Etudiant : [redacted]

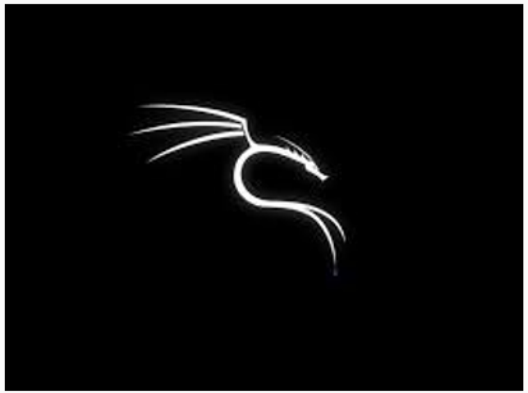
Enseignant : [redacted]

Démonstration - Port scan

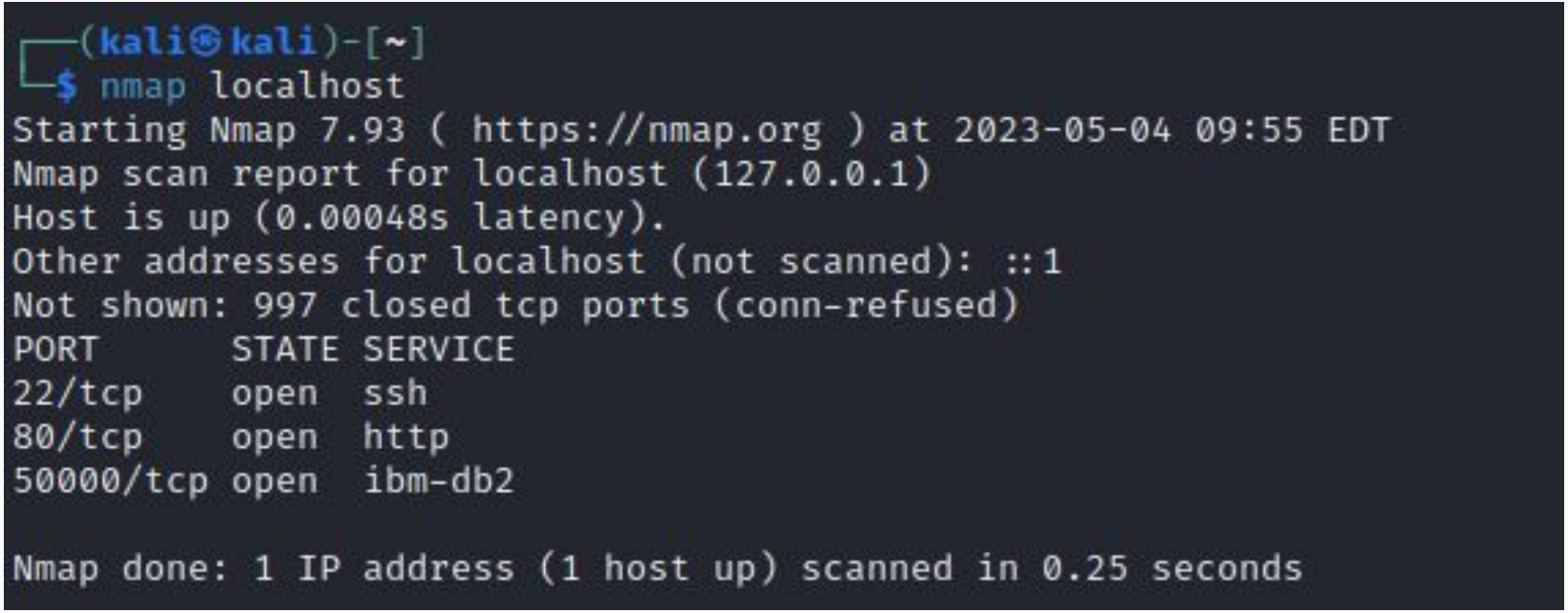
Sur une machine virtuelle Kali Linux contenant :

- *Un serveur vsftpd au port 50000 (FTP)*
- *Un serveur web Apache2 au port 80 HTTP (FTP)*
- *SSH au port 22 (FTP)*
- *Tftp au port 69 (UDP)*

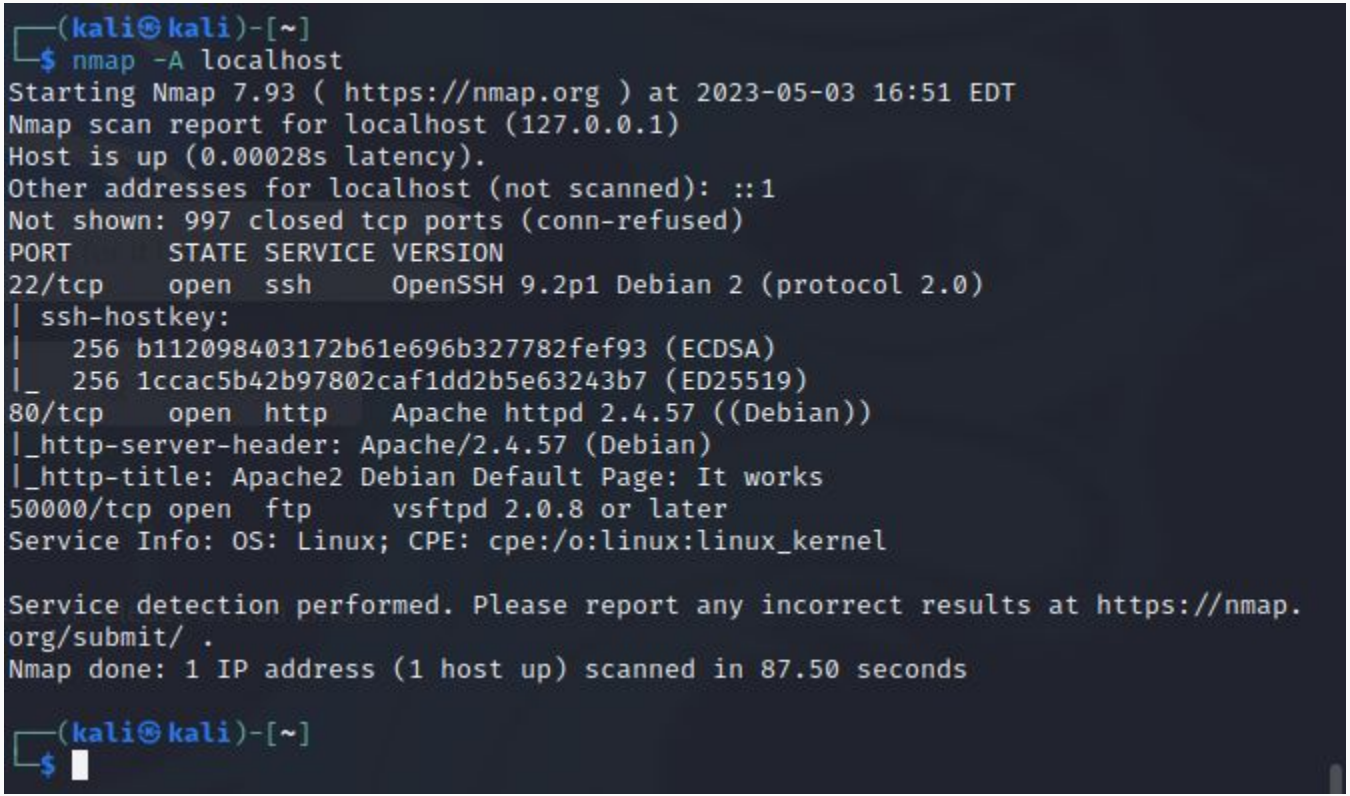
Il est possible de vérifier que ces services fonctionnent avec netstat.



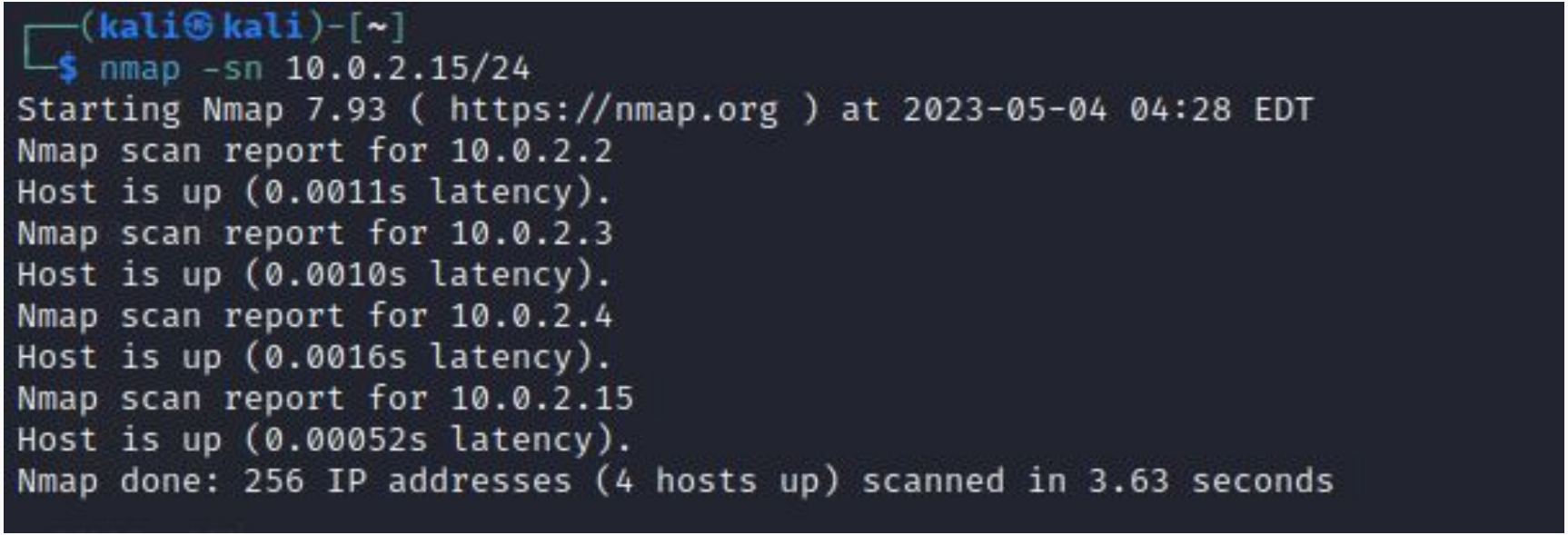
Logo de kali linux



