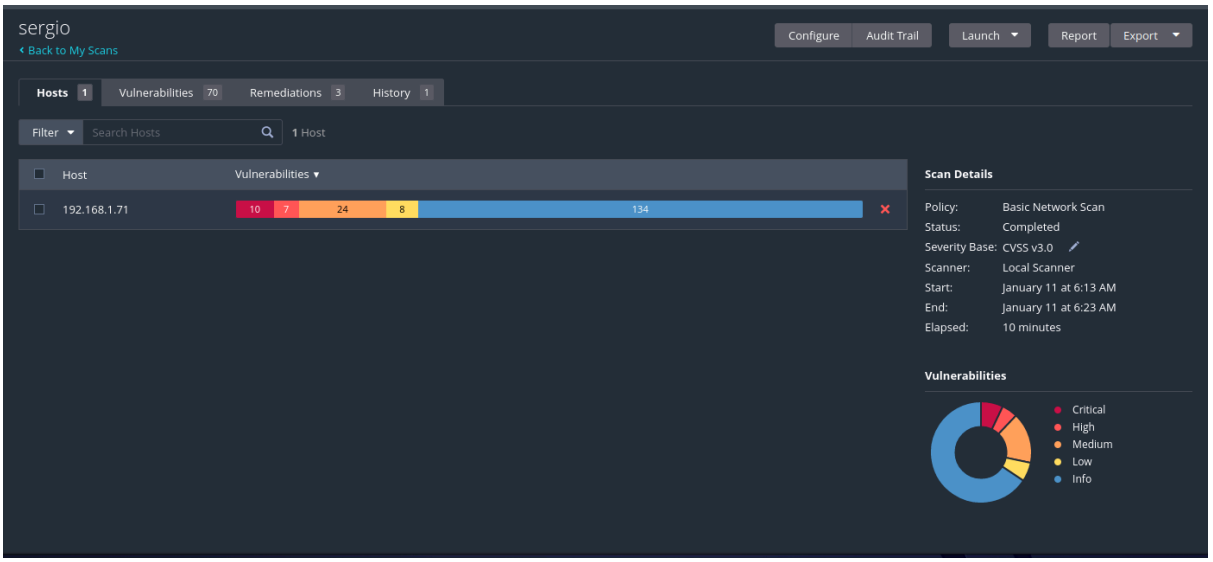
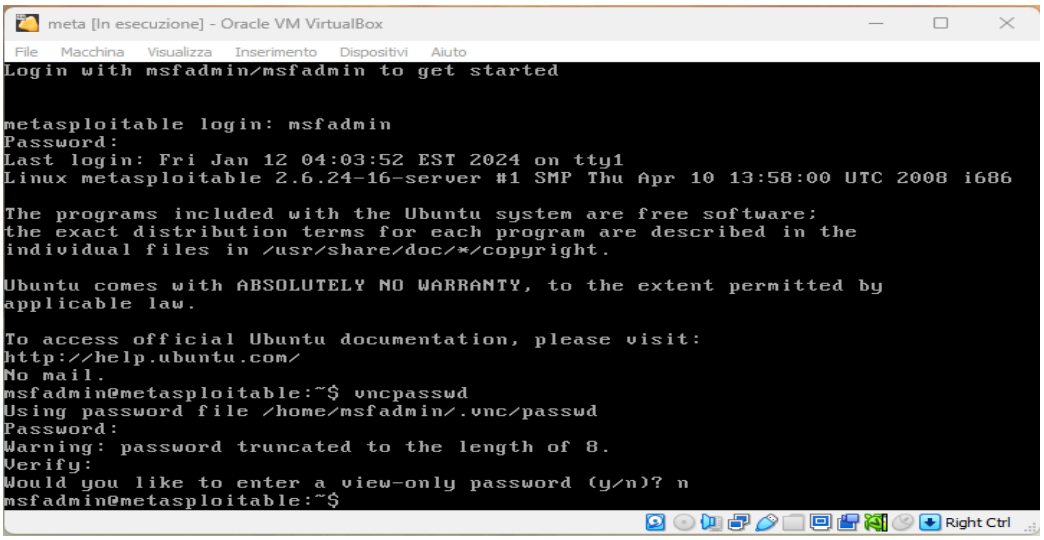
PROGETTO SETTIMANA 5

