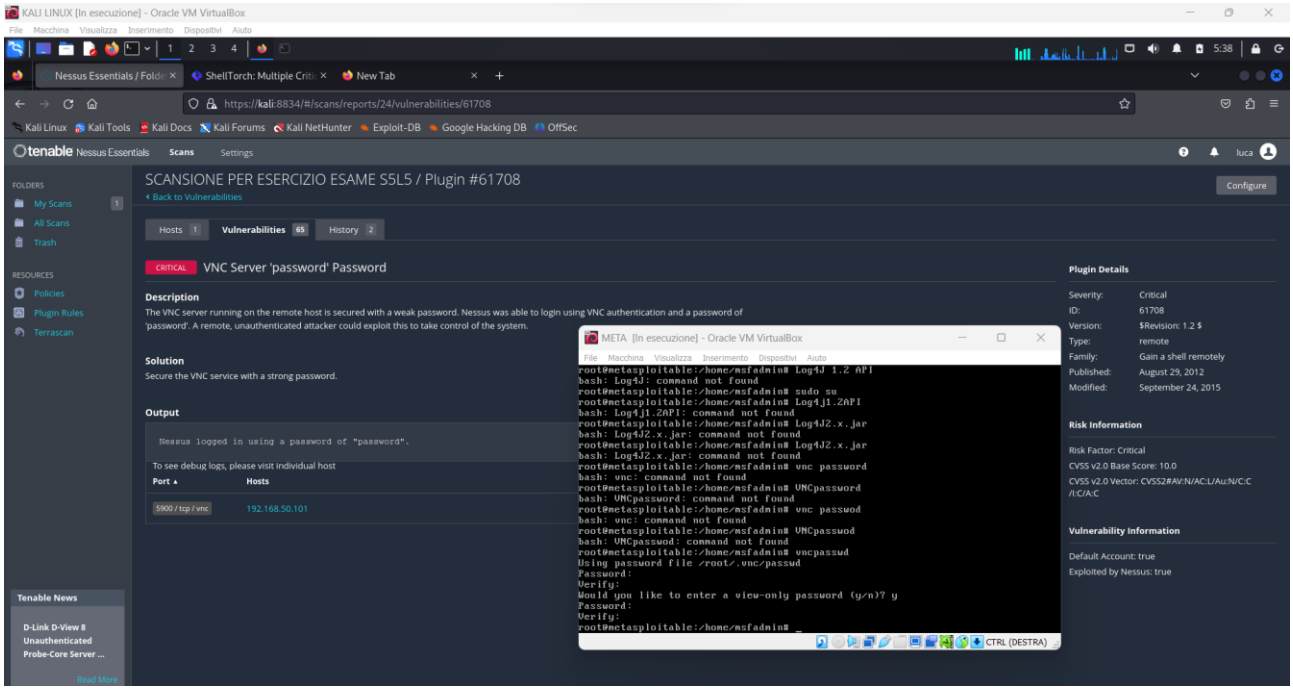
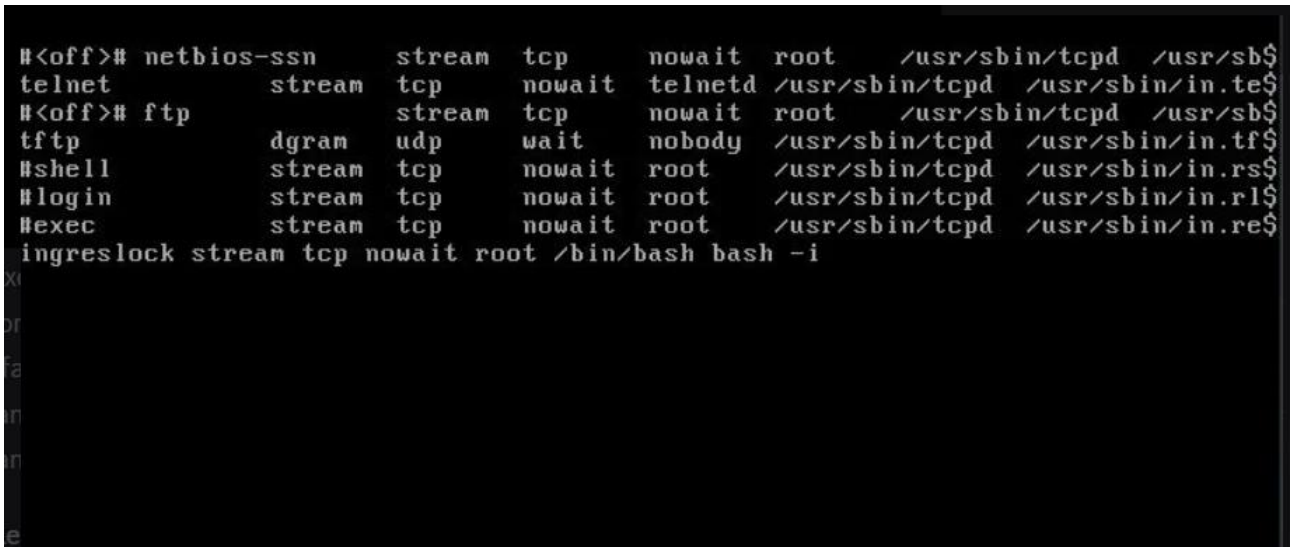
CONSEGNA ESERCIZIO S5L5

