# S5L5

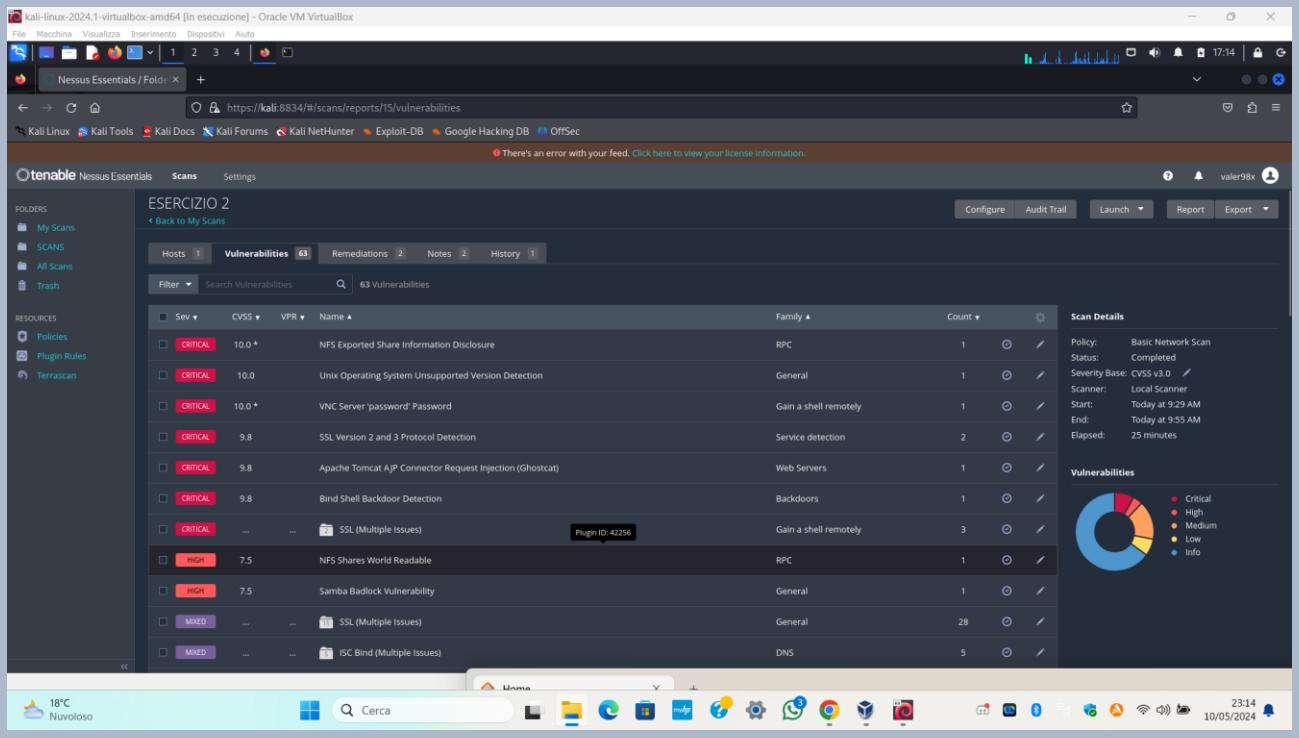
## TRACCIA:

Effettuare una scansione completa sul target Metasploitable.
Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.
Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Per questo esercizio, utilizzeremo Nessus. Come appreso nelle lezioni di questa settimana, Nessus è uno dei software più utilizzati per la scansione e la valutazione della sicurezza delle reti e dei sistemi informatici.

