Lo scopo di questo esercizio è quello di eseguire un'attività di **Vulnerability Assessment** su una macchina vulnerabile (Metasploitable) utilizzando lo strumento **Nessus**, al fine di individuare e analizzare le principali vulnerabilità presenti sul sistema.

L'obiettivo non è sfruttare le vulnerabilità, ma **identificarle, comprenderle e interpretarne l'impatto**, come avviene normalmente in un contesto professionale di sicurezza informatica.

Ambiente di laboratorio

L'attività è stata svolta all'interno di un ambiente virtualizzato tramite **VirtualBox**, composto da:

- **Kali Linux**: macchina utilizzata come scanner di sicurezza
- **Metasploitable**: macchina target vulnerabile
- Rete interna isolata (192.168.50.0/24) per evitare esposizioni esterne

L'indirizzo IP assegnato alla macchina Metasploitable è:

- **192.168.50.101**

Configurazione di Nessus

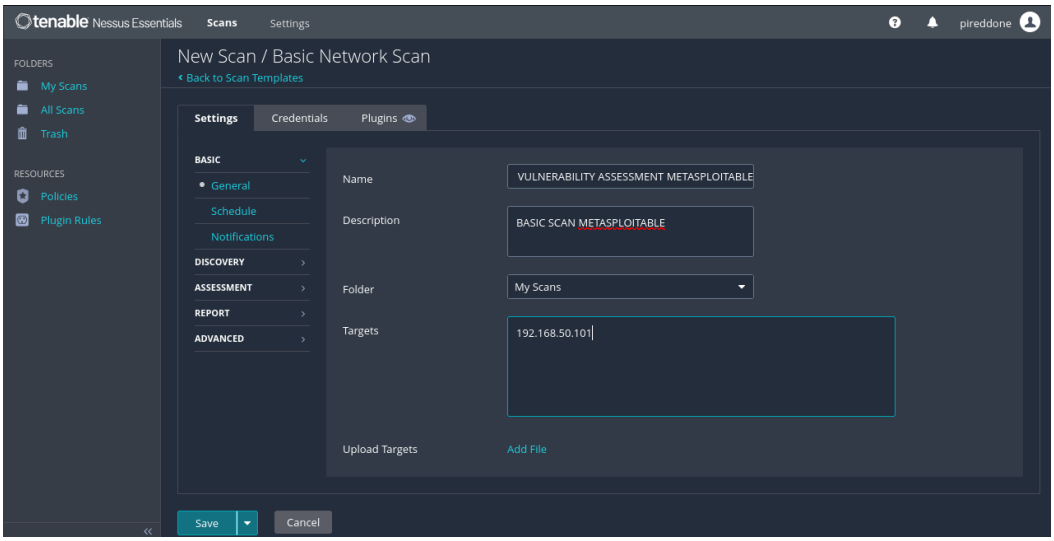
Nessus Essentials è stato installato e configurato su Kali Linux.
Prima di avviare la scansione è stato necessario **aggiornare i plugin**, operazione che richiede temporaneamente l'accesso a Internet.
Una volta completato l'aggiornamento, la macchina è stata nuovamente riportata sulla rete interna.

È stata configurata una scansione di tipo:

- **Basic Network Scan**

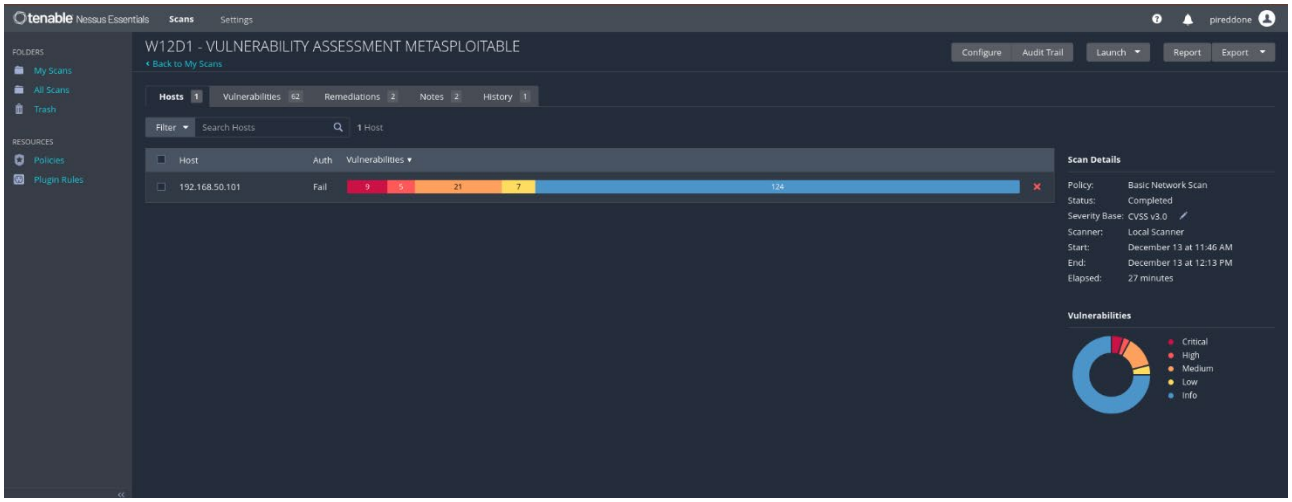
con le seguenti impostazioni:

- **Nome scansione**: Vulnerability Assessment Metasploitable
- **Target**: 192.168.50.101
- **Policy**: Basic Network Scan
- **Scanner**: Local Scanner



Esecuzione della scansione

La scansione è stata avviata correttamente e completata senza errori.
Nessus ha identificato l'host target e ha analizzato i servizi esposti, rilevando numerose vulnerabilità di diverso livello di gravità.



Analisi dei risultati

Al termine della scansione sono state individuate **62 vulnerabilità complessive**, suddivise in:

- **Critical**
- **High**
- **Medium**
- **Low**

- **Informational**

Le vulnerabilità critiche risultano particolarmente rilevanti, in quanto rappresentano un rischio immediato per la sicurezza del sistema.

Vulnerabilità critiche analizzate

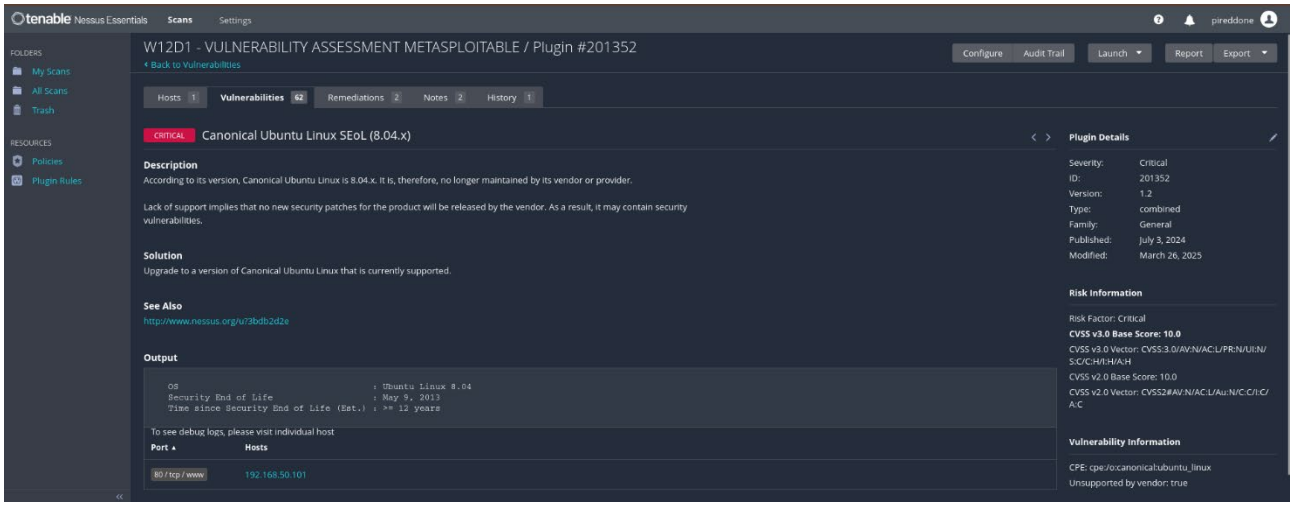
1 Sistema operativo non supportato (Ubuntu 8.04)

Nessus ha rilevato che il sistema operativo della macchina target è **Ubuntu Linux 8.04**, versione non più supportata dal vendor.

Questa condizione implica:

- assenza di aggiornamenti di sicurezza
- esposizione a vulnerabilità note
- elevato rischio di compromissione

La soluzione suggerita consiste nell'aggiornare il sistema operativo a una versione attualmente supportata.



---

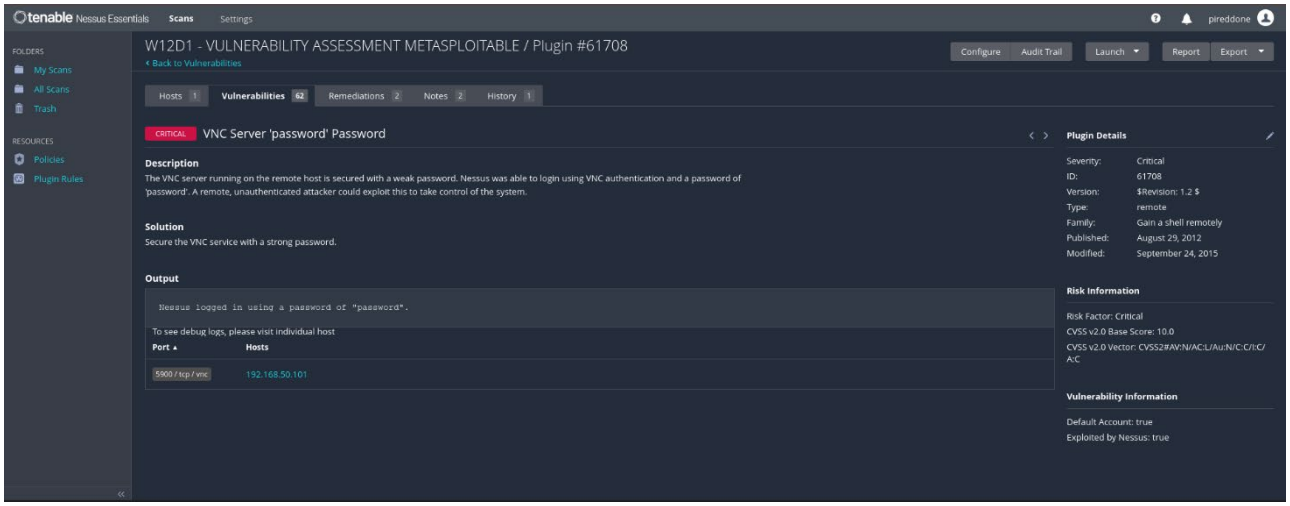
2 VNC con password debole

È stata individuata una vulnerabilità critica relativa al servizio **VNC**, protetto da una password estremamente debole ("password").
Nessus è riuscito ad autenticarsi con successo, dimostrando la possibilità di accesso remoto non autorizzato.

Questa vulnerabilità consente a un attaccante di:

- accedere graficamente al sistema
- ottenere il controllo completo della macchina

La soluzione suggerita consiste nell'impostare una password robusta o disabilitare il servizio se non necessario.



Considerazioni finali

L'esercizio ha dimostrato come uno strumento di Vulnerability Assessment permetta di individuare rapidamente gravi problemi di sicurezza, anche senza effettuare attività di sfruttamento attivo.

Nessus fornisce:

- identificazione delle vulnerabilità
- valutazione del rischio (CVSS)
- suggerimenti di remediation

Questo tipo di analisi è fondamentale in ambito **Blue Team**, auditing e sicurezza aziendale, dove l'obiettivo è prevenire incidenti piuttosto che attaccare i sistemi.

Conclusione

L'attività ha permesso di comprendere il funzionamento di uno scanner di vulnerabilità professionale e l'importanza della corretta interpretazione dei risultati.
Metasploitable si è dimostrato un ottimo ambiente didattico per osservare vulnerabilità reali in modo controllato.

✅ Checklist finale

- Scan configurata correttamente
- Target corretto

- Risultati analizzati
- Vulnerabilità critiche comprese