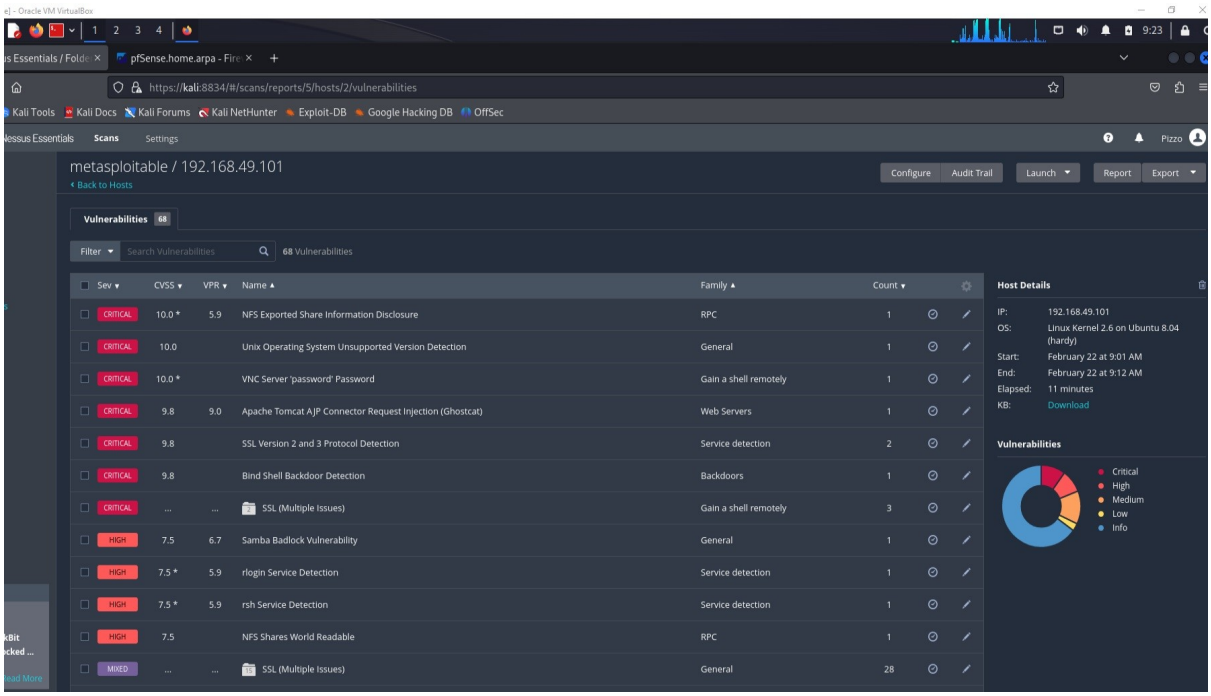
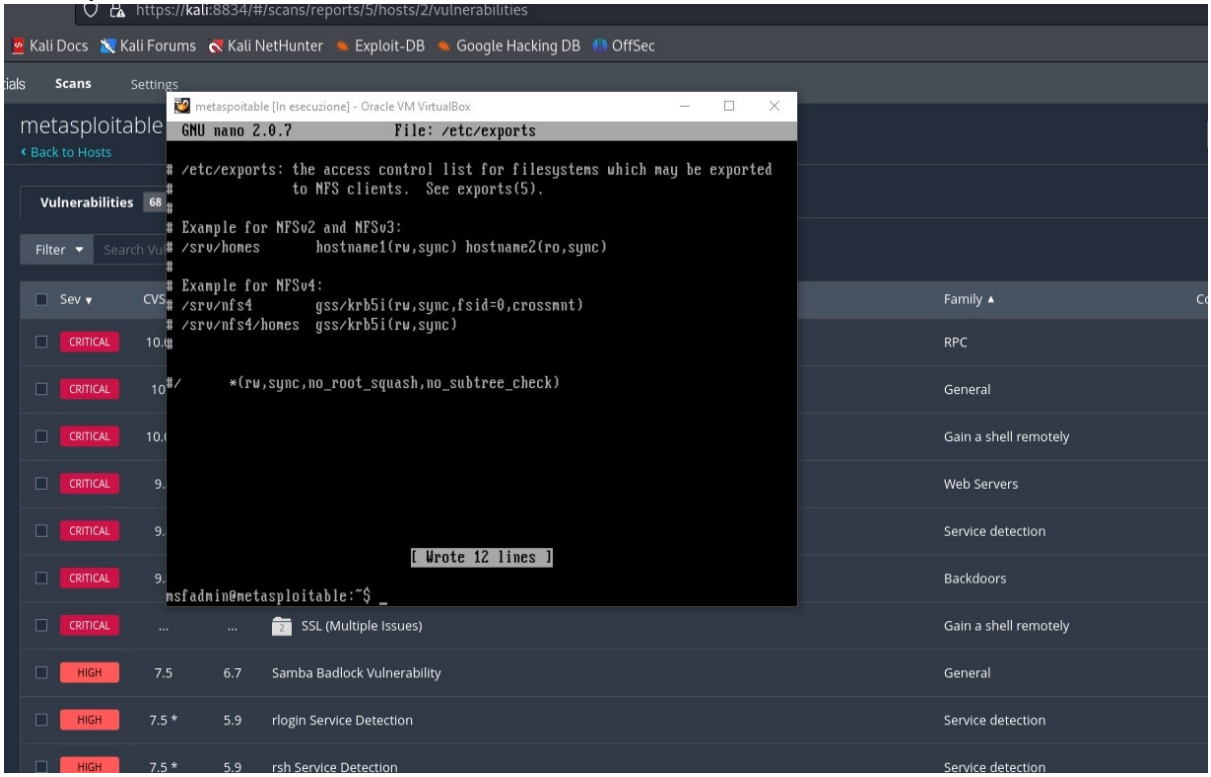


