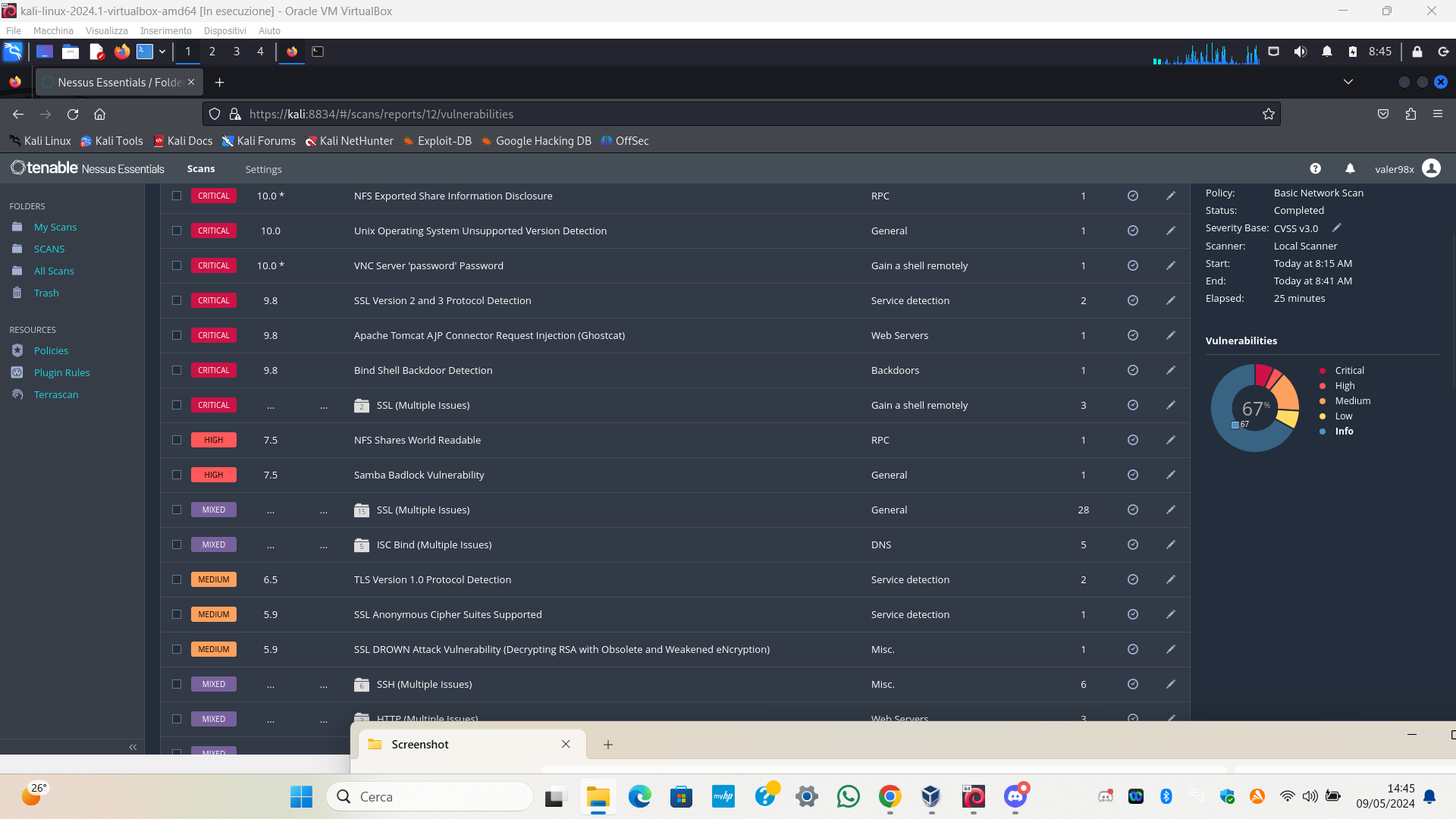
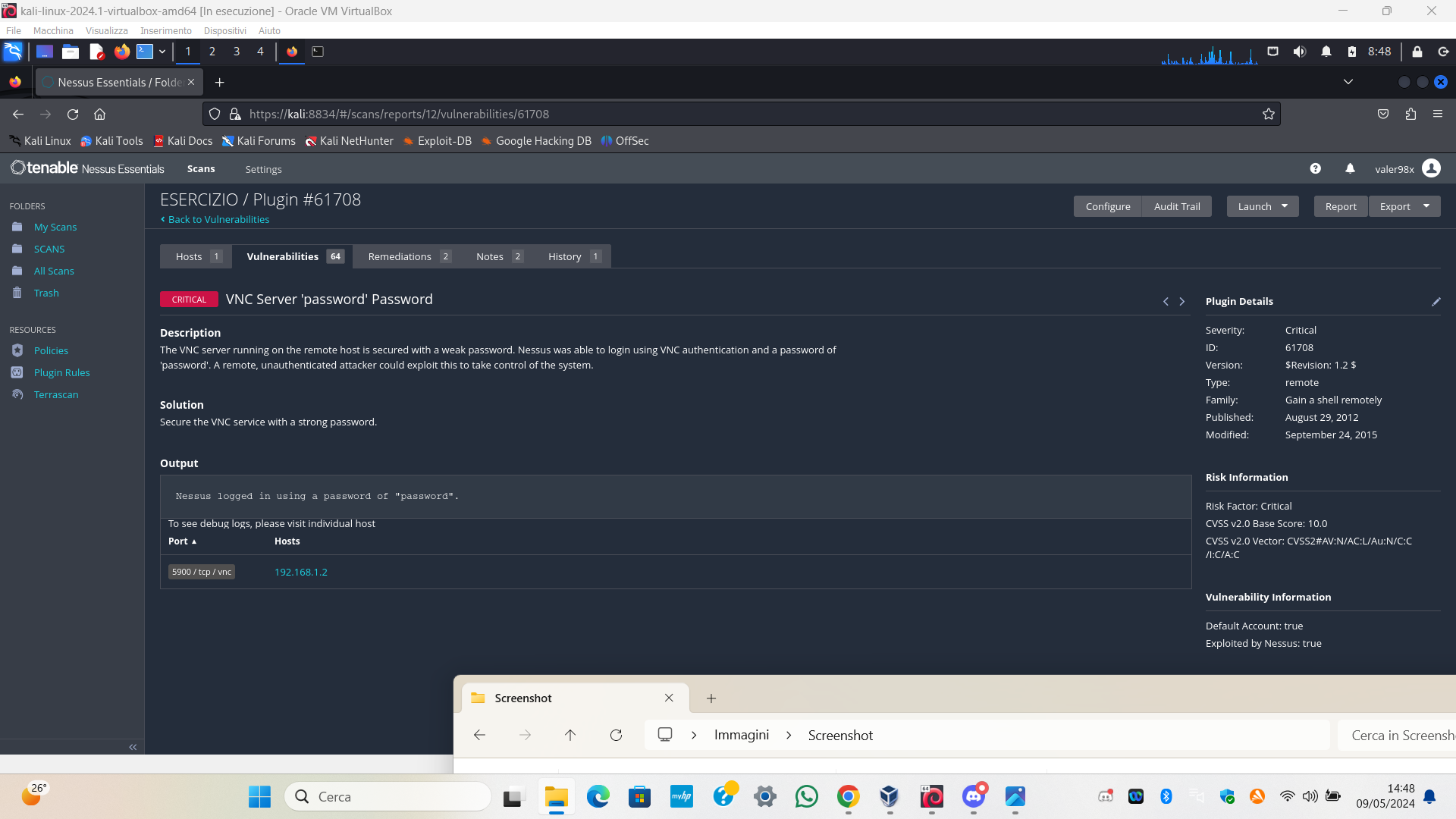
Nell’esercizio di oggi utilizziamo Nessus, un potente tool adatto al vulnerability assessment. Questo tipo di controllo su macchina risulta essere meno invasivo rispetto al penetration test.

