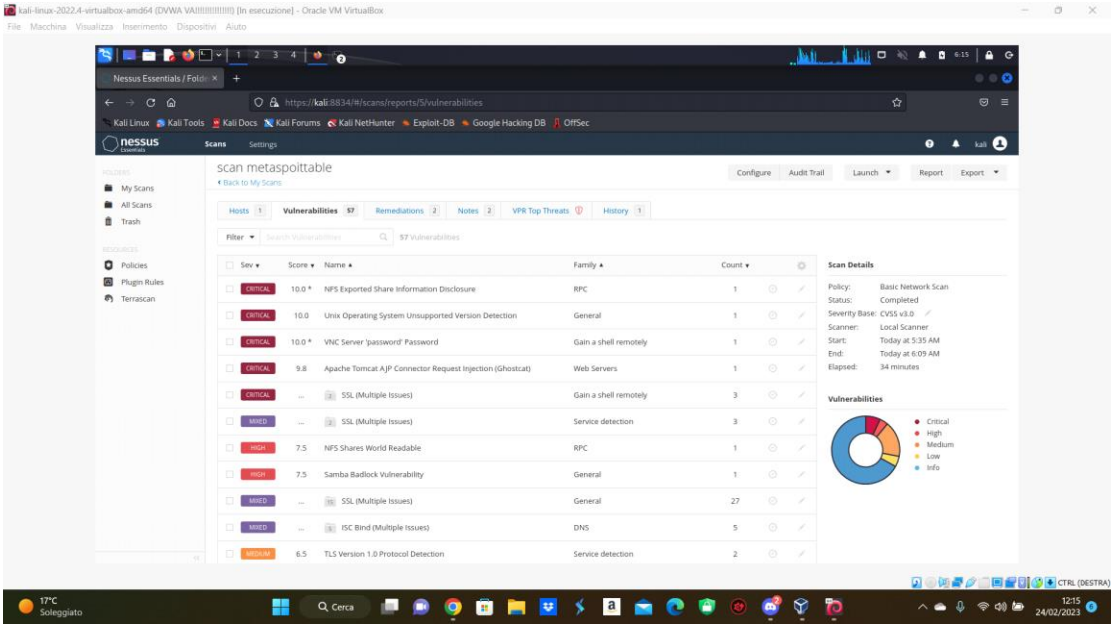


Dalla scansione effettuata con Nessus verso metaspoittable abbiamo rilevato 5 vulnerabilità critiche (come da screen).Di queste ne sono state risolte 2 , una non si poteva risolvere perchè la macchina va aggiornata

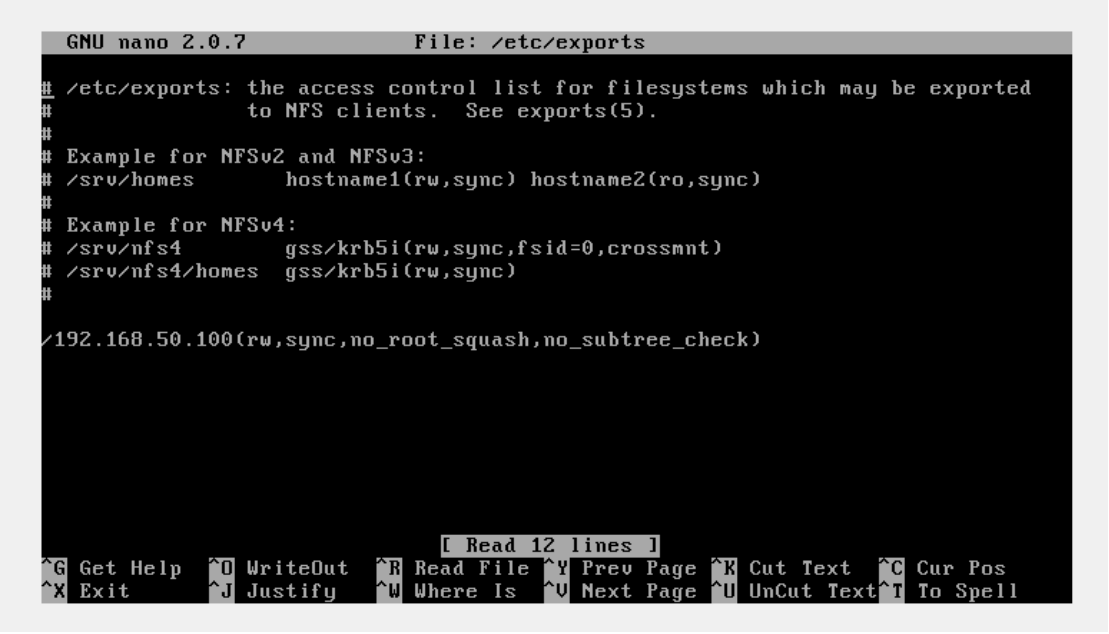
1)NFS Exported Share Information Disclosure:

È possibile accedere alle condivisioni NFS sull'host remoto.Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

REMEDIATION:

Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Comando: sudo nano /etc/exports e all interno del file ho limitato l accesso al solo ip inserito



2)Unix operating System Unsupported Version Detection:

Il sistema operativo in esecuzione sull'host remoto non è più supportato. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

REMEDIATION:

Aggiorna a una versione del sistema operativo Unix attualmente supportata.Non potendo aggiornare meta la vulnerabilità è rimasta

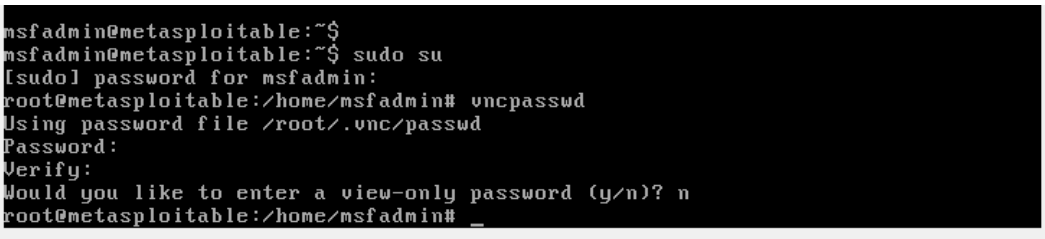
3)VNC Server 'password' Password:

Un server VNC in esecuzione sull'host remoto è protetto da una password debole. Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

REMEDIATION:

Proteggi il servizio VNC con una password complessa.

Abbiamo semplicemente impostato una password più complessa



4)Apache Tomcat AJP Connector Request Injection (Ghostcat):

C'è un connettore AJP vulnerabile in ascolto sull'host remoto. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JSP (JavaServer Pages) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

REMEDIATION: Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o versioni successive.

Scansione post Remediation