Scelta delle vulnerabilità (3)

- NFS Exported Share Information Disclosure
- VNC Server 'password' Password
- Bind Shell Backdoor Detection

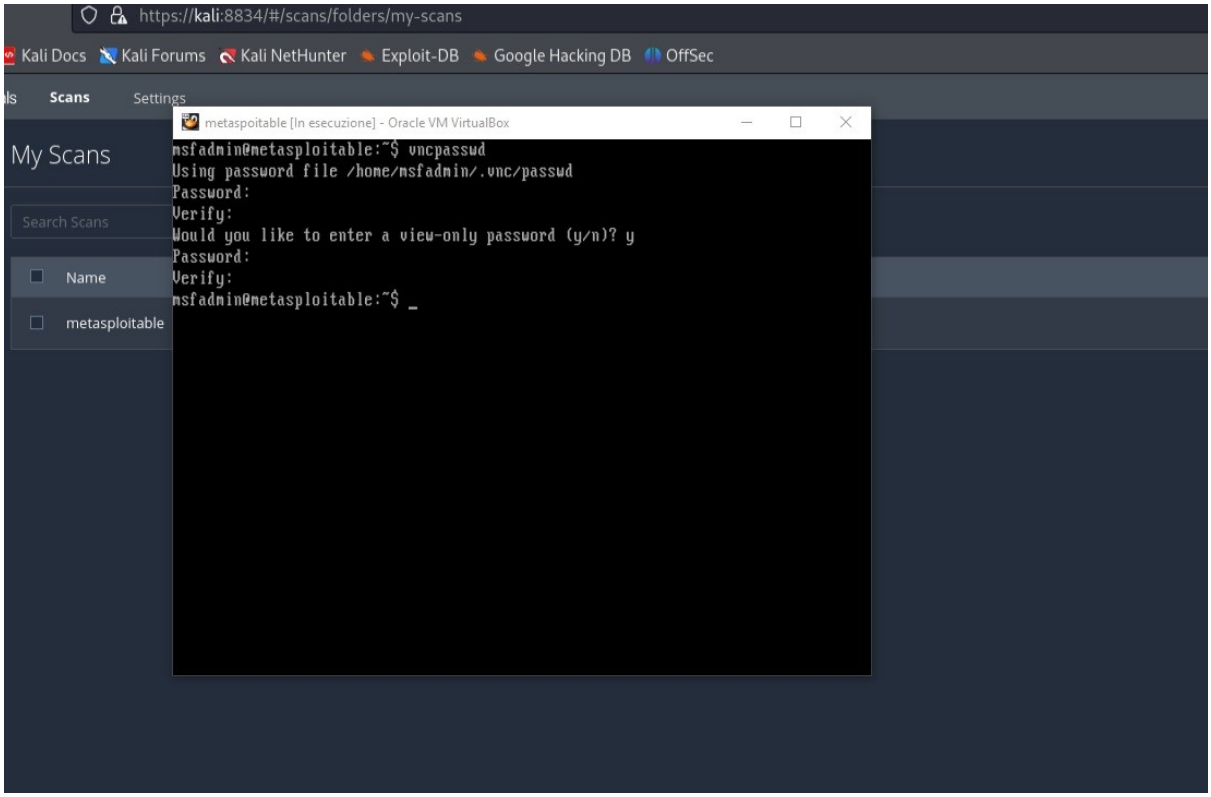
NFS Exported Share Information Disclosure



