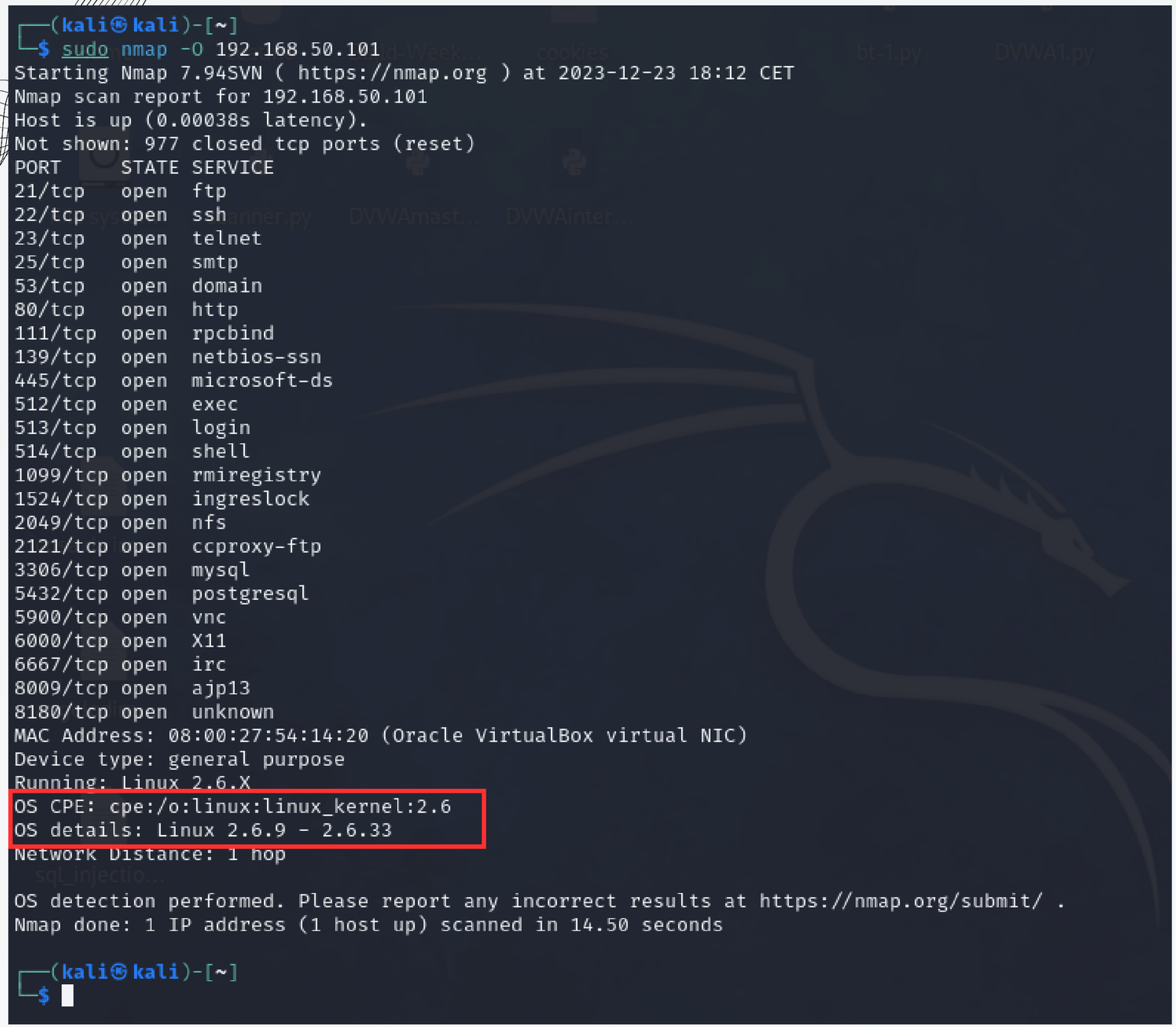
NMAP

KALI A META

OS FINGERPRINT

è una scansione per provare a identificare il sistema operativo di un dispositivo sulla rete.
Analizzando le risposte a pacchetti di prova, questa tecnica determina il tipo e la versione dell'OS