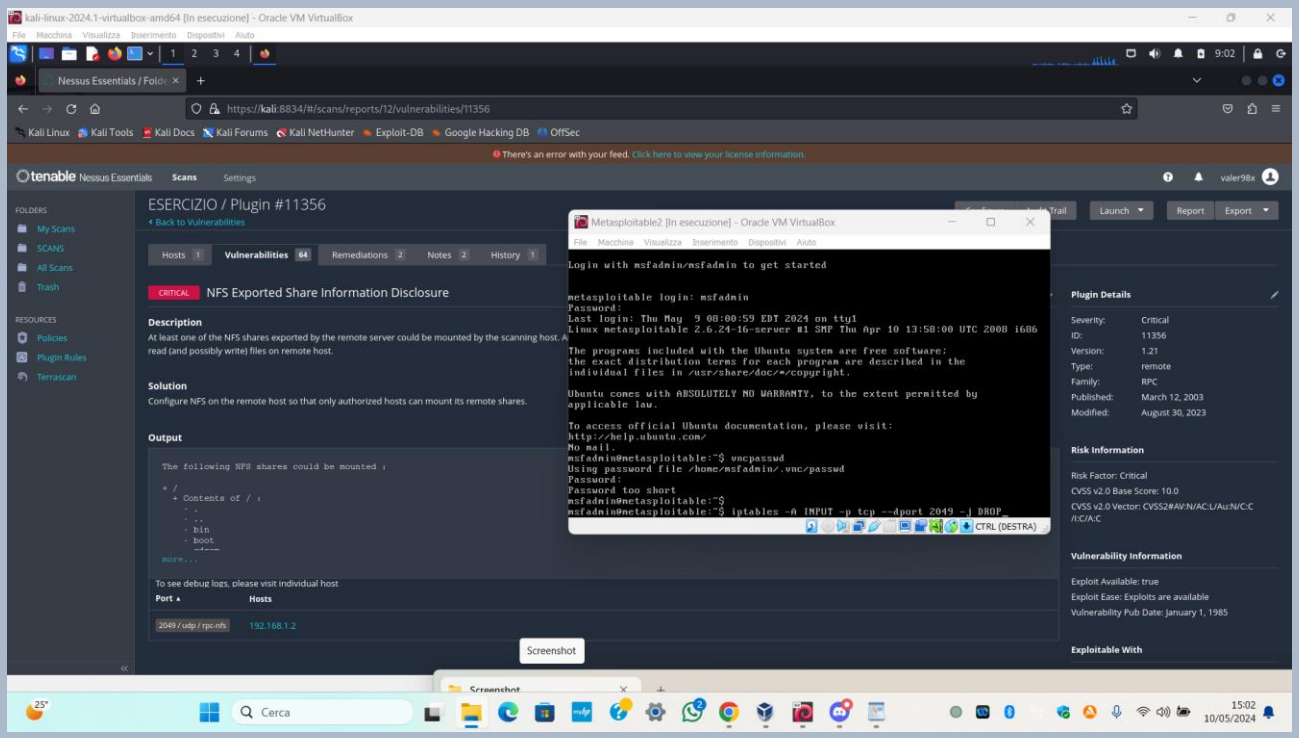
Esso effettua analisi approfondite delle vulnerabilità e delle configurazioni non sicure presenti sui dispositivi di rete, inclusi server, router, switch e dispositivi endpoint. Utilizzando una vasta gamma di plugin e tecniche di scansione, Nessus identifica vulnerabilità note, configurazioni errate e potenziali punti deboli che potrebbero essere sfruttati dagli attaccanti per compromettere la sicurezza di un sistema.

Una volta completata la scansione, Nessus fornisce report dettagliati con raccomandazioni per risolvere le vulnerabilità individuate e migliorare complessivamente la sicurezza del sistema.




Nella foto allegata sopra possiamo notare che ultimata la scansione con Nessus sulla macchina Metasploitable, ci vengono segnalate le vulnerabilità della macchina in ordine di criticità.

Di seguito vengono analizzate 3 vulnerabilità di livello critico a cui apporteremo delle azioni di rimedio come richiesto per il progetto di questa settimana.