La vulnerabilita' segnala che le informazioni all'interno di una condivisione NFS possono essere accessibili a utenti non autorizzati. Questo potrebbe includere la possibilità di visualizzare, copiare o modificare file all'interno della condivisione.
Una delle azioni per poter risolvere la vulnerabilità indicata è andare a disabilitare il servizio; dunque inserendo da terminale **sudo nano /etc/exports** si accede alla lista dei file esportabili.

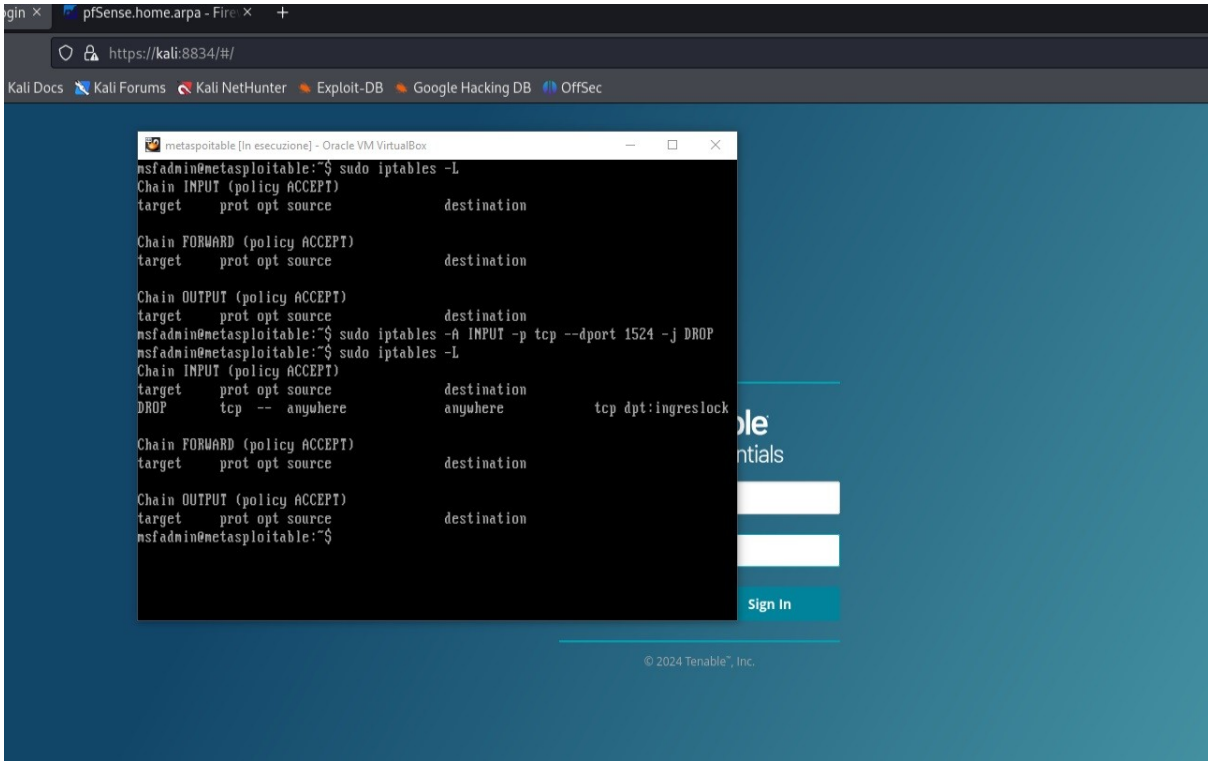
Il servizio era originariamente configurato per accettare tutte le connessioni da tutte le macchine assegnando i permessi di root con condivisione completa di tutto l'hard disk.
Modificando la riga e facendola diventare un commento, il servizio non ha piu' una lista di file disponibile e il servizio non e' attivo.

