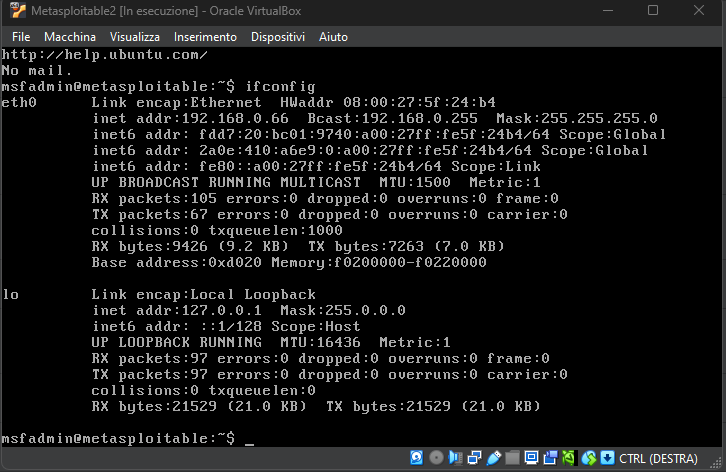
PRATICA 29 OTTOBRE 2024

NMAP

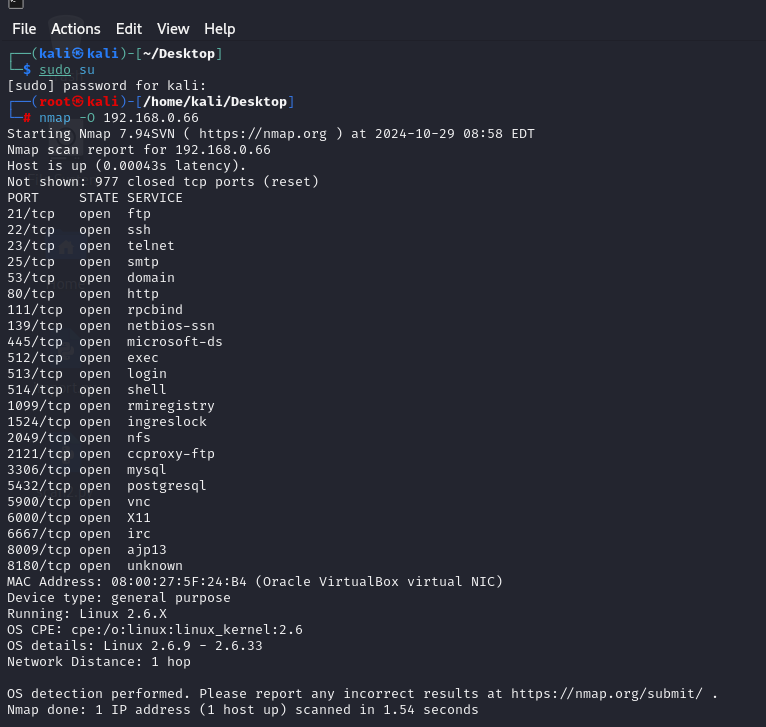
Traccia: Tecniche di scansione con Nmap

Utilizzando la VM di Kali Linux per effettuare i test, andremo a testare Nmap su due target: Metasploitable2 e Windows 7.

METASPLOITABLE2

Prendendo in considerazione l’indirizzo IP di Metasploitable2, ovvero 192.168.0.66, andremo ad estrapolare le informazioni che ci servono.

