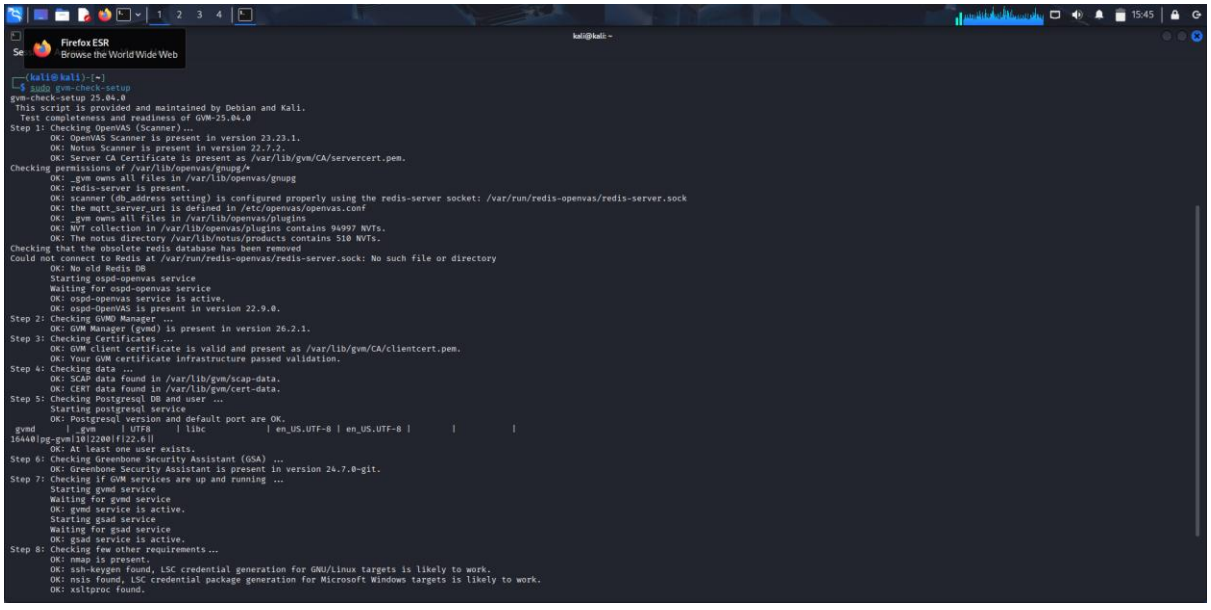
W12D4_PROGETTO 3_ANALISI DELLE VULNERABILITA’ E AZIONI DI RIMEDIO

La protezione delle reti e dei sistemi passa attraverso l'analisi delle vulnerabilità fatta in maniera costante. Durante un PT, nel momento in cui si effettua una scansione completa sul target attraverso l’utilizzo di tool come ad esempio Nessus o Greenbone, si vanno a rilevare tutti i servizi TCP e UDP attivi sulle porte che possono essere aperte o chiuse. Lo scanner effettua una ricerca delle vulnerabilità note per la versione del servizio con l’obiettivo di arrivare ad una Remediation action al termine della fase di exploit, cioè una o più azioni necessarie per andare a sanare i problemi di sicurezza che potrebbero altrimenti essere sfruttati.

L’utilizzo dello scanner di rete Greenbone sul target metasploitable aiuta ad individuare tutta una serie di vulnerabilità note che ne restituisce una fotografia in base alla gravità (CVSS), questo per dare priorità all’azione di rimedio da adottare di conseguenza.