VNC Server 'password' Password

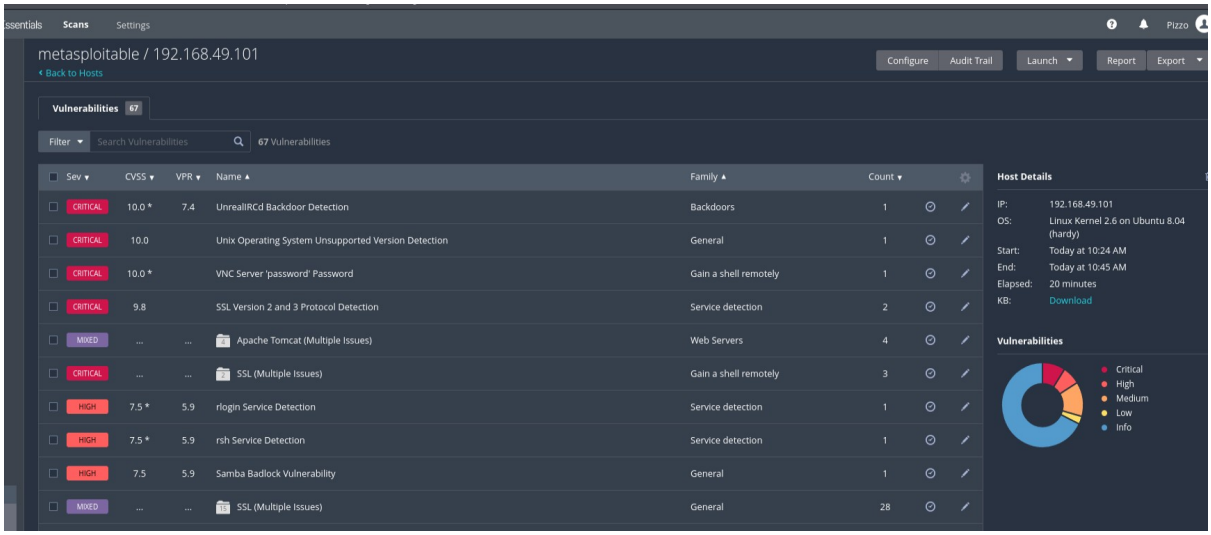


sudo exportfs -ra per restartare il NFS
La vulnerabilita' segnala che la password del servizio vnc e' debole in quanto Nessus e' stato in grado di accedervi semplicemente usando la parola "password". Il comando **vncpasswd** sulla macchina metasploitable, permette di cambiare la password di default

Bind Shell Backdoor Detection



La vulnerabilita' segnala che una shell e' in ascolto sulla porta 1524 e quindi puo' essere usata per inviare comandi da remoto. Una possibile soluzione e' impostare una regola nel firewall di metasploitable per chiudere quella porta.
sudo iptables -A INPUT -p tcp --dport 1524 -j DROP per impostare la regola.



Come si evince dall'immagine, due delle tre vulnerabilita' sono state risolte; la vulnerabilita' dellla password del vnc e' ancora presente ma probabilmente per un errore di ricezione di metasploitable; probabilmente se si riprovasse a modificarla di nuovo risulterebbe l'esito desiderato ma per motivi di tempistica non e' possibile ripetere la scan