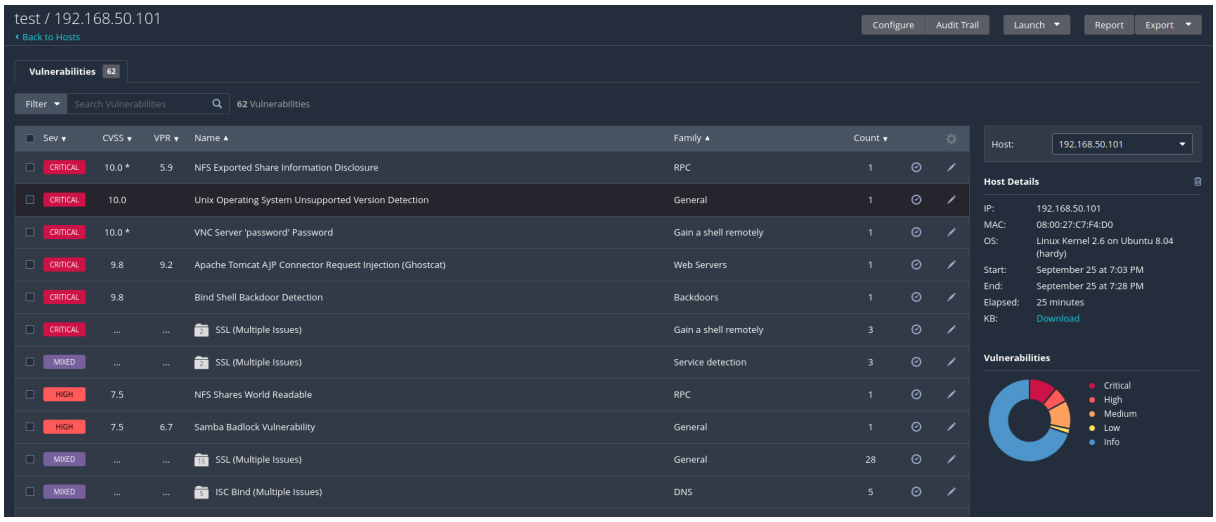
D8. PT – Attacchi alle Web APP (1)

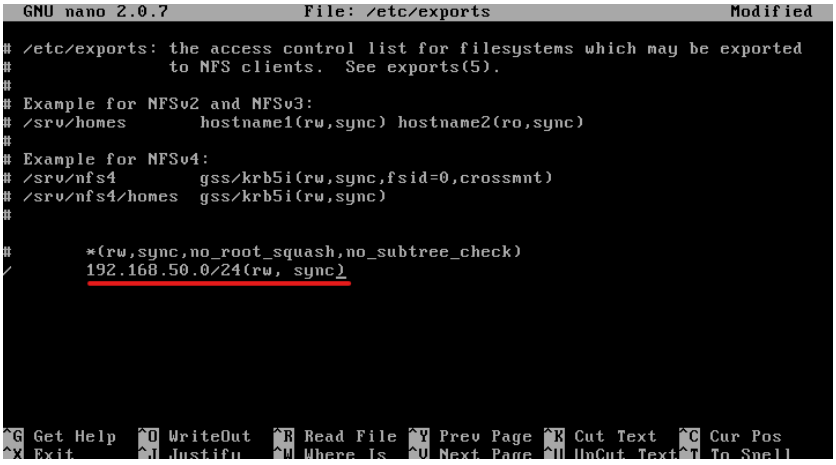
Prima scansione con Nessus



Nell'immagine sopra riportata possiamo vedere la scansione effettuata con Nessus dalla macchina Linux(attaccante) alla macchina Metasploitable(vittima). Tra le vulnerabilità richieste dalla traccia dell'esercizio possiamo vedere **NFS Exported Share Information Disclosure**, **VNC Server 'password' Password** e **Bind Shell Backdoor Detenction**. Non è stata invece trovata la vulnerabilitá **rexecd Service Detenction**.

