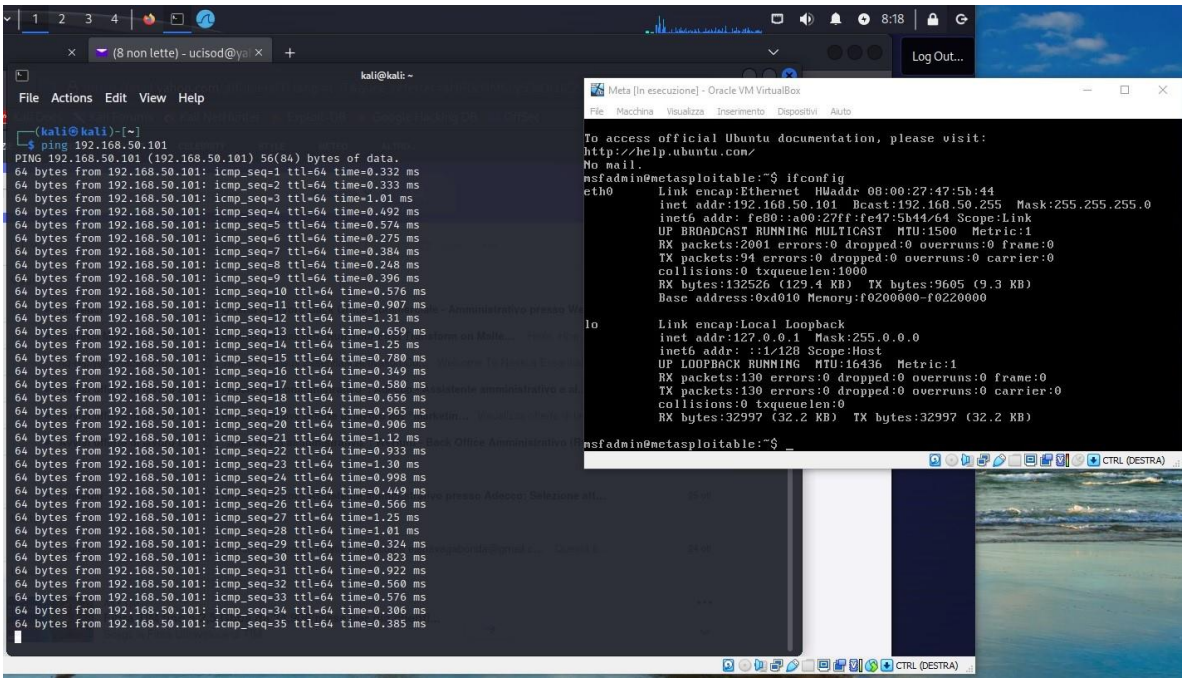