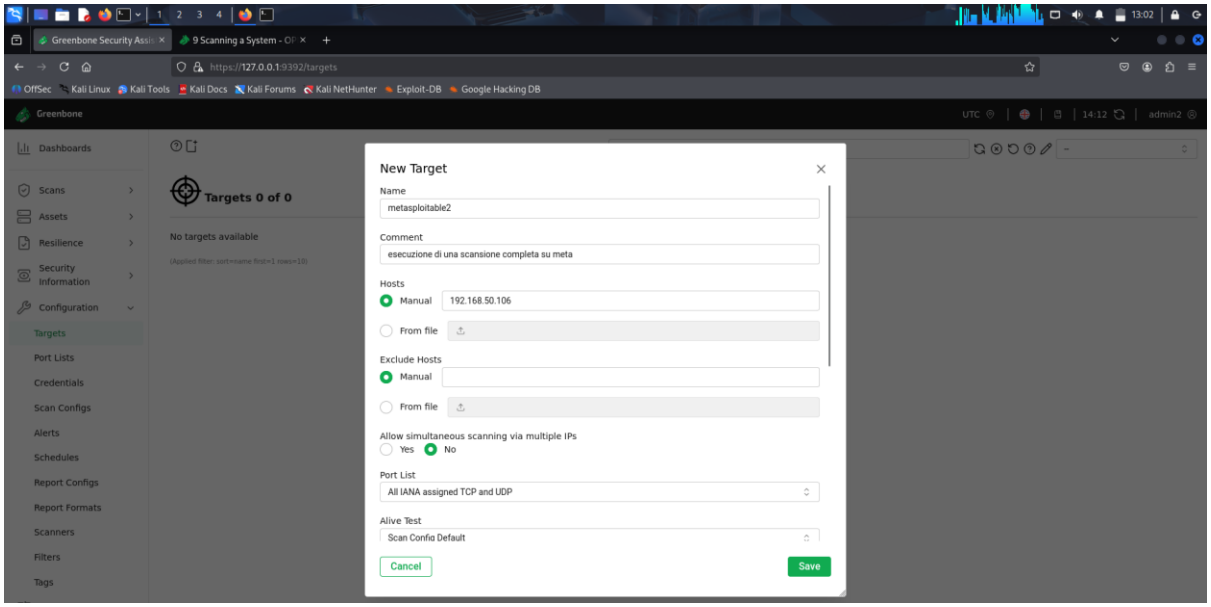
Sul target metaspoitable con ip 192.168.50.106 si implementa una scansione delle potre TCP e UDP ovvero i protocolli di trasporto sui quali si trovano porte e servizi.

Avvio del tool Greenbone



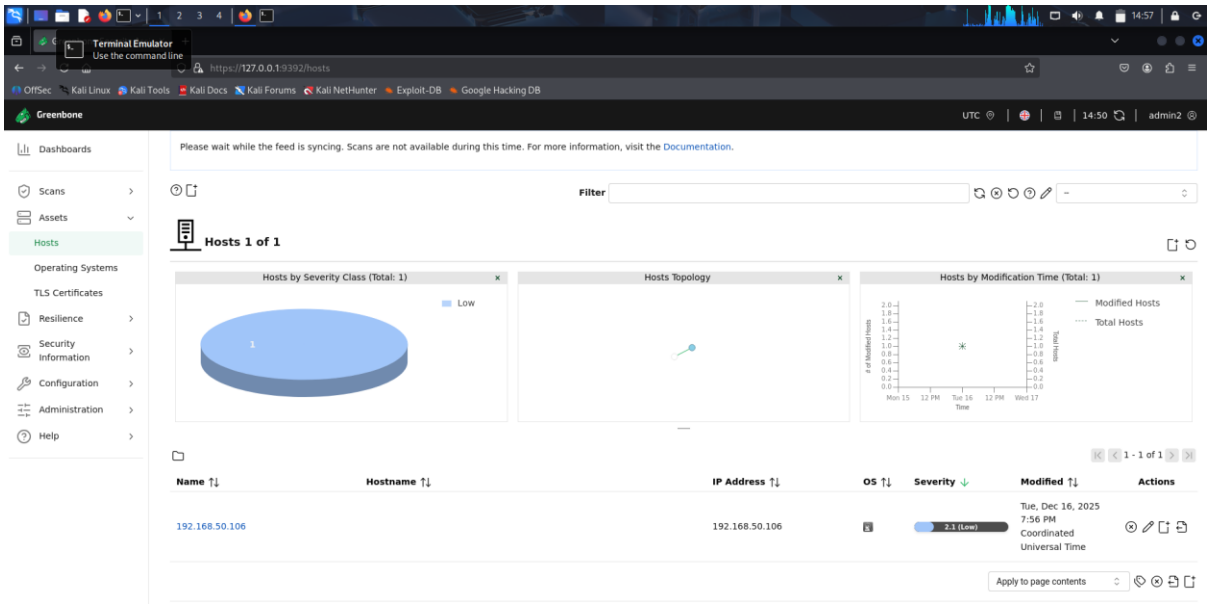
Selezione delle porte ed individuazione del target

