W12D4 - Pratica - parte uno - scansione Nessus

Giacomo di Giacinto

EPICODE | W12D4 - Pratica PDF | Esercizio — Traccia e requisiti

Traccia:

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche** e provate ad **implementare delle azioni di rimedio**.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili.
Vi consigliamo tuttavia di utilizzare magari questo approccio **per non più di una vulnerabilità**.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

Consegna:

1. Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - **ScansioneInizio.pdf**
2. **Screenshot e spiegazione dei passaggi della remediation - RemediationMeta.pdf**
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - **ScansioneFine.pdf**

   Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.

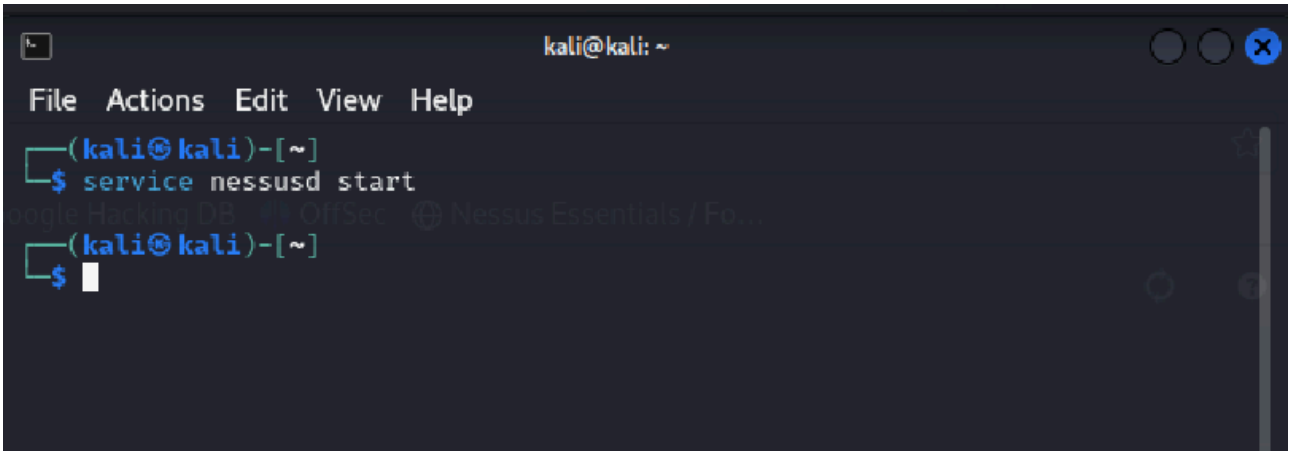
Nota: i report possono essere lasciati in inglese, senza problemi.

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall

La prima parte di questo progetto consiste nell'effettuare una scansione con l'applicativo Nessus su Metasploitable.

Di seguito mostro i passaggi per effettuare la scansione. Le due macchine sono in bridge e hanno gli indirizzi IP impostati in DHCP, l'indirizzo target della scansione è 192.168.1.246

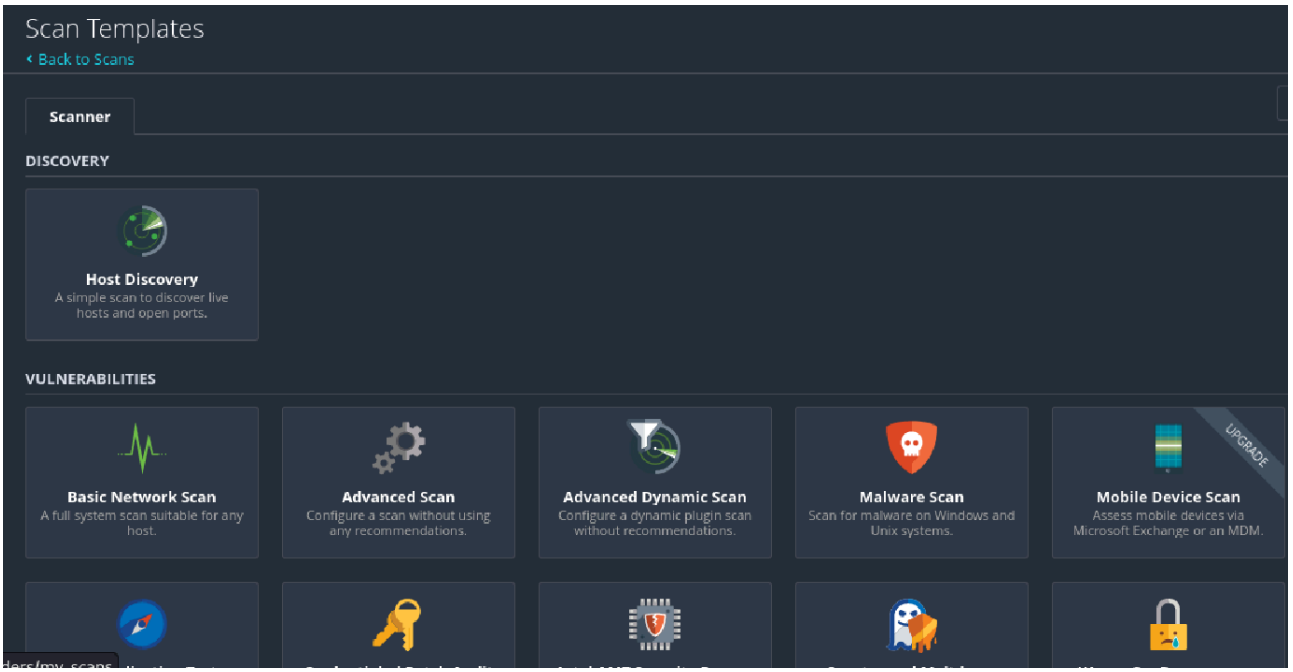
- Per effettuare una scansione con nessus, inizialmente deve essere attivato il servizio con il segiente comando