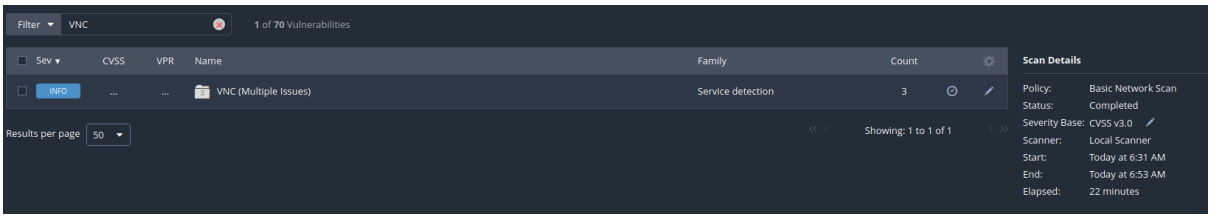
Nel progetto di oggi ci viene chiesto di effettuare una scansione sulla macchina metasploitable con il programma Nessus per verificare le vulnerabilità per poi andare a risolvere. Eseguita la scansione possiamo notare che la macchina metasploitable ha diverse vulnerabilità (anche troppe), ne abbiamo 10 critiche 7 high 24 medie 8 basse e 134 info. Come si può notare nell'immagine.



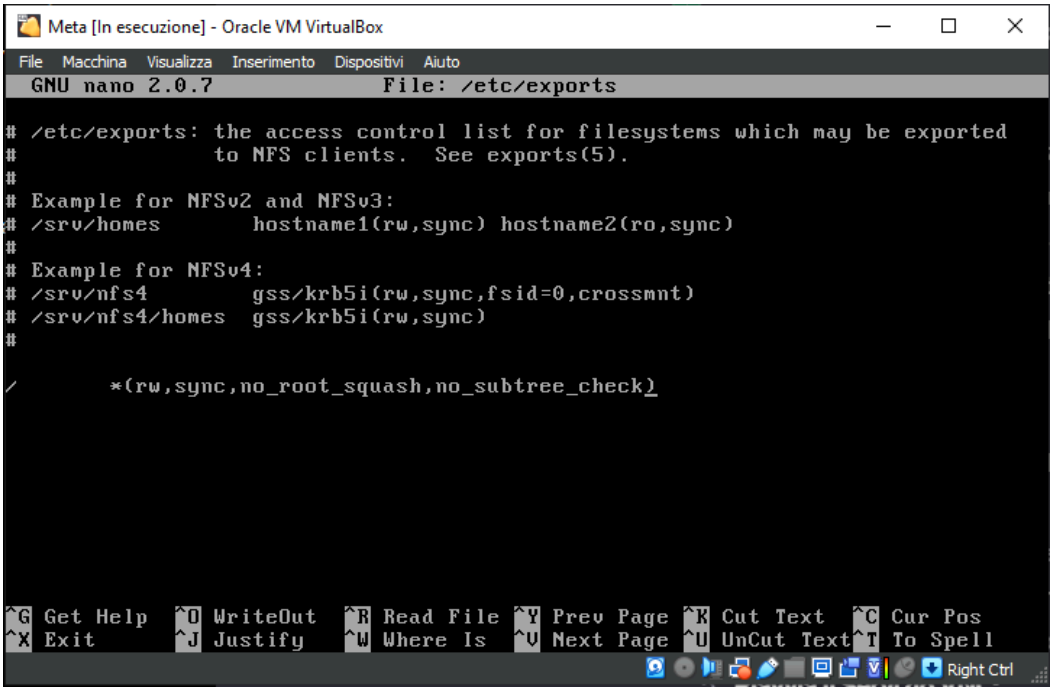
Come vulnerabilita ho scelto " VNC Server 'password' Password, dalla descrizione di Nessus capiamo che la password del VNC è molto debole poiché la password attuale è "password", quindi ho eseguito il comando vncpasswd per andare ad inserire una password più sicura, ho scelto una alfanumerica.