IP: 192.168.50.106

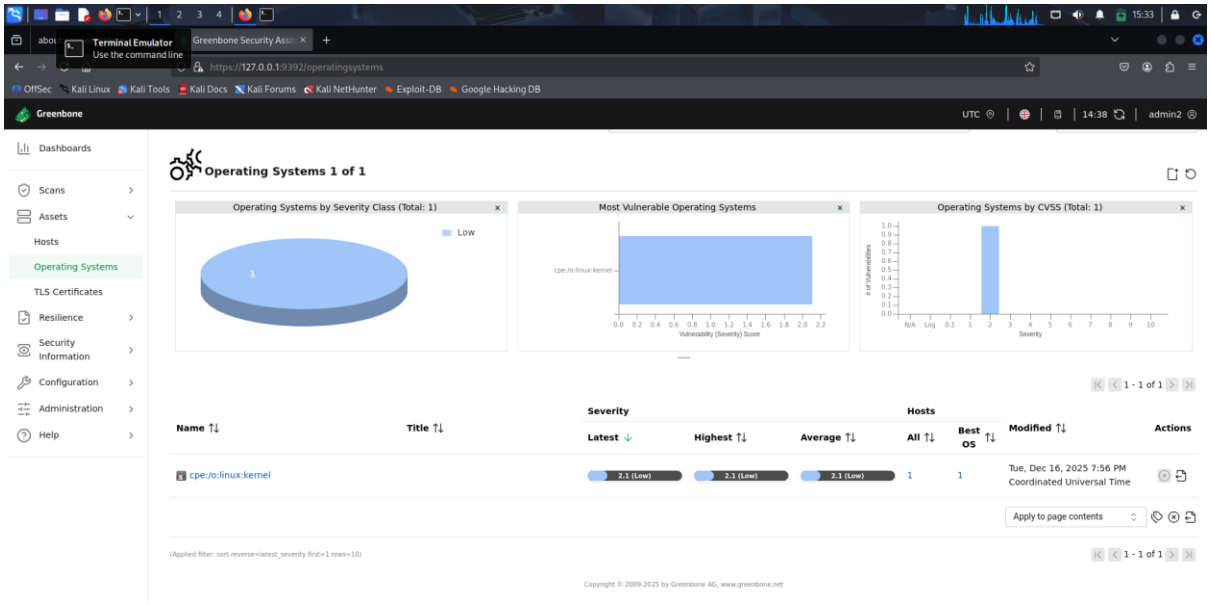


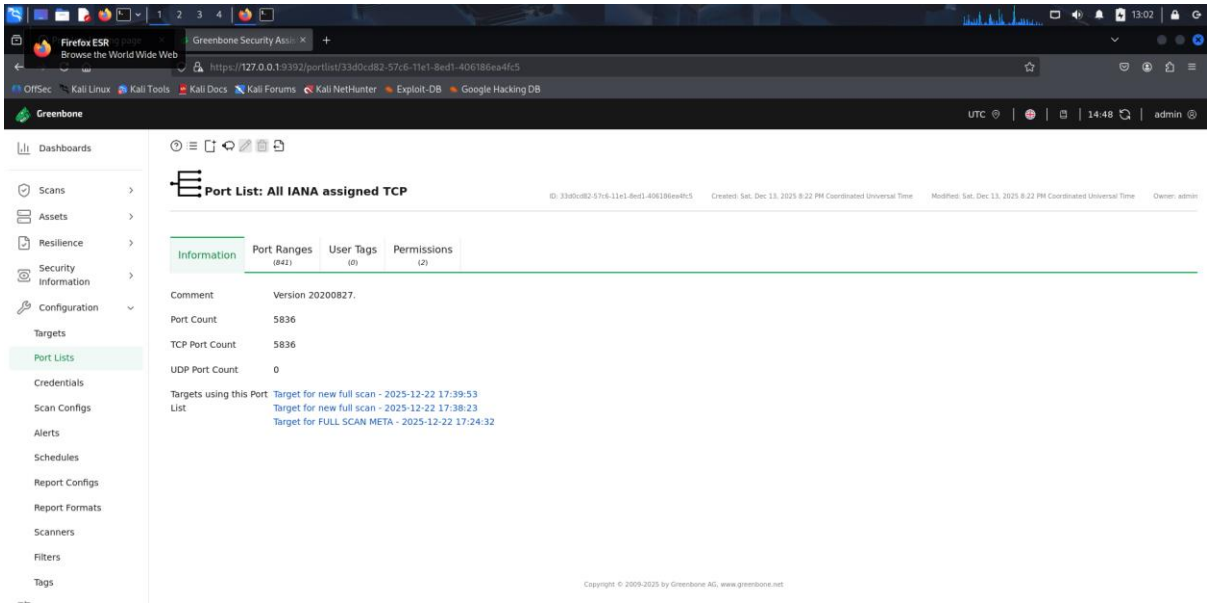
Primi risultati della scansione

