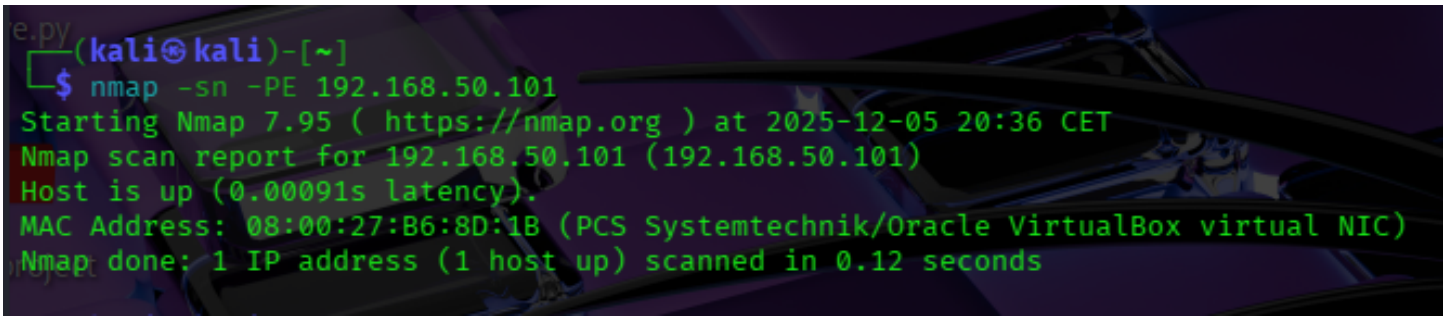
Traccia Esercizio

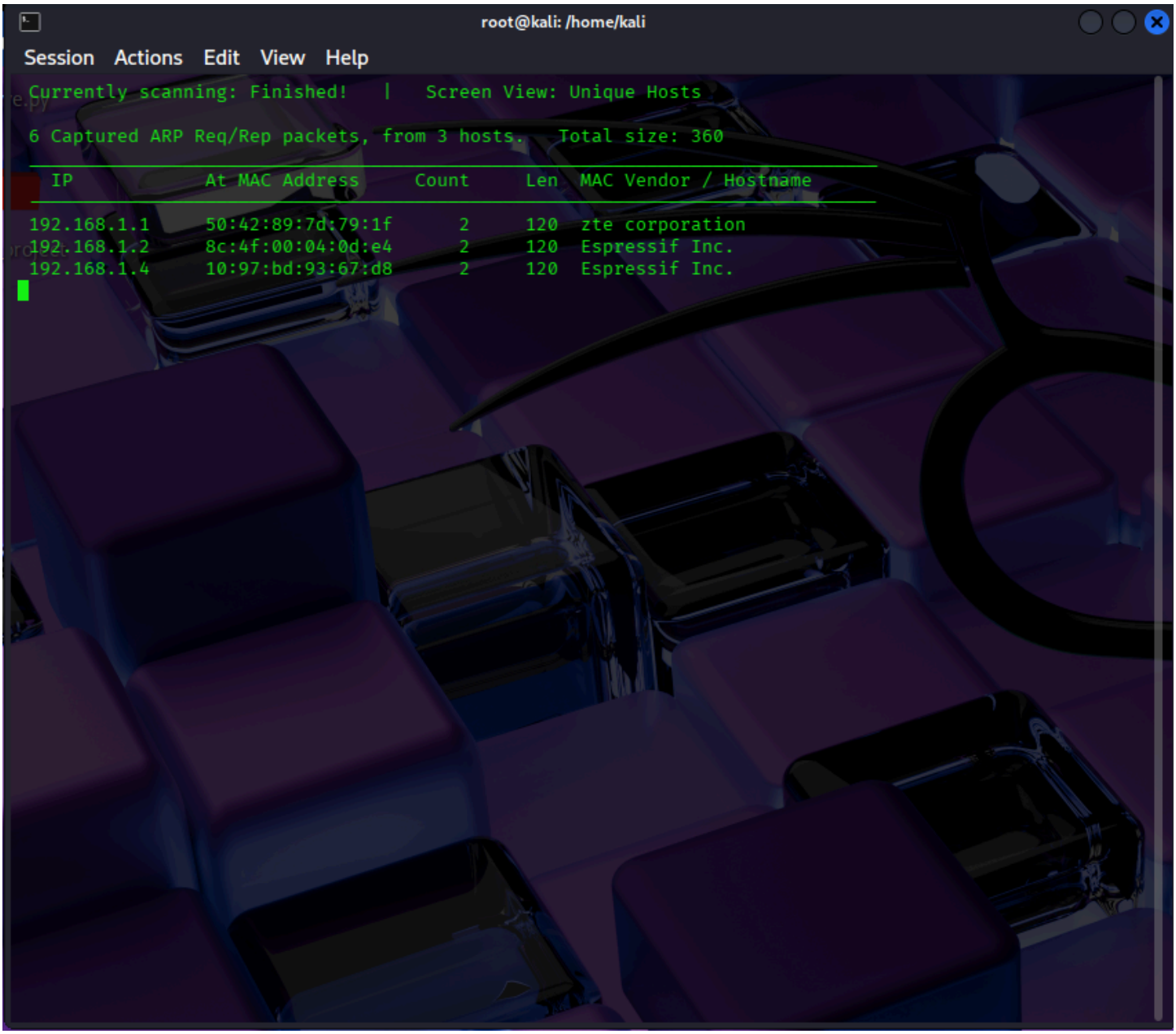
Dopo aver visitato il sito https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/ Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report.

