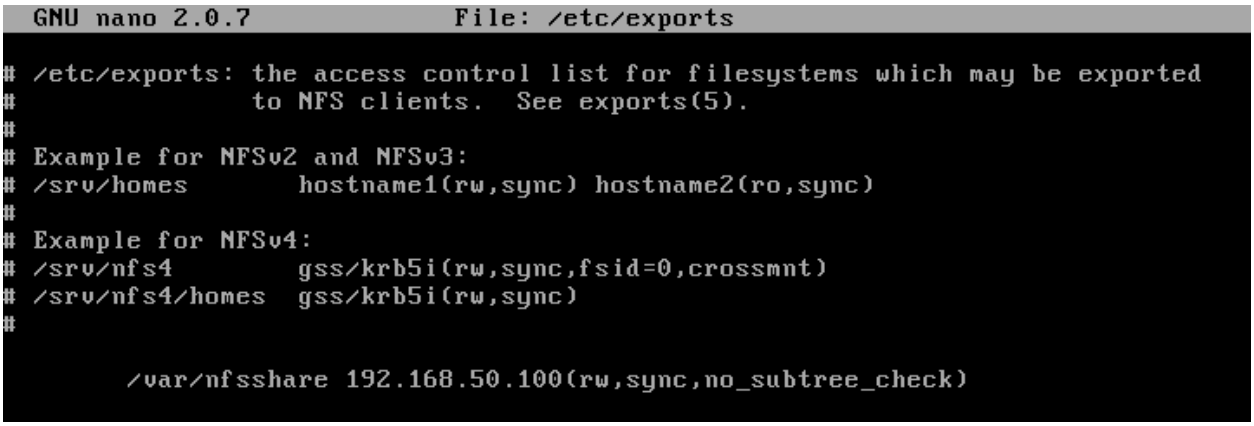
Descrizione:

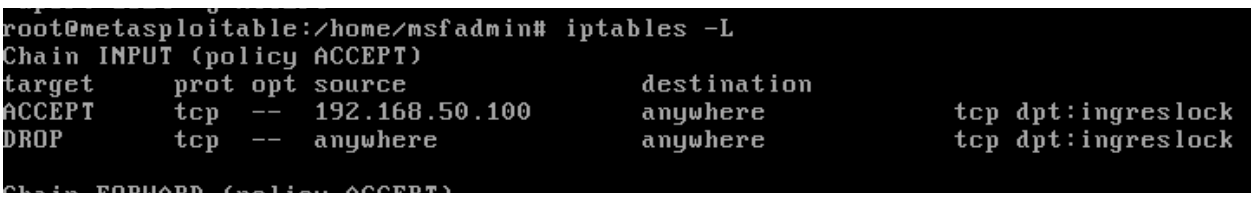
In questa fase, sono state implementate una serie di azioni correttive per mitigare le vulnerabilità identificate nella scansione iniziale. Di seguito vengono presentati gli screenshot e una spiegazione dei passaggi seguiti per la remediation.

Passaggi della Remediation:

- ➔ **VNC Server 'password' Password**:
  - É stata cambiata la password con una più sicura, tramite il comando ' *vncpsswd* '. In seguito è stato eseguito un riavvio del servizio VNC.
- ➔ **NFS Exported Share Information Disclosure:**
  - Per porter mettere in sicurezza, è stato modificato il file di esportazione NFS */etc/exports* (mostrato nell'immagine seguente). Inoltre è stata creata una directory(*/var/nfsshare*) da esportare che è stata aggiunta all' host a cui è consentito l'accesso.

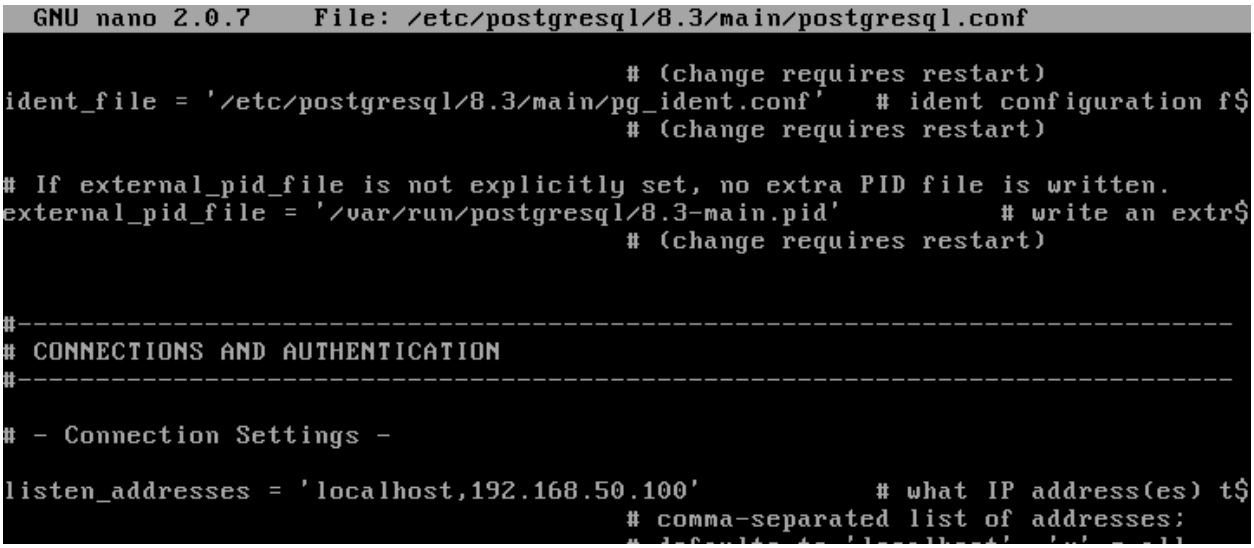


- ➔ **Bind Shell Backdoor Detection**:
  - Per mettere in sicurezza, è stata creata una regola firewall per la porta 1524. Di seguito,l' 'immagine con le seguenti regole applicate

