

REPORT SETTIMANA 5

L'esercitazione di questa settimana prevedeva, durante una prima fase, la scansione delle vulnerabilità presenti su metasploitable tramite il software di vulnerability assessment 'Nessus essentials' e, a seguire, la messa in sicurezza della macchina virtuale tramite la risoluzione delle vulnerabilità più critiche. Come prima cosa ho avviato la scansione basic su Nessus, impostando l'ip di meta come target, e una volta terminata ho esportato il report contenente tutte le vulnerabilità riscontrate.

In questa prima scansione Nessus ha trovato 10 vulnerabilità critiche, 5 di livello di rischio alto, 24 medio e 5 basso.

192.168.50.101



32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

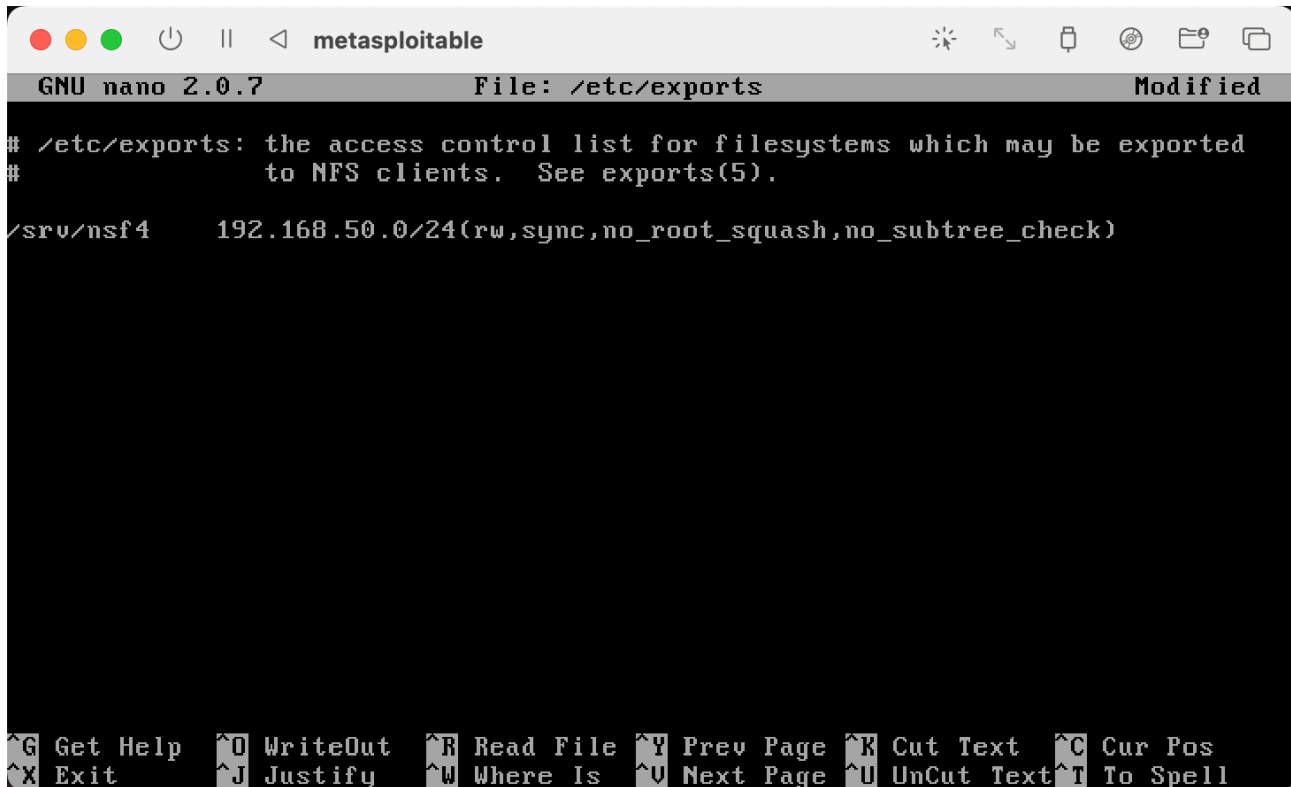
La prima vulnerabilità che ho risolto riguardava le chiavi host SSH che, a causa di pacchetti contenenti bug presenti su meta, erano troppo deboli e avrebbero permesso ad un malintenzionato un facile attacco man in the middle. Per risolvere questa vulnerabilità ho generato una nuova coppia di chiavi più sicure, tenendo le vecchie come backup.

```
root@metasploitable:~# cd /etc/ssh
root@metasploitable:/etc/ssh# ls
moduli      sshd_config  ssh_host_dsa_key.pub  ssh_host_rsa_key.pub
ssh_config  ssh_host_dsa_key  ssh_host_rsa_key
root@metasploitable:/etc/ssh# mv ssh_host_rsa_key ssh_host_rsa_key.old
root@metasploitable:/etc/ssh# mv ssh_host_dsa_key ssh_host_dsa_key.old
root@metasploitable:/etc/ssh# dpkg-reconfigure openssh-server
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
* Restarting OpenBSD Secure Shell server sshd
root@metasploitable:/etc/ssh# service ssh restart_
```

11356 - NFS Exported Share Information Disclosure

La seconda vulnerabilità era causata dal protocollo NFS che, non correttamente configurato, permetteva a chiunque di accedere alle informazioni contenute in meta,

Ho quindi provveduto ad limitare l'accesso ai soli ip appartenenti alla sottorete di meta.



