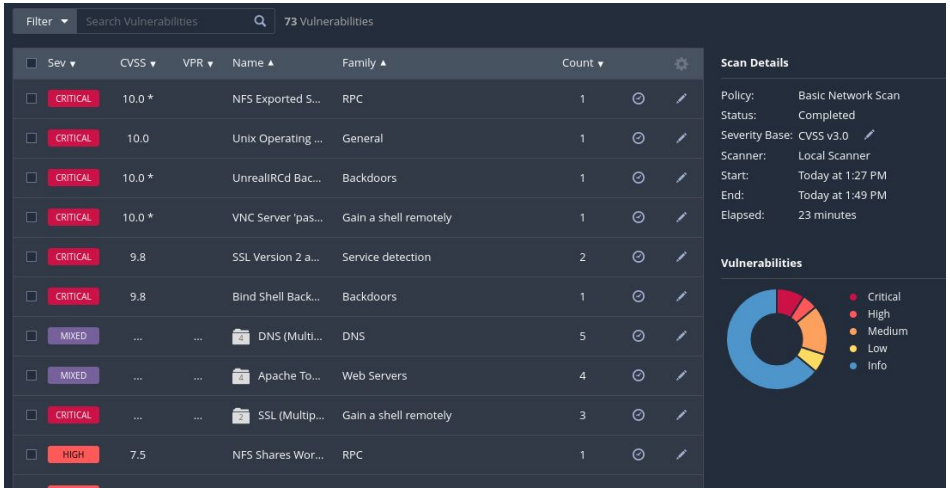
# Progetto S5-L5

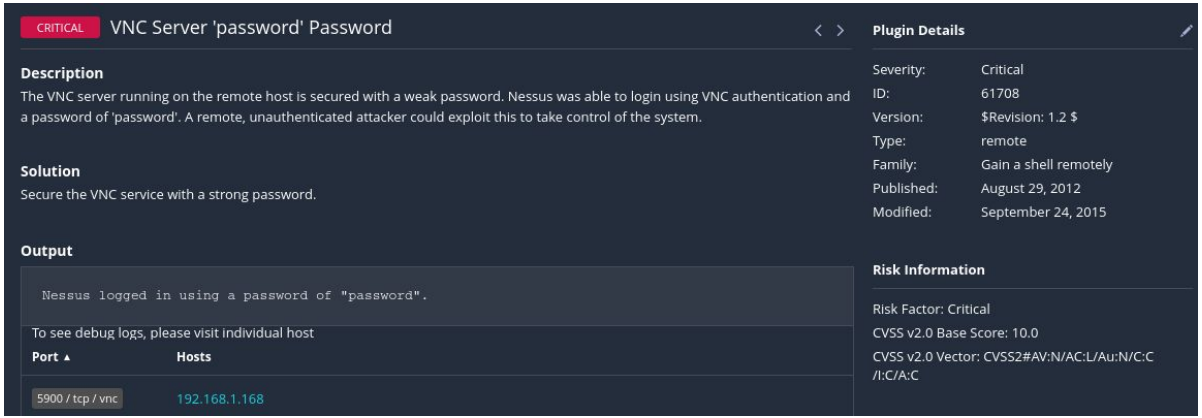
# Nessus

Dopo aver completato questa procedura, possiamo visualizzare un elenco delle vulnerabilità, ognuna classificata con un livello di pericolo che può essere 'Info', 'Low', 'Medium', 'High', o 'Critical'. Le vulnerabilità classificate come 'Critical' sono quelle che dovremmo risolvere prioritariamente.



# Nessus

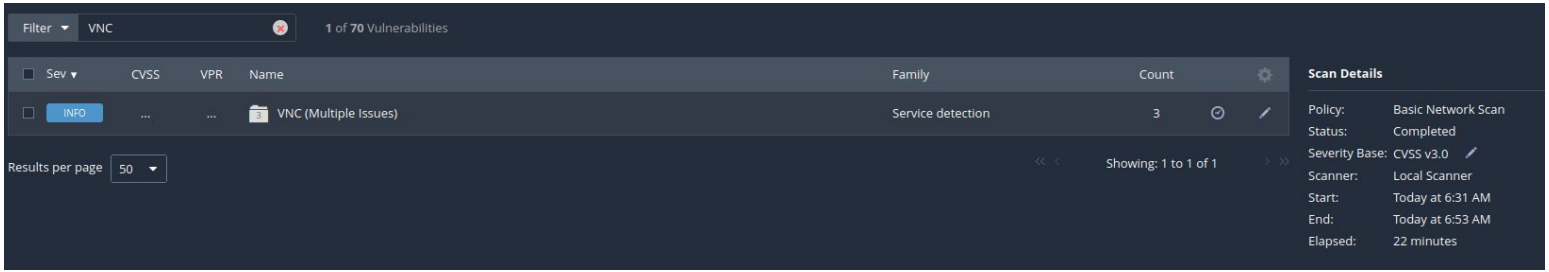
In questo caso, abbiamo identificato una password piuttosto debole nel VNC server, (immagina di avere un computer (il server) e vuoi accedere e controllare il suo desktop da un altro computer (il client) situato in un luogo diverso), e attraverso una simulazione di attacco, Nessus è riuscito a penetrare facilmente. . La soluzione consigliata sarebbe quindi di utilizzare una password robusta.



