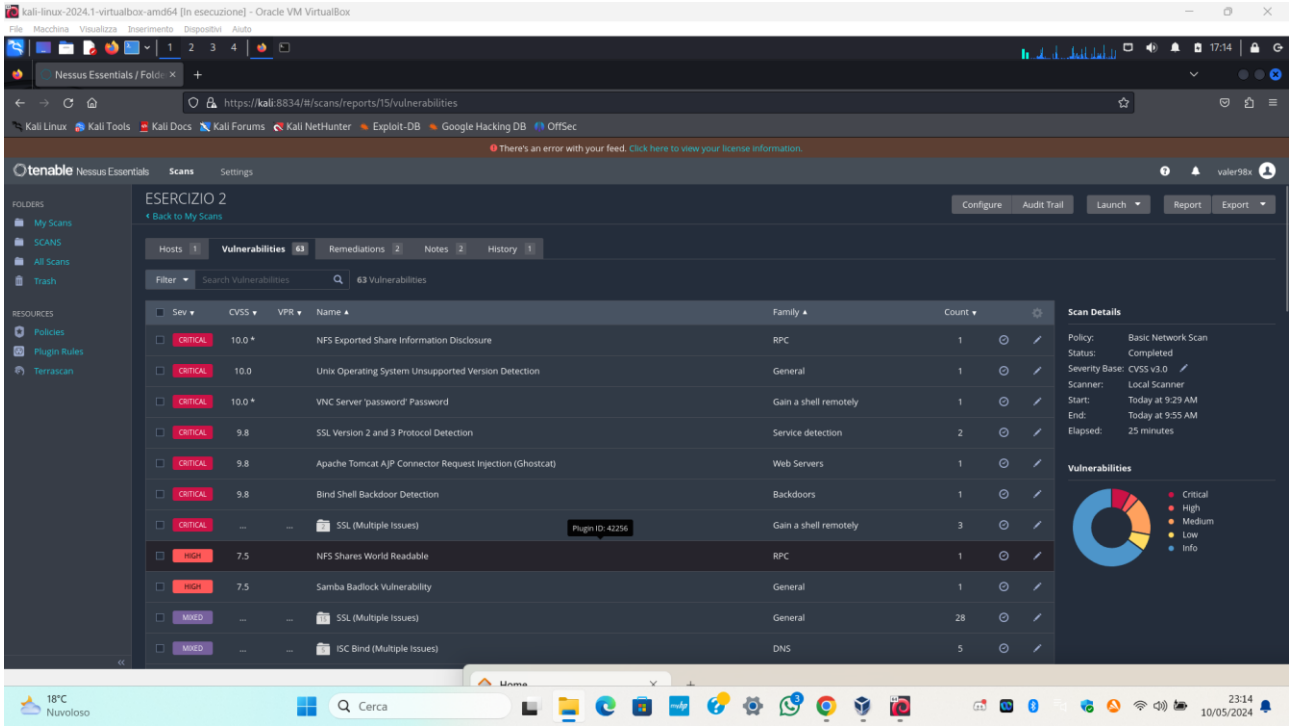
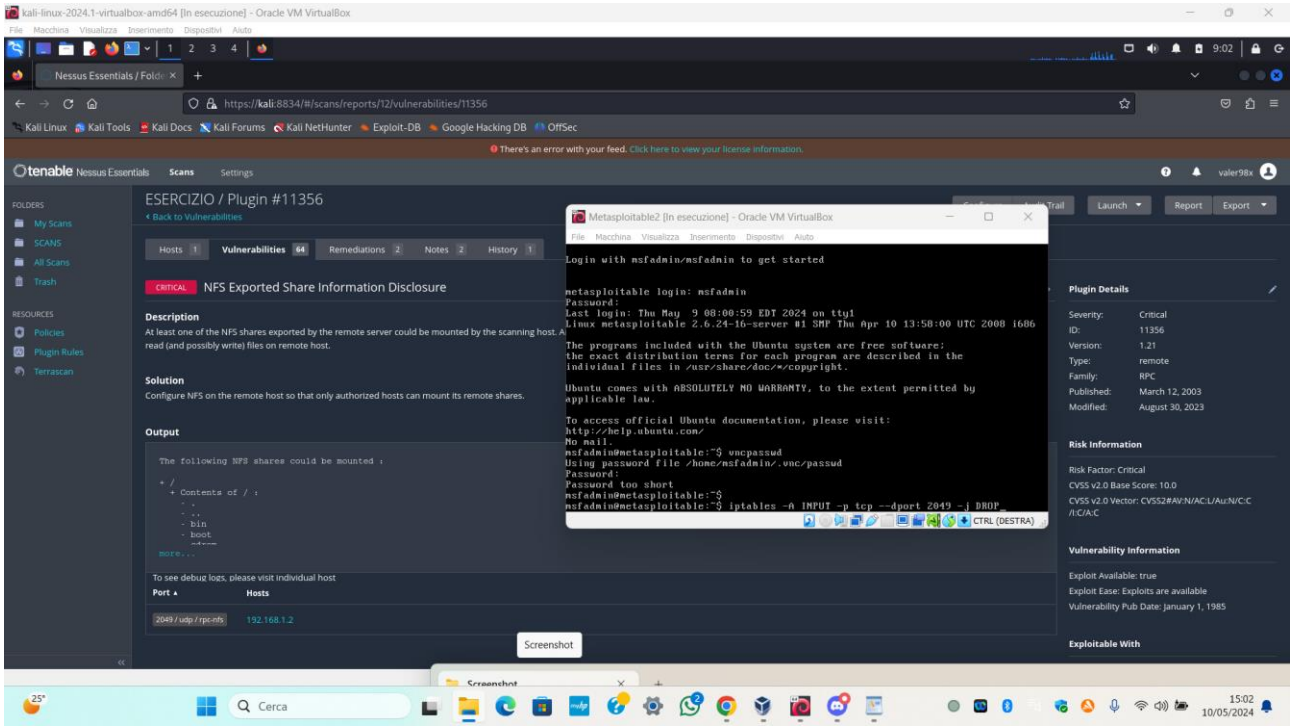
Dopo aver effettuato una scansione con Nessus sulla macchina Metasploitable notiamo che ci vengono restituite le vulnerabilità principali della macchina in ordine di criticità.