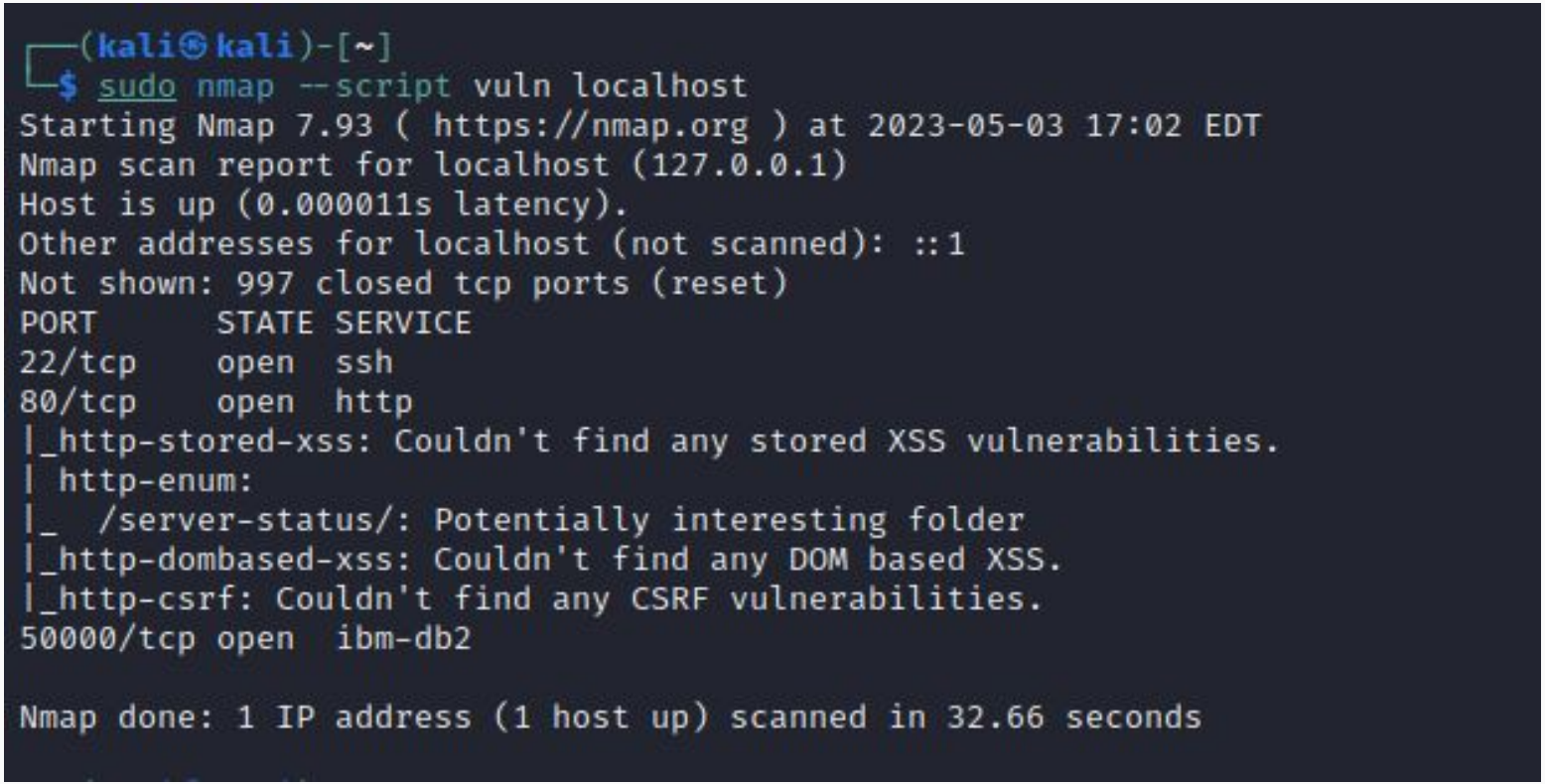
Analyse de port simple : **nmap localhost**



Scan avancé : **nmap -A localhost**



Analyse des hôtes sur le le localhost (eth0), avec 24 bit de prefixe de sous réseau : **nmap -sn IP_ETH0/24**


(kali㉿kali)-[~]
$ sudo nmap --script vuln localhost
Starting Nmap 7.93 (https://nmap.org) at 2023-05-03 17:02 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000011s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_ /server-status/: Potentially interesting folder
