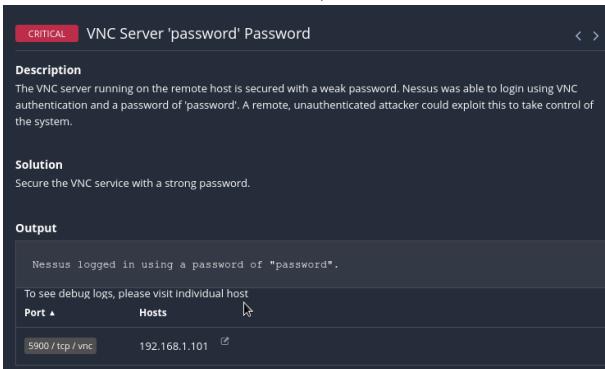
REPORT NESSUS

Durante il primo scan di Meta sono emerse 3 vulnerabilità critiche di cui:

- VNC Server 'password' Password
- NFS Exported Share information Disclosure
- rexecd Service Detection

Per risolvere la vulnerabilità VNC Server 'password' Password



Dobbiamo eseguire il comando su Meta:

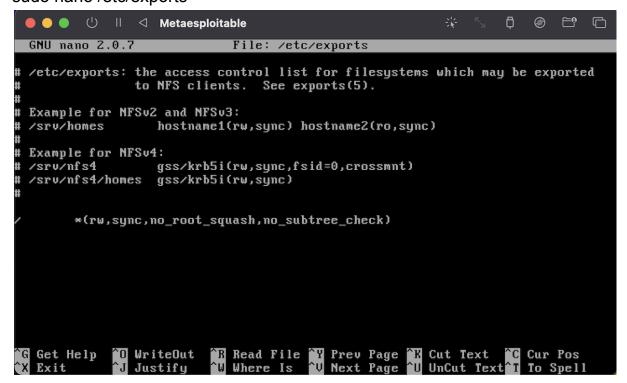
```
root@metasploitable:~# sudo su
root@metasploitable:~# cd /
root@metasploitable:/# ls
      dev
                    lost+found nohup.out root
bin
           initrd
                                                    sys
boot
      etc
            initrd.img media
                                                          umlinuz
                                    opt
                                              sbin tmp
cdrom home lib
                                                     usr
                        mnt
                                    proc
                                               srv
root@metasploitable:/# cd /root
root@metasploitable:~# ls
Desktop reset_logs.sh vnc.log
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# ls
metasploitable:0.log metasploitable:1.log
                                           passwd
metasploitable:0.pid metasploitable:2.log
                                           xstartup
root@metasploitable:~/.vnc# rm passwd
root@metasploitable:~/.vnc# ls
metasploitable:0.log metasploitable:1.log
                                           xstartup
metasploitable:0.pid metasploitable:2.log
root@metasploitable:~/.vnc# _
```

facendo ciò andremo a togliere la password da root e potremo eseguire l'accesso solamente da msfadmin. (non più da remoto)

Per risolvere la vulnerabilità NFS Exported Share information Disclosure



Dobbiamo eseguire il comando su Meta: sudo nano /etc/exports



Successivamente modificare il root /

*(rw,sync,no_root_squash,no_subtree_check) in questo modo:

```
/ *(noaccess,root_squash<u>)</u>
```

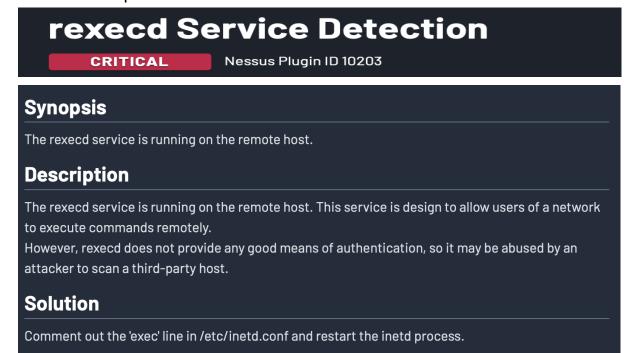
Prima

- Con (rw,sync,no_root_squash,no_subtree_check) un Host da remoto poteva avere sia lettura che scrittura e poteva prendere i privilegi Risolvendo la vulnerabilità
- Con (no access,root_squash) all'Host gli neghiamo l'accesso e gli togliamo i privilegi.

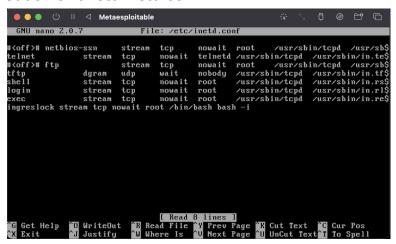
Con questa configurazione vado a risolvere anche una vulnerabilità HIGH



Per risolvere questa vulnerabilità



Dobbiamo entrare nel file di configurazione con il comando: sudo nano /etc/inetd.conf



E modificarlo mettendo # prima di exec in questo modo:

Ciandri Leonardo