Vediamo di seguito alcune modalità per gestire 3 di queste vulnerabilità di livello critico.

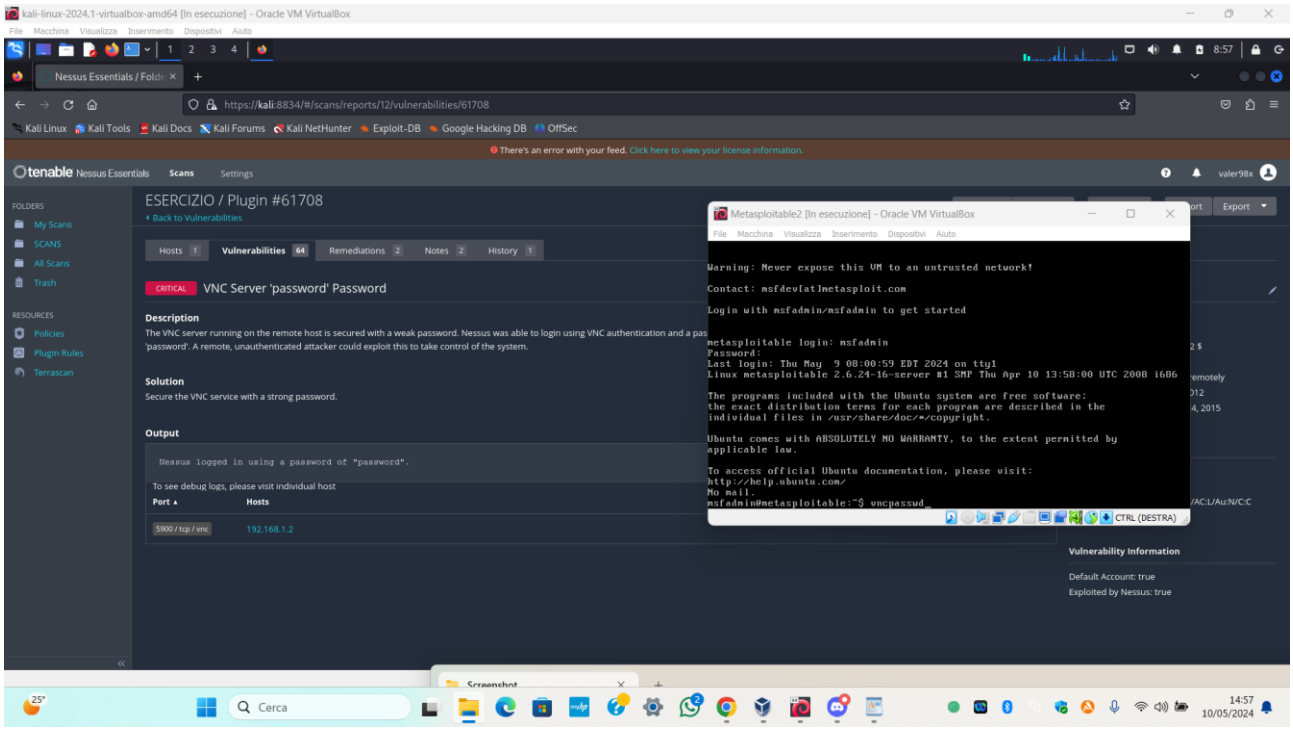
1) “NFS EXPORTED SHARE INFORMATION DISCLOSURE”

Qui ci viene detto che la porta 2049, su cui è attivo il protocollo Network File System (Protocollo usato per la condivisione dei dati) è vulnerabile. Possiamo utilizzare un firewall per bloccare le connessioni con altri host e prevenire attacchi tramite il comando: “iptables –A INPUT –p tcp –dport 2049 –j DROP”. Impostando questo comando la porta verrà bloccata e il traffico ad essa associato sarà interrotto, impedendo eventuali attacchi.