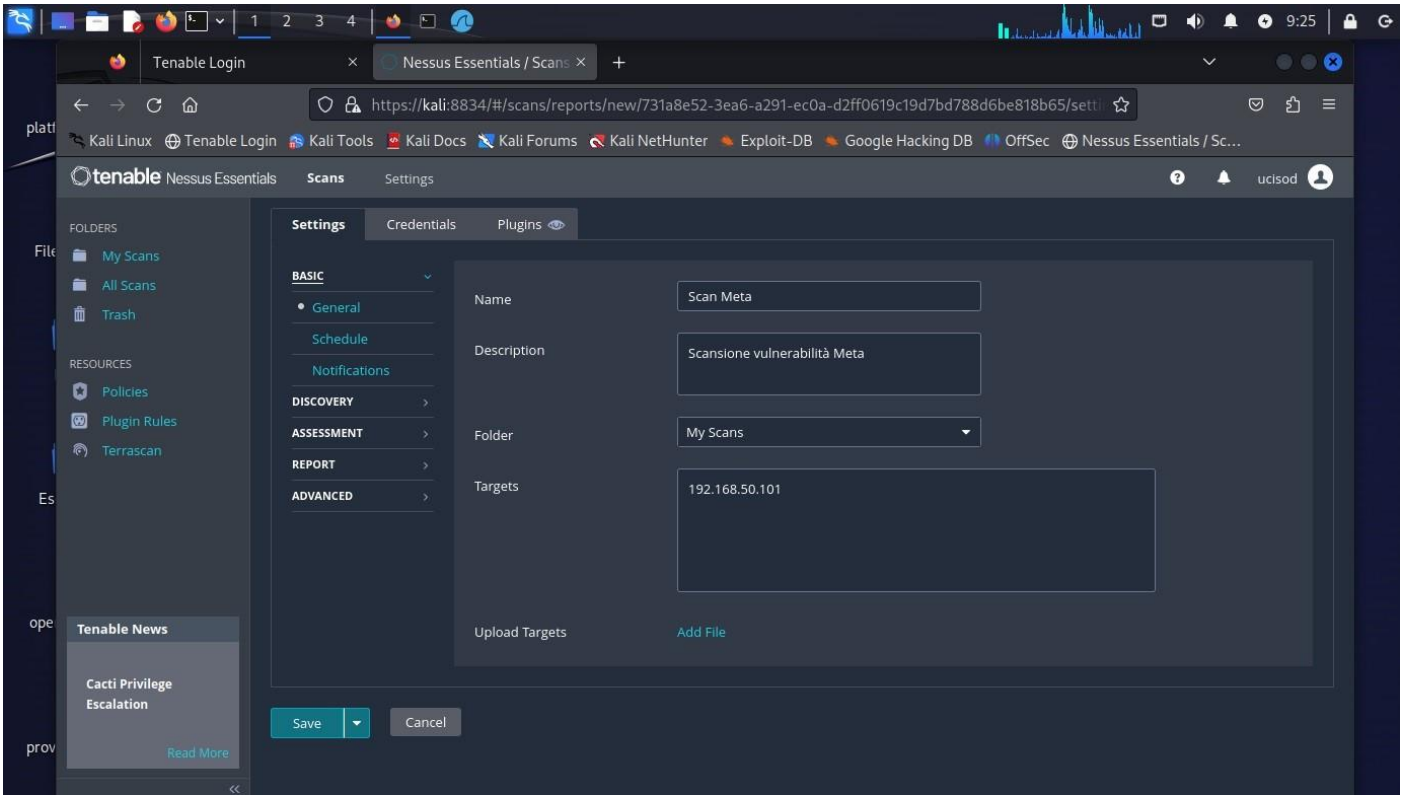
Esercitazione 26/10/2023