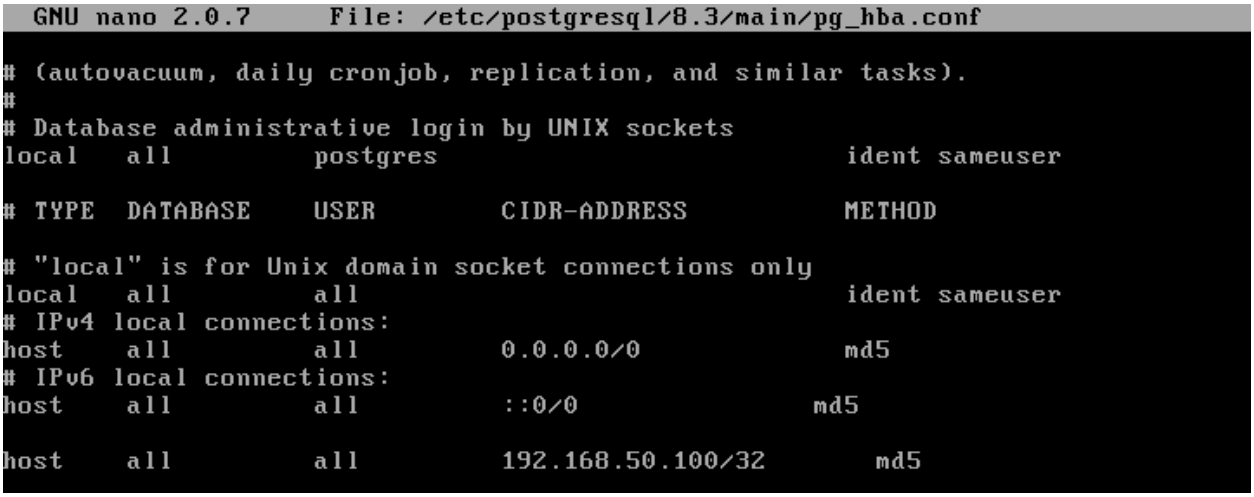


➔ **SSL v. 2.0 e v. 3.0 Protocol Detection**:

- Sono state effettuate varie operazioni. Per quanto riguarda la porta 5432(PostgreSQL), tramite un editor di testo all 'interno del file *postgresql.conf* in cui è stata modificata la riga *listen_address*, che si trova nel percorso */etc/postgresql/<version>/main/* ; nella stessa directory(/main/) è stato modificato,sempre tramite editor di testo il file *pg_hba.conf* aggiungendo una riga(presente nell'immagine seguente).

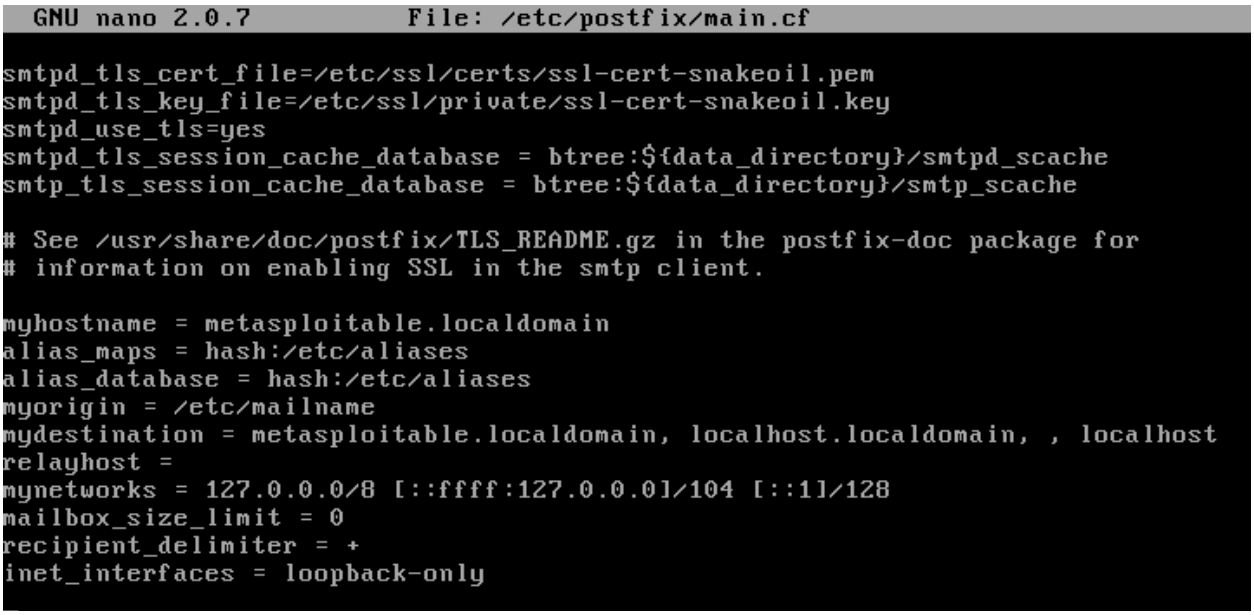


(postgresql.conf)



(pg_hba.conf)

- Per quanto riguarda la porta 25 (STMP), tramite editor di testo è stata modificata la riga *inet.interfaces* all'interno del file *main.cf* nella directory */etc/postfix/* .



- Eseguite le precedenti azioni,è stato eseguito un riavvio.

Risultati della Remediation:

Tutte le azioni di remediation sono state documentate e verificate. Successivamente è stata eseguita una nuova scansione per verificare la veridicità delle problematiche risolte.