RISOLUZIONE VULNERABILITA' VNC SERVER



Per risolvere la seguente criticità siamo andati a variare la **password del server VNC** mettendone una più sicura in modo da non permettere ad un attaccante di entrare con facilità.

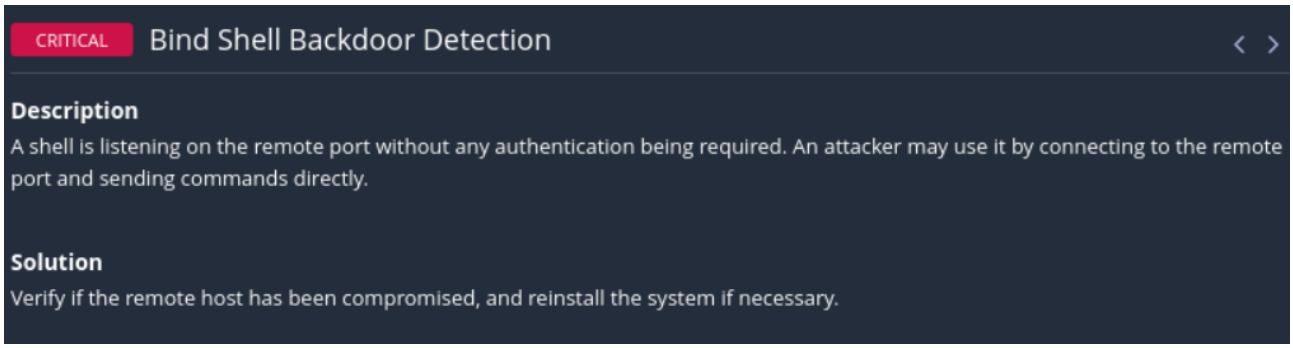
RISOLUZIONE VULNERABILITA' "RLOGIN SERVICE DETECTION" E "RSH SERVICE DETECTION"



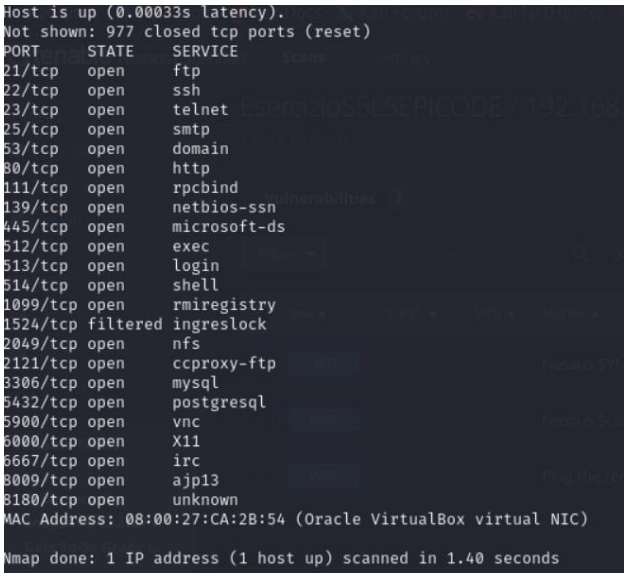
Per risolvere la seguente criticità abbiamo reso commenti la linea di **login** e **exec**, rendendole quindi #login e #exec.