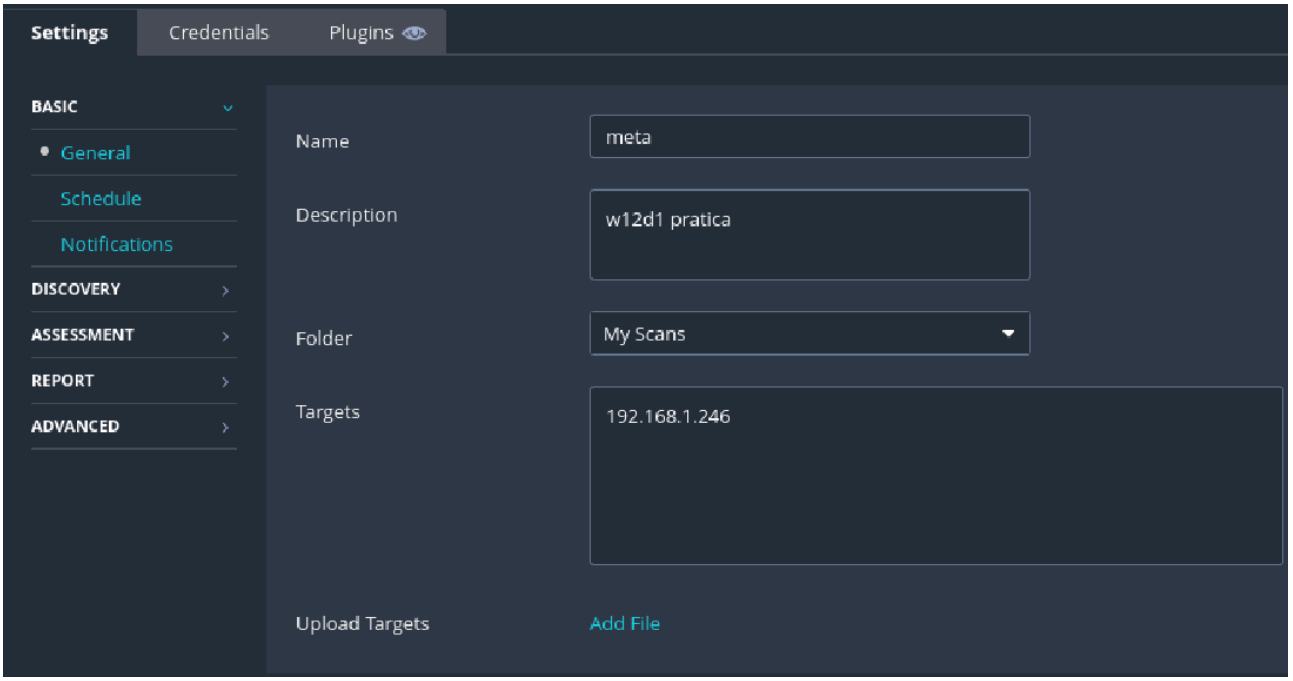
- Successivamente dal web browser deve essere inserito il seguente url

https://kali:8834

- Una volta aperto il programma deve essere selezionata "new scan" e poi "Basic Network Scan"