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
50000/tcp open ibm-db2
Nmap done: 1 IP address (1 host up) scanned in 32.66 seconds

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --traceroute -T4 -A -v localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 04:30 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:30
Completed NSE at 04:30, 0.00s elapsed
Initiating NSE at 04:30
Completed NSE at 04:30, 0.00s elapsed
Initiating NSE at 04:30
Completed NSE at 04:30, 0.00s elapsed
Initiating SYN Stealth Scan at 04:30
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 50000/tcp on 127.0.0.1
Completed SYN Stealth Scan at 04:30, 0.09s elapsed (1000 total ports)
Initiating Service scan at 04:30
Scanning 3 services on localhost (127.0.0.1)
Completed Service scan at 04:31, 56.14s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against localhost (127.0.0.1)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 04:31
Completed NSE at 04:32, 30.15s elapsed
Initiating NSE at 04:32
Completed NSE at 04:32, 0.07s elapsed
Initiating NSE at 04:32
Completed NSE at 04:32, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
|   256 b112098403172b61e696b327782fef93 (ECDSA)
|_  256 1ccac5b42b97802caf1dd2b5e63243b7 (ED25519)
```

Figure 1/2

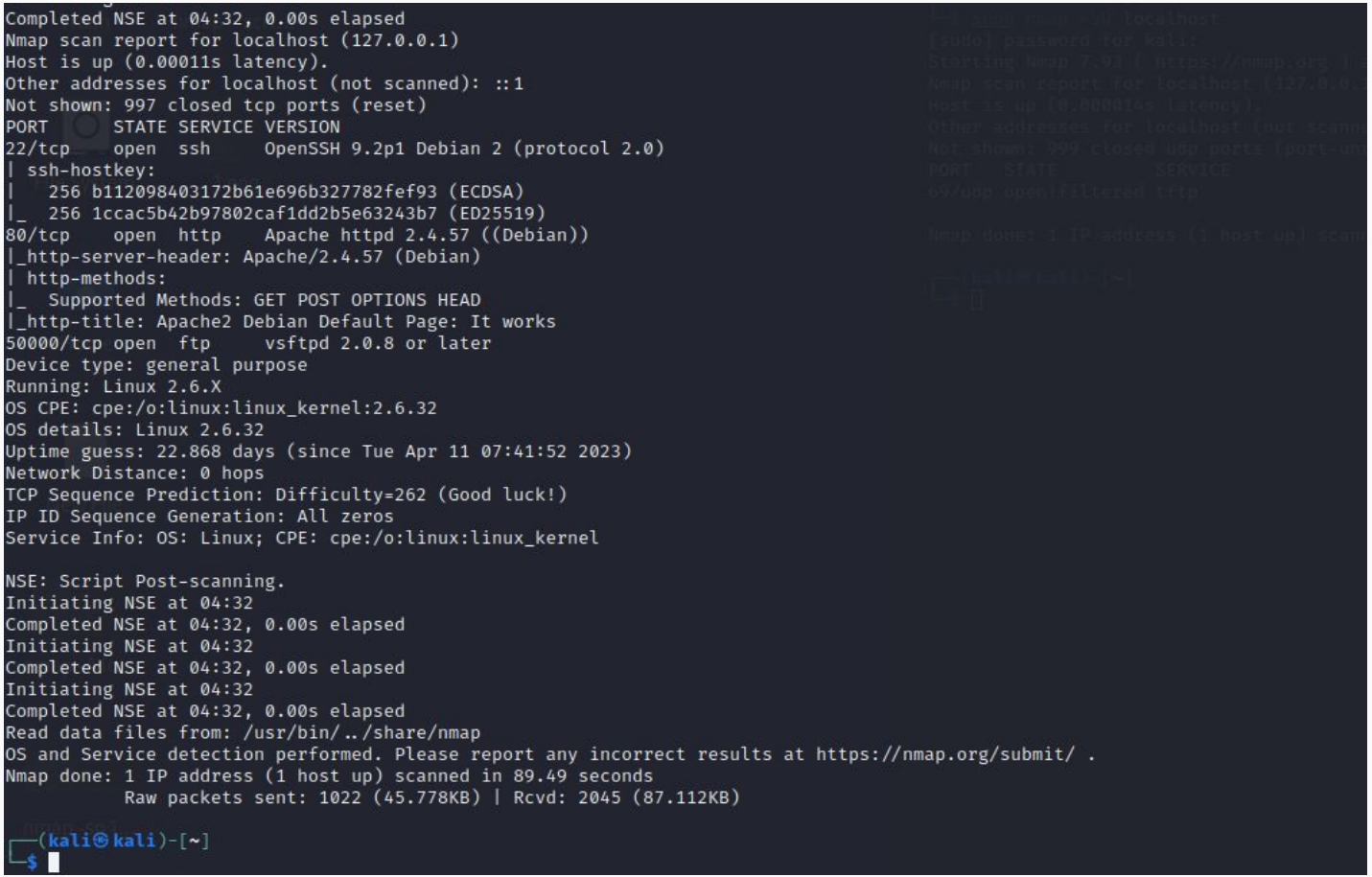
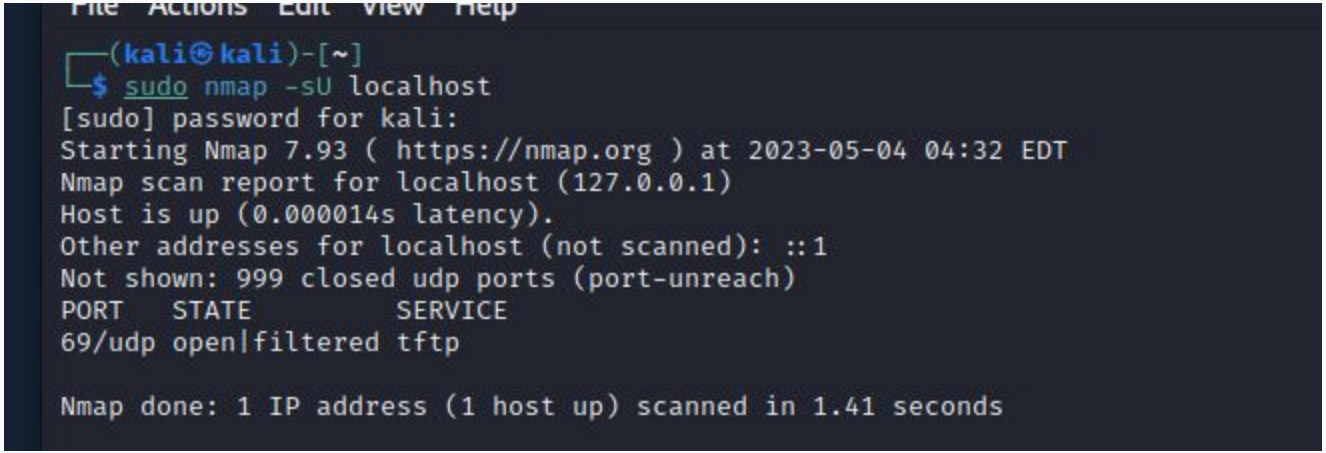
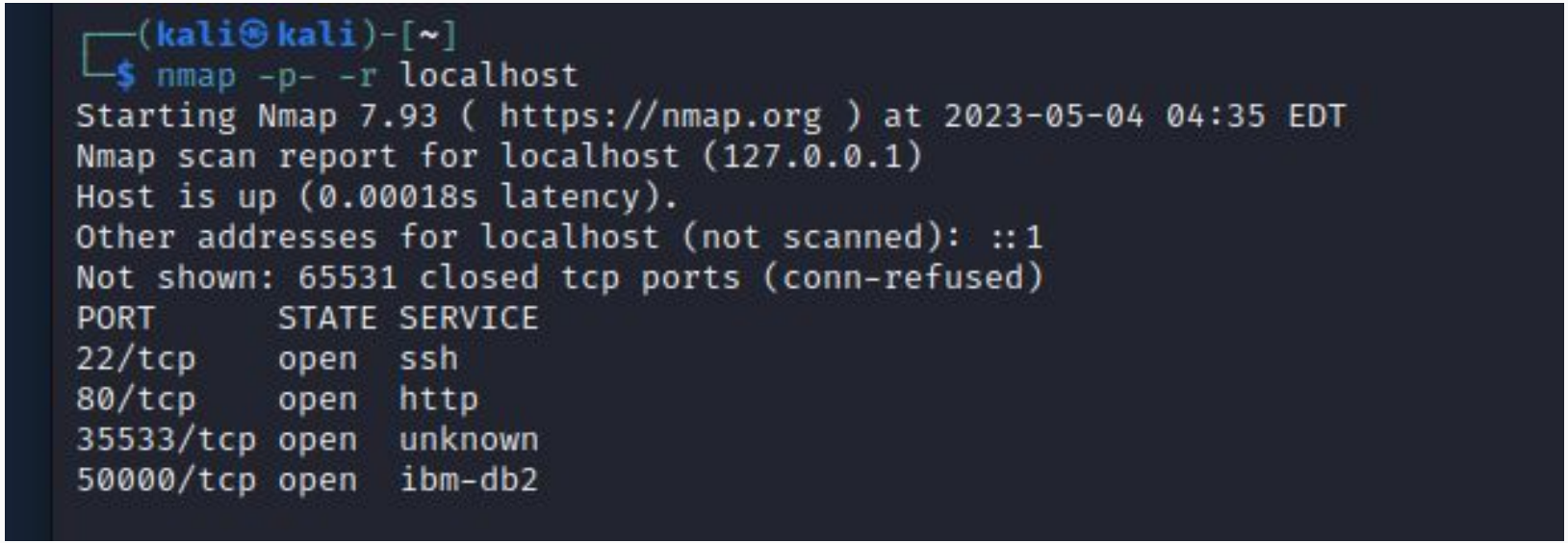

Completed NSE at 04:32, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
| 256 b112098403172b61e696b327782fef93 (ECDSA)
|_ 256 1ccac5b42b97802caf1dd2b5e63243b7 (ED25519)
80/tcp open http Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
