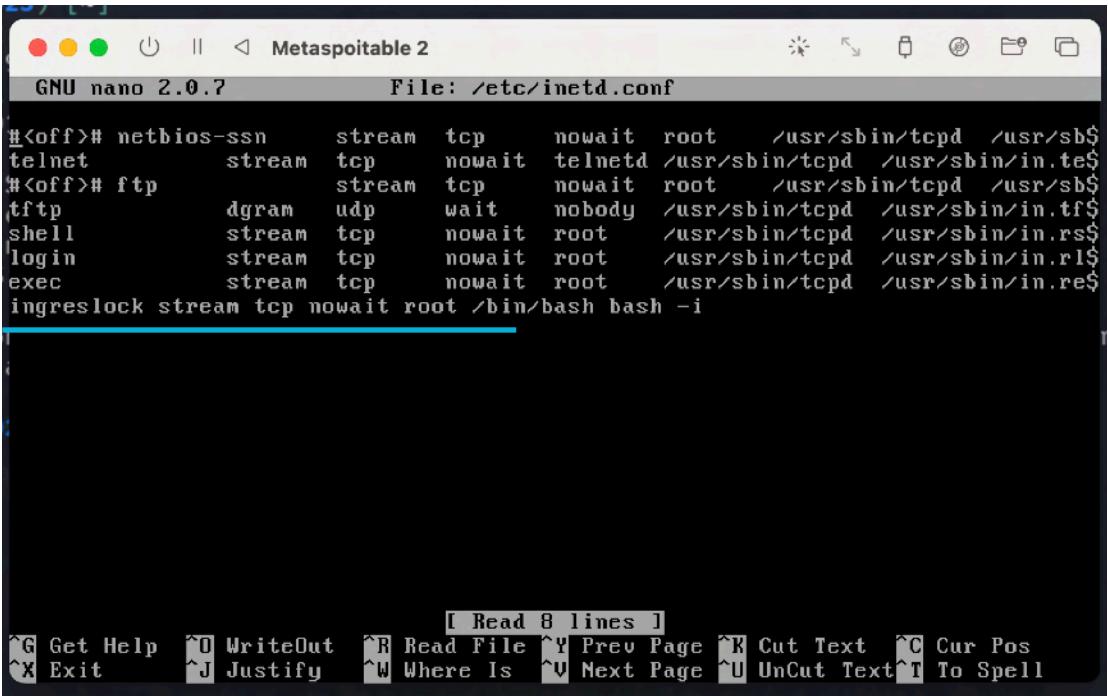
PORT      STATE SERVICE VERSION
2049/tcp  closed nfs
```

Nmap prima e dopo i comandi

3. Exec

Vulnerabilità riscontrata sulla porta 512.

Questa mitigazione è stata altrettanto facile in quanto mi è bastato visualizzare il la configurazione e disattivarne le funzionalità inserendo il cancello trasformando l'istruzione in un commento implicandone lo spegnimento :



```
GNU nano 2.0.7          File: /etc/inetd.conf

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd /usr/sbin/tcpd
telnet      stream  tcp    nowait  telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd
#<off># ftp       stream  tcp    nowait  root    /usr/sbin/tcpd /usr/sbin/in.ftpd
tftp        dgram   udp    wait    nobody  /usr/sbin/tcpd /usr/sbin/in.tftpd
shell       stream  tcp    nowait  root    /usr/sbin/tcpd /usr/sbin/in.rshd
login       stream  tcp    nowait  root    /usr/sbin/tcpd /usr/sbin/in.rlogind
exec        stream  tcp    nowait  root    /usr/sbin/tcpd /usr/sbin/in.rexd
ingreslock stream  tcp    nowait  root    /bin/bash bash -i

[ Read 8 lines ]
G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit     ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

La riga di riferimento è quella sottolineata, alla quale ho aggiunto “#”.