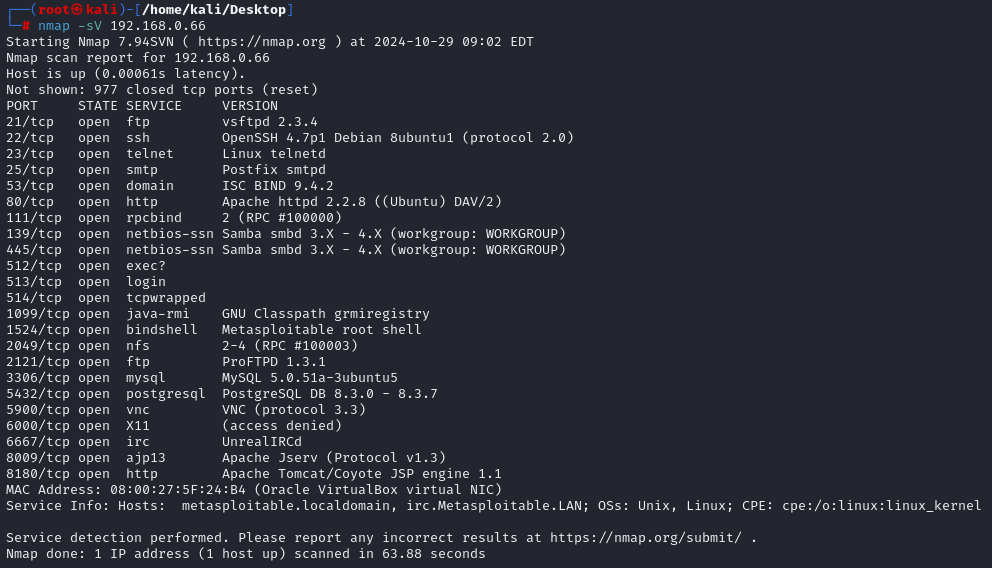
Inizieremo la ricerca utilizzando il comando -O che ci permetterà di rilevare il sistema operativo del target.

Esempio di comando: nmap -O 192.168.0.66

Grazie a questo comando adesso sappiamo che il target monta Linux 2.6 come SO.

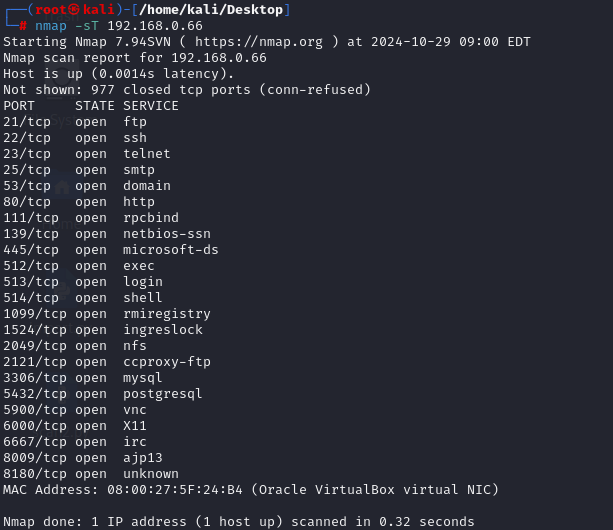
Procediamo col prossimo comando, ovvero -sV.   
Con -sV si va ad utilizzare il banner grabbing, ovvero una tecnica che serve a raccogliere le informazioni di un servizio attivo su una porta aperta.

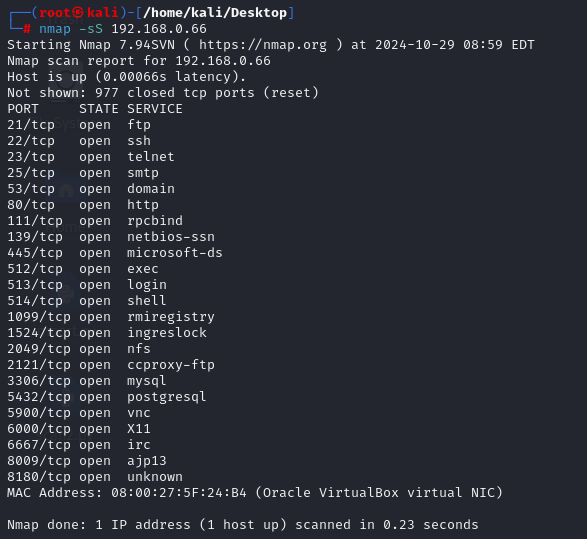
Di seguito un esempio di comando: nmap -sV 192.168.0.66



Adesso si può vedere nel dettaglio quali sono i servizi attivi in ogni porta per poter identificare e valutare potenziali vulnerabilità.  
  
