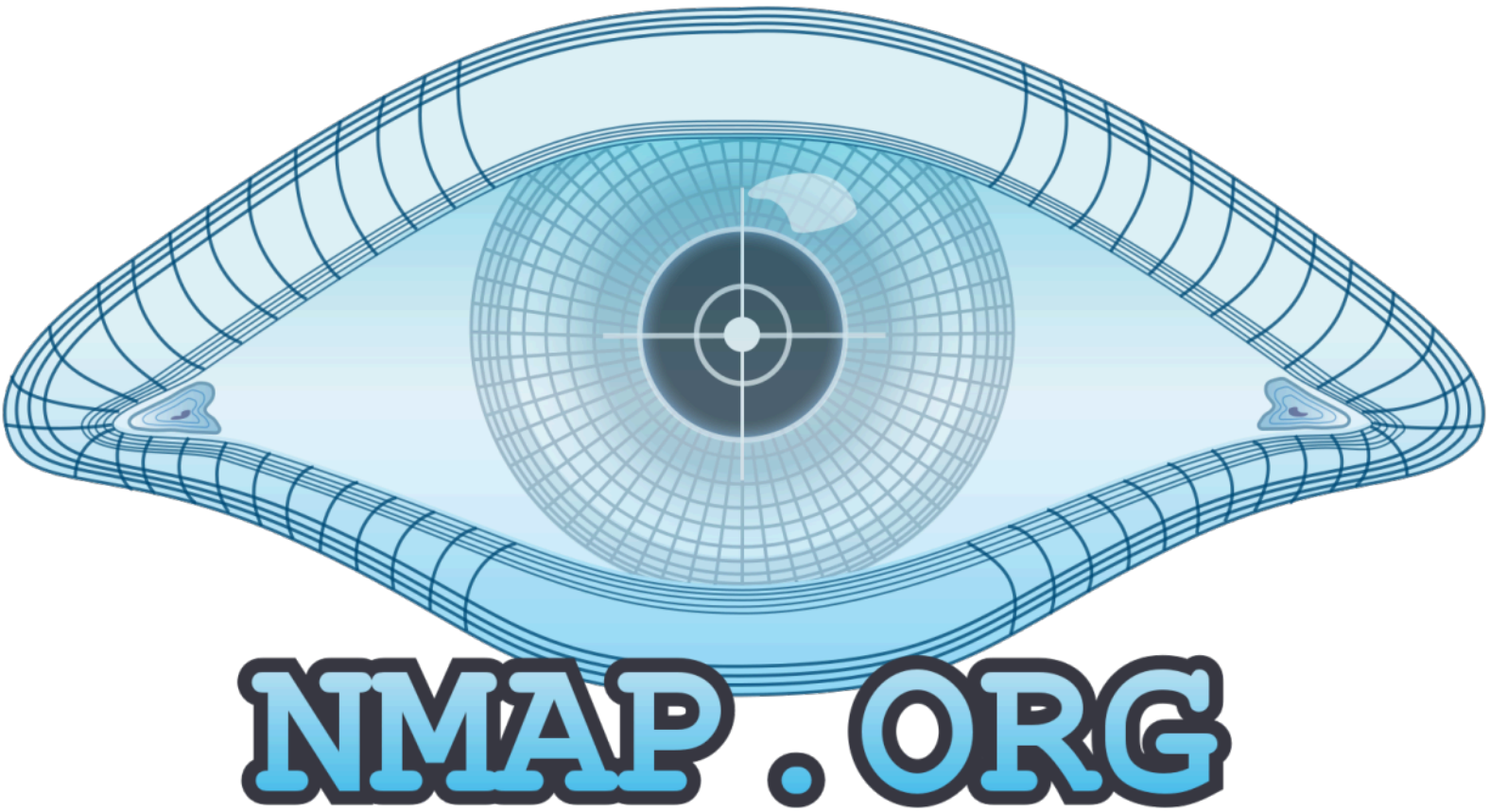
Ghassan Haouem



NMAP .ORG

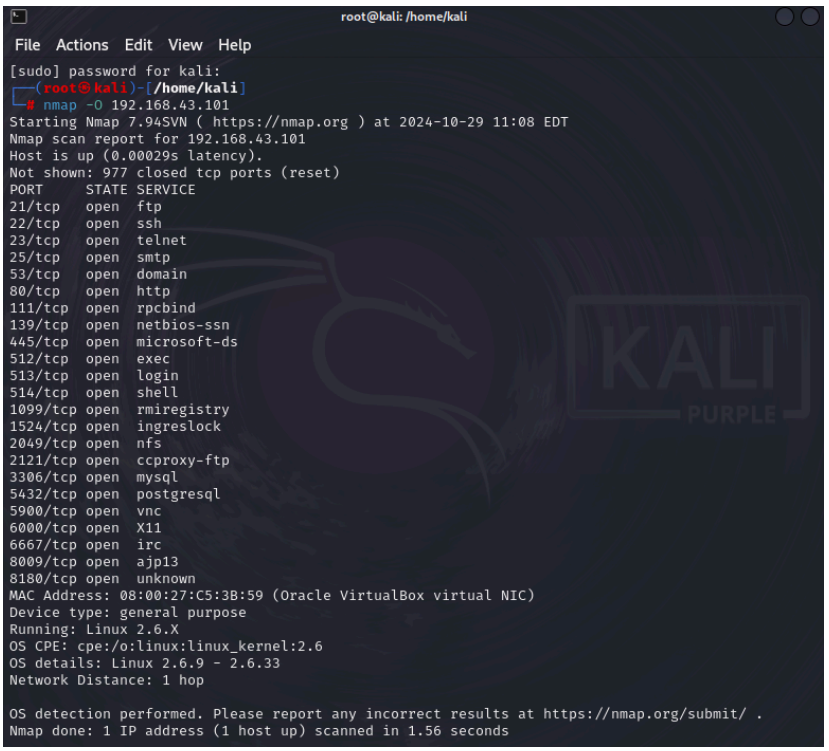
è prevista la produzione di un report contenente le seguenti info (dove disponibili):
- IP.
- Sistema Operativo.
- Porte Aperte.
- Servizi in ascolto con versione.