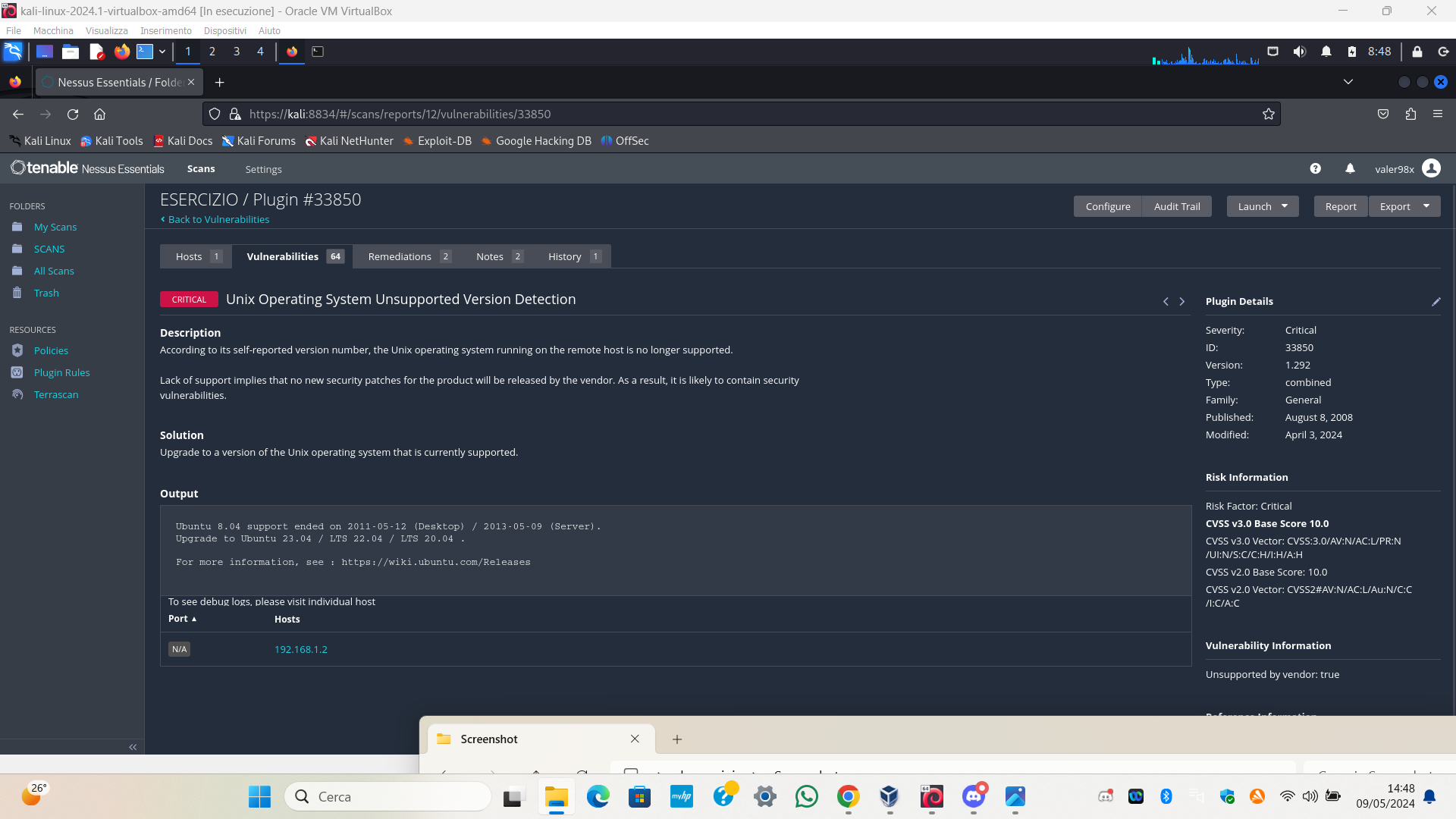
Effettuiamo lo scan sulla macchina Metasploitable per metterne in evidenza le vulnerabilità con “New Scan”.