# Nessus

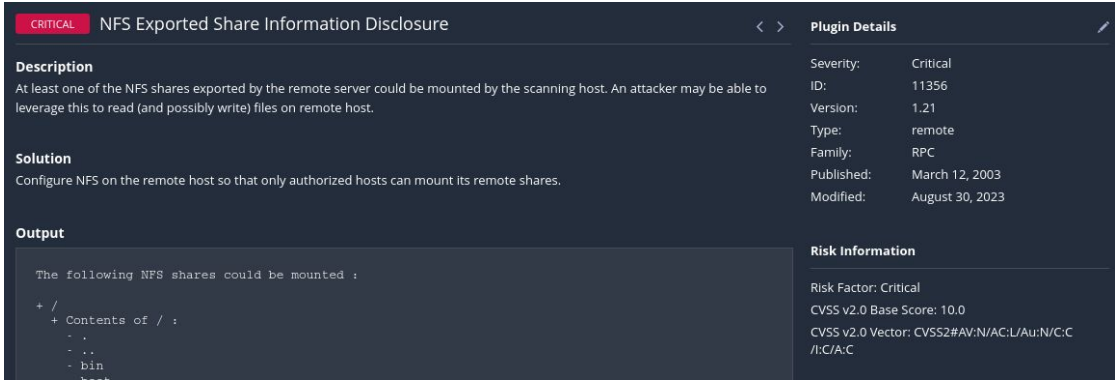
Andiamo su metasploitable e inseriamo i vari comandi dove su **password** e **verify** andiamo a scegliere la nuova password. Dopo facciamo un sudo reboot.

```
root@metasploitable:/home/msfadmin# sudo su
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# sudo reboot
```



# Nessus

NFS (Network File System) è un protocollo che consente di condividere file e risorse tra computer su una rete. In questo caso, abbiamo un dispositivo remoto che potrebbe essere facilmente attaccato, aumentando il rischio di perdita, rimozione o modifica dei file da parte di un black hat. Per prevenire questo problema, è sufficiente modificare il dispositivo in modo tale che siano autorizzati solo i dispositivi da noi desiderati.

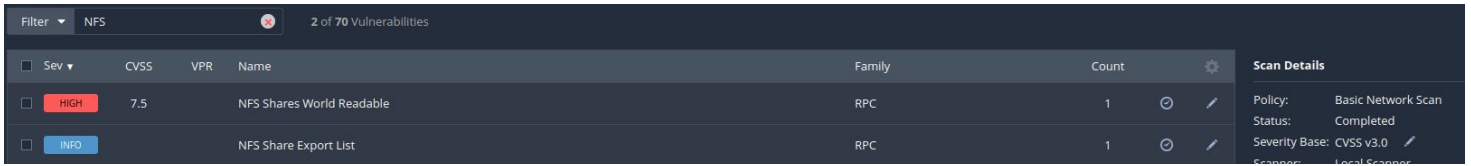


# Nessus

Per questo è po più complicato, scrivere prima il comando `sudo nano /etc/exports` ed andiamo a scrivere una nuova riga sotto.

```
/                       *(rw,sync,no_root_squash,no_subtree_check)
/home/user/share        192.168.1.167(rw,sync,no_root_squash)
```

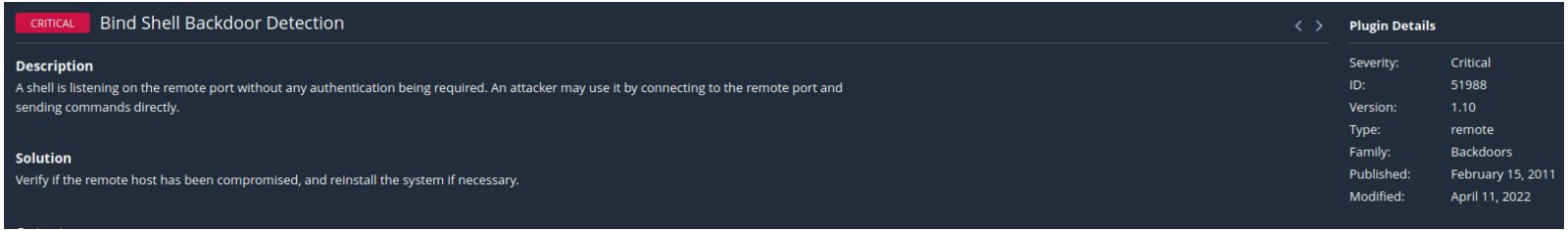
dove la prima parte è la cartella in cui andiamo a salvare e l'ip sono gli host autorizzati, se mettete un * qualsiasi host è autorizzato. Dopo riavviamo con un sudo reboot.




