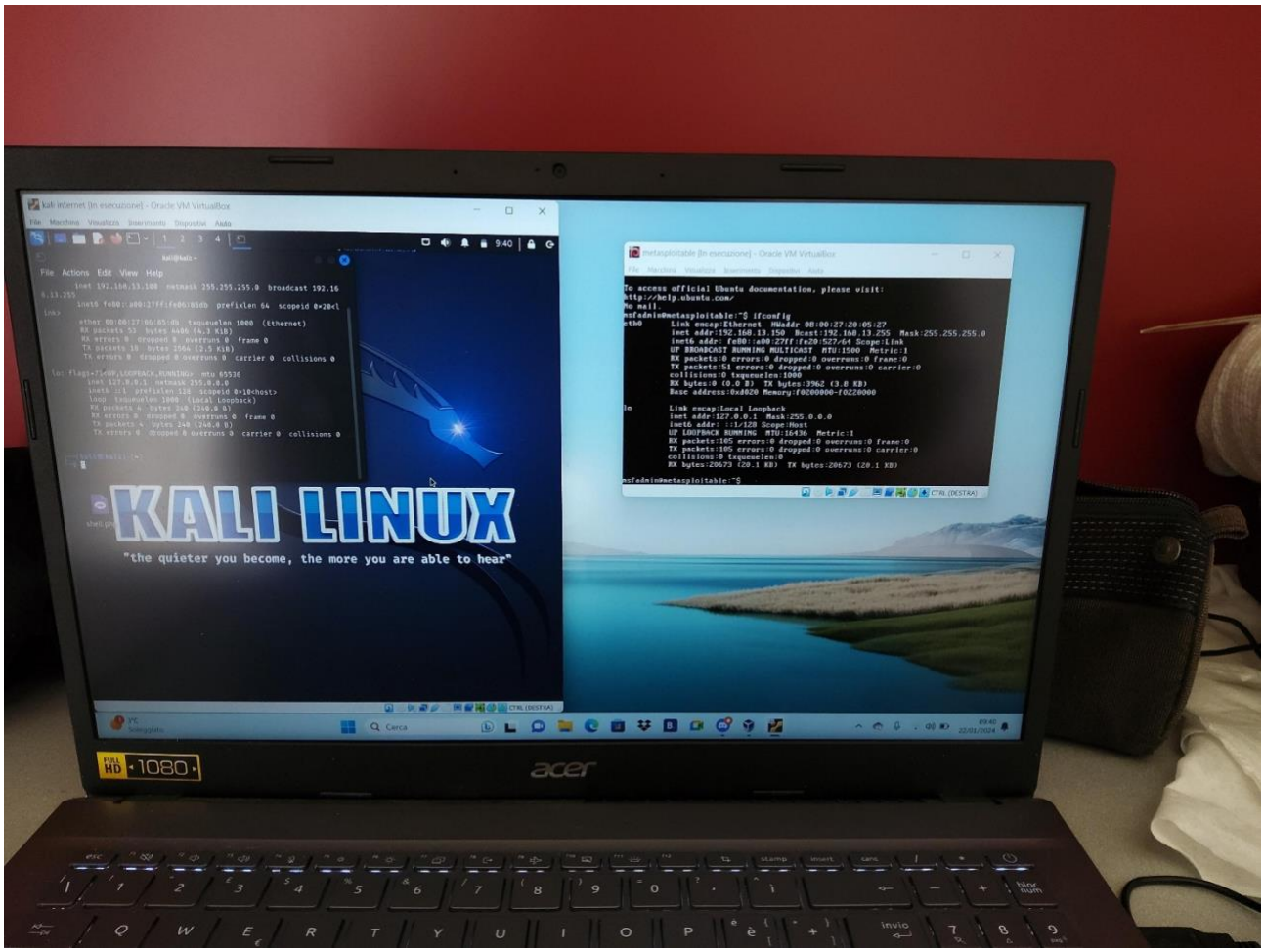
Scansione delle vulnerabilità sulla macchina e Implementazione delle soluzioni

