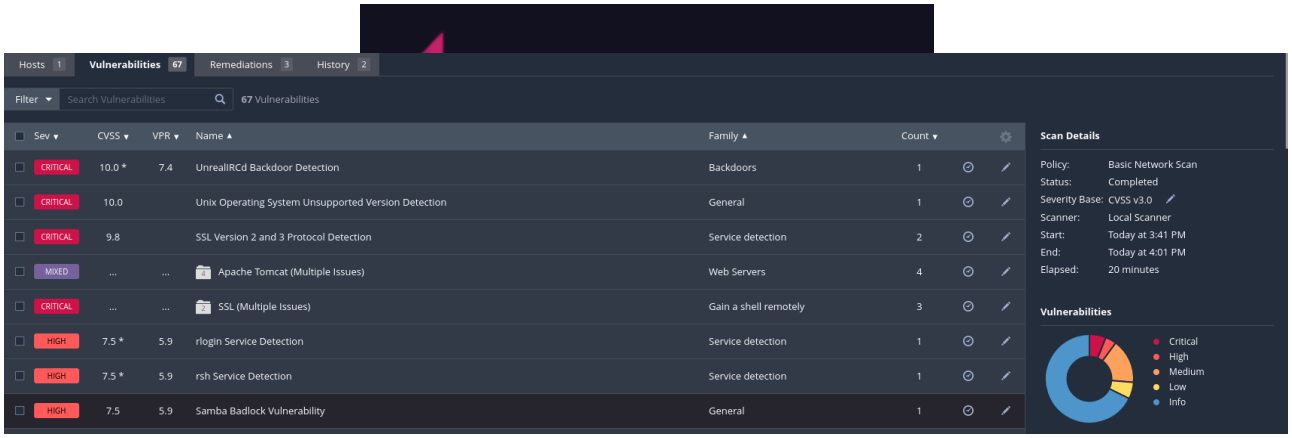


EPICODE-CS0124

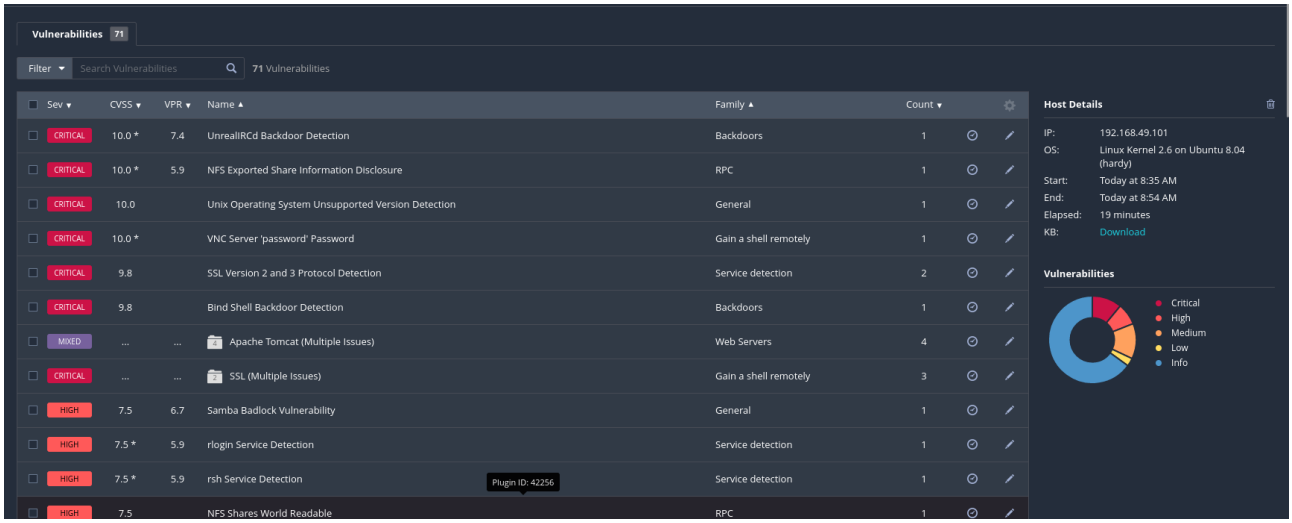
SETTIMANA 5 – PROGETTO FINALE

REPORT FINALE

La traccia del compito richiede di effettuare uno scan sul target Metasploitable, scegliere massimo 4 vulnerabilita' e successivamente cercare di migliorarle attraverso delle azioni di rimedio.

