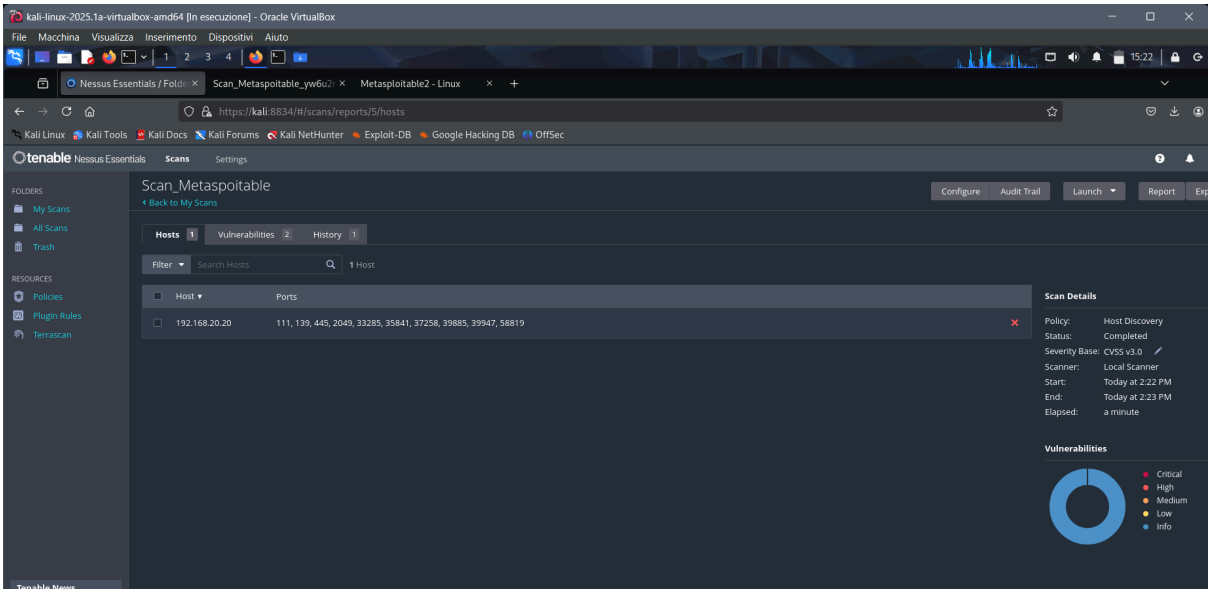
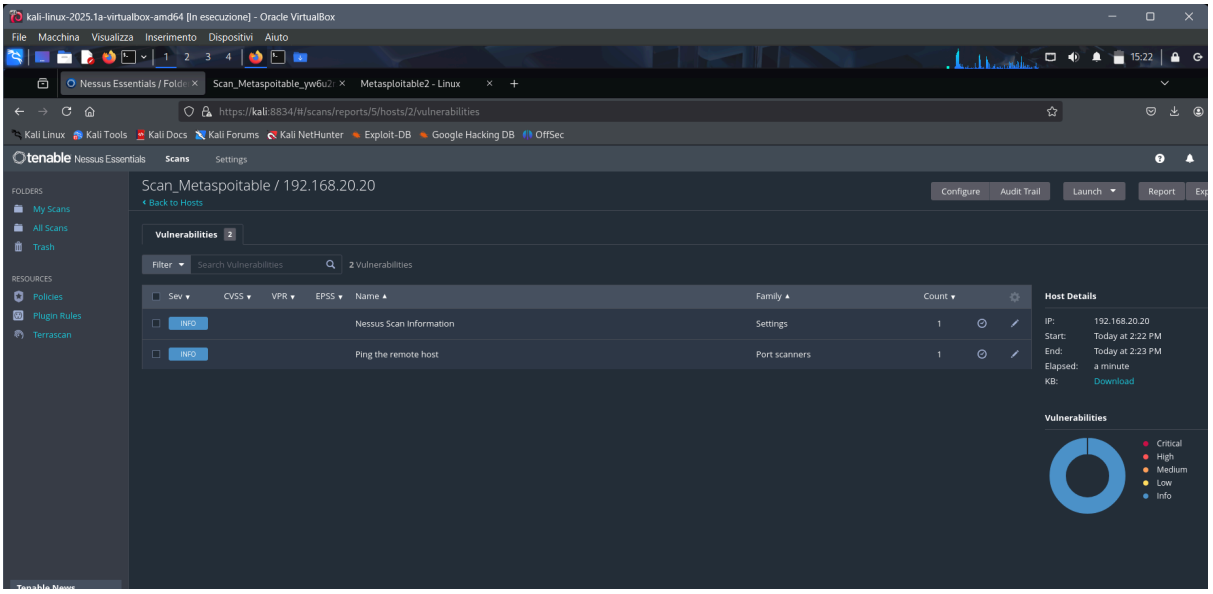
Scansione di Metaspotable con Nessus Essentials

Avviata la macchina virtuale Kali Linux apriamo il terminale con il comando, *sudo service nessusd start*, per avviare il servizio su Firefox che sarà in ascolto sulla porta 8834 sul localhost. Inseriamo le credenziali di admin per iniziare la configurazione dello scanner su “create new scan”, compilando le schede e salvando la scansione per poi farla partire.





La scansione ha trovato solo 2 vulnerabilità a basso rischio, Info.
La prima è solamente un’informazione tecnica per descrivere i dettagli della scansione, che serve solo a fini di audit e debugging, ma non per segnalare problemi nel sistema target.
La seconda ci dice che il sistema target è raggiungibile rispondendo al ping. Non è una vera e propria vulnerabilità, ma una possibile remediation, volendo, può essere nascondere la presenza del sistema, volendo, disabilitando le risposte ICMP dal firewall o bloccare le richieste ping in entrata.

Nel caso, comunque, siano presenti vulnerabilità molto più critiche il servizio ci può dare una descrizione, una soluzione e dei link utili da consultare per documentarci su di essa.