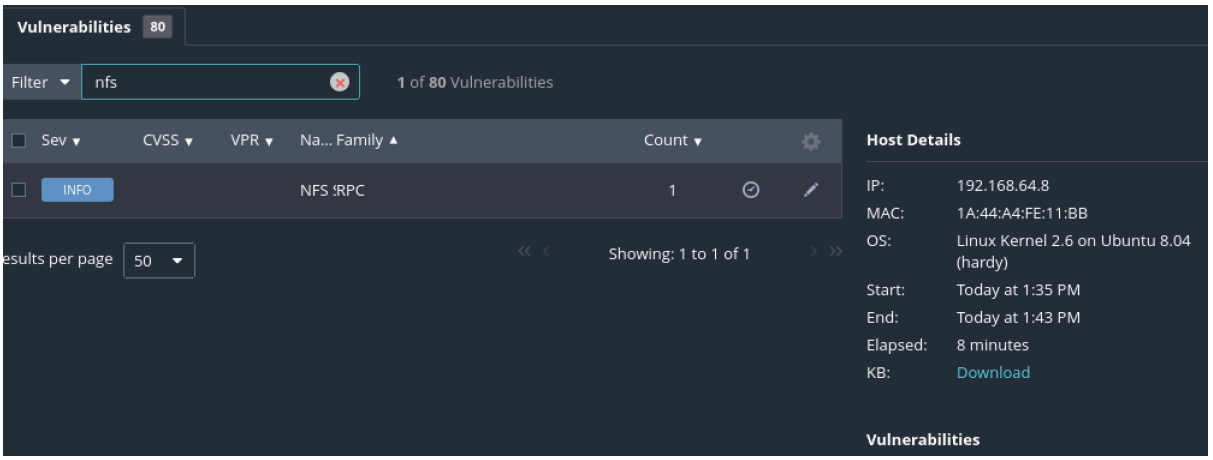


Come vediamo nella foto non si trova più nelle vulnerabilità.

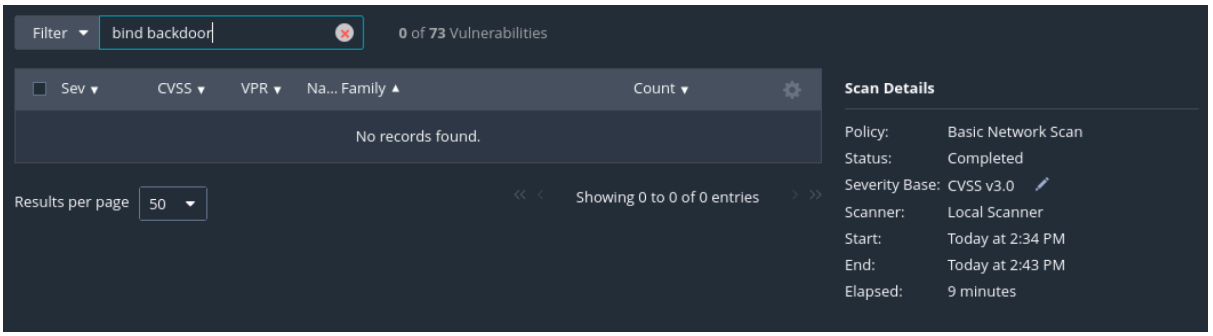


Come seconda vulnerabilità da sistemare ho scelto “NFS Exported Share Information Disclosure” poiché le informazioni sono facilmente intercettabili da host non autorizzati che potrebbero leggere o scrivere sul nostro server da remoto. Per sistemare questa vulnerabilità sono entrato nella directory (/etc/exports) ed ho eliminato i permessi (ovvero l’ultima stringa).





Come terza vulnerabilità ho scelto “Bind Shell Backdoor Detection” ovvero che esiste una shell in ascolto su una porta remota che non ha bisogno di autenticazione, un criminale informatico potrebbe usarla per inviare comandi da remoto. Per risolverla ho utilizzato sia nmap che meta , nessus ci dice che la porta aperta è la numero 1524, quindi ho eliminato il processo da meta per riuscire ad eliminarlo ho individuato il processo tramite il comando lsof -i :1524 , dopodichè l’ho eliminato con il comando kill, verificando la sua chiusura anche con nmap.



Infine abbiamo lo scan finale dove possiamo vedere che non ci sono più le tre vulnerabilità.