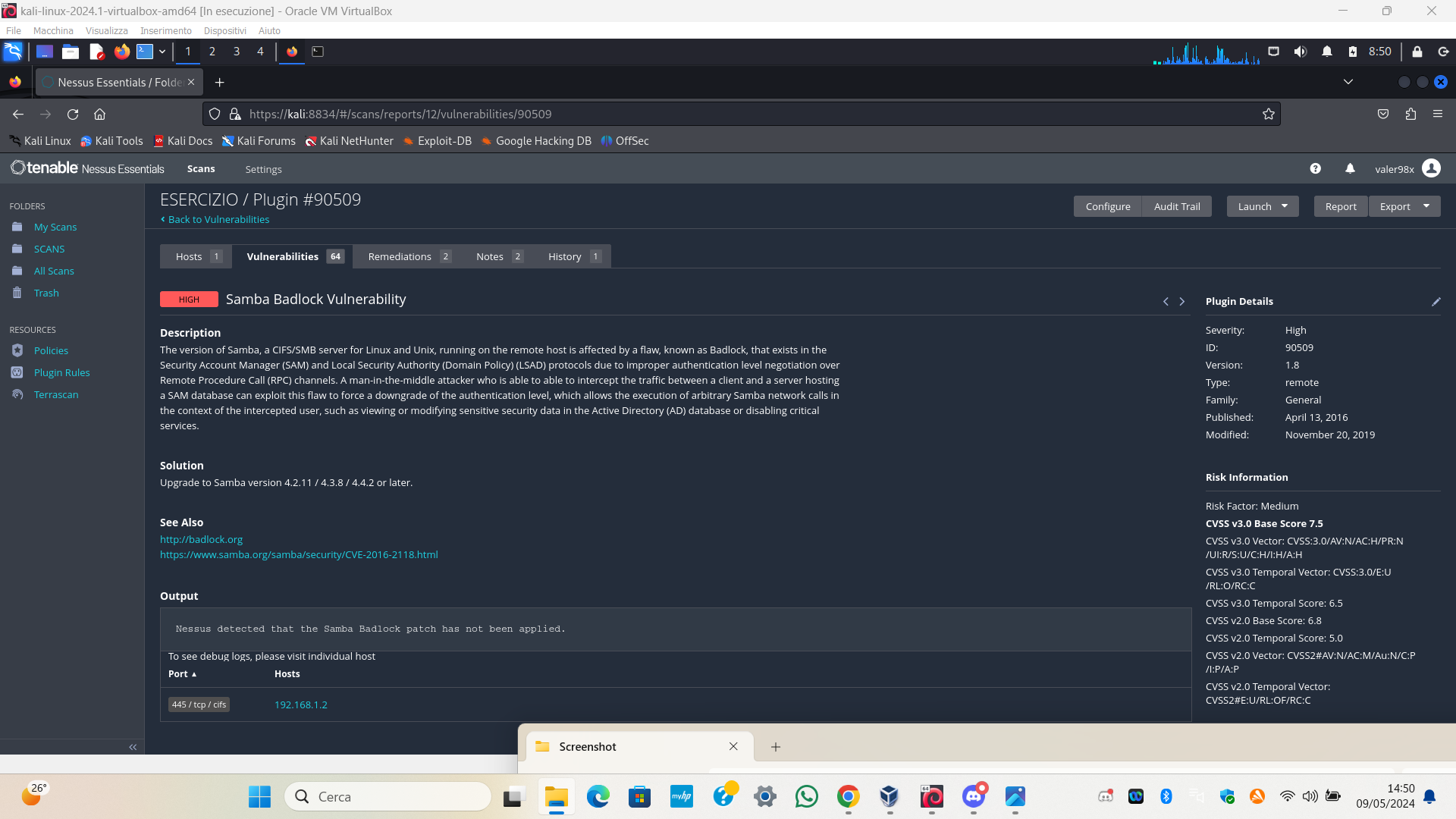
Il programma ci restituisce una schermata contenente le vulnerabilità della macchina target in ordine di criticità. In primo luogo il programma riconosce che Metasplitable è protetta da una password molto debole, come vediamo nella figura di seguito.



Un altro fattore non trascurabile è dato dalla versione del sistema operativo. Questo, quando non è aggiornato alla versione più recente può presentare delle vulnerabilità che sono state rese pubbliche che potrebbero essere sfruttate da un malintenzionato.



Troviamo anche una vulnerabilità piuttosto comune: quella legata al protocollo “Samba”. Molti attacchi man-in-the-middle sono stati effettuati grazie alle vulnerabilità di questo protocollo. Il protocollo Samba non è aggiornato all’ultima versione, pertanto Nessus ci consigli di fare un upgrade.



Sebbene queste vulnerabilità possano essere gestite efficacemente con degli aggiornamenti, è sempre bene continuare a monitorare la macchina poiché il “rischio 0” non esiste e i database di exploit si aggiornano costantemente con nuove vulnerabilità presenti nelle ultime versioni dei sistemi operativi, programmi e protocolli.