Al fine di effettuare uno scan completo di Metasploitable abbiamo utilizzato il software Nessus precedentemente installato su kali linux.

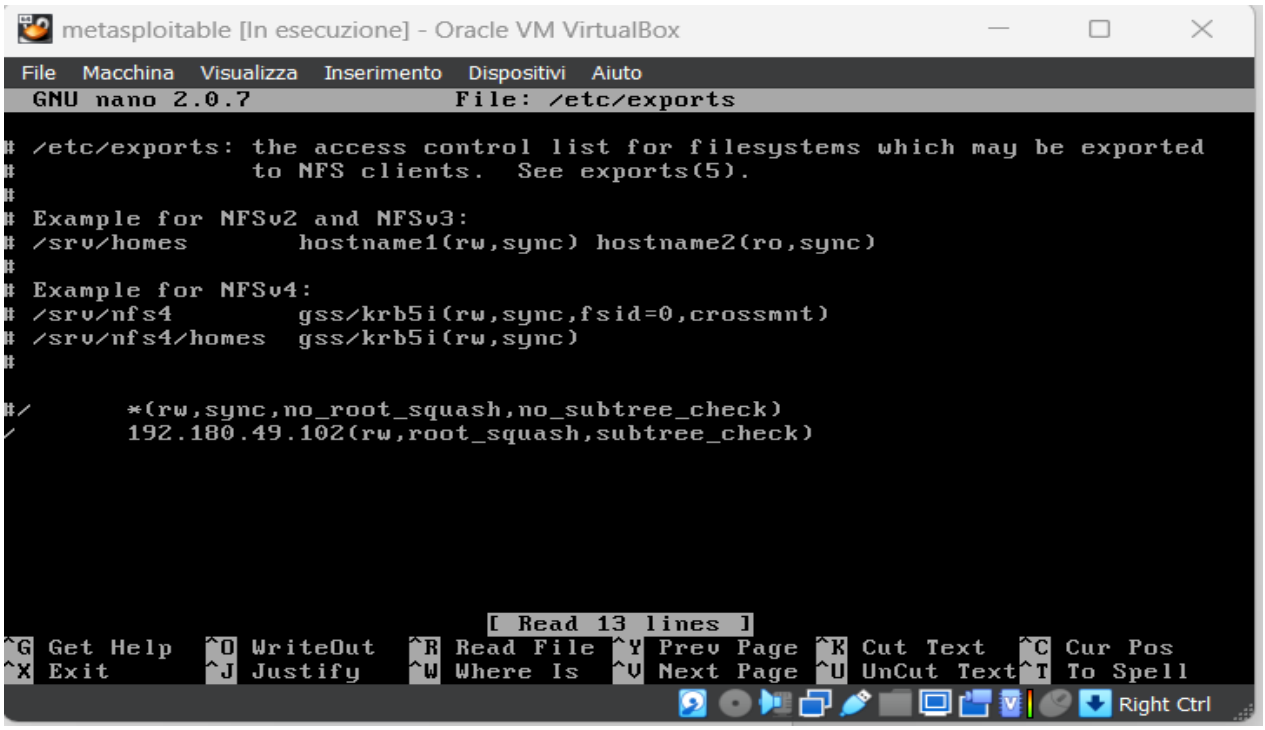
Dallo scan si evince che su Meta sono presenti diverse vulnerabilita' , evidenziando quelle critiche(High risk) in rosso;