Successivamente abbiamo fatto il restart del servizio **xinetd**.

RISOLUZIONE DELLA VULNERABILITA' BIND SHELL BACKDOOR DETECTION



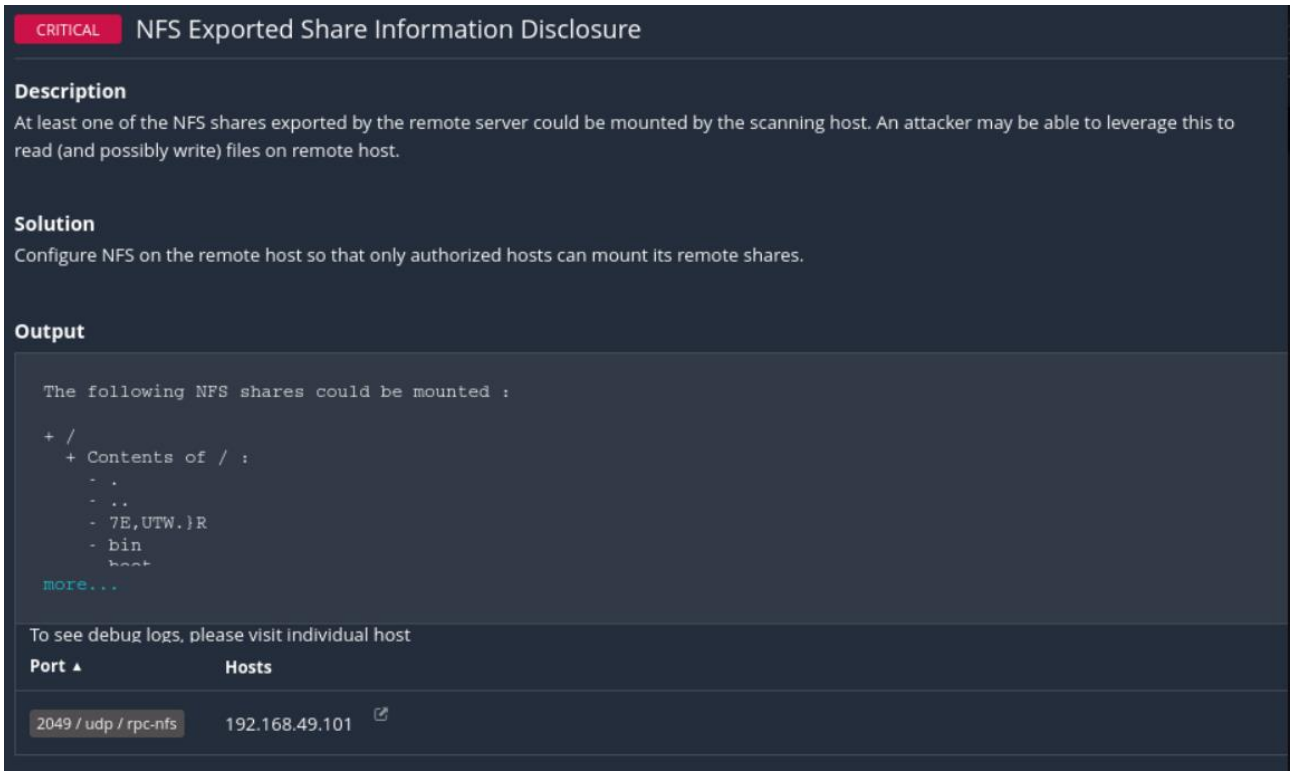
Questa criticità è stata risolta andando a chiudere la porta **tcp:1524** attraverso la riga di comando sovrastante.