Ora mi rimane da risolvere l'altro problema con NFS in uno scenario reale.

# Nessus

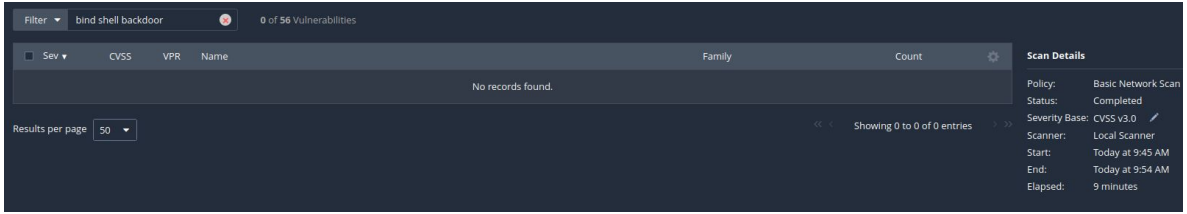
Per questa vulnerabilità abbiamo sostanzialmente una porta aperta la 1024 che funge da backdoor dove l'attaccante può creare dei problemi dando dei comandi diretti. La soluzione che io ho trovato è diversa da quella detta da Nessus



# Nessus

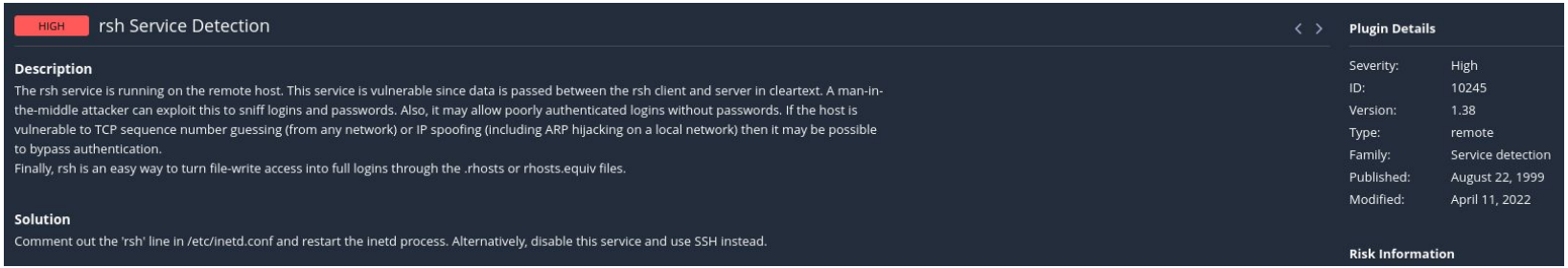
Constatato che la porta 1524 non ci serve, ho deciso di disattivarla usando il firewall iptables, vado ad utilizzare i seguenti comandi. `sudo iptables -A INPUT -p tcp --dport 1524 -j DROP` poi l'altro per assicurarsi che sia corretto `sudo iptables -L`.

```
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 1524 -j DRO
P
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@metasploitable:/home/msfadmin#
```



# Nessun

Il servizio RSH (Remote Shell) è un protocollo di rete che consente di eseguire comandi su un computer remoto su una rete. In parole più semplici, RSH permette a un utente di eseguire comandi su un altro computer attraverso la rete, come se fosse direttamente connesso a quel computer. Stesso discorso di prima questa porta mi serve, e andrò nel file ad inserire un # per non considerare la shell.



# Nessus

Su metasploitable facciamo sudo nano/etc/inetd.conf e cerchiamo la shell dove vediamo la dicitura rsh e mettiamo un # per renderlo un commento.

```
#shell          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
```

A questo punto salviamo e facciamo sudo reboot.

# Fine

Grazie a queste piccole soluzioni siamo riusciti a rimuovere le vulnerabilità e dopo avere scansionato nuovamente possiamo vedere se effettivamente sono state risolte, infatti le mie vulnerabilità iniziali da 73 sono scese a 56 (probabilmente alcuni problemi low derivano da quelli critical o high quindi risolvendo uno ne risolvi molteplici).