nmap -sn -PE <target>



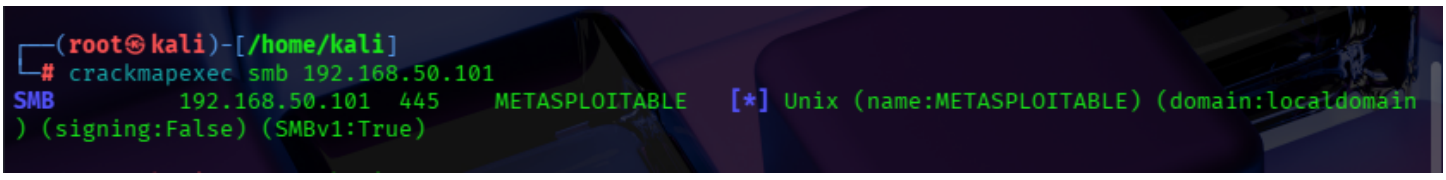
Con questo primo scan riusciamo a scoprire che la macchina target è attiva

netdiscover -r <target>



Qui possiamo vedere tutti i dispositivi attivi in una determinata rete, compresi di indirizzo MAC

crackmapexec protocollo <target>



Ecco qui che scopriamo che la macchina con cui comunichiamo ha come OS metaspoitable

nmap <target> –top-ports 10 –aperto

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.50.101 -top-ports 10 -open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 20:51 CET
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00076s latency).
Not shown: 3 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:B6:8D:1B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.78 seconds
```

In questo caso il comando è autoesplicativo, scopriamo altre informazioni importanti, cioè le porte aperte sulla macchina

nmap <target> -p- -sV –reason –dns-server ns

-p- → scansiona **tutte le porte (1–65535)**

-sV → identifica la **versione dei servizi** su ogni porta aperta

--reason → ti mostra **perché** una porta risulta aperta/chiusa (il “motivo” del risultato)

--dns-server <ns> → usa **quel DNS specifico** invece di quello di default

info raccolte

IP: 192.168.50.101

DISPOSITIVI NELLA RETE: 3

OS: META

PORTE APERTE: 21 22 23 25 80 139 445

MAC: 08:00:27:B6:8D:1B