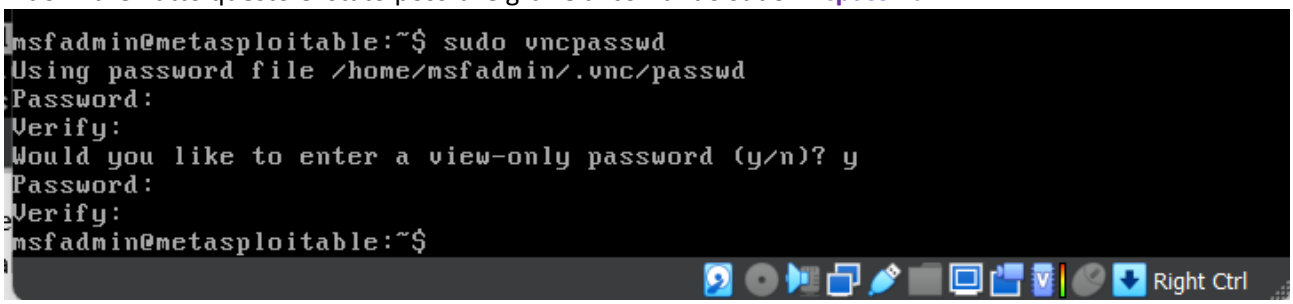
Una volta che abbiamo rilevato il quadro generale e acquisito la base di informazioni che ci interessano si passa all'azione su macchina Meta.

La prima vulnerabilita' di cui ci siamo occupati e' stata la NFS Exported Share information Disclosure .

Attraverso questa vulnerabilita' tutti gli host hanno accesso al protocollo NFS che serve per accedere a cartelle condivise da server remoti.Attraverso il comando **sudo nano /etc/exports/** abbiamo modificato il numero di host che si possono connettere mantenendo un host aperto con accesso al protocollo e mitigando i rischi da attacchi futuri.

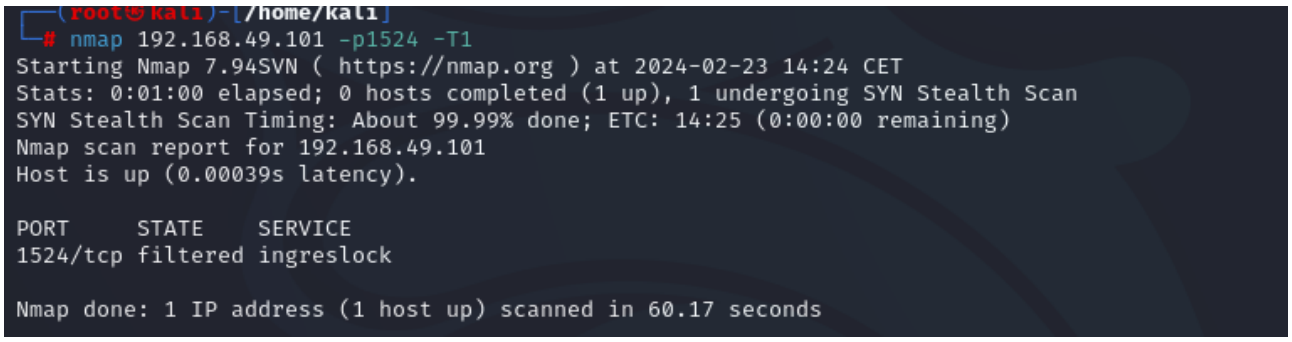


La seconda vulnerabilita' che abbiamo scelto di modificare e' stata l'inserimento di una nuova password per connettersi al Virtual Network Computing, dal momento che quella in uso era obsoleta. Siamo andati quindi a modificare la password attuale e l'abbiamo sostituita con una password piu' efficace e meno facile da indovinare.Tutto questo e' stato possibile grazie al comando sudo **vncpasswd**



L'ultima grande vulnerabilita' che abbiamo rilevato e' stata la backdoor sulla porta tcp 1524. Al fine di evitare possibili attacchi hacker da parte di esterni siamo intervenuti prima accedendo alla lista delle regole di input tramite il comando **sudo iptables -L --line-numbers** e inserendo una regola di chiusura della porta di riferimento tramite comando **sudo iptables -A INPUT -p tcp --dport 1524 -j DROP .**

Eseguendo una scansione nmap da kali possiamo quindi confermare che la porta sia chiusa.



CONCLUSIONE

A questo punto avviamo uno scan per verificare che tutte le vulnerabilita' che abbiamo preso come target siano state assolte, e possiamo vedere che a fronte delle 71 iniziali adesso ne risultano 67, quindi possiamo dedurre che il lavoro che abbiamo svolto e' andato a buon fine.