Il risultato determina la chiusura della porta e spegnimento del servizio evidenziato attraverso un nuovo Nmap:

```
(kali㉿kali2023) [~] $ nmap -sV 192.168.50.101 -p 512,2049
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-28 19:12 CEST
Nmap scan report for 192.168.50.101
Host is up (0.010s latency).

PORT      STATE SERVICE VERSION
512/tcp    closed  exec

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.12 seconds

(kali㉿kali2023) [~] $ nmap -sV 192.168.50.101 -p 512
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-28 19:12 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0017s latency).

PORT      STATE SERVICE VERSION
512/tcp    open   nfs    2-4 (RPC #100003)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.15 seconds
```

4. Bindshell

L'ultima vulnerabilità mitigata per il completamento dell'esercizio è quella della bindshell riscontrata sulla porta 1524.

Qui ho semplicemente provveduto ad attivare una regola firewall tramite *iptables*.

```
metasploitable login: msfadmin
Password:
Last login: Sat Sep 27 12:54:25 EDT 2025 on ttym1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ iptables -I INPUT -p tcp --dport 1524 -j DROP
iptables v1.3.8: can't initialize iptables table 'filter': Permission denied (you
u must be root)
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
msfadmin@metasploitable:~$
```

Difatti la porta risulta ora essere filtrata.

```
(kali㉿kaliz023)~]$ nmap -sV 192.168.50.101 -p 1524
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-27 17:11 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).
PORT      STATE SERVICE      VERSION
1524/tcp  open  bindshell    Metasploitable root shell

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

(kali㉿kaliz023)~]$ nmap -sV 192.168.50.101 -p 1524
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-27 17:13 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00087s latency).

PORT      STATE SERVICE      VERSION
1524/tcp  filtered  ingreslock

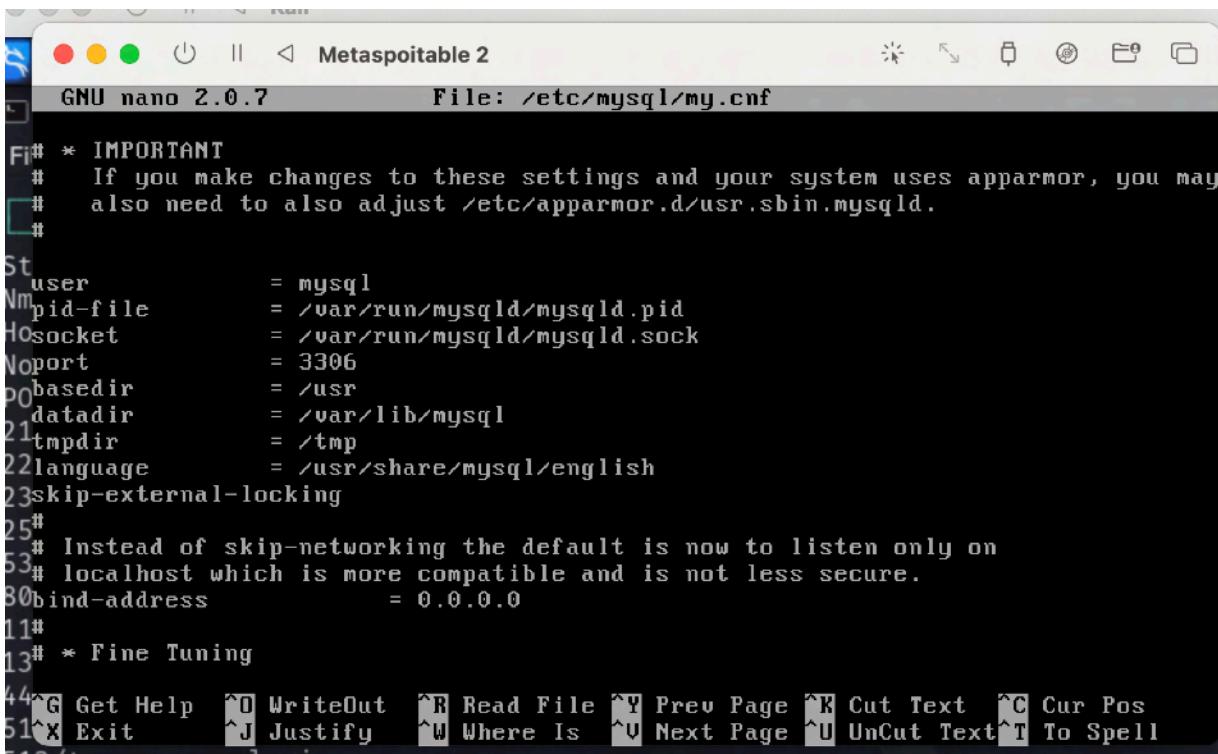
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

(kali㉿kaliz023)~]$
```