-host

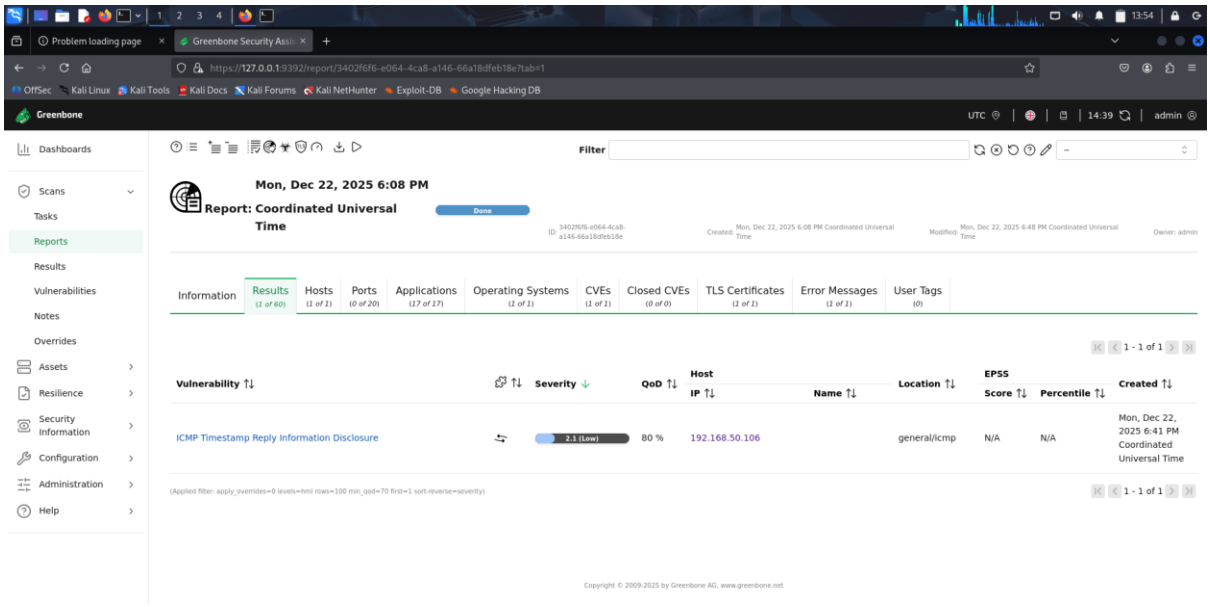


Sistema operativo





S



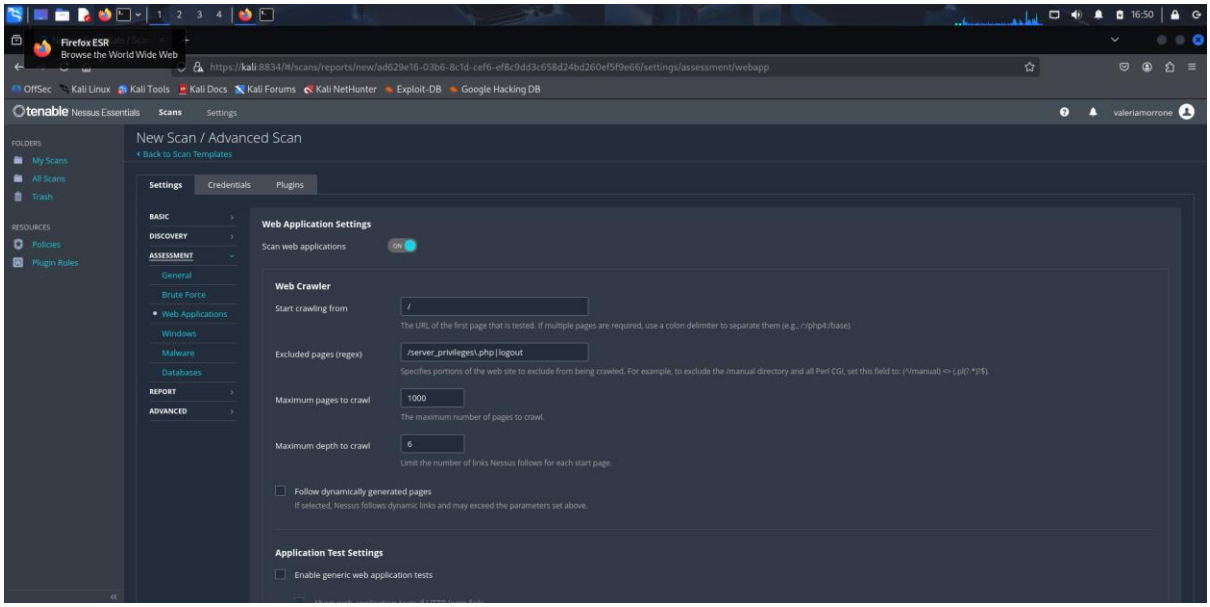
Sulla sezione report è possibile individuare e controllare quelle che sono le informazioni riguardanti la scansione.