Per concludere, utilizzeremo i comandi -sT e -sS. Entrambi servono ad effettuare una “TCP Connect Scan”, la differenza sta nel fatto che -sT effettua una three-way handshake completa mentre -sS si ferma al SYN interrompendo poi la stretta di mano.

Esempio di comando: nmap -sT 192.168.0.66, nmap -sS 192.168.0.66

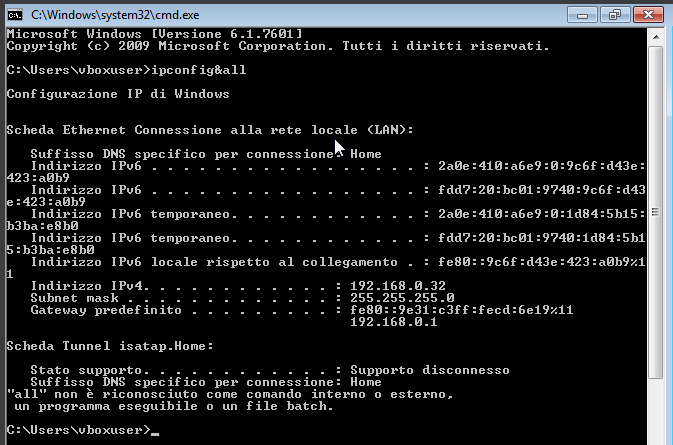




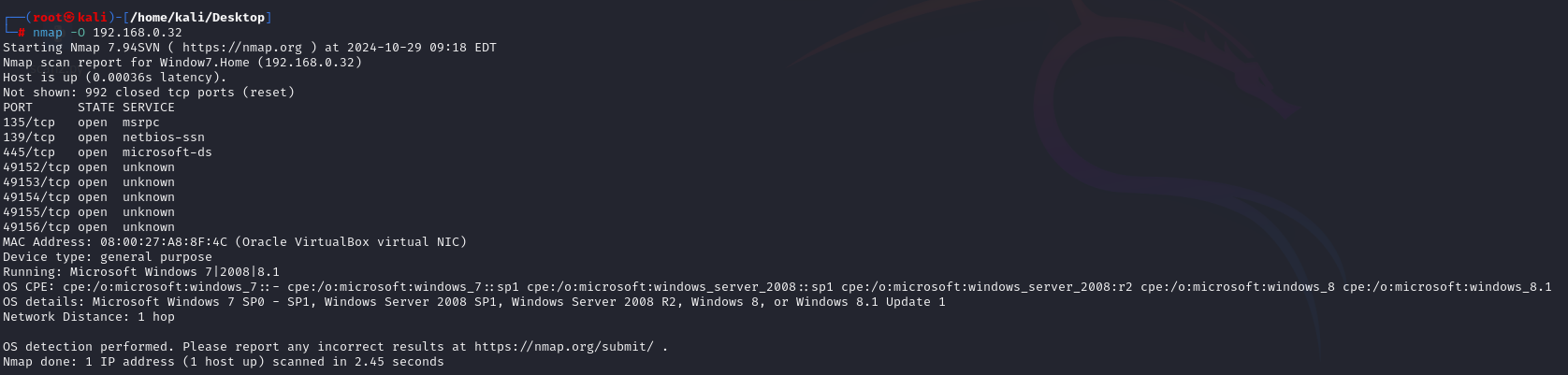
WINDOWS 7

Prendendo in considerazione l’indirizzo IP di Windows 7

192.168.0.32 andremo ad utilizzare il comando -O per estrarre tutte le informazioni necessarie sul SO.



Di seguito le informazioni estrapolate utilizzando il comando

-O

In conclusione possiamo affermare che nmap