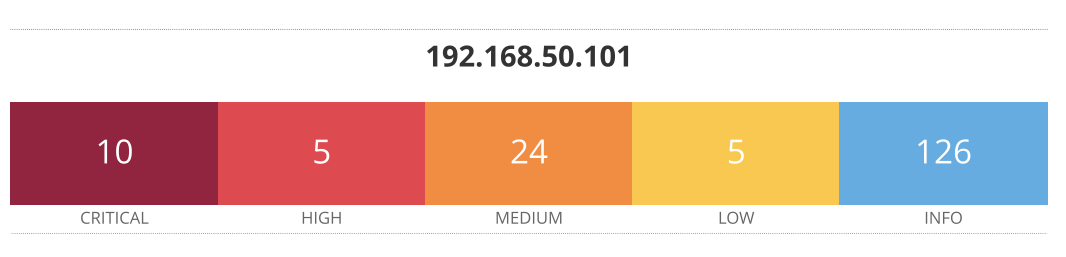
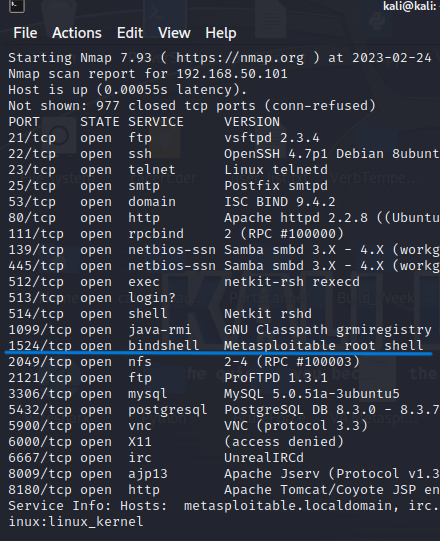
Esercizio 24-02

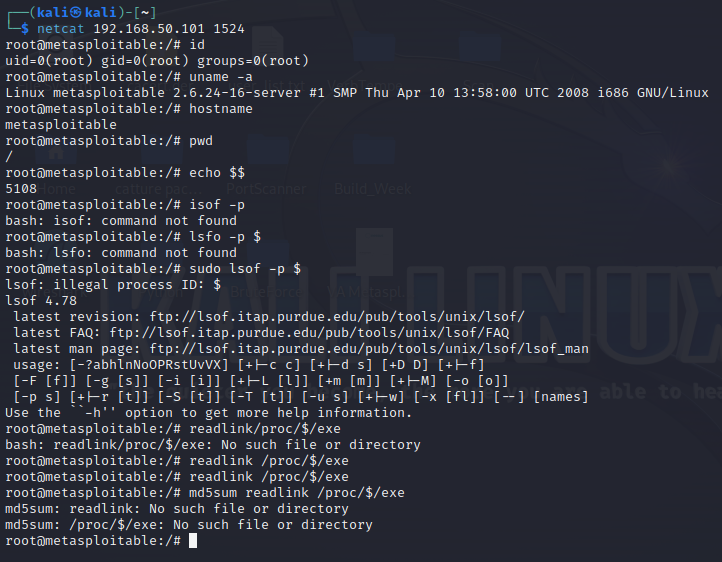
Traccia: effettuare una scansione delle vulnerabilità sulla macchina Metasploitable e risolvere da un minimo di 2 a un massimo di 4/5 vulnerabilità di livello critico tra quelle trovate.

Indicazioni: le soluzioni non possono essere raggiunte aggiornando sistemi/applicazioni a versioni più recenti, devono essere operazioni manuali da dentro la macchina. l’utilizzo di regole Firewall vale per un massimo di 1 soluzione.

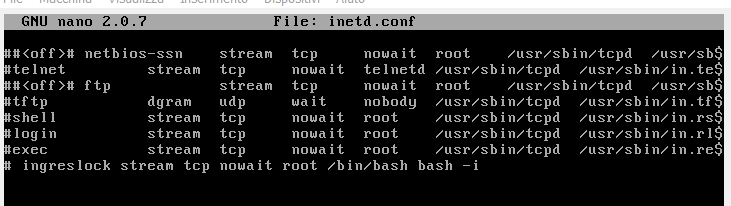
Correzione errore 51988

Effettuando una scansione nmap da Kali verso l’indirizzo di Metasploitable troviamo una porta con servizio attivo “bindshell”, porta 1524.

Tento di connettermi al servizio con il comando netcat IP di Metasploitable e 1524 (porta)

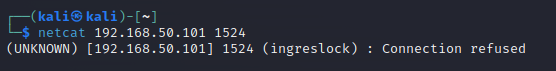
Dopo essere riuscito a connettermi eseguo qualche comando per testare le funzionalità che mi concede la backdoor.

Da terminale di Metasploitable mi muovo nella cartella /etc e cerco la backdoor.

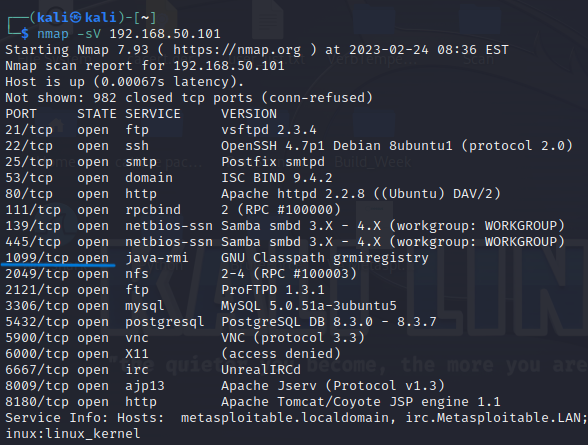


Utilizzo del comando sudo nano inetd.conf, la backdoor, e commentando le righe di codice la rendiamo “vuota”.

