Pratica S5/L4

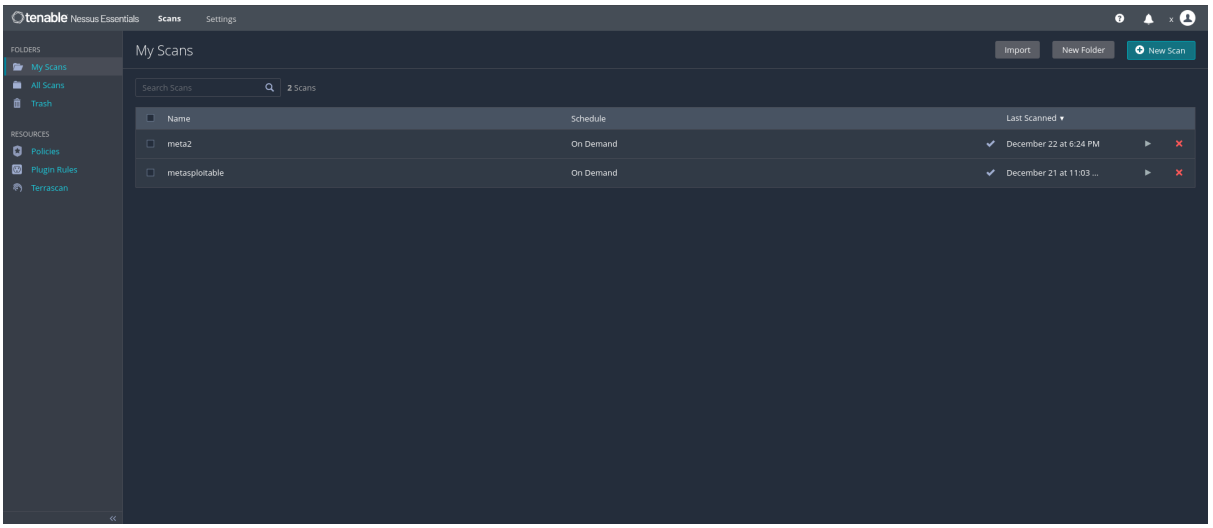
Traccia:

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)

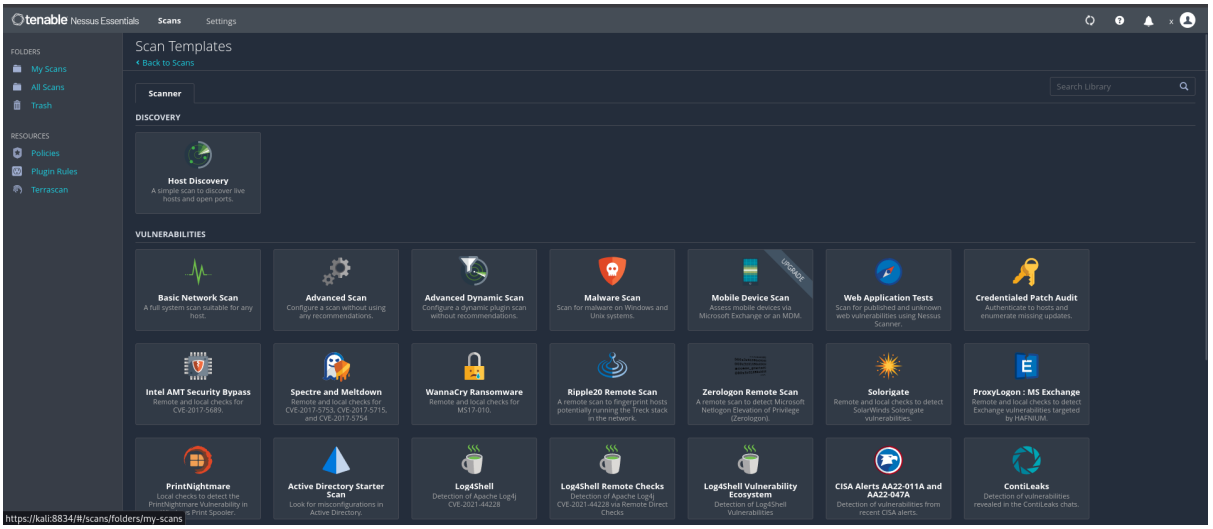
Strumento utilizzato : Nessus (un Vulnerability scanner semplice da usare e molto potente, che è molto utilizzato dalle compagnie per coprire reti piuttosto estese)

Lo strumento viene scaricato dal sito ufficiale di Nessus (https://www.tenable.com/products/nessus) , una volta scaricato si estrae con il comando "sudo dpkg -i (versione di Nessus scaricata)" e per avviarlo si utilizza " sudo systemctl start nessusd.service" ,tutto svolto nel terminale.