| http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_http-title: Apache2 Debian Default Page: It works
50000/tcp open ftp vsftpd 2.0.8 or later
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Uptime guess: 22.868 days (since Tue Apr 11 07:41:52 2023)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
NSE: Script Post-scanning.
Initiating NSE at 04:32
Completed NSE at 04:32, 0.00s elapsed
Initiating NSE at 04:32
Completed NSE at 04:32, 0.00s elapsed
Initiating NSE at 04:32
Completed NSE at 04:32, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 89.49 seconds
Raw packets sent: 1022 (45.778KB) | Rcvd: 2045 (87.112KB)
(kali㉿kali)-[~]
$

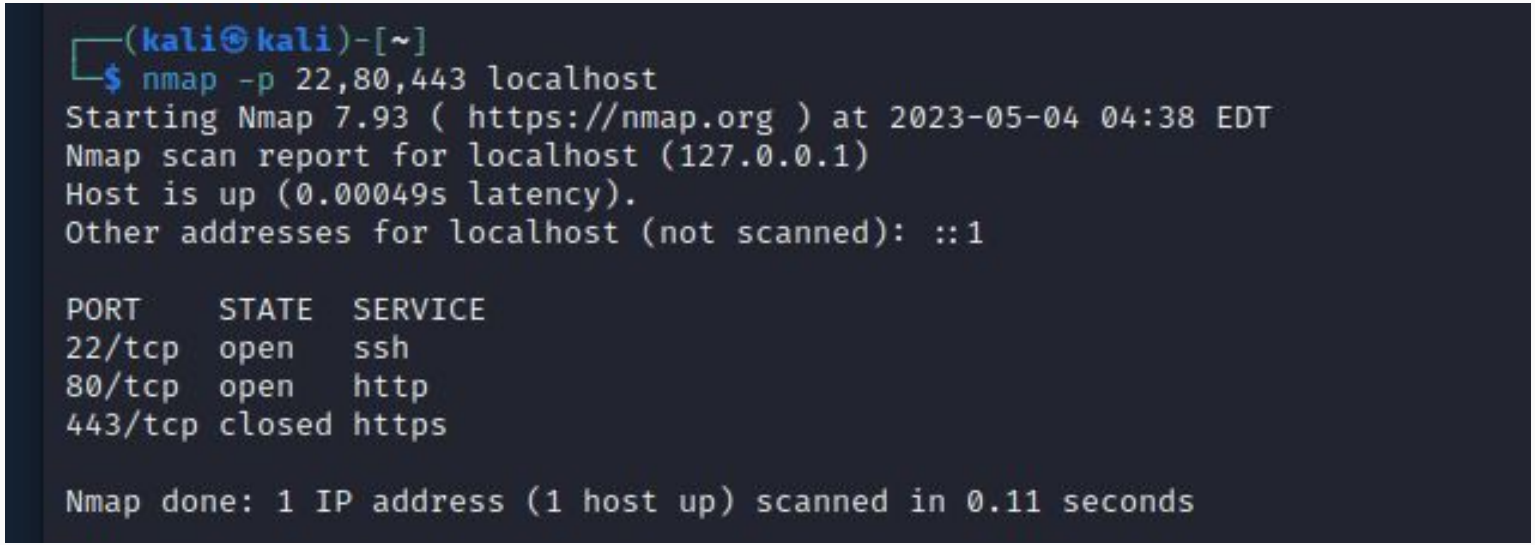
Figure 2/2



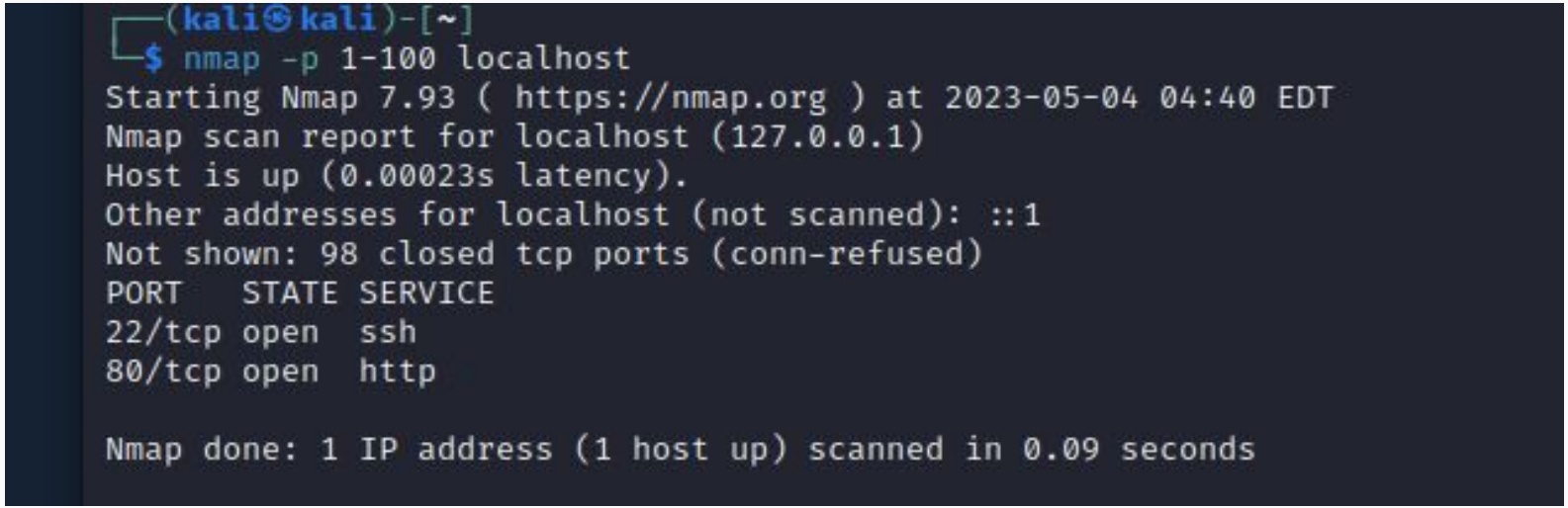
Scan UDP : **nmap -sU localhost**



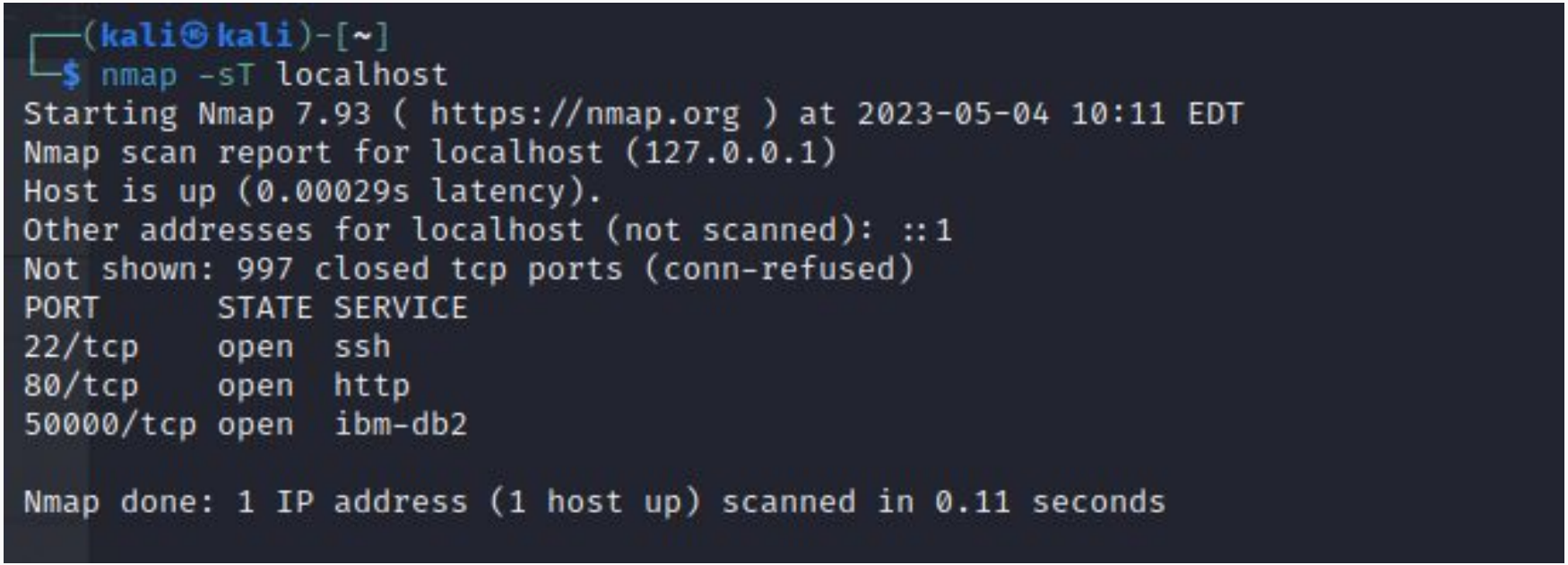
Scan de port aléatoire : **nmap -p- -r localhost**



Scan de port ciblé ssh, http et https : **nmap -p 22,80,443 localhost**



Scan rapide sur les 100 premiers ports : **nmap -p 1-100 localhost**