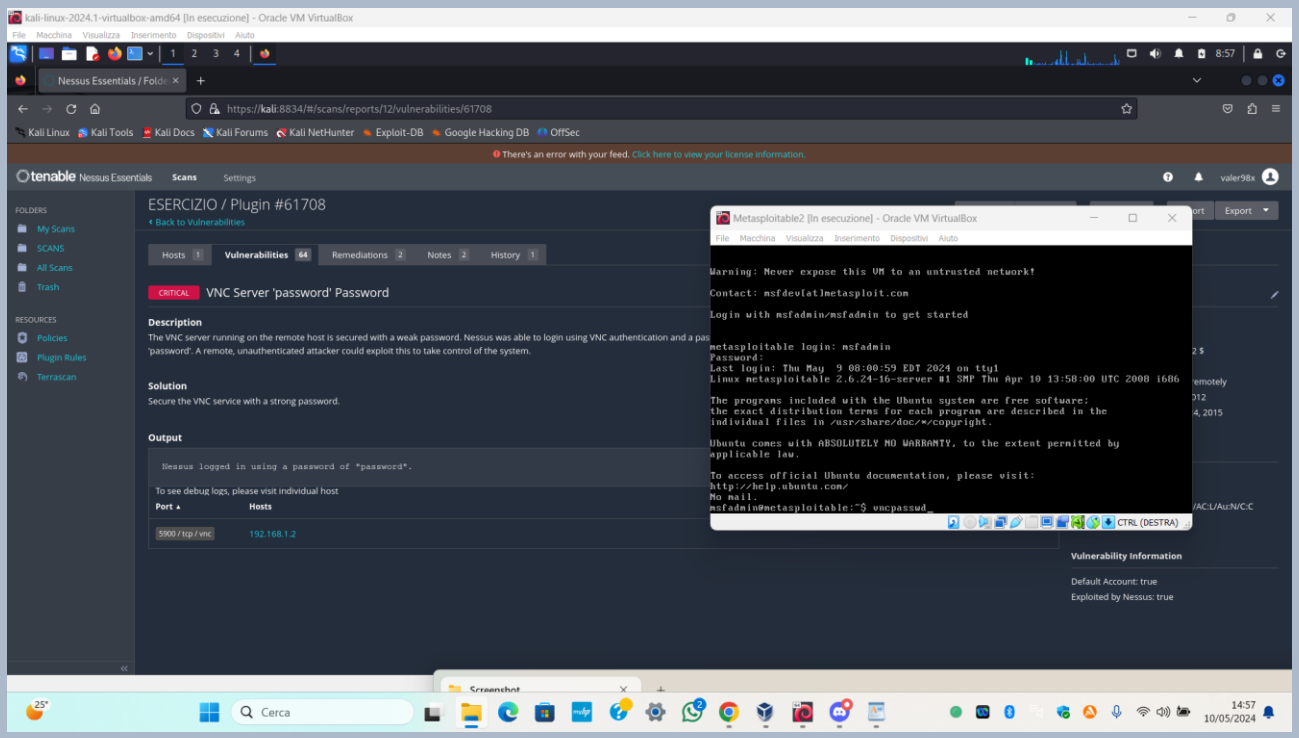



**NFS EXPORTED SHARE INFORMATION DISCLOSURE**
Rilevamento di informazioni sensibili tramite condivisione NFS

Durante l'analisi è emerso che la porta 2049, utilizzata per il controllo Network File System (NFS), presenta una potenziale vulnerabilità che potrebbe compromettere la sicurezza dei dati condivisi. Al fine di mitigare questo rischio, si può implementare una regola del firewall per bloccare le connessioni in ingresso sulla porta 2049. Una possibile configurazione consiste nell'utilizzare il seguente comando iptables:

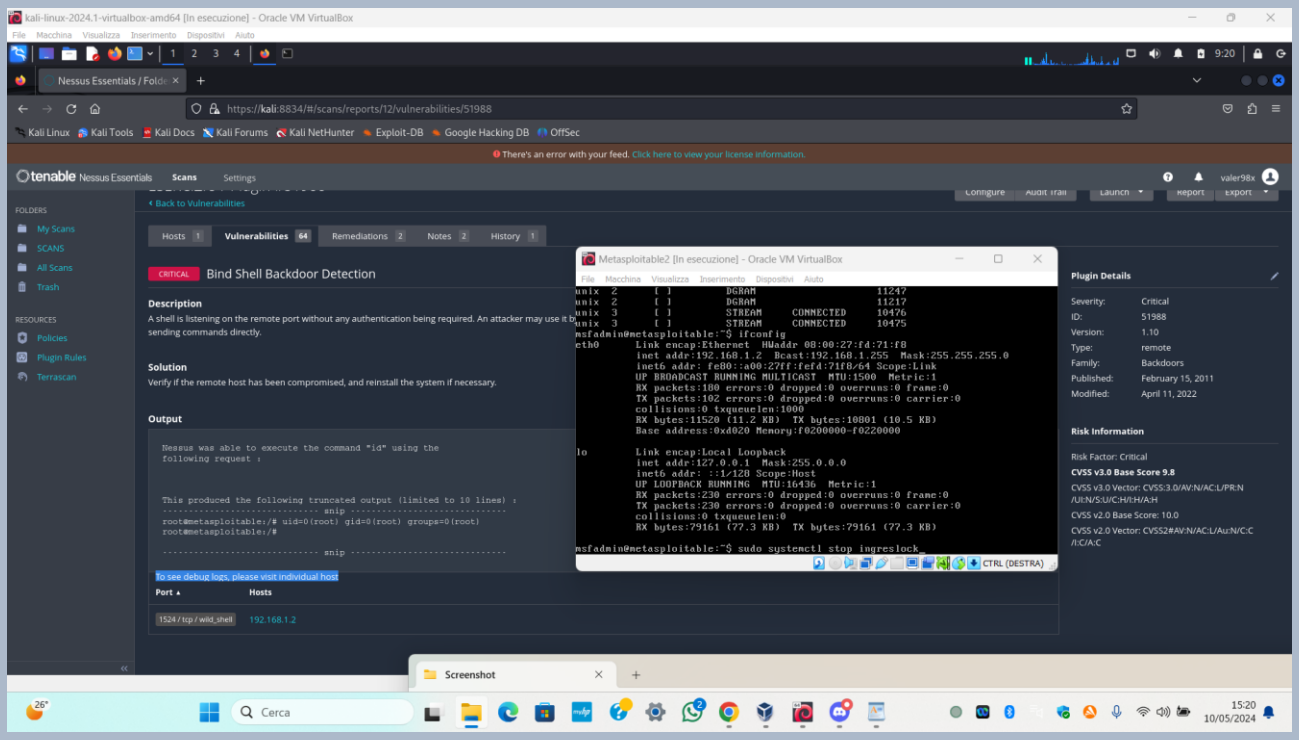
```
iptables -A INPUT -p tcp -dport 2049 -j DROP
```

L'esecuzione di questo comando comporterà il blocco della porta e la cessazione del traffico associato ad essa, contribuendo così a prevenire potenziali attacchi e proteggere l'integrità dei dati condivisi.




**VNC SERVER ‘PASSWORD’ PASSWORD**
Debolezza della password del server VNC

Durante lo scan, è stato rilevato che la password utilizzata per il servizio VNC server risulta estremamente vulnerabile. L’analisi condotta tramite Nessus ha evidenziato che il programma è stato in grado di accedere remotamente alla macchina Metasploitable bypassando la password predefinita “password”.
Al fine di rafforzare la sicurezza del sistema, sostituiamo la password VNC con una più robusta e complessa, ad esempio “xTn6ChM5”.




**BIND SHELL BACKDOOR DETECTION**
Rilevamento di Backdoor con Bind Shell

Durante l'analisi, è stata individuata la potenziale presenza di una backdoor tramite Bind Shell, che potrebbe consentire a un attaccante di assumere il controllo remoto della macchina bersaglio.