Facoltativo

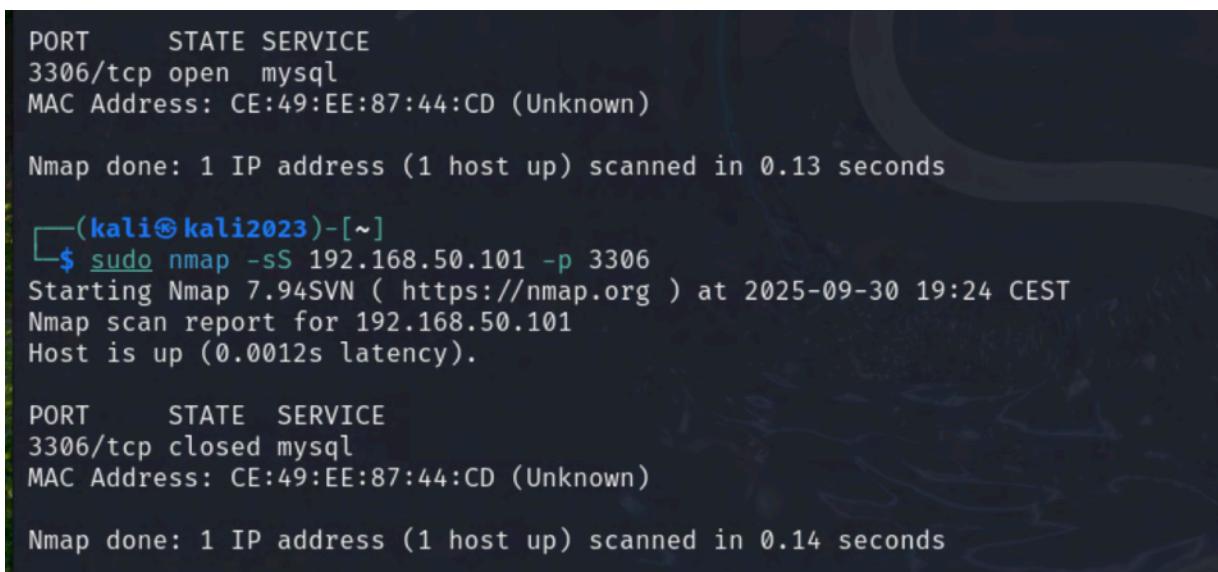
Ho provato a mitigare e chiudere una quinta vulnerabilità, ovvero l'apertura della porta 3306 che espone il database ad attacchi esterni con possibilità di exploit , recupero credenziali , accesso/copia dati , attacchi DoS ...

Quello che andiamo a fare è accedere alla configurazione del “ mysql” . Come vediamo il bind address è settato su 0.0.0.0 , permettendo quindi la connessione da qualsiasi indirizzo IP esterno su tutte le interfacce di rete . Cambio l'indirizzo IP in modo che accetti connessioni solo dal localhost : 192.168.50.101.



```
File: /etc/mysql/my.cnf
# * IMPORTANT
# If you make changes to these settings and your system uses apparmor, you may
# also need to also adjust /etc/apparmor.d/usr.sbin.mysqld.
#
# Bind variables
# user          = mysql
# pid-file      = /var/run/mysqld/mysqld.pid
# socket        = /var/run/mysqld/mysqld.sock
# port          = 3306
# basedir       = /usr
# datadir        = /var/lib/mysql
# tmpdir         = /tmp
# language       = /usr/share/mysql/english
# skip-external-locking
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
# bind-address    = 0.0.0.0
#
# * Fine Tuning
```

Verifico infatti come la porta da aperta passi a chiusa con un Nmap verso la macchina target :



```
POR STATE SERVICE
3306/tcp open  mysql
MAC Address: CE:49:EE:87:44:CD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds

(kali㉿kali2023)-[~]
$ sudo nmap -sS 192.168.50.101 -p 3306
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-30 19:24 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).

PORT      STATE SERVICE
3306/tcp  closed mysql
MAC Address: CE:49:EE:87:44:CD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```