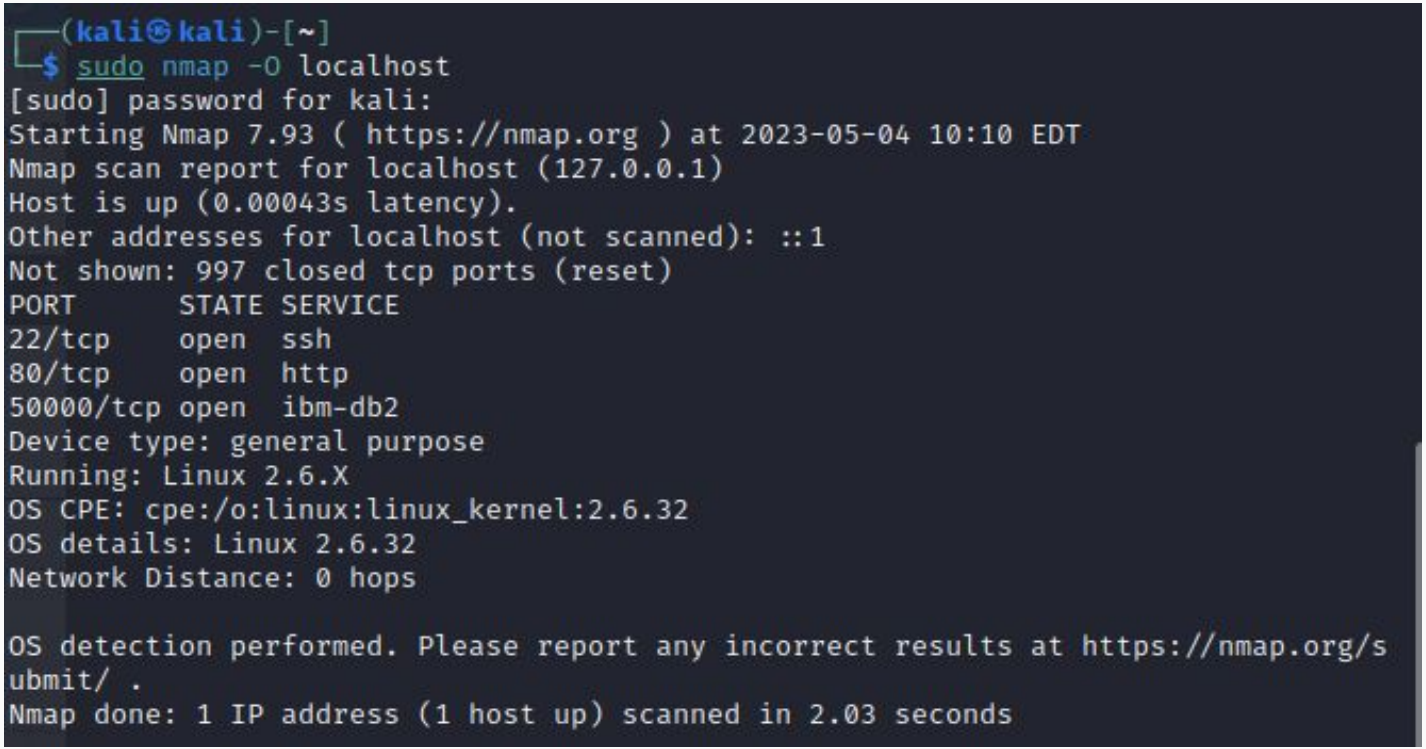


Scan connect() complet : **nmap -sT localhost**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -T4 -PN localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 10:12 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000011s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
50000/tcp open  ibm-db2

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Scan stealth (scanning discret qui minimise le trafic réseau) : **nmap -sS -T4 -PN localhost**



Scan de fingerprinting : **nmap -O localhost**