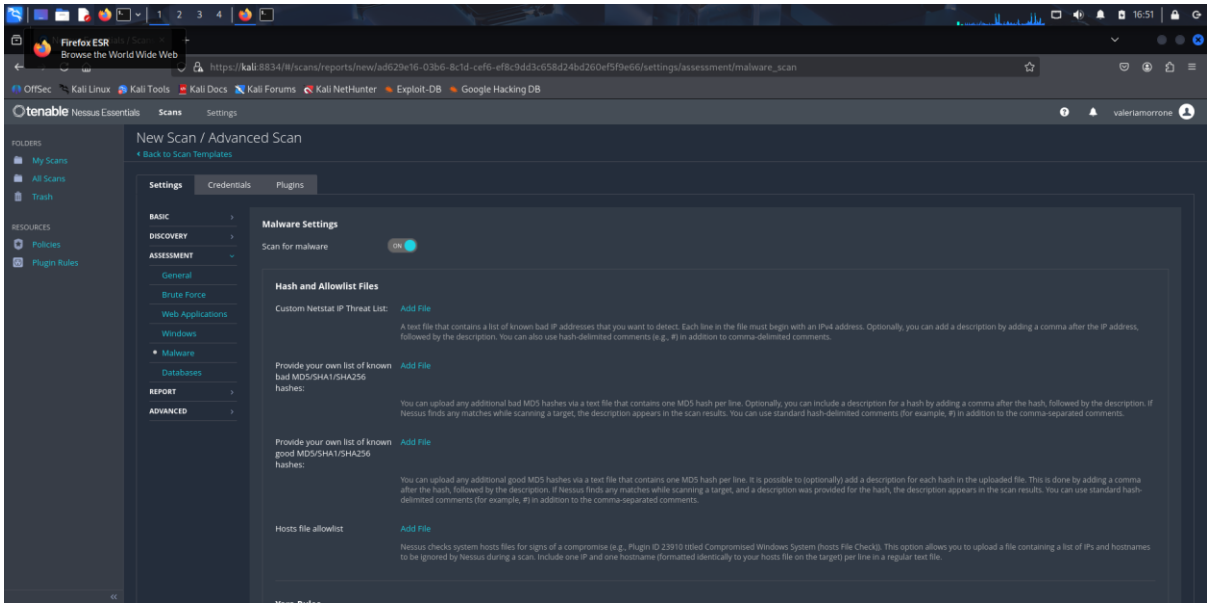
/

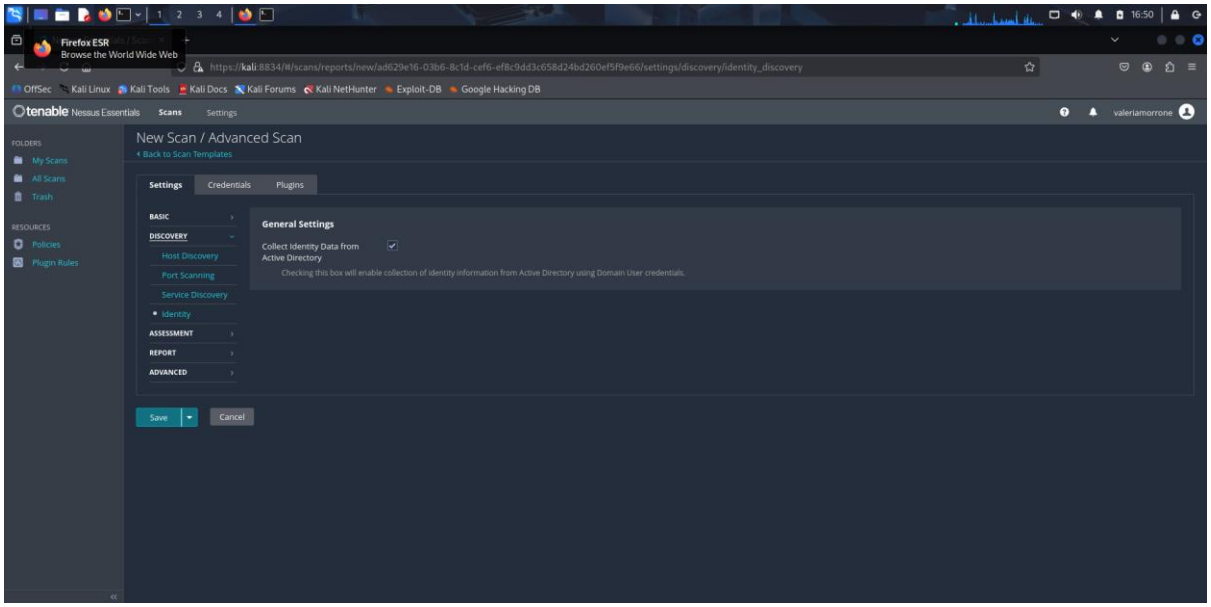
Sono state effettuate varie scansioni ma non sono state trovate vulnerabilità sul target.

(è stato effettuato un tentativo anche con l'utilizzo dello scanner di rete Nessus ma non è andato a buon fine in quanto il programma consente un numero limitato di scansioni, per tale motivo l'attività è stata effettuata con il tool Greenbon.)

Segue immagine rappresentativa dei passaggi







Da una prima scansione effettuata le vulnerabilità sulla macchina risultano essere 54 che sono poi scese successivamente a 14.

NOTE FNALI:

Implementate le azioni di rimedio per le vulnerabilità scelte e con livello di gravità più elevato, si effettua l'esecuzione di una seconda scansione della rete che deve restituire un risultato diverso da quello della precedente.

Una volta avuta quindi una panoramica delle porte e dei servizi attivi è importante ridurre al minimo i tentativi di attacco.

Fine progetto 22/12/2025