EPICODE-CS0124
S5/L4 - Pratica

Flaviano Sedici

Pratica

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo).

A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Gli obiettivi dell'esercizio sono:

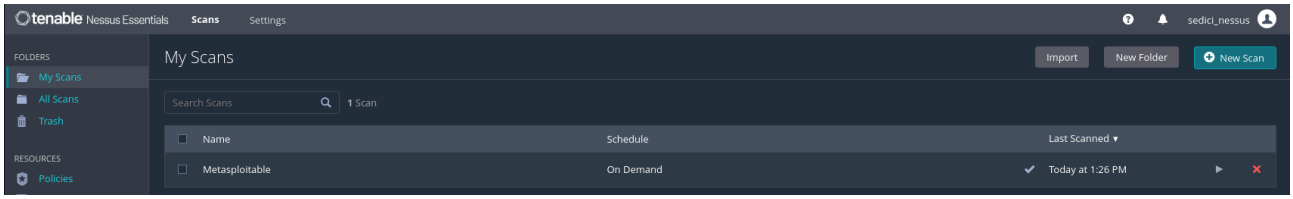
Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.

Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

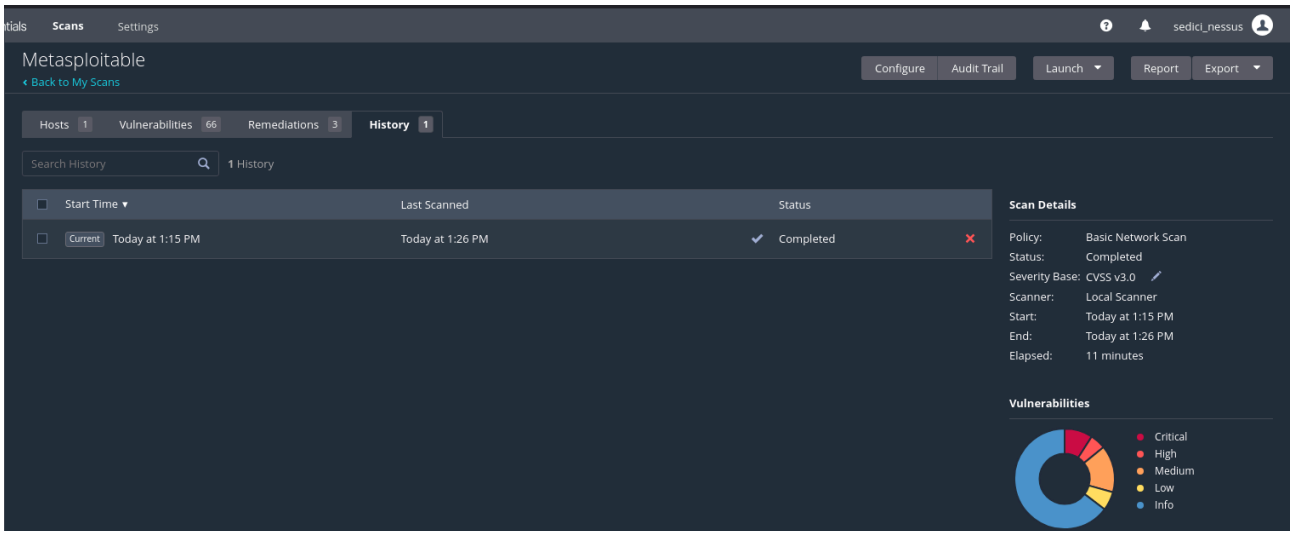
1. Configurazione Nessus scan su Metasploitable

Per configurare la scansione delle vulnerabilità di Metasploitable, con IP 192.168.60.101, sono state utilizzate le impostazioni di default con la funzionalità "basic network scan".

La scansione ha richiesto circa 11 minuti.