Ritento l’accesso alla backdoor da kali

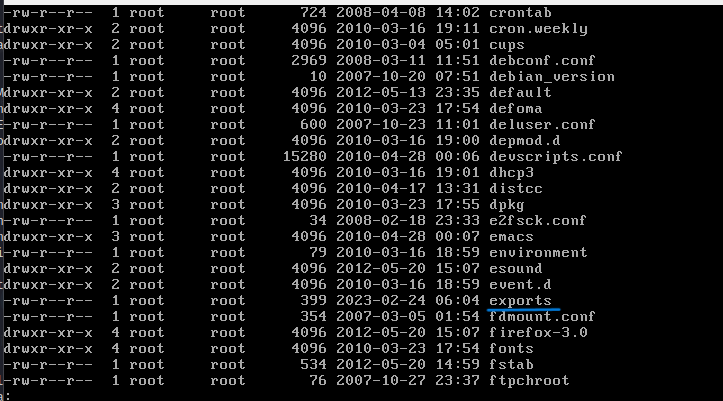


Connessione rifiutata, per sicurezza lancio di nuovo una scansione nmap.

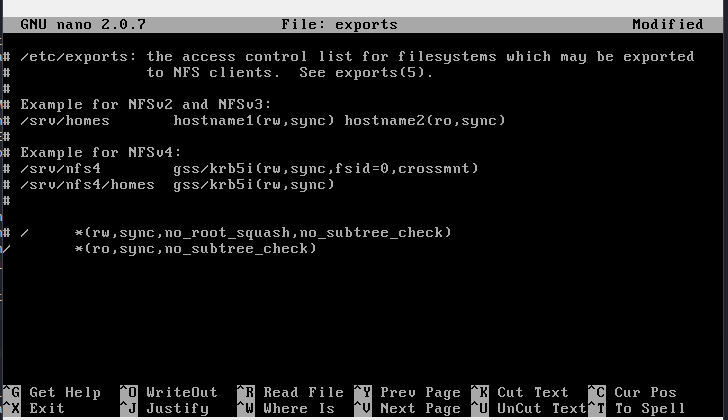
La porta 1524 non è più tra le porte aperte.

Correzione errore 11356

Mi sposto nella cartella /etc alla ricerca del file exports.

Utilizzo del comando ls -l | less per movimento verticale nella lista.

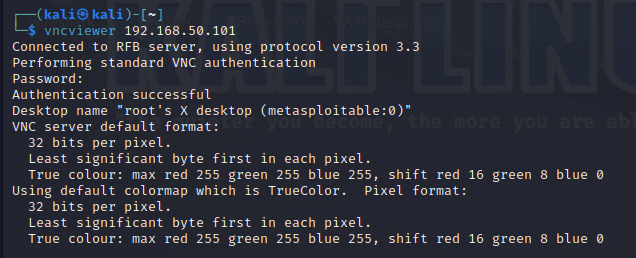
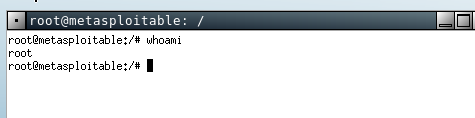
Apertura del file con editor di testo con comando sudo nano exports.



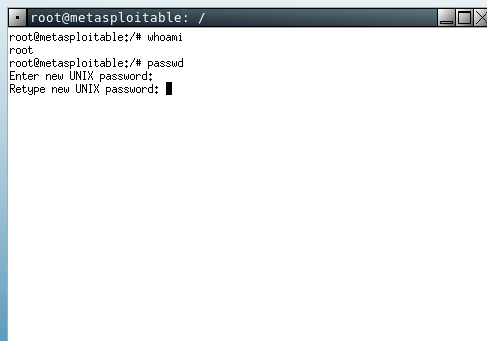
La penultima riga conferiva l’accesso da qualunque directory, lettura e scrittura file, privilegi amministratore. Commentata così da rendere nulla e aggiunta una nuova riga che conferisce sola lettura a chi accede.

Correzione errore 61708

Nessus indica questa vulnerabilità critica perchè con l’utilizzo della password “password” ha effettuato il login.

Provo a effettuare la login con password “password”, login riuscita.

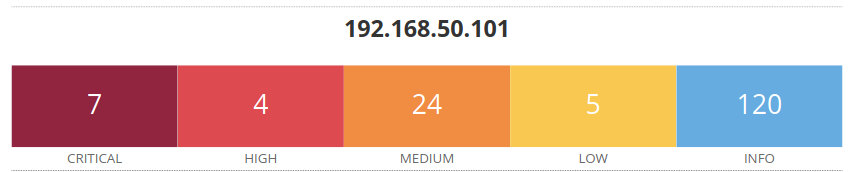
Procedo con la sostituzione per una password più sicura.



Ritento l’accesso con password “password”, login fallito.

La nuova password è “25PASSword”



Risultati dello scan Nessus post remediation actions.