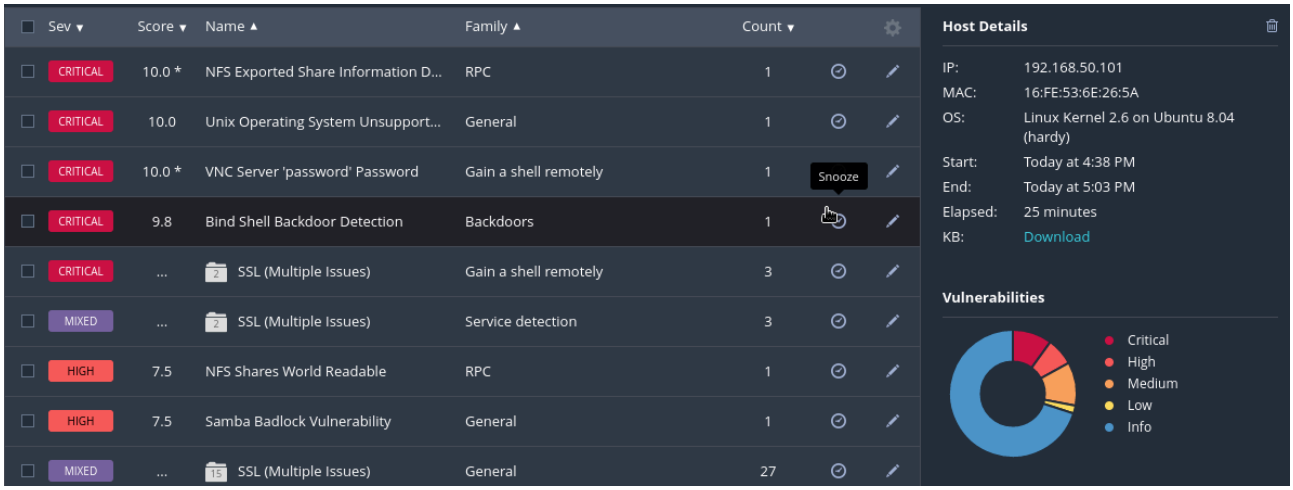
Relazione Progetto

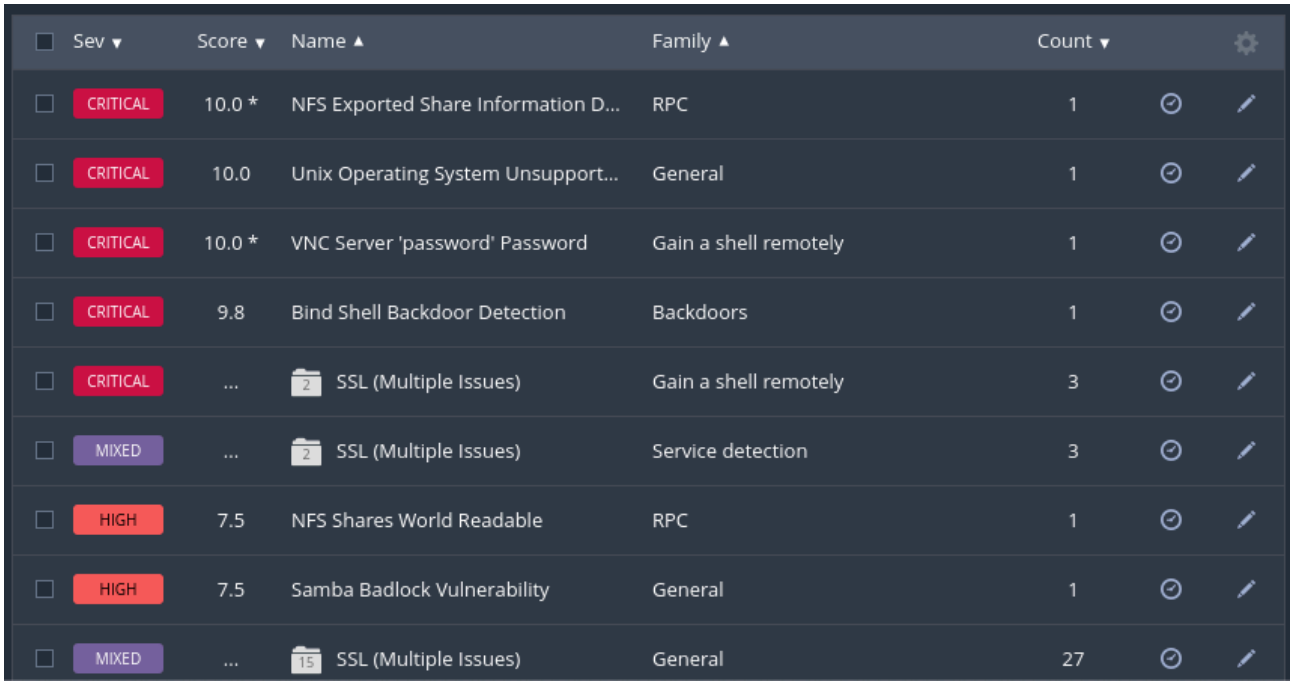
Le scansioni d'oggi le andremo a fare con il vulnerability scanner di Nessus, con questo scanner andremo a fare una scansione completa del sistema di metasploitable.

