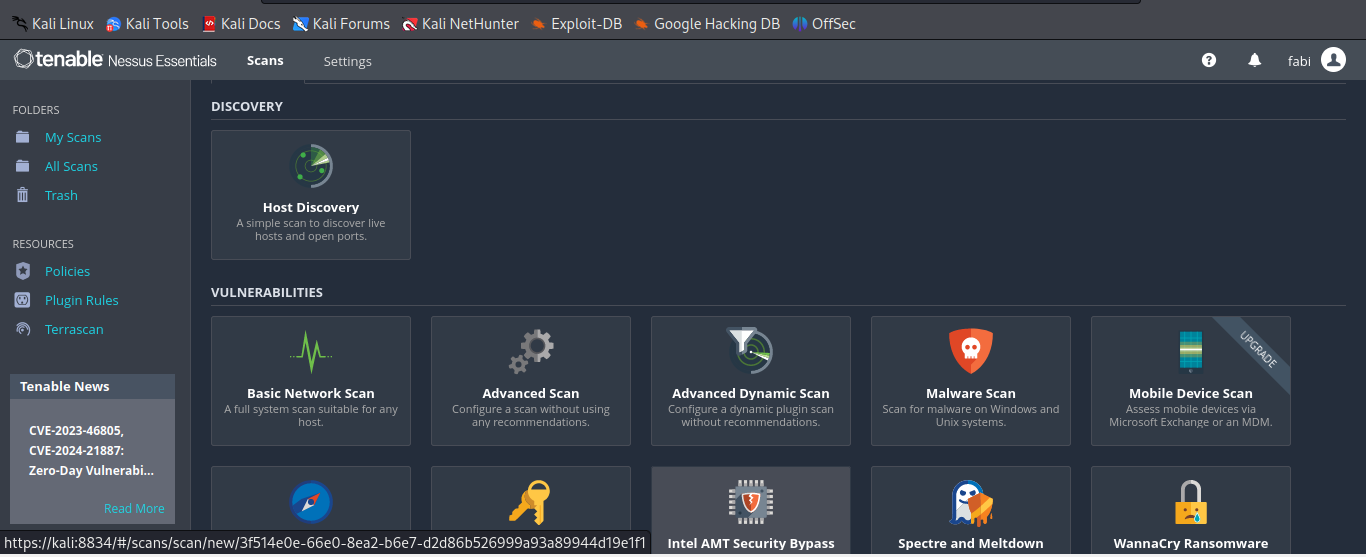
**Traccia:** Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable. A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate e esponetene due critical e una high.

Nessus è uno dei software di scansione della sicurezza (Vulnerability scanner) più popolari e ampiamente utilizzati.

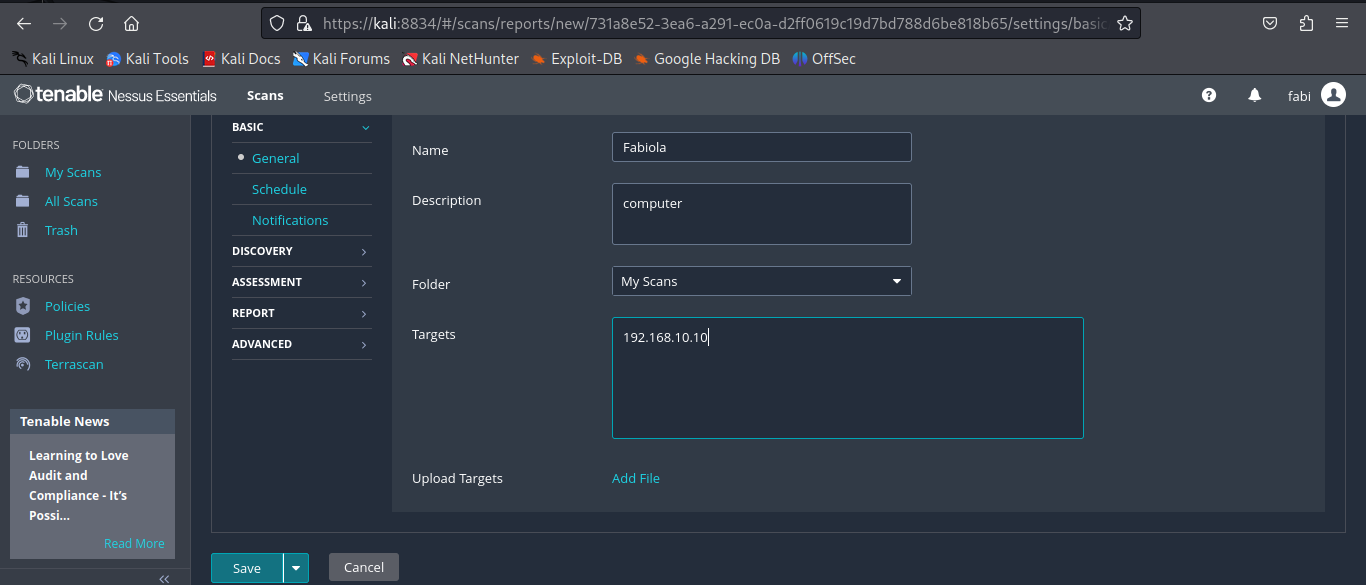
È un'applicazione progettata per identificare e valutare, attraverso le scansioni sui sistemi, vulnerabilità note, configurazioni errate e altre debolezze di sicurezza che potrebbero essere sfruttate dagli attaccanti.

