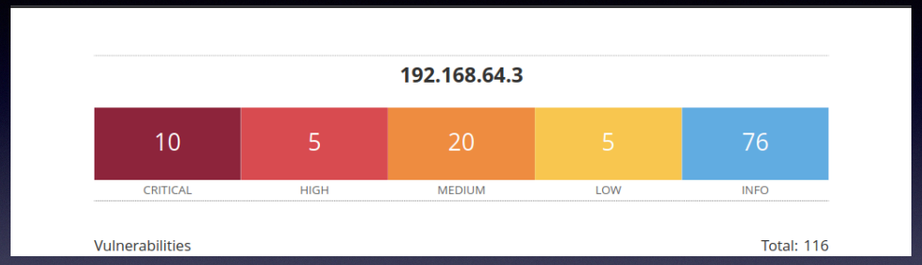
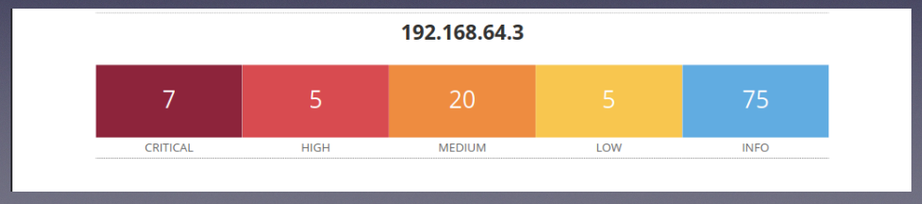
REPORT NESSUS

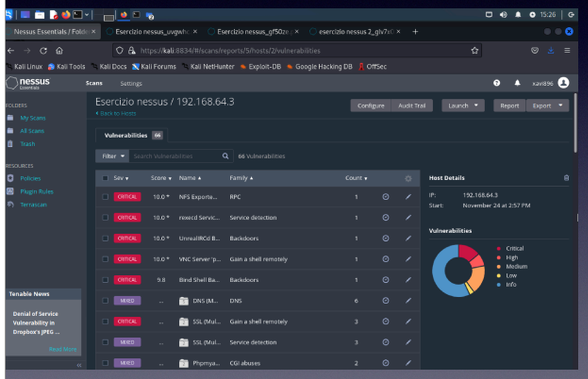
Questo report ha come scopo di illustrare come come risolvere eventuali vulnerabilità riscontrate nelle scansioni del programma nessus.

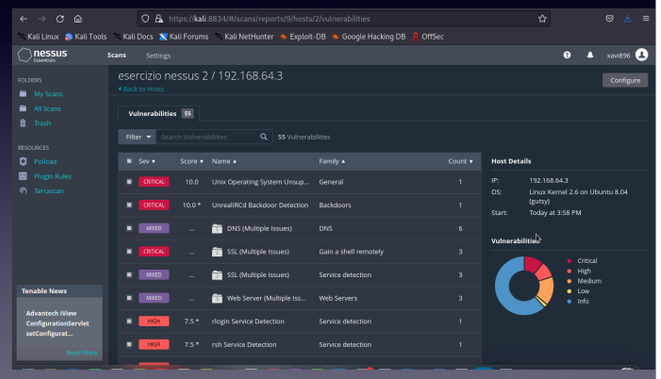
Queste immagini riportano il risultato delle scansioni effettuate prima e dopo.





Queste immagini ci riportano due tipi di scansioni, la prima a sinistra ci illustra una scansione iniziale, dove la macchina bersaglio ci espone tutte le sue vulnerabilità. La seconda a destra invece ci mostra come la situazione sia cambiata dopo che abbiamo risolto tre vulnerabilità critiche.