IP

Per questa volta la macchina target è Metasploitable 2 , il quale IP è il seguente 192.168.43.101 , questa informazione è vitale per le operazioni che andremo a fare , essendo autorizzati non subiremo nessuna denuncia .

Sistema operativo

Per determinare il sistema operativo del target (OS Fingerprint), si usa il flag `-O`. Questo comando consente di identificare il sistema operativo cercando di riconoscere alcune caratteristiche specifiche del sistema target:



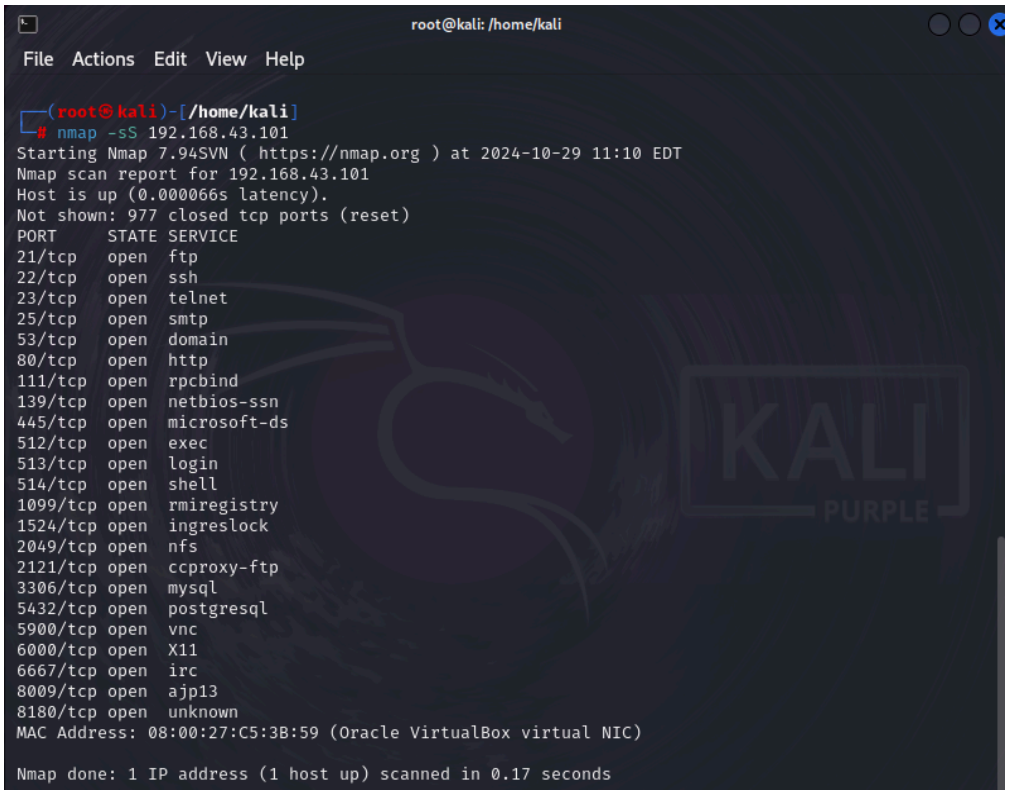
È importante sapere che il rilevamento del sistema operativo è più preciso se Nmap riesce a trovare e analizzare porte aperte e chiuse.

Ghassan Haouem

Porte Aperte

Per effettuare la scansione delle porte aperte abbiamo diversi comandi che possiamo lanciare :

1) nmap -sS
   Utilizza il comando SYN Scan per una scansione veloce e stealth



Questo metodo è molto utilizzato perché è veloce, discreta e consente di identificare le porte aperte senza stabilire una connessione TCP completa.

Piu' sicura perchè non finisce le 3 way handshake.

Servizi in ascolto con versione

Per rilevare i servizi in ascolto con le loro versioni su un target, si può utilizzare l'opzione -sV di Nmap. Questa opzione permette di identificare il tipo di servizio in ascolto su una porta e, quando possibile, la versione esatta del servizio.

Comando in questione :
1) nmap -sV