2) “VNC server ‘password’ Password”

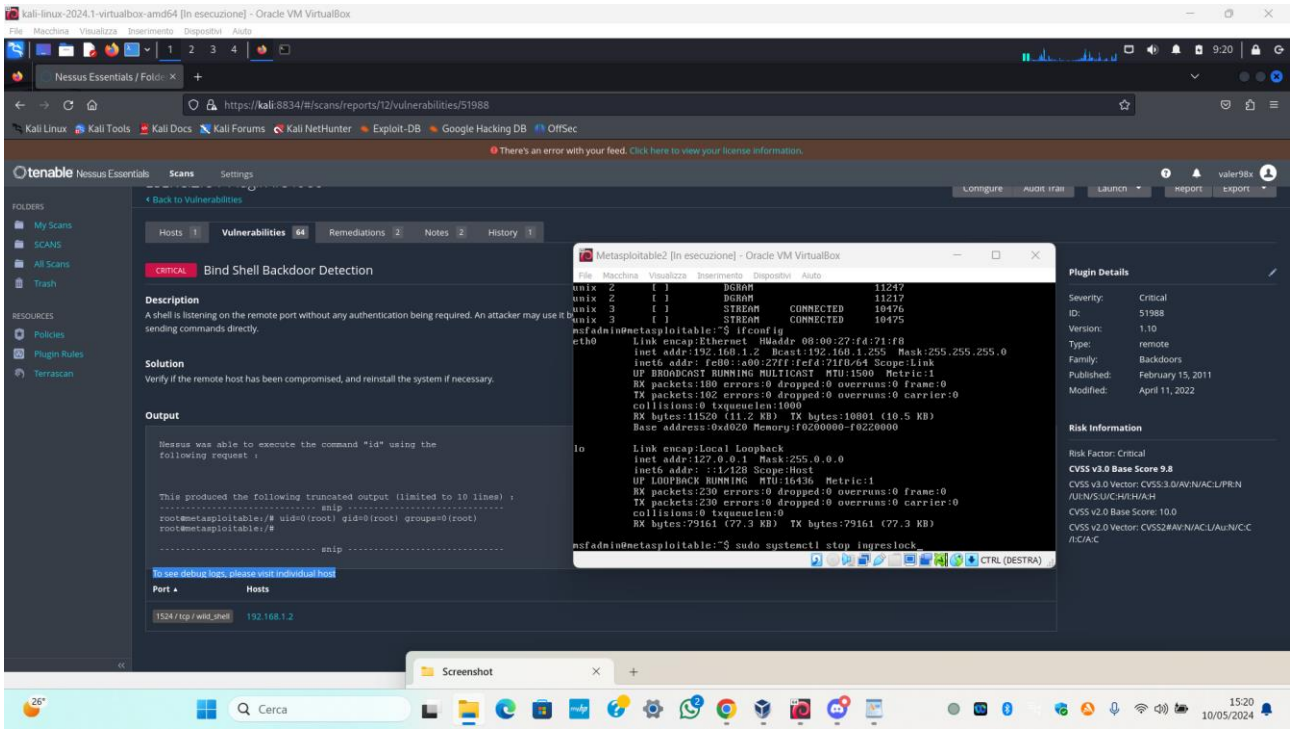
Nessus ci comunica che la password associata al servizio VNC server è molto debole. Il programma di scanning, infatti, ha effettuato un tentativo di accesso remoto alla macchina Metasploitable, riuscendo ad aggirare facilmente la password (ovvero “password”). In questo caso basterà semplicemente cambiare la password VNC con una più complessa (per esempio xTn6ChM5).



3) “Bind shell backroom detection”

Si tratta della concreta possibilità che un malintenzionato crei una backdoor ed inizi a controllare a distanza la nostra macchina. Dallo scan di rete effettuato con kali, vediamo che alla porta 1524 è associato il servizio ingreslock (che gestisce e coordina l’accesso di più utenti al database).

Supponiamo di essere l’unico utente ad accedere alla macchina Metasploitable (dunque il servizio diventa di utilità trascurabile); è possibile, in questo caso, disattivare il servizio stesso. Utilizziamo il comando “sudo systemctl stop ingreslock”.



Per essere sicuri di aver sistemato le vulnerabilità effettuiamo una nuova scansione.