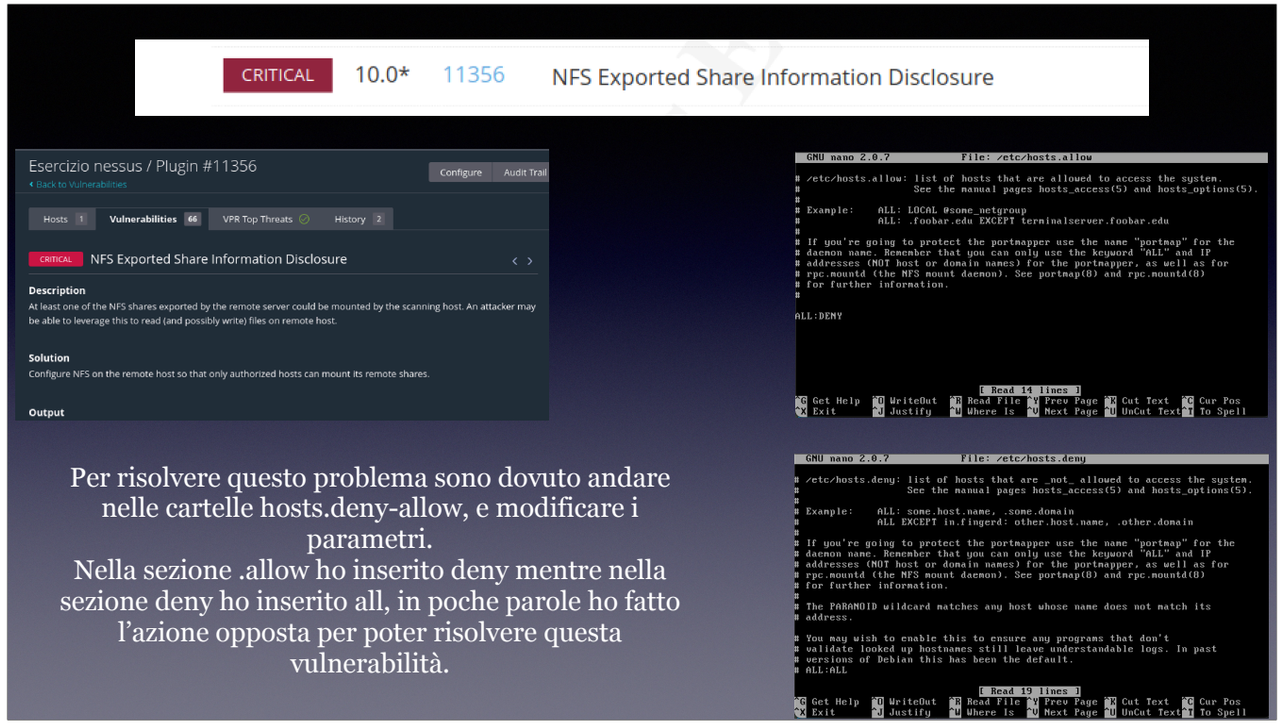




Le prossime slide ci illustreranno come siamo andati a risolvere tre di queste vulnerabilità

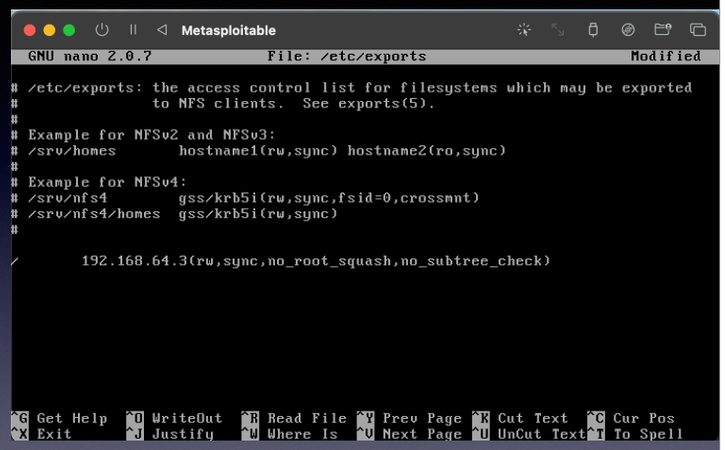
Vulnerabilità da analizzare e risolvere:

CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	61708	VNC Server 'password' Password
CRITICAL	9.8	51988	Bind Shell Backdoor Detection

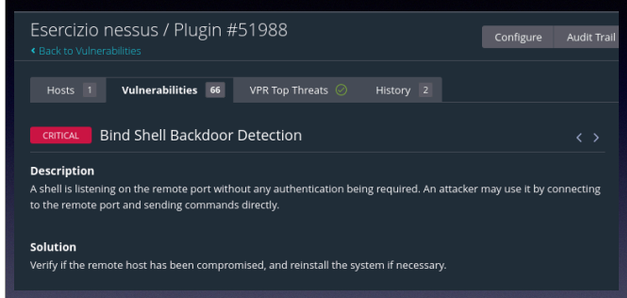


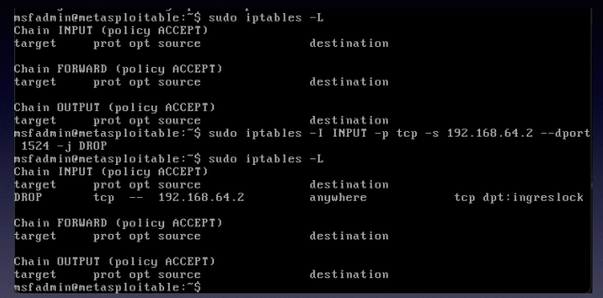
Per risolvere questo problema sono dovuto andare nelle cartelle hosts.deny-allow, e modificare i parametri.
Nella sezione .allow ho inserito deny mentre nella sezione deny ho inserito all, in poche parole ho fatto l'azione opposta per poter risolvere questa vulnerabilità.

In alternativa potevamo ovviare allo stesso problema tramite comando (sudo nano /etc/exports) e inserire inserire indirizzo ip della macchina bersaglio in modo da bloccare in automatico la vulnerabilità NFS.



Questa vulnerabilità è stata semplice da risolvere in quanto non c'era una password di accesso e quindi la macchina attaccante poteva effettuare login molto facilmente. In risposta a ciò ho creato una password complessa in modo che nessun altra macchina possa effettuare l'accesso.





Per risolvere il problema delle backdoor in entrata sono andato a modificare il firewall tramite il comando iptables (sudo iptables -I INPUT -p tcp IP target — dport 1524 - DROP).
In questo modo la macchina bersaglio non accetta comunicazioni con la macchina attaccante.

EPICODE

In conclusione, possiamo dedurre che le scansioni hanno come scopo di mostrare eventuali vulnerabilità e risolverne quante più possibili in modo da ridurre potenziali rischi e attacchi da parte di malintenzionati.

GRAZIE

Epicode