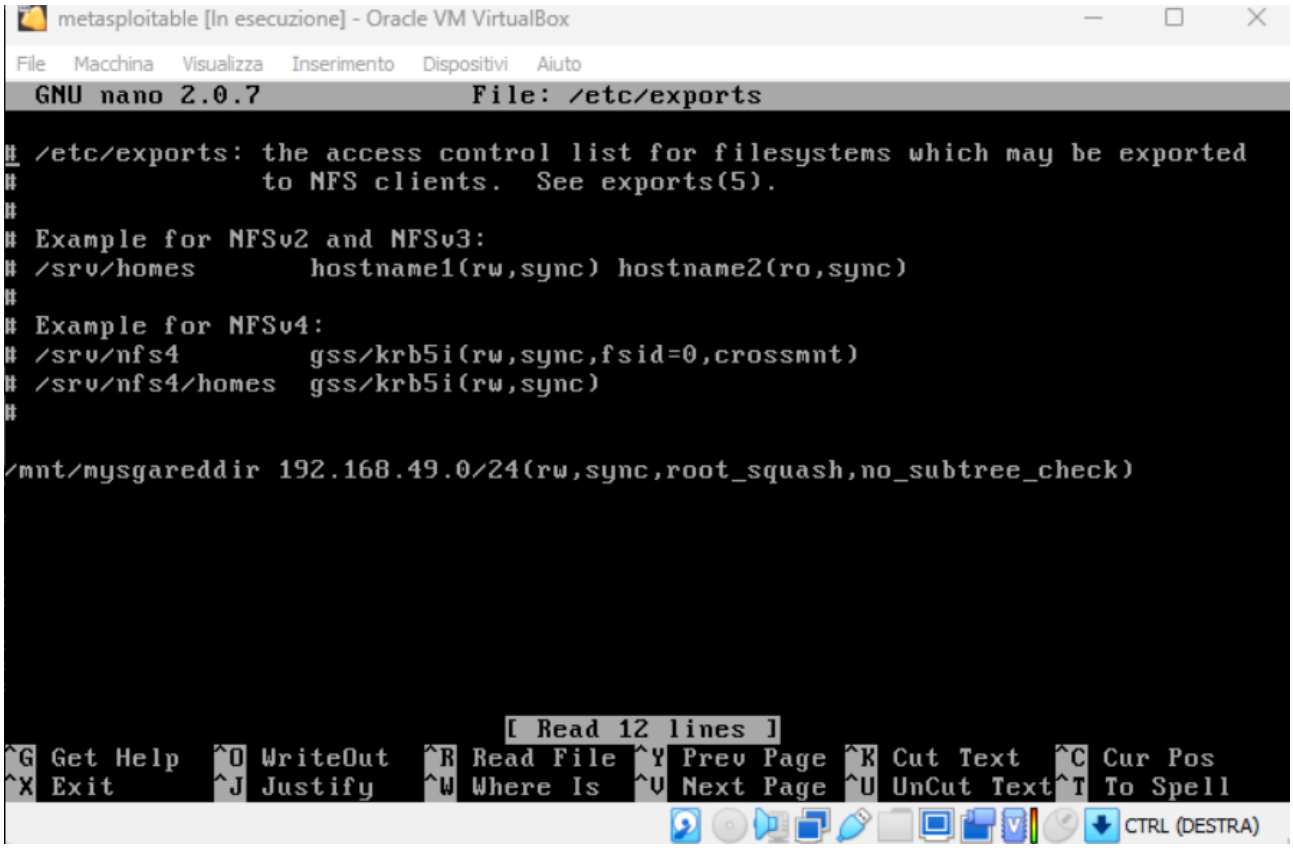


Come possiamo dall'immagine di sopra e stato eseguito un comando <<nmap>> per controllare che la porta **tcp:1524** risultasse effettivamente **filtered** dal **firewall**.

Successivamente è stato eseguito un controllo ulteriore attraverso **NESSUS** per controllare che la **vulnerabilità** fosse scomparsa.

RISOLUZIONE DELLA CRITICITA' : NFS EXPORTED SHARE INFORMATION DISCLOSURE





Questa criticità è stata risolta limitando gli accessi ai soli utenti sotto lo stesso **Network** così da impedire a utenti esterni l'accesso.