**Il** software utilizza un vasto database di vulnerabilità per identificare e classificare le vulnerabilità rilevate durante la scansione e fornisce report dettagliato, inclusi suggerimenti su come mitigarle o risolverle.

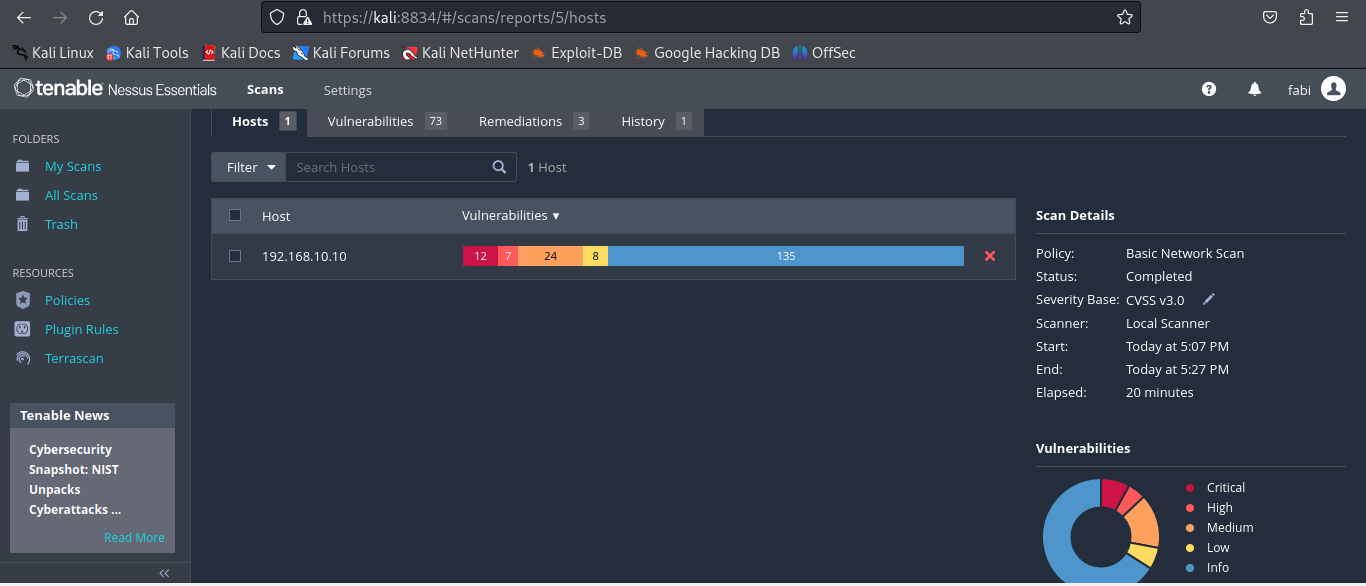
Una volta scaricato, si presenta con la seguente interfaccia, semplice e intuitiva. Per il nostro esempio useremo il Basic Network Scan:



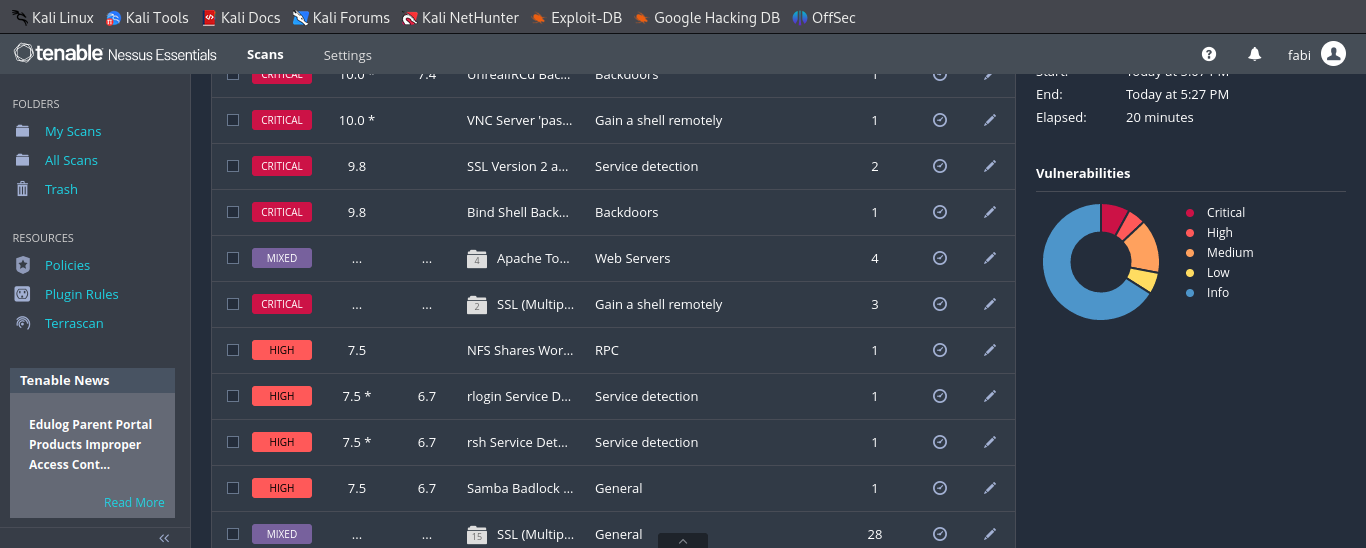
Imposteremo il nome, la descrizione del dispositivo da scannerizzare, la cartella in cui verrà salvata la scansione e il target, nel nostro caso l’IP di Metaspoitable:



A scansione ultimata possiamo a colpo d’occhio individuare il numero di vulnerabilità rilevate, la cui criticità è distinta in base al colore:



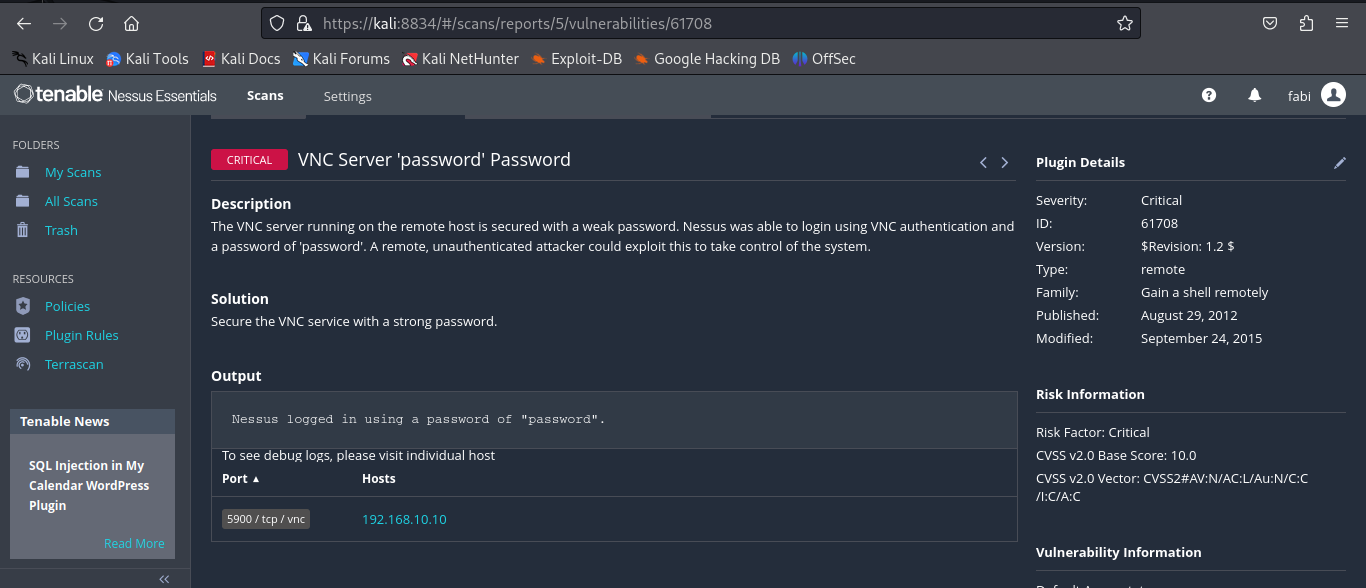
In seguito possiamo, una ad una, analizzare le vulnerabilità rilevate sul dispositivo:



Prendiamo, ad esempio, una prima vulnerabilità di livello critical. Nessus descriverà nel dettaglio il tipo di vulnerabilità, cosa si rischia in caso di attacco dall’esterno e quale soluzione potrebbe mitigare tale possibilità.

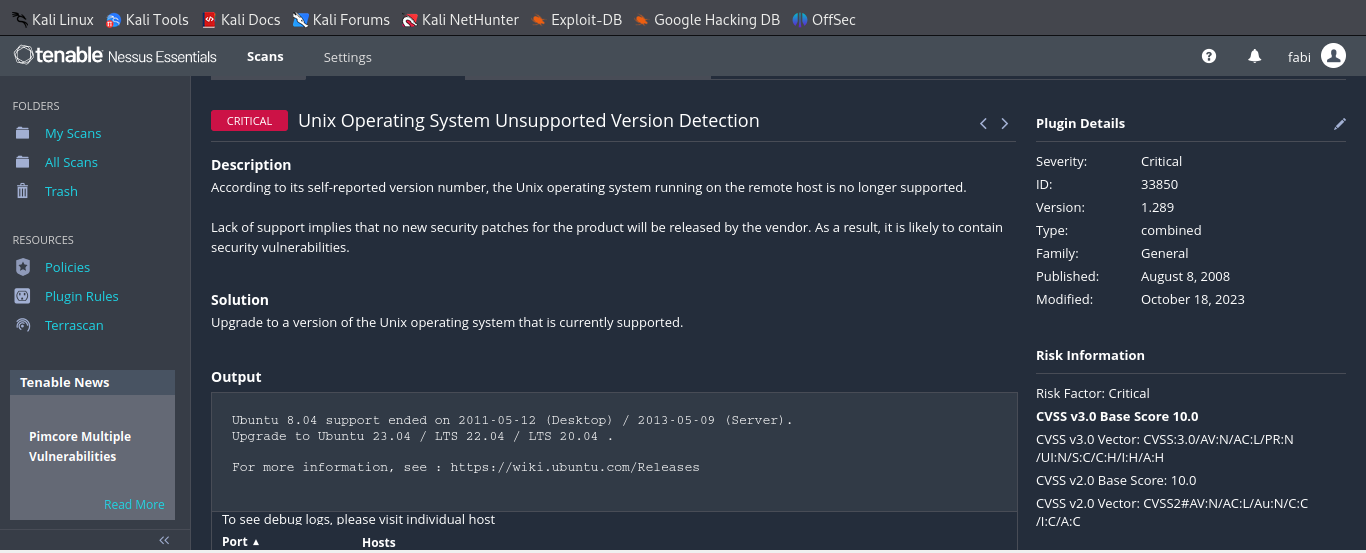
In questo caso mette in guardia l’amministratore di sistema in quanto il server VNC, un software che consente la condivisione del desktop o di un'applicazione tra un server e un client su una rete, in esecuzione sull'host remoto è protetto con una password debole (indica anche il tipo di password con cui Nessus è riuscito ad entrare, ovvero "password"). Quindi un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

Una soluzione suggerita è ovviamente quella di proteggere il servizio VNC con una password complessa, meglio se una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali, che eviti di riprendere dati personali facilmente reperibili. Inoltre si potrebbe suggerire di valutare la crittografia della trasmissione e un continuo aggiornamento del software per implementare al massimo la sicurezza.