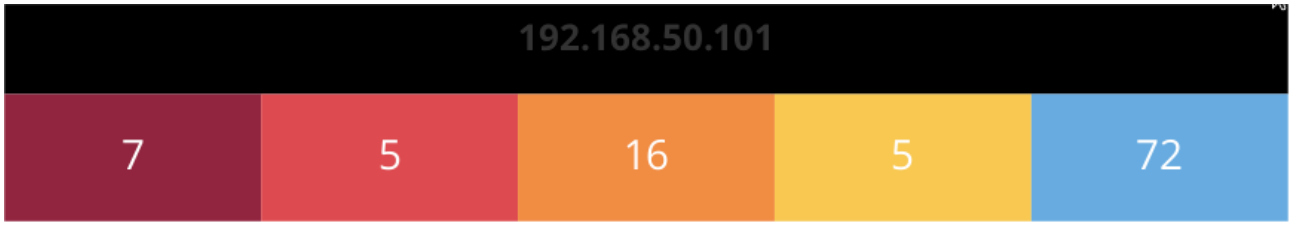
Scanzione Iniziale

Con la scansione iniziale si va verificare quali sono le problematiche che presenta Metasploitable.



Con questa prima scansione ci mostra tutte le vulnerabilità che ha riscontrato nella nostra macchina, in questo caso metasploitable.