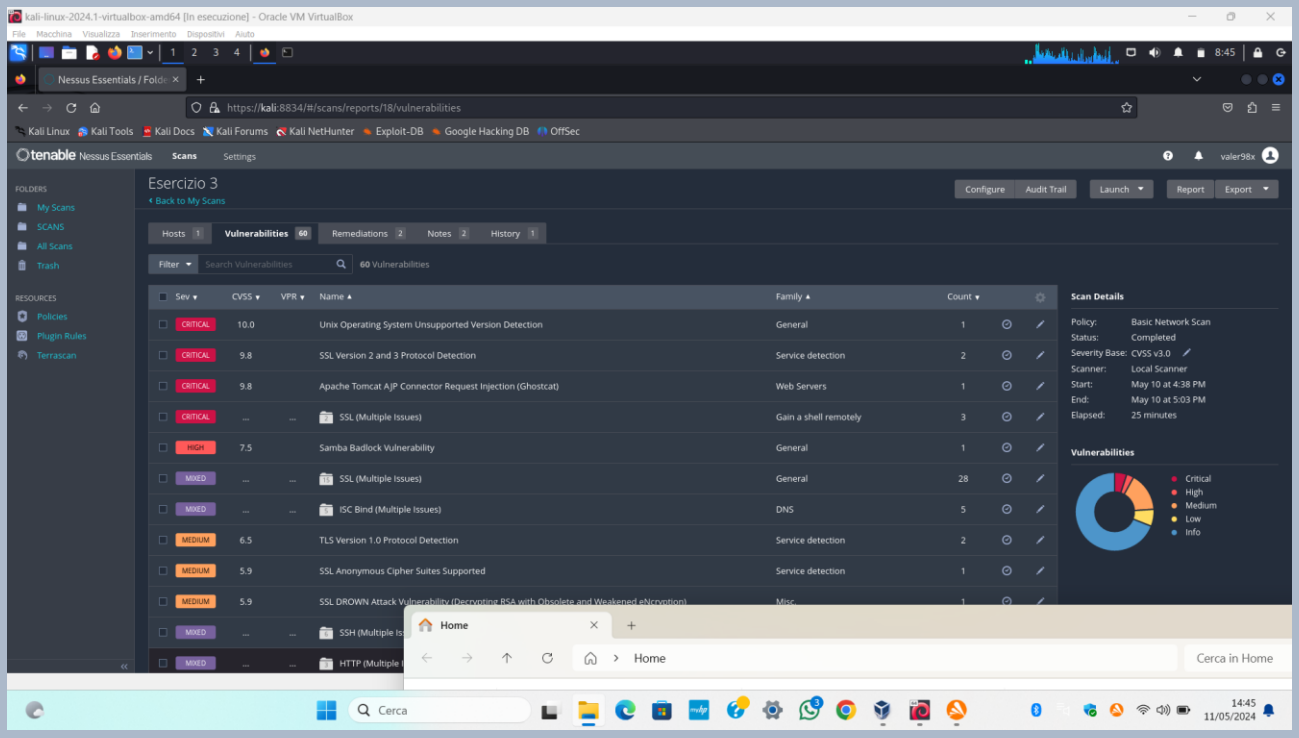
L'ispezione della rete effettuata, ha rilevato che alla porta 1524 è associato il servizio "ingreslock", il quale gestisce l'accesso multiutente al database.

Considerando che l'accesso alla macchina Metasploitable è limitato a un unico utente, l'utilità di questo servizio diventa trascurabile. Di conseguenza, è opportuno disattivarlo con le istruzioni

sudo systemctl stop ingreslock

Questo comando mitigherà il rischio di possibili attacchi e garantirà la sicurezza del sistema.

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




**NB: questo progetto è stato effettuato in collaborazione con Valerio Zampone che ha cordialmente offerto aiuto riguardo la scansione della macchina Metasplotable a causa di problemi di esecuzione di Nessus sulla mia macchina.**