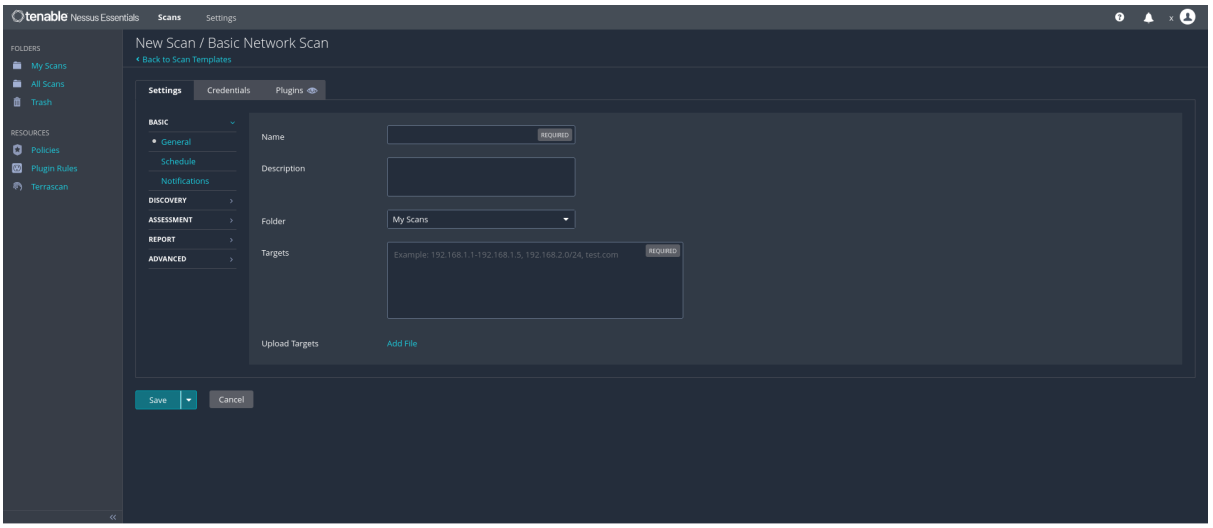
Dopo l'avvio del Nessus (che non darà nessun risultato) si apre il browser e cerca il seguente sito "https://(nome dell'utente in uso , in questo kali perché sono dentro con l'utente kali):8824" , vi si comparirà la schermata di nessus con login o registrati , vi registrate se non lo avete fatto ; se l'email (in questo caso gmail) non vi funziona , dovete registrarvi andato nel loro sito ufficiale .



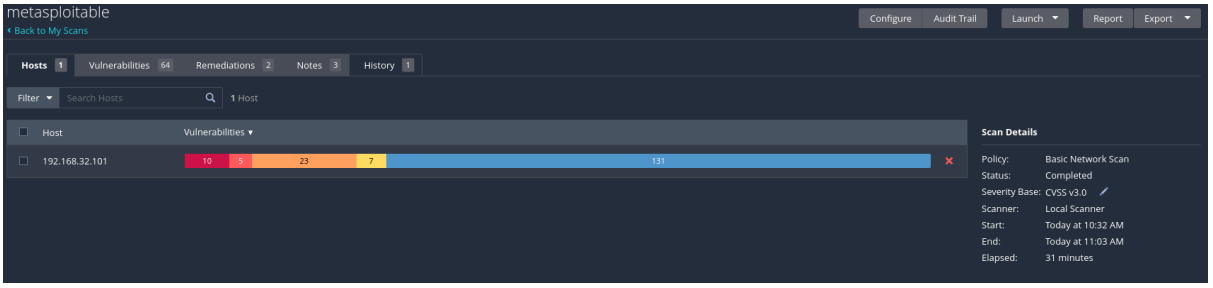
Una volta entrati non troverete le scan ma una pagina vuota , in altro a destra c'è un'icona molto piccola , dovete attendere che scarichi tutti gli plugin e dopo di che potete cliccare su "New scan"



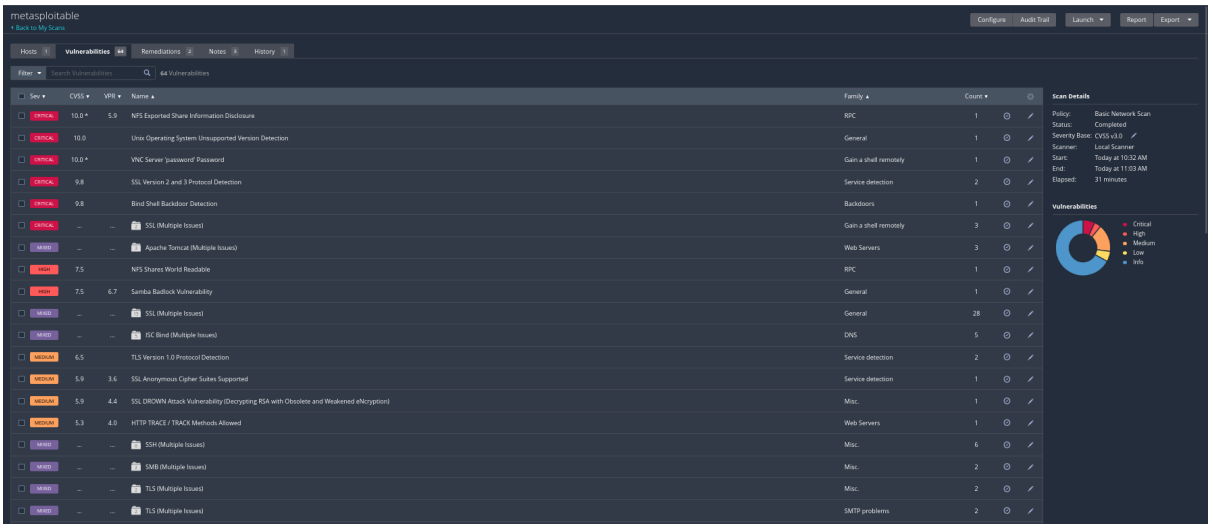
Vi comparirà questa schermata , in questo esercizio viene utilizzato la “Basic Network Scan”



Al “Name” il nome date voi a questa operazione scan e al “Target” l’indirizzo della macchina che dovete scanzionalizzare (in questo ip della macchina di metasploitable : 192.168.32.101) e infine lo salvate.



Fate partire lo scan e aspettate che finisce e infine vi darà una serie d’informazioni



Dopo lo scan vi restituirà un report con tutti gli punti vulnerabili della macchina metasploitable , classificandole in base alla loro gravità .