The screenshot shows a terminal window titled 'metasploitable' with a standard macOS window header (red, yellow, green buttons, power, zoom, and window icons). The terminal is running GNU nano 2.0.7, editing the file /etc/exports. The content of the file is as follows:

```
# /etc/exports: the access control list for filesystems which may be exported
#                to NFS clients.  See exports(5).

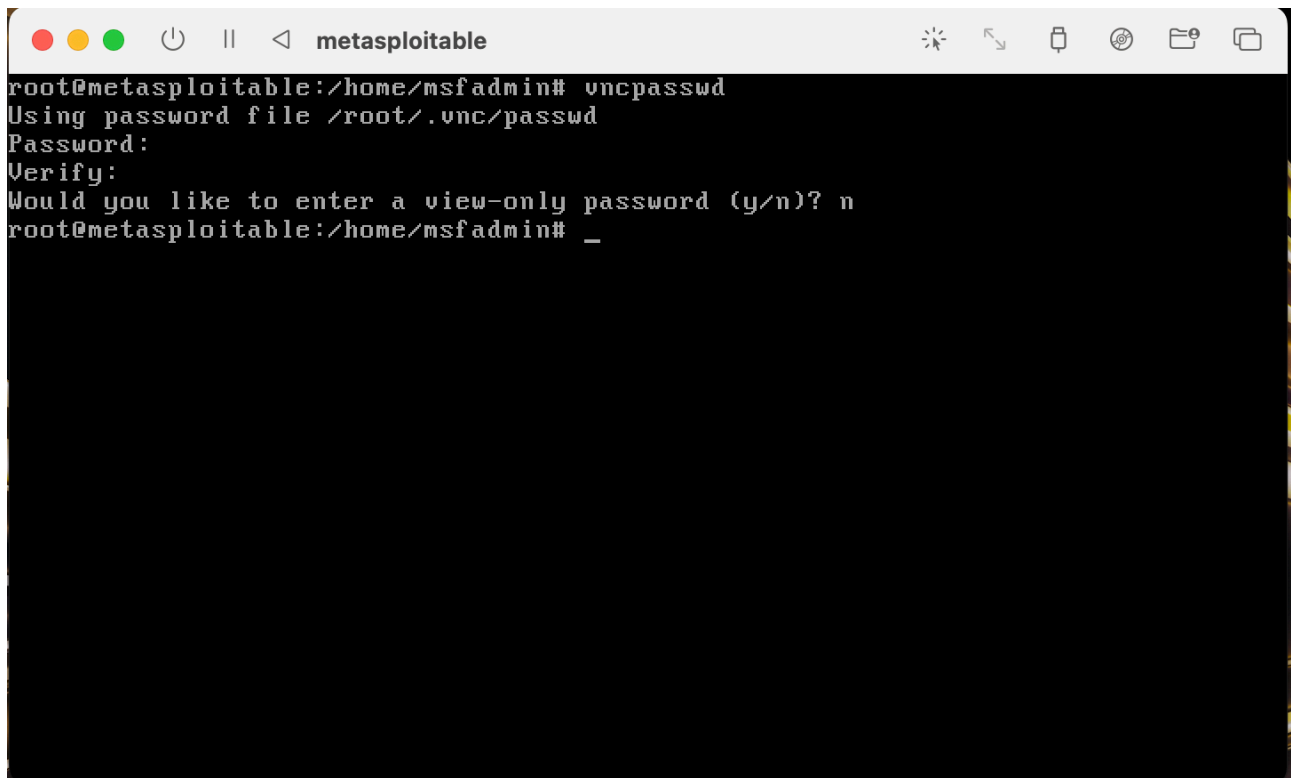
/srv/nsf4      192.168.50.0/24(rw,sync,no_root_squash,no_subtree_check)
```

The bottom of the terminal displays the nano editor's help menu with the following options:

^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

61708 - VNC Server 'password' Password

La terza vulnerabilità era causata dalla semplicità della password di VNC che poteva essere trovata in pochi istanti tramite un attacco brute force. Ho quindi cambiato la password, inserendone una più sicura.

A terminal window titled 'metasploitable' with standard macOS window controls. The terminal shows the execution of the 'vncpasswd' command as root user. It prompts for a password, then a verification, and asks if a view-only password should be set. The user enters 'n' for no. The prompt returns to the root shell.

```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin# _
```

51988 - Bind Shell Backdoor Detection

La quarta vulnerabilità era causata da una backdoor sulla porta 1524 che avrebbe permesso a chiunque di accedere al nostro sistema.

Ho quindi implementato una regola di firewall tramite il comando iptables per ovviare a questa vulnerabilità.

```
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/home/msfadmin# iptables -L -n -v
Chain INPUT (policy ACCEPT 89095 packets, 5819K bytes)
 pkts bytes target     prot opt in     out     source         destination
    2  120 DROP      tcp  --  *      *       0.0.0.0/0      0.0.0.0/0
    0    0 DROP      tcp  --  *      *       0.0.0.0/0      0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source         destination
Chain OUTPUT (policy ACCEPT 82688 packets, 11M bytes)
 pkts bytes target     prot opt in     out     source         destination
root@metasploitable:/home/msfadmin# _
```

Una volta risolte queste quattro vulnerabilità ho effettuato nuovamente la scansione per assicurarmi che non fossero più sfruttabili.

192.168.50.101