Nell'esercizio odierno ci viene richiesta una scansione delle vulnerabilità del programma Metaspoitable attraverso l'uso di Nessus e di commentare le prime criticità

Prima di tutto controllo che le macchine riescano a pingare tra loro

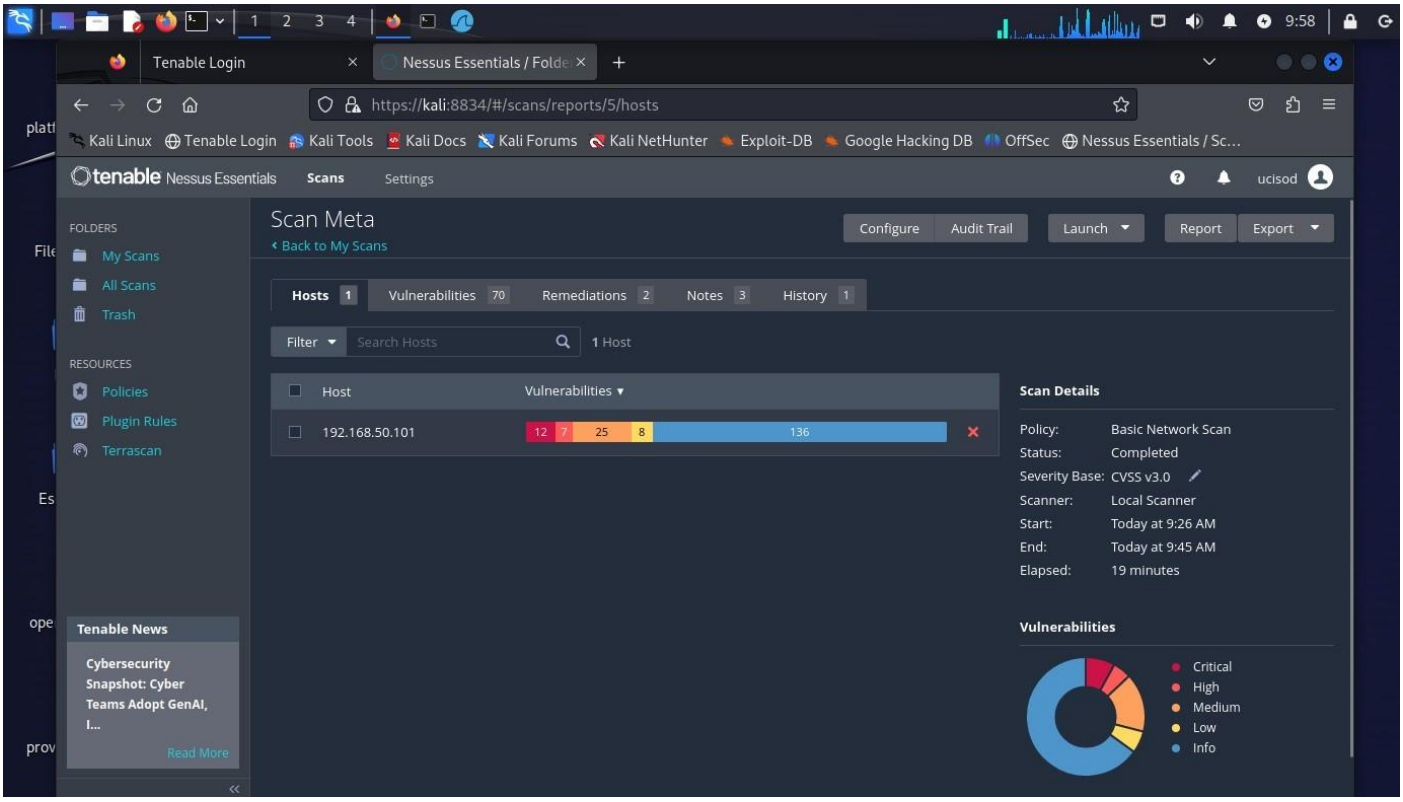


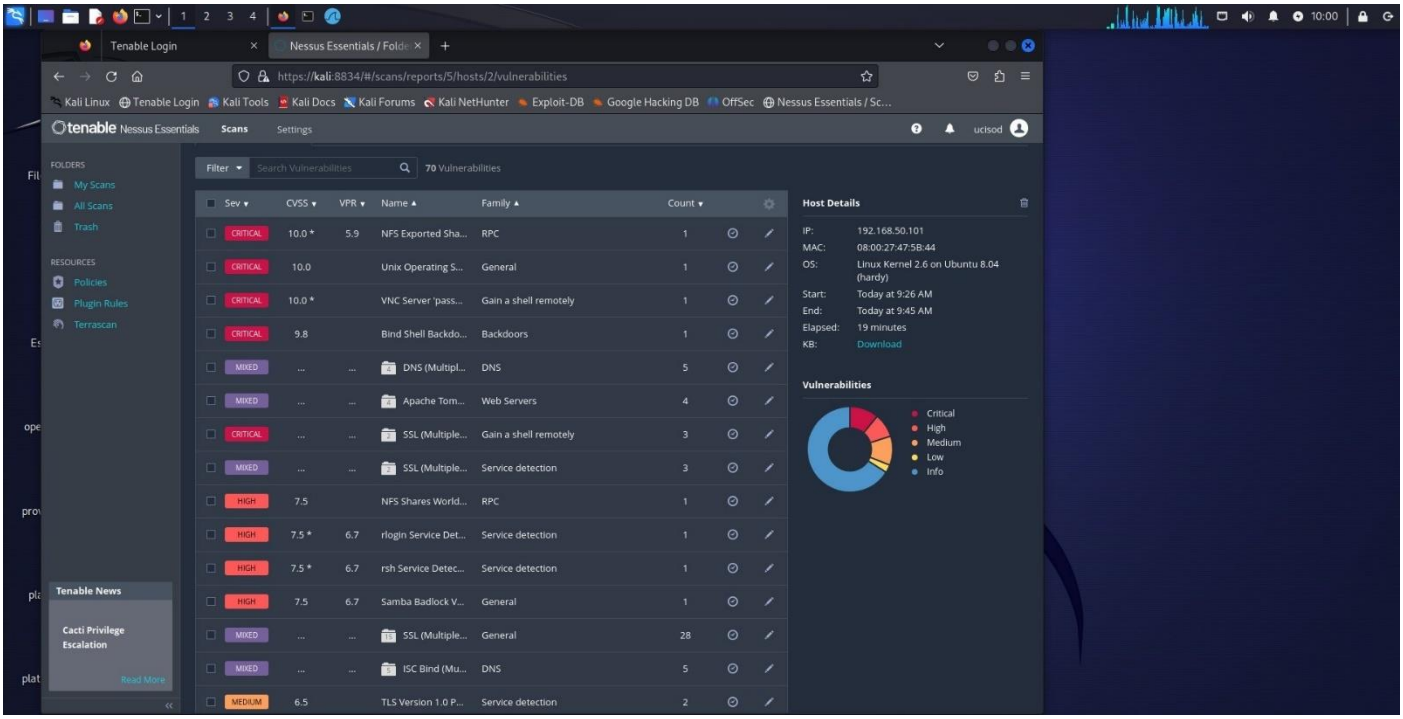
Fatto ciò avvio la scansione (tipo di scansione port scan "common ports") con il comando "Launch"



A questo punto il sistema ci ha trovato un totale di 70 vulnerabilità tra cui:

- 5 Critical
- 10 Mixed
- 4 High
- 3 Medium
- 2 Low





1 vulnerabilità livello critico:

Nome: **NFS Exported Share Information Disclosure**

Descrizione: la descrizione ci riporta che almeno un file NFS (Network File System), cioè un file o directory che sono presenti su un server NFS che li rende accessibili ai soli client che hanno i permessi per accedervi, non è sufficientemente protetto, pertanto un utente malintenzionato potrebbe avere accesso a questa condivisione e sfruttarla per accedere al file sull'host remoto, leggendolo o modificandolo.

Soluzione: Come possibile soluzione ci riporta quella di configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni

Osservazioni: Il programma ci riporta alcune informazioni utili quali, oltre a quelle già citate, i dettagli del plugin informazioni sui rischi

2 vulnerabilità livello critico:

Nome: **Unix Operating System Unsupported Version Detection**