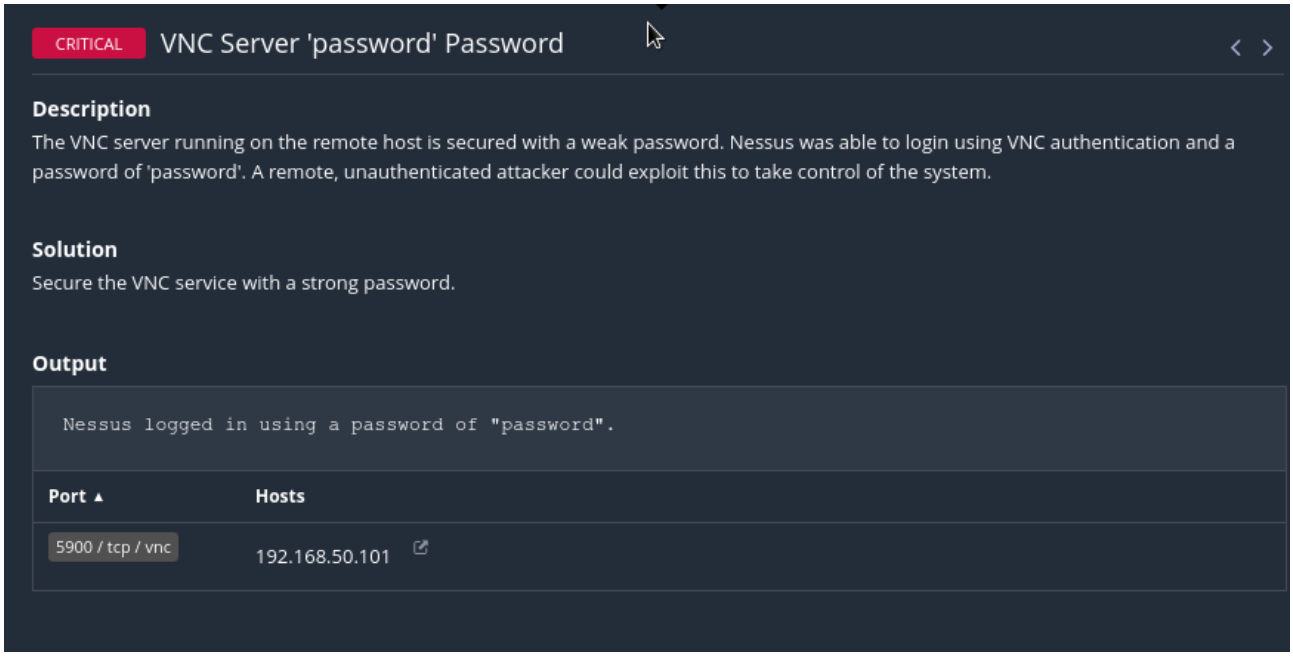


Le vulnerabilità che troviamo sono:

- ☞ Info
- ☞ Low
- ☞ Medium
- ☞ High
- ☞ Critical

Le vulnerabilità più pericolose per il nostro sistema sono le “Critical” queste sono quelle più dannose per il nostro sistema e sono quelle sulle quali siamo andati ad agire.

Una delle vulnerabilità critiche che troviamo è quella **VNC Server ‘password’**



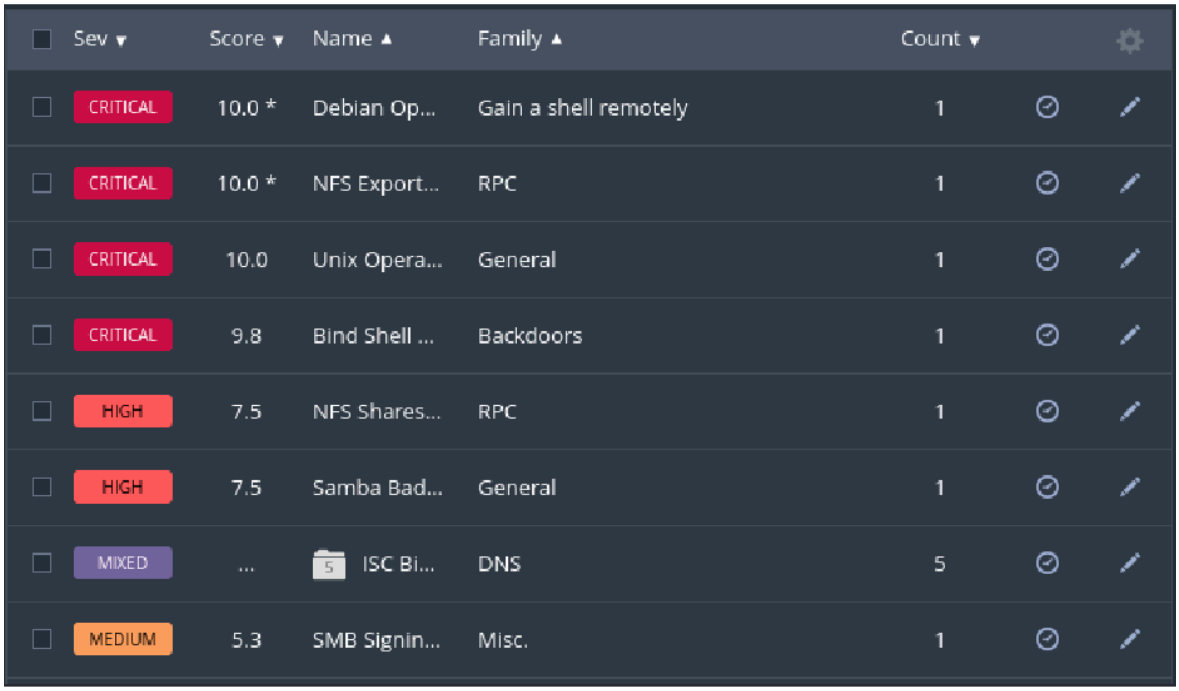
Per risolvere questo problema mi sono basato sulla descrizione del problema il quale chiede che la sorgente di vnc necessità una password forte.

```
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd .vnc
root@metasploitable:/home/msfadmin/.vnc# ls
metasploitable:1.log  metasploitable:1.pid  passwd  xstartup
root@metasploitable:/home/msfadmin/.vnc# 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/.vnc#
```