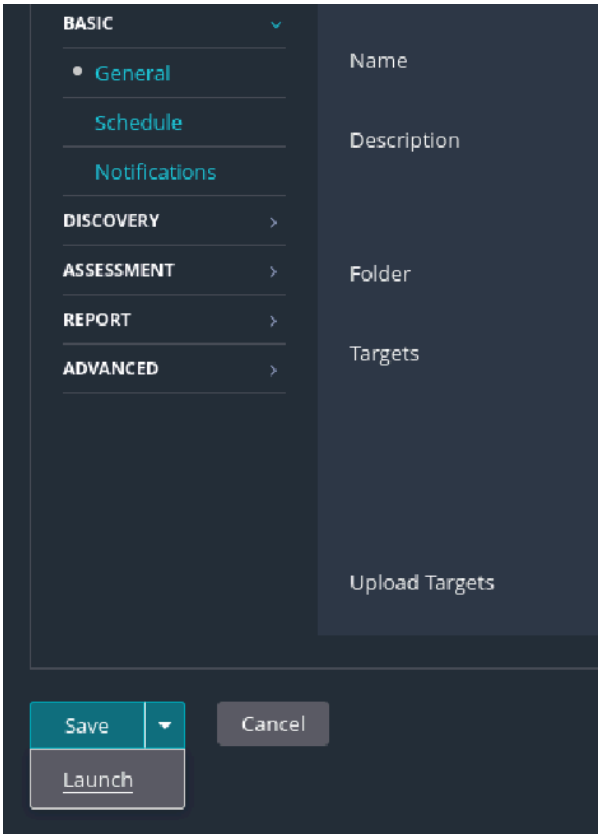


- Deve poi essere impostata la scansione, inizialmente con il nome, descrizione ed il target

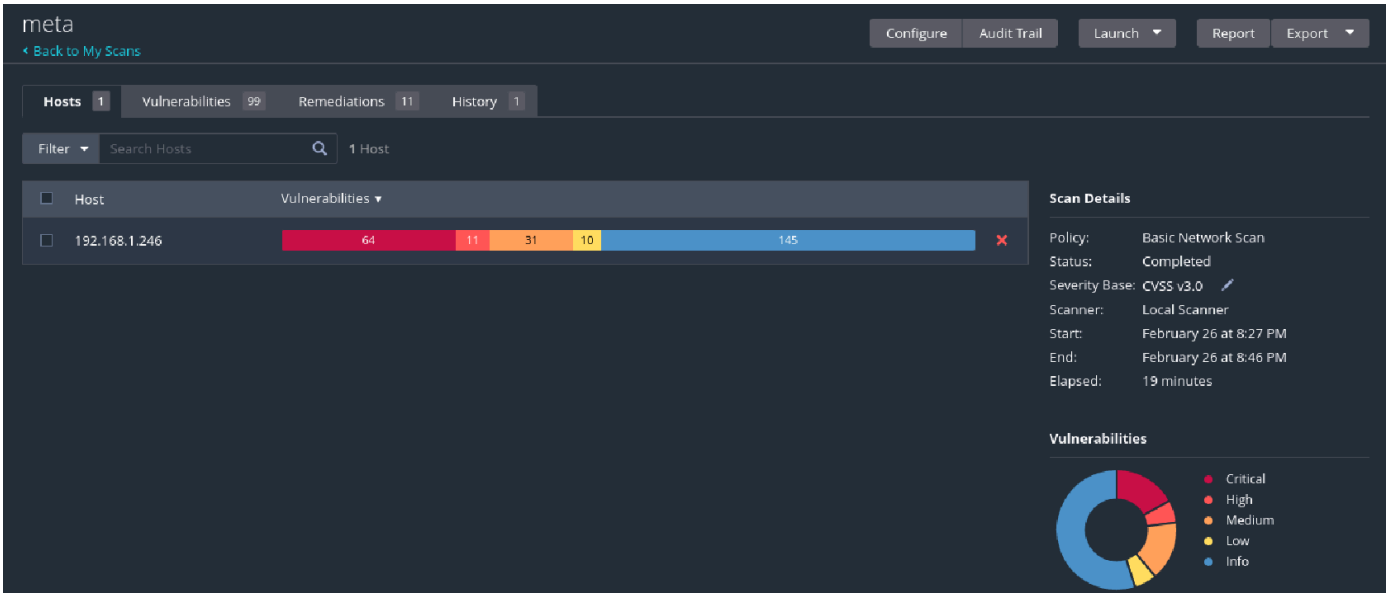


- Le altre impostazioni devono essere impostate secondo l'esigenza del momento; per questa scansione i settings sono stati lasciati standard.

- finite le impostazioni deve essere attivata la scansione con il bottone "launch"



- alla fine della scansione il sistema evidenzia il risultato a video



- per ottenere esportare i report dobbiamo cliccare nel bottone export ed indicare i parametri necessari.

Allego nella seguente cartella il pdf con il report della scansione.