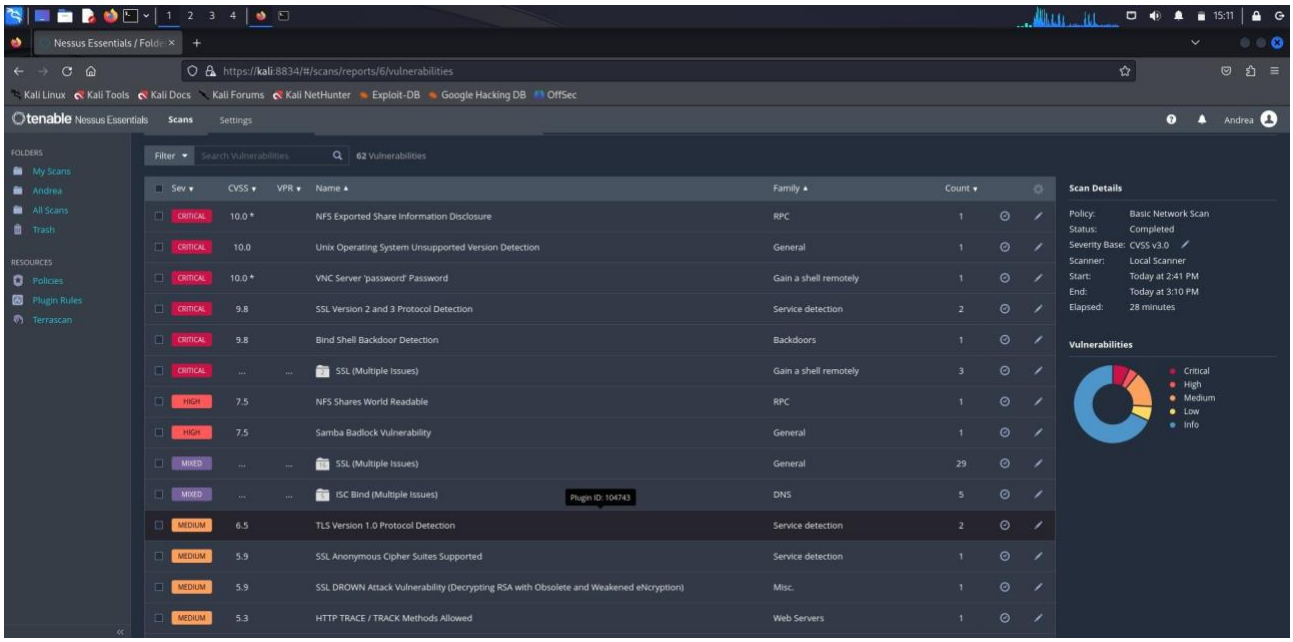
Il progetto di questa settimana ci chiederà di effettuare una scansione completa sul target Metasploitable per poi scegliete da un minimo di due vulnerabilità critiche / high e provare ad implementare delle azioni di rimedio.

Come prima azione bisogna collegare le macchine kali e Metasploitable in modo da effettuare la scansione tramite il Nessus, per effettuare il collegamento utilizzeremo il comando “Ping” seguito dalla indirizzo IP dell’altra macchina.



Una volta collegate le due macchine azioniamo il Nessus tramite il comando “sudo systemctl start nessusd.service” in seguito accediamo alle sue funzioni tramite l’indirizzo “https://kali:8834”.

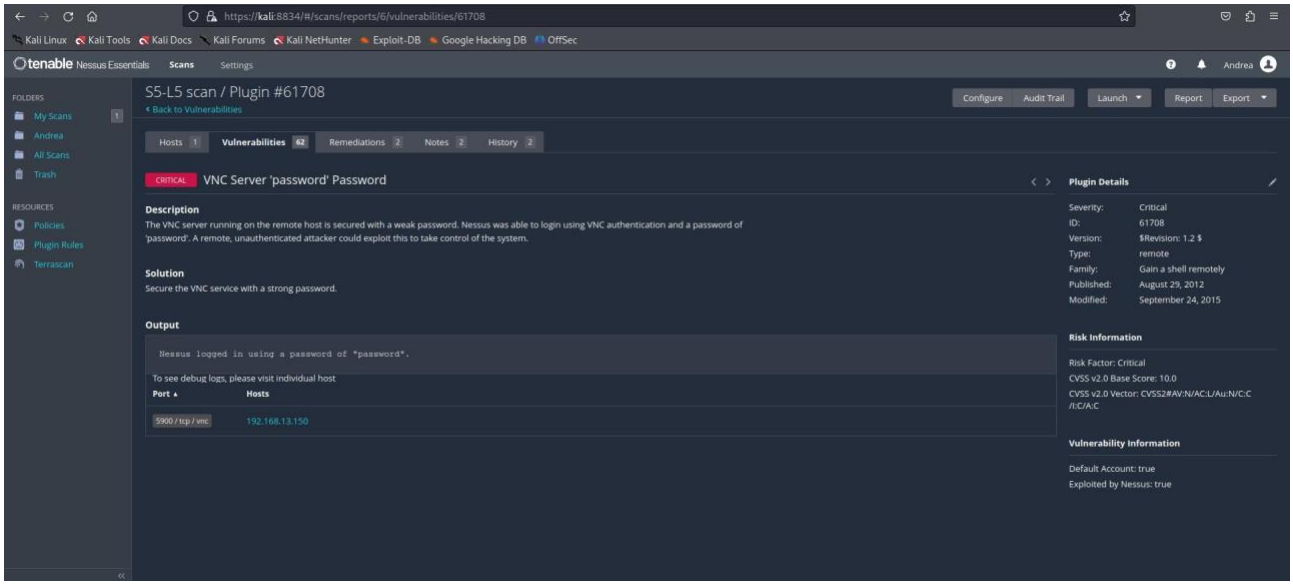
Una volta avviata la scansione ci apparirà una schermata con tutte le vulnerabilità presenti sulla macchina Metasploitable.



Le vulnerabilità che prenderemo in considerazione ai fini dell’esercizio sono due:

- VNC Server “password” Password (Critical Vulnerability)
- Samba Badlock Vulnerability (high Vulnerability)

Cliccando sulle vulnerabilità in questione possiamo capire come risolvere il problema in particolare per il VNC Server “password” Password il Vulnerability scanner mostra come sia troppo semplice accedere al server da remoto in quanto la password: ”Password” è troppo banale e rende il sistema vulnerabile ad attacchi di potenziali malintenzionati



Infine per il Samba Badlock Vulnerability il Nessus ci mostra come sia troppo obsoleto e che ormai esistono versioni più recenti e sicure dello stesso, infatti, una fragilità in questo campo permetterebbe una più facile penetrazione da parte di attacchi Man in the middle.