TRACCIA 4: BWII

Exploit Metasploitable con Metasploit

Traccia Giorno 4:

Sulla macchina Metasploitable ci sono diversi servizi in ascolto potenzialmente vulnerabili. È richiesto allo studente di:

• Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Metasploitable

• Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole (vedere suggerimento)

• Eseguire il comando «ifconfig» una volta ottenuta la sessione per verificare l’indirizzo di rete della macchina vittima

Requisiti laboratorio Giorno 4:

IP Kali Linux: 192.168.75.100

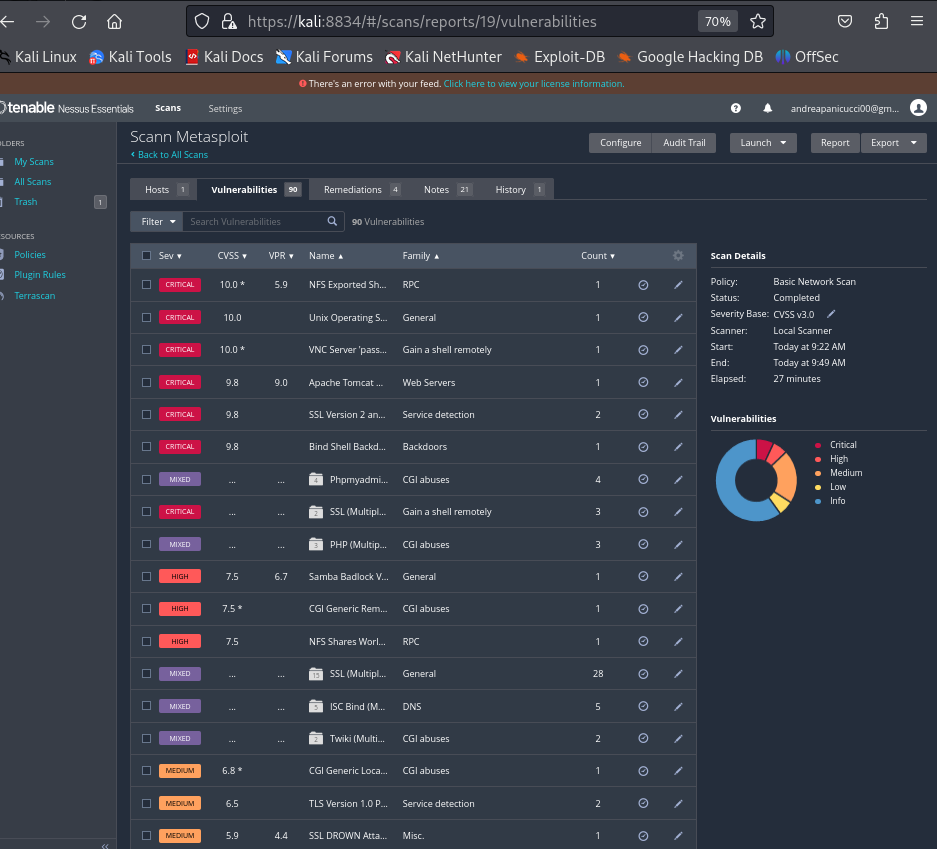
IP Metasploitable: 192.168.75.150

Listen port (nelle opzioni del payload): 4455

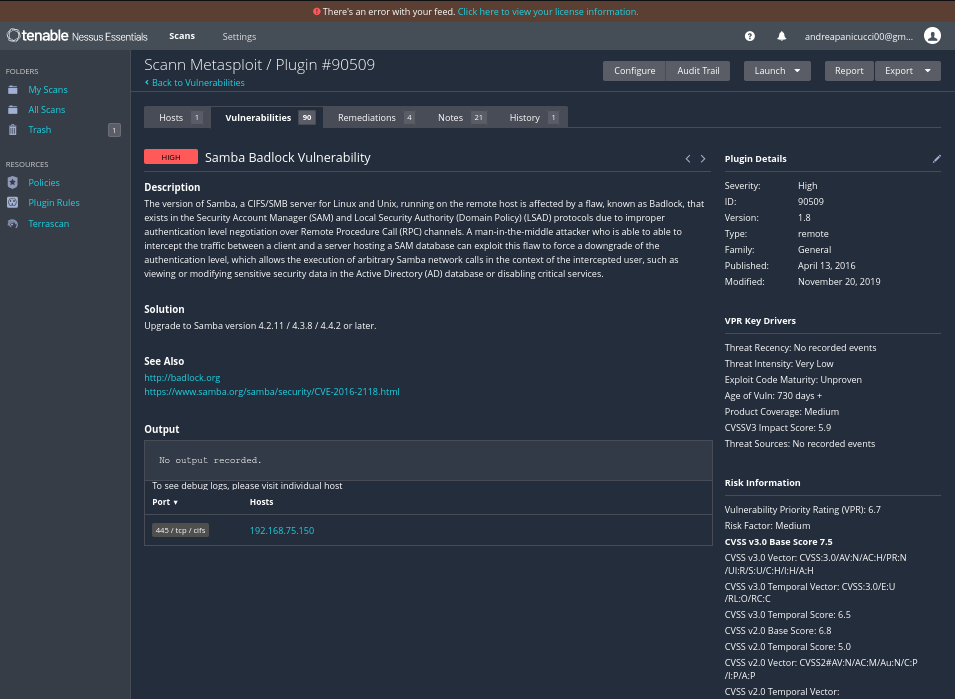
Suggerimento: Utilizzate l’exploit al path exploit/multi/samba/usermap\_script (fate prima una ricerca con la keyword search)

GUIDA:

Per prima cosa facciamo lo scanner delle vulnerabilità (basic scann) con Nessus:



