# ENUMERAZIONE DELLE VULNERABILITA’

**Traccia:**

- 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

Consegna:

•Report PDF per «tecnico» Report tecnico è inteso come "quasi completo" che va ad indicare sia le porte che la vulnerabilità che la risoluzione, in modo da poter intervenire.

•Suggerimento: fare traduzione in italiano della descrizione e/o remediation

## svolgimento

Prima di effettuare la scansione vera e propria, sono andata ad effettuare l’installazione e configurazione del tool Nessus.

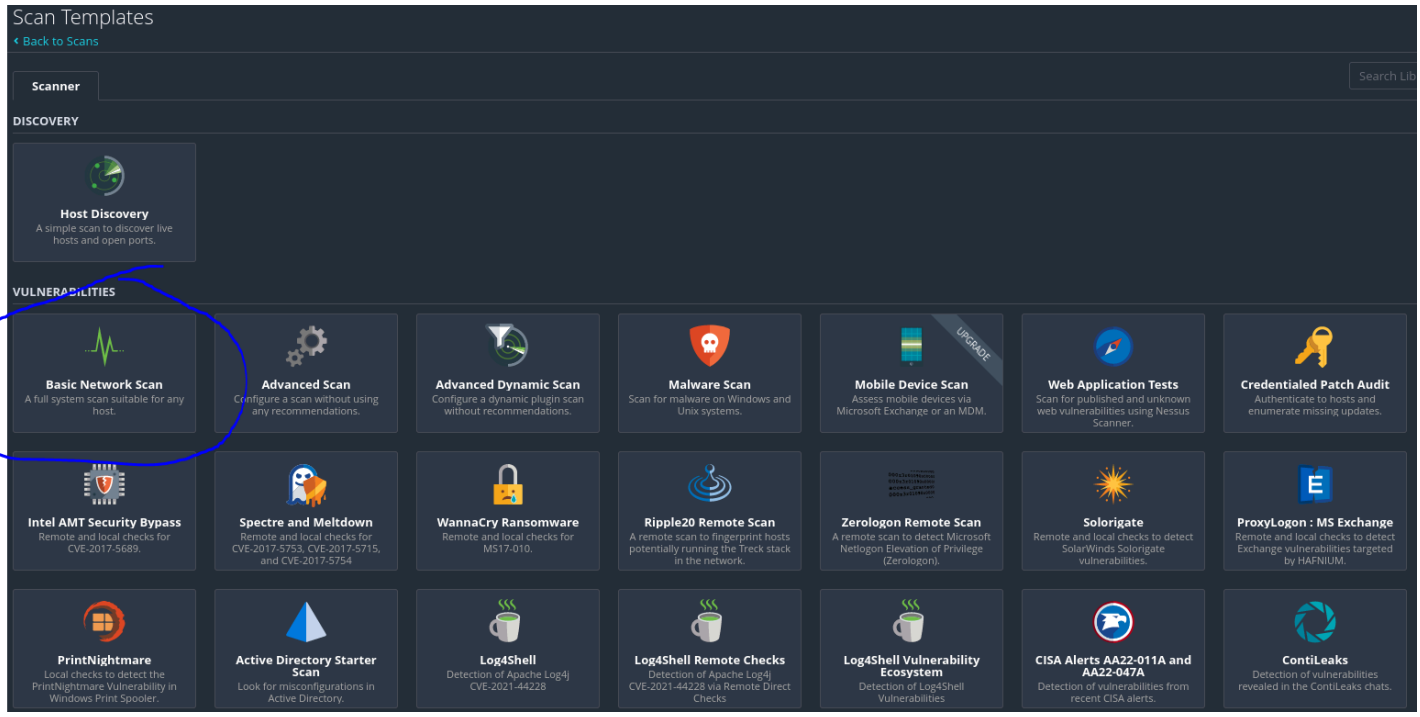
Ho provveduto a registrarmi e a installare sulla macchina virtuale Kali Linux la versione Debian più recente di Nessus.

Fatto ciò, ho avviato per la prima volta il tool e l’ho impostato seguendo questi comandi:

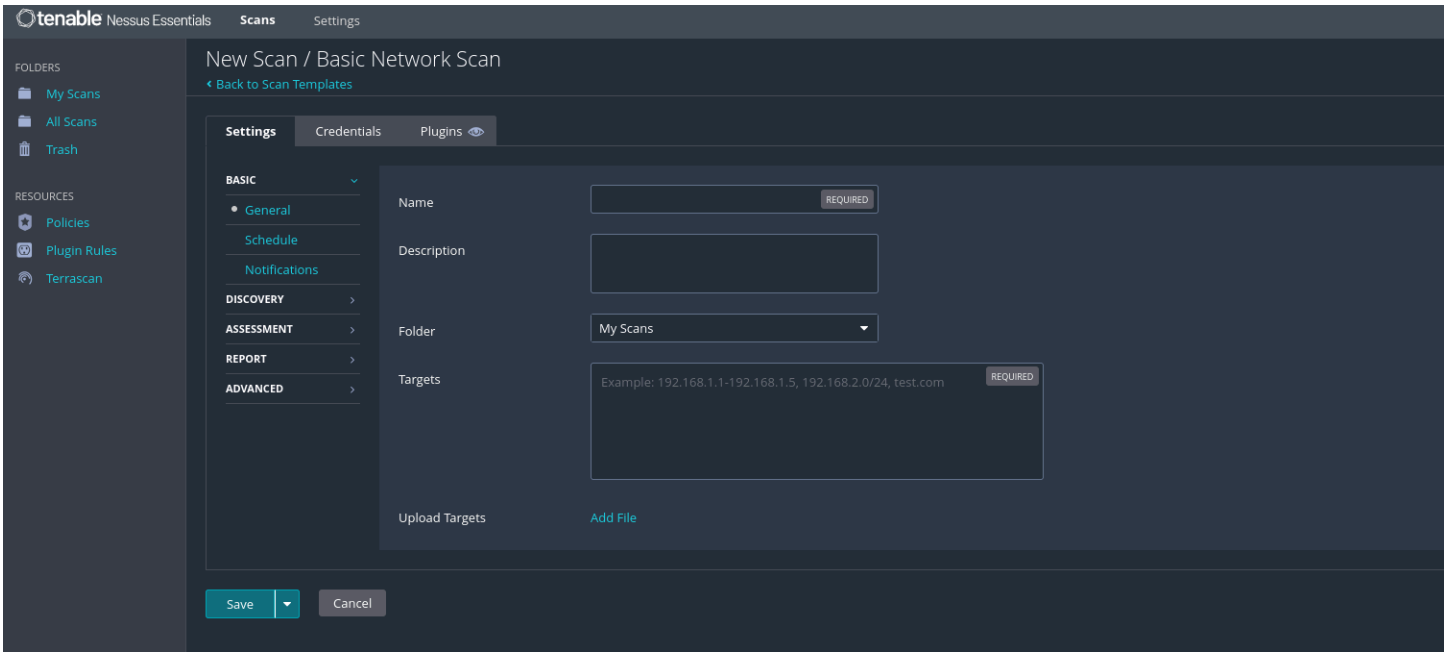
- sudo systemctl start nessusd.service
- sudo systemctl status nessusd (per vedere lo stato del tool)
- sudo systemctl enable nessusd (per attivare il servizio di Nessus)
- https://localhost:8834/#/