Fase di remediation

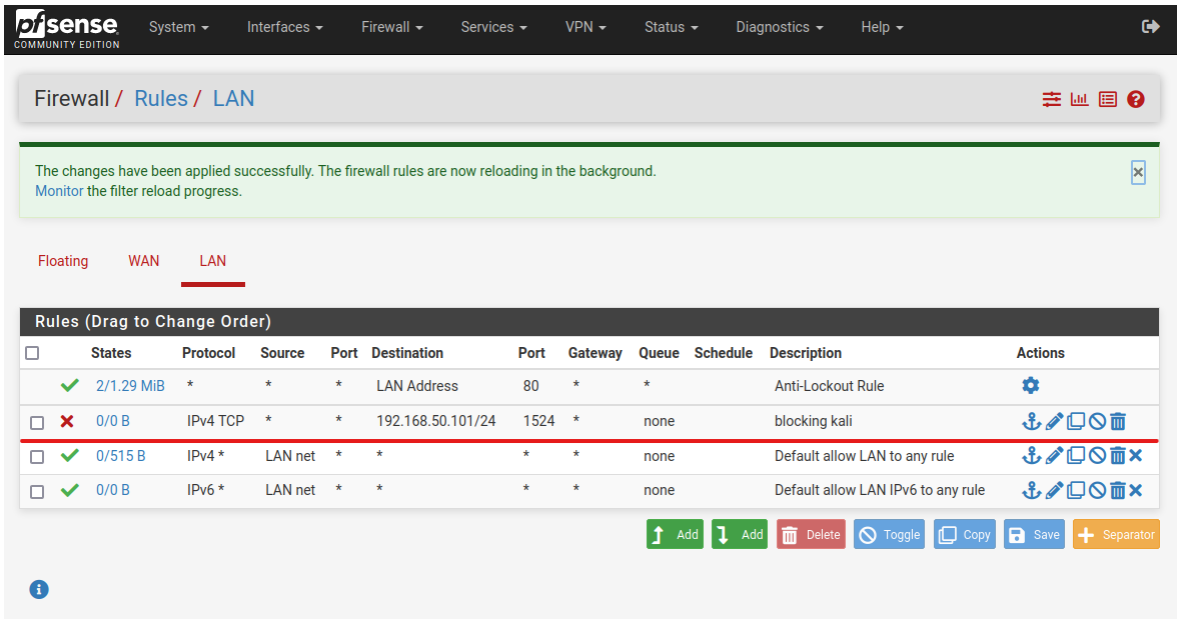
La vulnerabilità **NFS Exported Share Information Disclosure** può essere sfruttata da un'attaccante per poter leggere e scrivere file grazie al file system condiviso. Per fixare questa vulnerabilità ho modificato i permessi di lettura e scrittura limitando i permessi solo agli host appartenenti alla rete della macchina Metasploitable.



La vulnerabilità **VNC Server 'password' Password** riguarda la password di accesso al server e dove Nessus indica che è troppo debole e che quindi va cambiata. Per motivi puramente pratici e didattici ho scelto una password facile e non sicura ovvero "Vale123!".

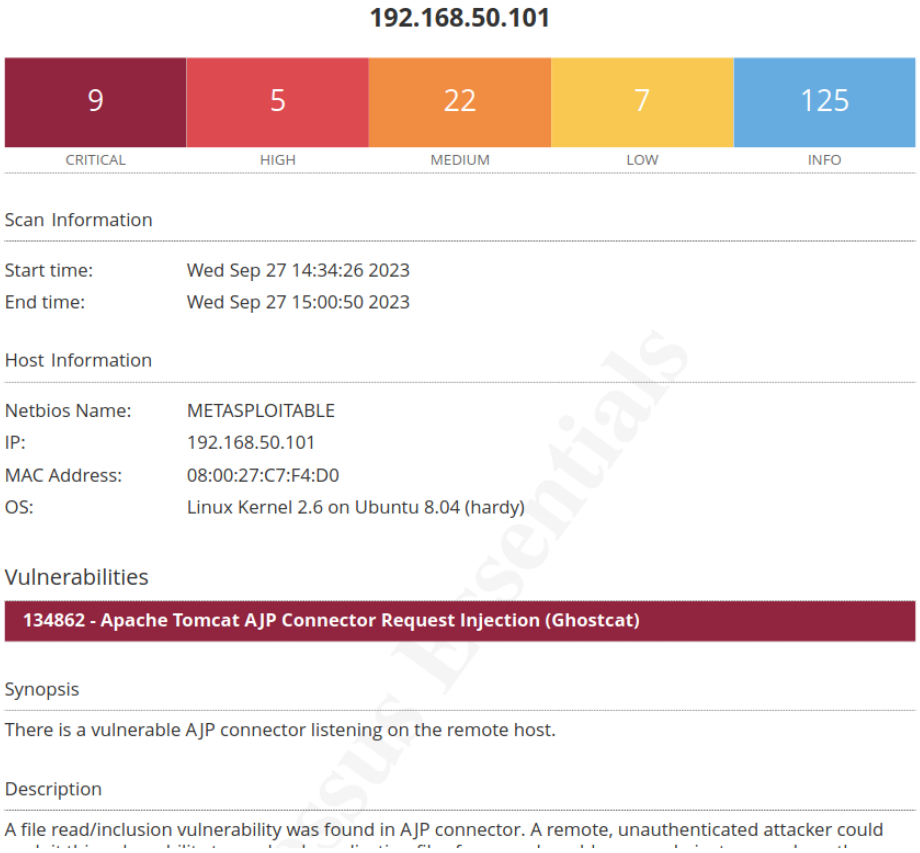
```
root@metasploitable:/# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/# _
```

Per quanto riguarda la **Bind Shell Backdoor Detenction** ho provveduto ad impostare una regola di firewall impedendo alla macchina metasploitable di ricevere pacchetti TCP sulla porta 1524.



Invece per quanto riguarda la vulnerabilità **rexecd Service Detenction** che non è stata trovataho provveduto comunque ad entrare nel file inetd.conf ed ho commentato la linea exec per evitare l'esecuzione di comandi da utenti non autenticati.

Scansione finale con Nessus



Come possiamo vedere dal report sono rimaste solo le vulnerabilità non fixate come ad esempio la prima riportata.