Come seconda cosa andiamo a vedere la vulnerabilità che a noi interessa:



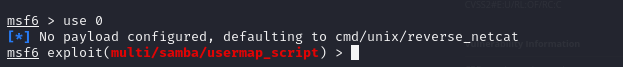
Ho usato nmap per verificare che la porta 445 fosse aperta.



Una volta avviato msfconsole cerco l’exploit suggerito:



E con use 0 lo utilizzo:



Una volta utilizzato l’exploit con il comando options/show options posso vedere i “current settings” dell’exploit stesso, dove posso settare RHOST e RPORT, rispettivamente, con l’IP della macchina target e la porta della macchina target con il comando set.

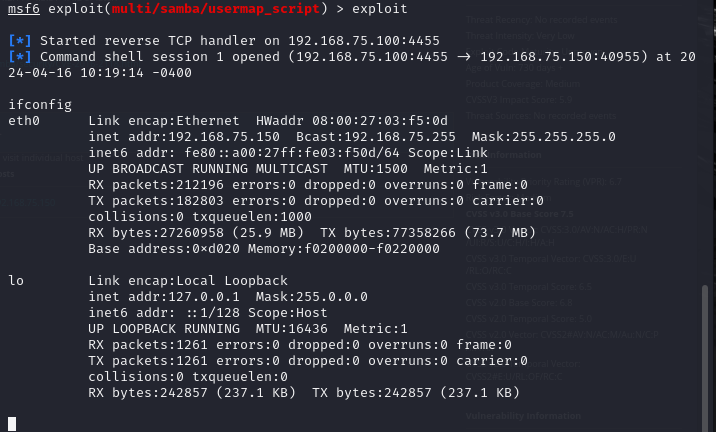




E come da suggerimento, settare la local port sulla porta: 4455



Dopo di che con il comando run/exploit che mi permette di avviare una sessione sulla macchina target: (Reverse TCP Handler)



Infatti, scrivendo il comando ifconfig riusciamo a vedere l’Indirizzo di rete della macchina target.