Analizzando un'altra vulnerabilità tra le critical possiamo notare che, secondo il numero di versione riportato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato. La mancanza di supporto implica che il fornitore non rilascerà alcuna nuova patch di sicurezza per il prodotto, il che impedisce la correzione di possibili vulnerabilità.

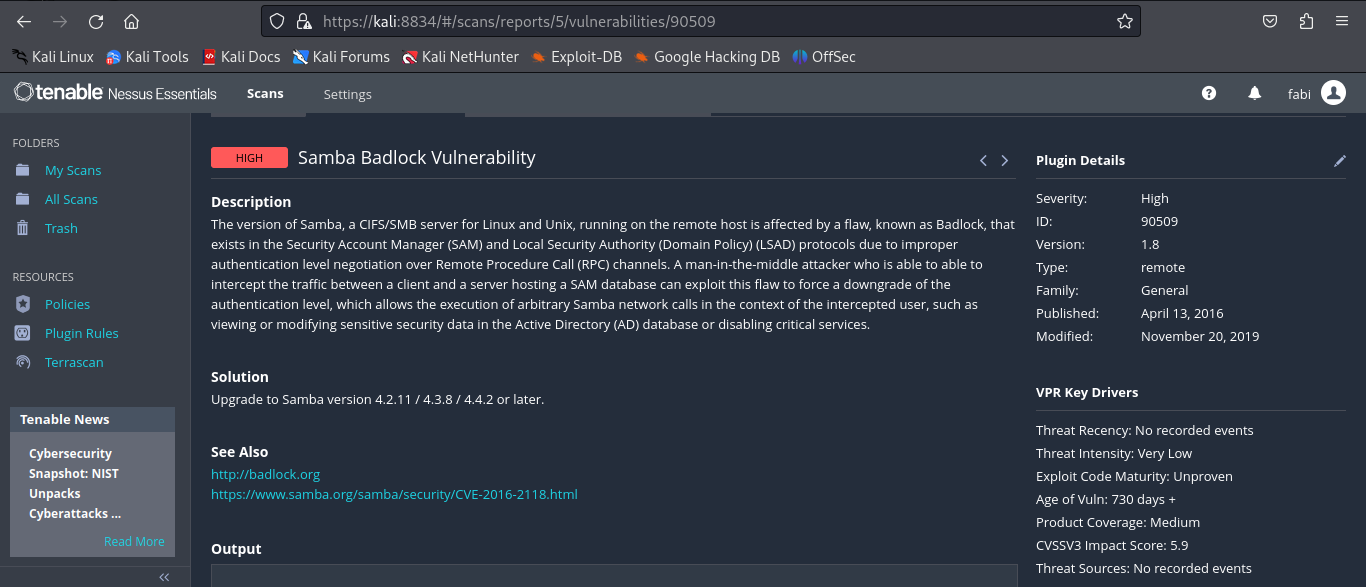
La soluzione più ovvia è eseguire l'upgrade a una versione del sistema operativo Unix attualmente supportata.



E, infine, analizziamo una vulnerabilità di livello high. In questo caso Nessus avverte che la versione di Samba, un server per Linux e Unix che fornisce servizi di rete per interagire con ambienti di rete Windows, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock.

Un malintenzionato, sfruttando questa falla, può forzare il sistema Samba e ottenere accesso non autorizzato a risorse di rete o attuare un attacco "Man-in-the-Middle" (MitM), una forma di attacco informatico in cui un attaccante si colloca tra la comunicazione tra due entità (come un utente e un sito web o due dispositivi) e può monitorare, intercettare o manipolare i dati in transito.

La soluzione consigliata è quella di aggiornare alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.



Infine, Nessus da la possibilità di ottenere un report dettagliato delle vulnerabilità riscontrate. Ne fornisce una versione più dettagliata ed una più schematica, come quella che vediamo qui di seguito (consultabile per intero qui: [Report\_Vulnerabilita.pdf](file:///C:\Users\fabio\OneDrive\Desktop\Report_Vulnerabilita.pdf)):