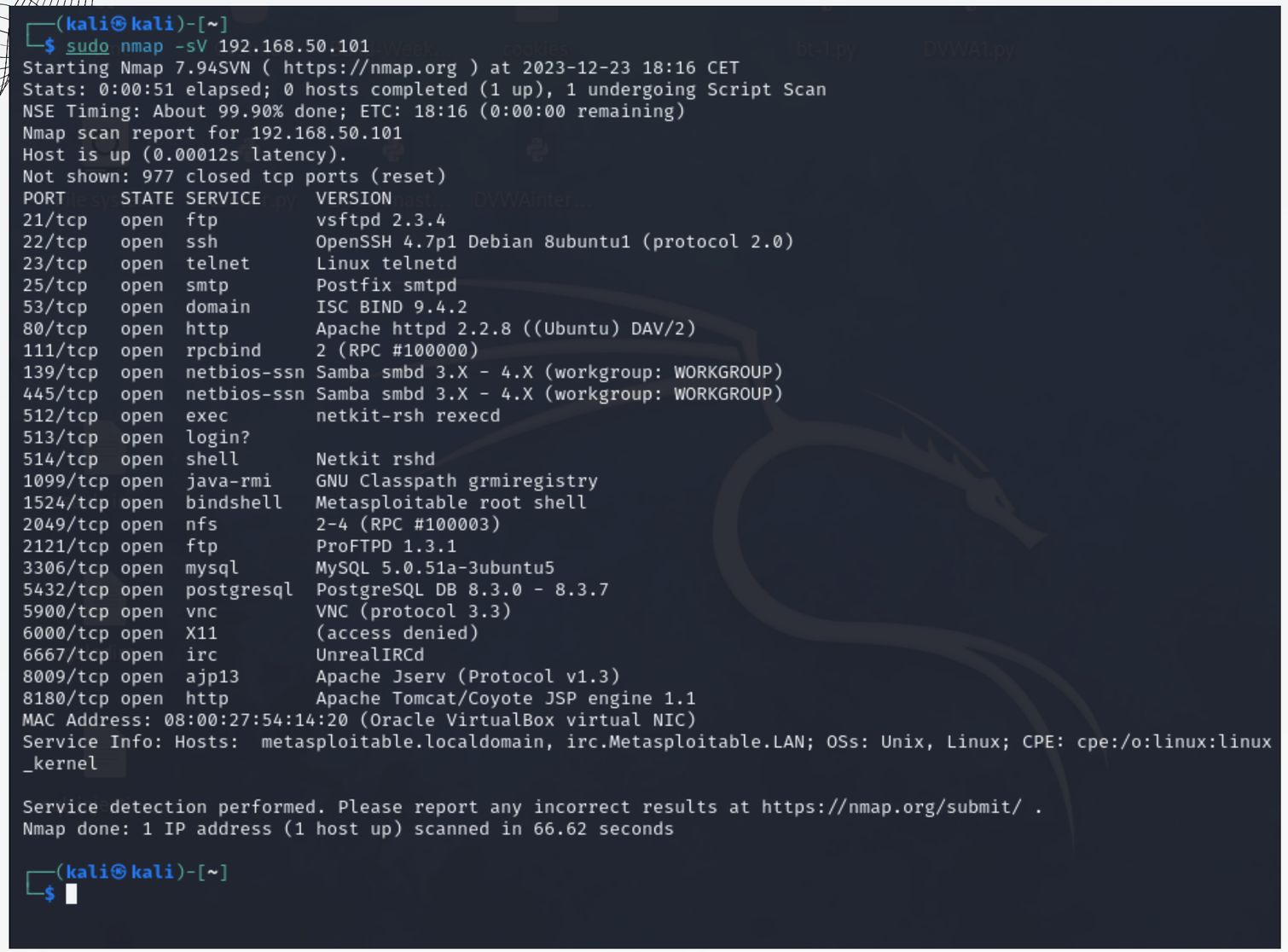
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-23 18:14 CET
Nmap scan report for 192.168.50.101
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:54:14:20 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