Descrizione: Secondo il numero di versione riportato il programma ci avvisa che il sistema operativo Unix in esecuzione sull'host remoto non è più supportato e questa mancanza implica che il fornitore non rilascerà alcuna patch di sicurezza (correzione o aggiornamento software progettato proprio per risolvere le vulnerabilità).

Soluzione: Il programma ci consiglia di eseguire l'upgrade ad una versione sistema operativo Unix che sia supportata

3 vulnerabilità livello critico:

Nome: **VNC Server 'password' Password**

Descrizione: La terza criticità si riferisce al fatto che il server VNC (Virtual Network Computing) in esecuzione sull'host remoto non è sufficientemente protetto poiché ha una password debole e ci avvisa del fatto che Nessus è riuscito ad accedervi utilizzando una password standard "password". Un utente malintenzionato non autenticato, dunque, potrebbe sfruttare questa situazione per assumere il controllo del sistema

Soluzione: Nessus ci consiglia di proteggere il servizio VNC con una password complessa

4 vulnerabilità livello critico:

Nome: **Bind Shell Backdoor Detection**

Descrizione: Una shell (una componente software tramite la quale è possibile impartire comandi e richiedere l'avvio di programmi) è in esecuzione senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione: Il programma ci indica di verificare se l'host remoto è stato compromesso e, se necessario, di reinstallare il sistema