Dopo aver compilato tutti i plugin, necessari per effettuare uno scan preciso ed esteso del sistema preso in analisi, ho proceduto ad effettuare il primo scan sulla macchina indicata dall’esercizio, ovvero Metasploitable.

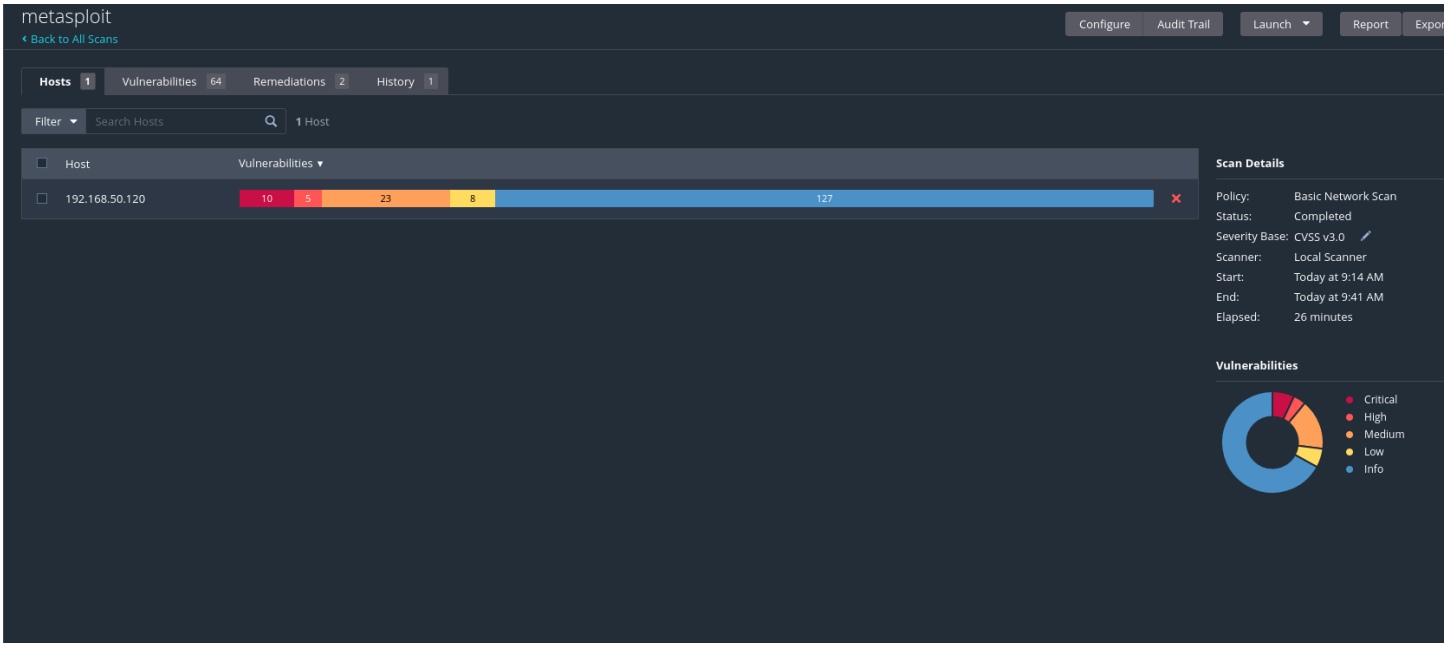
Ho selezionato lo scan “Basic Network Scan”, il quale comporta l’analisi di tutte le porte più comuni.




Dopo ciò ho inserito l'indirizzo ip della macchina presa in esame, che in questo caso per Metasploitable è 192.168.50.120




Dopo circa 30 minuti, i risultati dello scan vengono mostrati attraverso un grafico realizzato direttamente dal tool Nessus.


metasploit
Back to All Scans
Configure
Audit Trail
Launch
Report
Expor
Hosts 1
Vulnerabilities 64
Remediations 2
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.50.120
10
5
23
8
127
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:14 AM
End: Today at 9:41 AM
Elapsed: 26 minutes
Vulnerabilities
Critical
High
Medium
Low
Info