┌──(kali㉿kali)-[~]
└─$
```

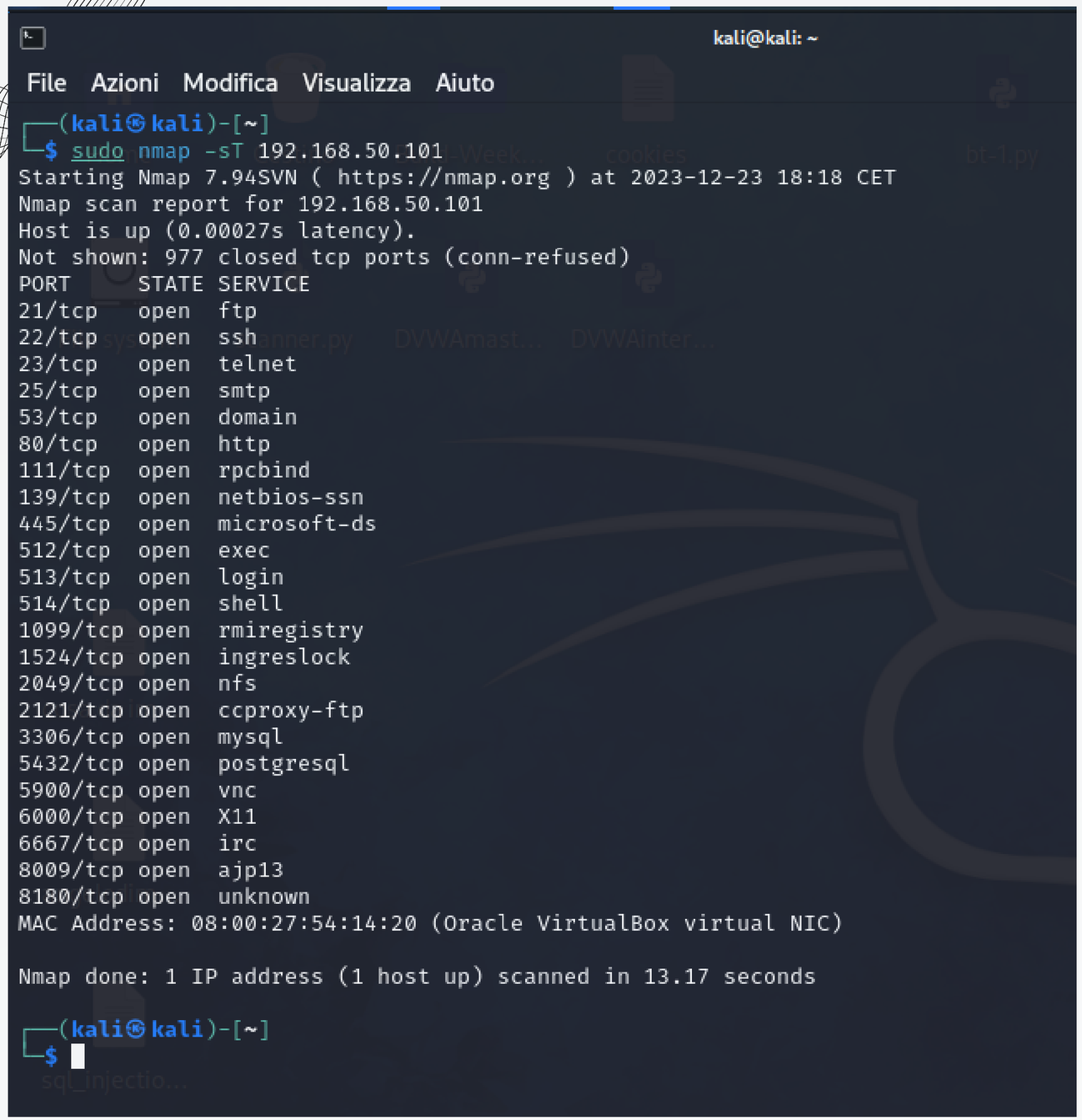
SYN SCAN

La scansione Syn, è un modo discreto di esaminare i porti di un computer per vedere quali sono aperti. Invece di stabilire una connessione completa, invia solo un messaggio di inizio,



VERSION SCAN

La scansione con l'opzione -sV è un processo di identificazione delle versioni software e dei servizi in esecuzione su un server o dispositivo



SCANSIONE TCP

La scansione con l'opzione -sT è una tecnica di analisi dei porti che utilizza connessioni complete TCP

SCAN TCP

- Metodo: Utilizza una connessione completa TCP per verificare lo stato dei porti.
- Rilevabilità: Più invasiva e di solito più facilmente rilevabile rispetto alla scansione -sS.
- Uso: Utile quando la rilevabilità non è una preoccupazione e si desidera ottenere informazioni dettagliate sullo stato dei porti.

SCAN SYN

- Metodo: Utilizza solo il passo iniziale di una connessione TCP, noto come handshake SYN, per determinare lo stato dei porti.
- Rilevabilità: Meno invasiva e solitamente più discreta, poiché non completa mai le connessioni TCP.
- Uso: Adatta a situazioni in cui la rilevabilità è una preoccupazione e si vuole eseguire una scansione più silenziosa.

NMAP

KALI A WIN7