Riepilogo Scan



Tempistiche di Scan

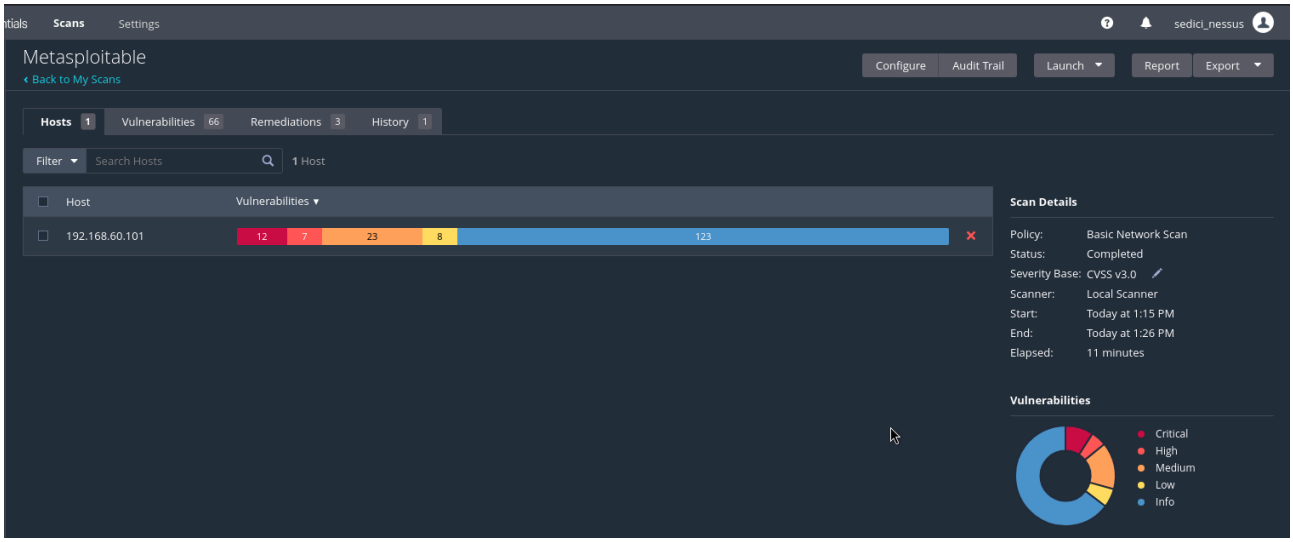
2. Risultati dell’analisi

L’analisi ha rilevato 12 vulnerabilità critiche tra cui ad esempio:

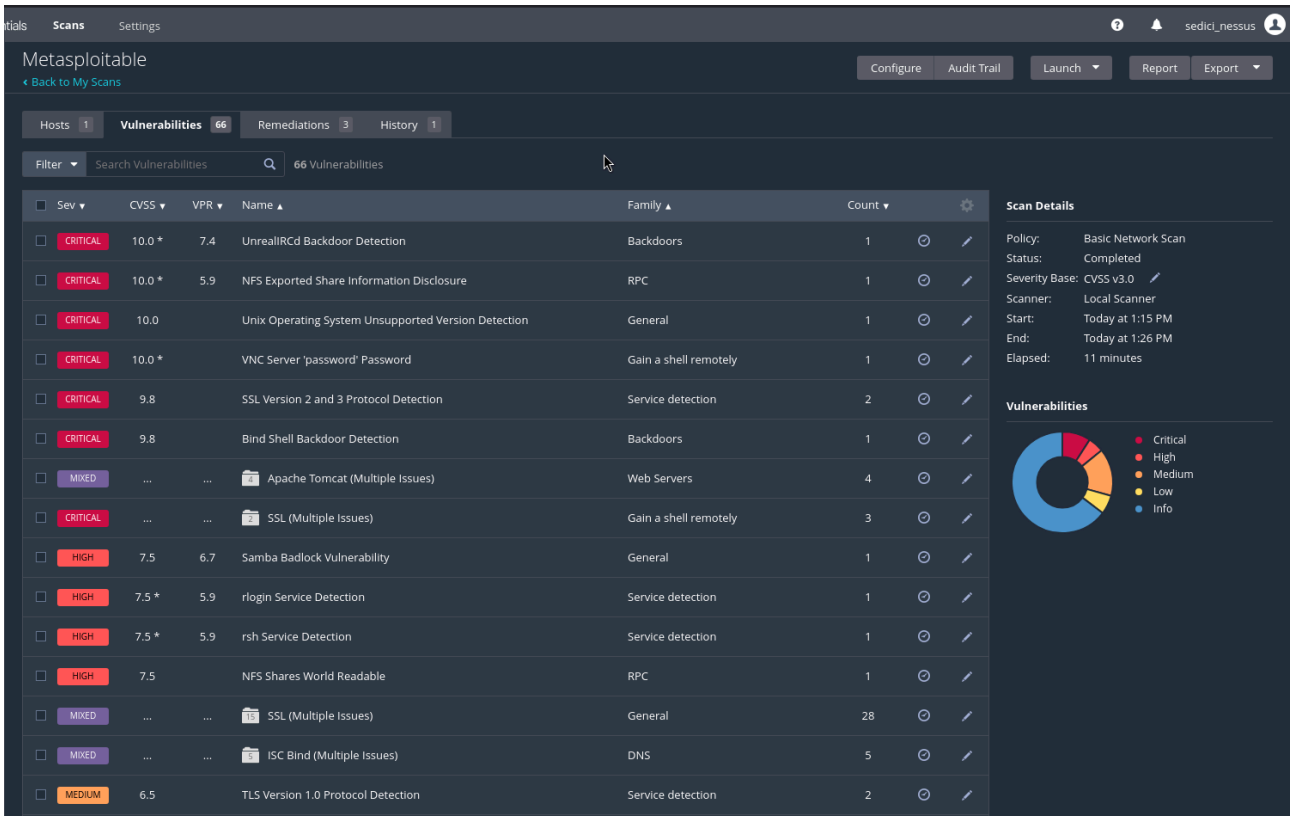
2 backdoors

2 possibili accessi da shell remota

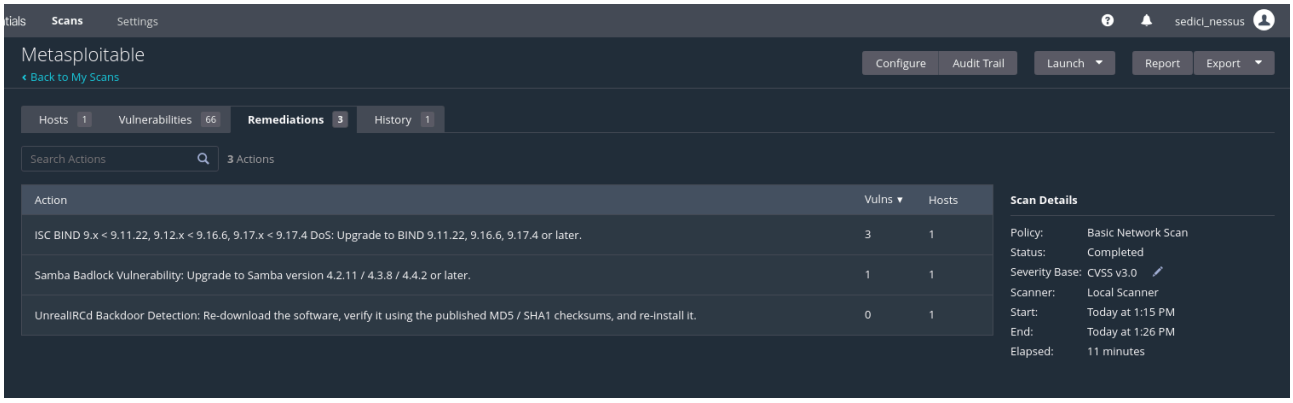
2 sui web servers



Risultati generali della scansione



Dettaglio dei risultati di scansione



Dettaglio delle possibili remediations

Nessus restituisce anche dei possibili consigli sulle remediations di alcune vulnerabilità.