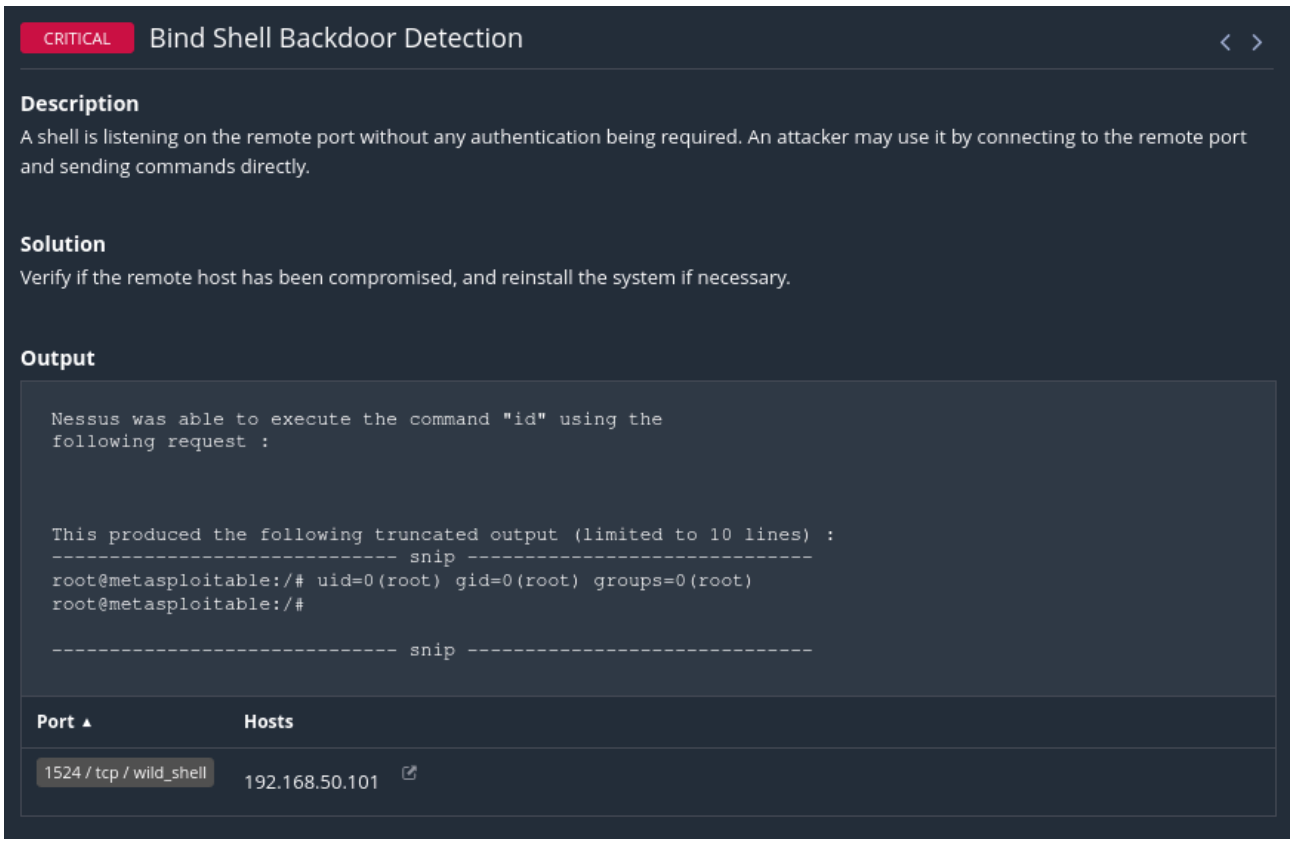
Come si può vedere dall'immagine nella pagina precedente possiamo migliorare la sicurezza andando a fare delle modifiche nella macchina attaccata:

1. Con il comando sudo su entriamo nella sezione d'amministratore.
2. Con cd .vnc entriamo nella cartella
3. Con il ls verifichiamo se il file che stiamo cercando è all'interno
4. Dopo aver selezionato il il file che ci serve andiamo modificare la password, la quale ci verrà fatta una richiesta di verifica
5. Dopo aver verificato la password ci chiederà se vogliamo che la password sia visibile, noi selezioniamo "n"

Come possiamo vedere nell'immagine non presenta più la vulnerabilità di prima.



Un’altra delle vulnerabilità critiche che troviamo è quella **Band Shell Backdoor Detection**



Questo problema ci dice che un attaccante può essere in ascolto sulla porta, per migliorare le difese della macchina bisogna andare a mettere un firewall sulla macchina (Porta 1524), come si può vedere nella immagine di sotto: