

## **W11D1 – Nicholas di Angelo -**

relazione sulle differenze di scansione con Nmap da Kali Linux all'indirizzo IP 192.168.1.100 a Metasploitable2 all'indirizzo IP 192.168.1.101 utilizzando i seguenti comandi:

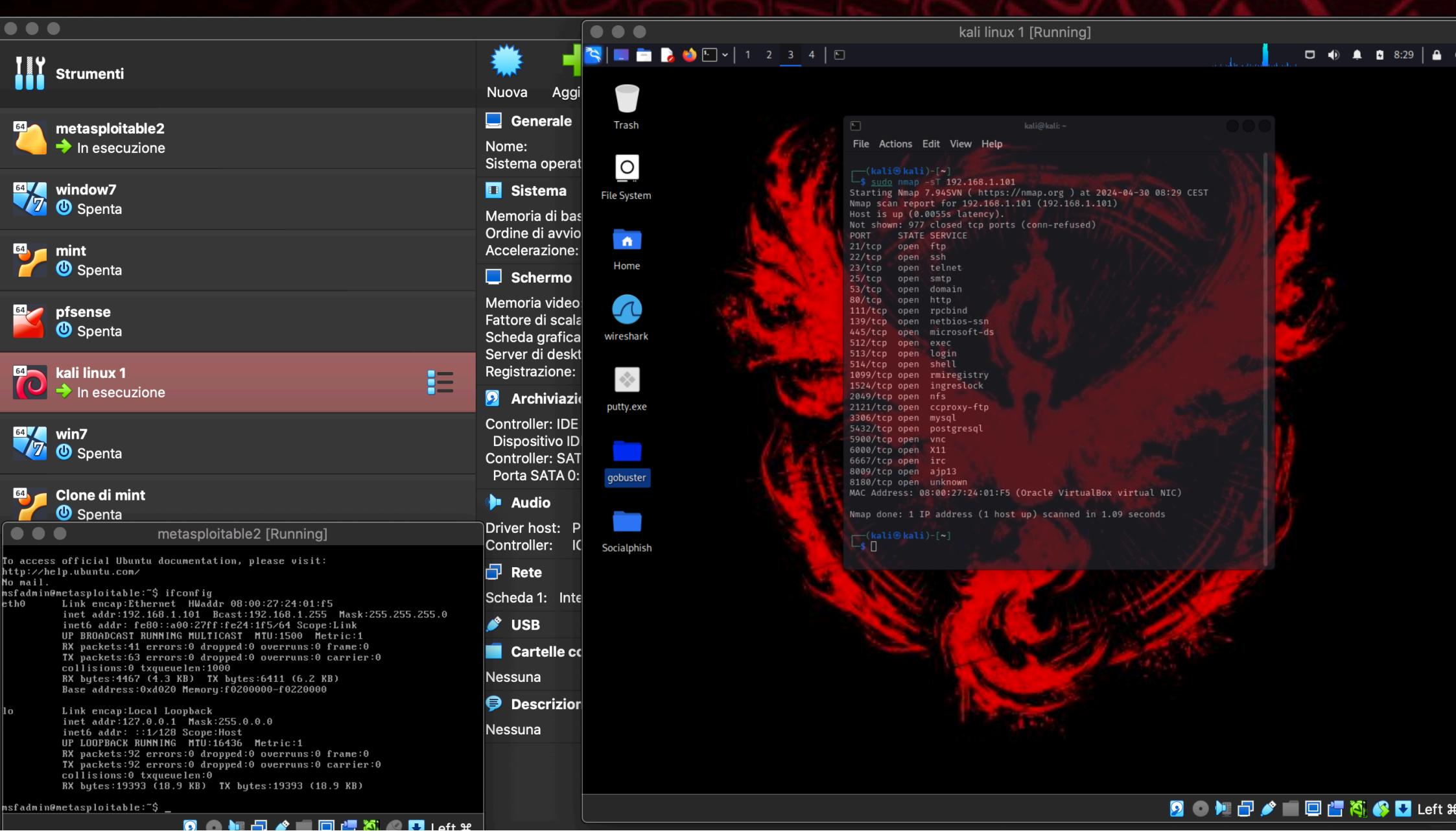
1. nmap -O: Questo comando esegue una scansione per determinare il sistema operativo del target. Esso invia pacchetti specializzati e analizza le risposte per identificare il sistema operativo in esecuzione sul target.
2. nmap -sS: Questo comando esegue una scansione stealth SYN. Utilizza pacchetti SYN per eseguire una scansione delle porte sul target. Questo metodo di scansione è stealth perché non completa la connessione TCP, ma invia solo il pacchetto SYN e analizza le risposte per determinare lo stato delle porte.
3. nmap -sT: Questo comando esegue una scansione di tipo TCP Connect. Si connette effettivamente alle porte del target per verificare se sono aperte o chiuse. Questo metodo di scansione è meno stealth rispetto alla scansione SYN, poiché completa la connessione TCP.
4. nmap -sV: Questo comando esegue una scansione per determinare le versioni dei servizi in esecuzione sulle porte aperte del target. Analizza le risposte ai pacchetti inviati per identificare le versioni dei servizi e le applicazioni in esecuzione.
5. nmap -oN report1: Questo comando esegue una scansione e salva i risultati in un file di output nel formato specificato, in questo caso "report1". I risultati possono essere successivamente analizzati e utilizzati per riferimento futuro.

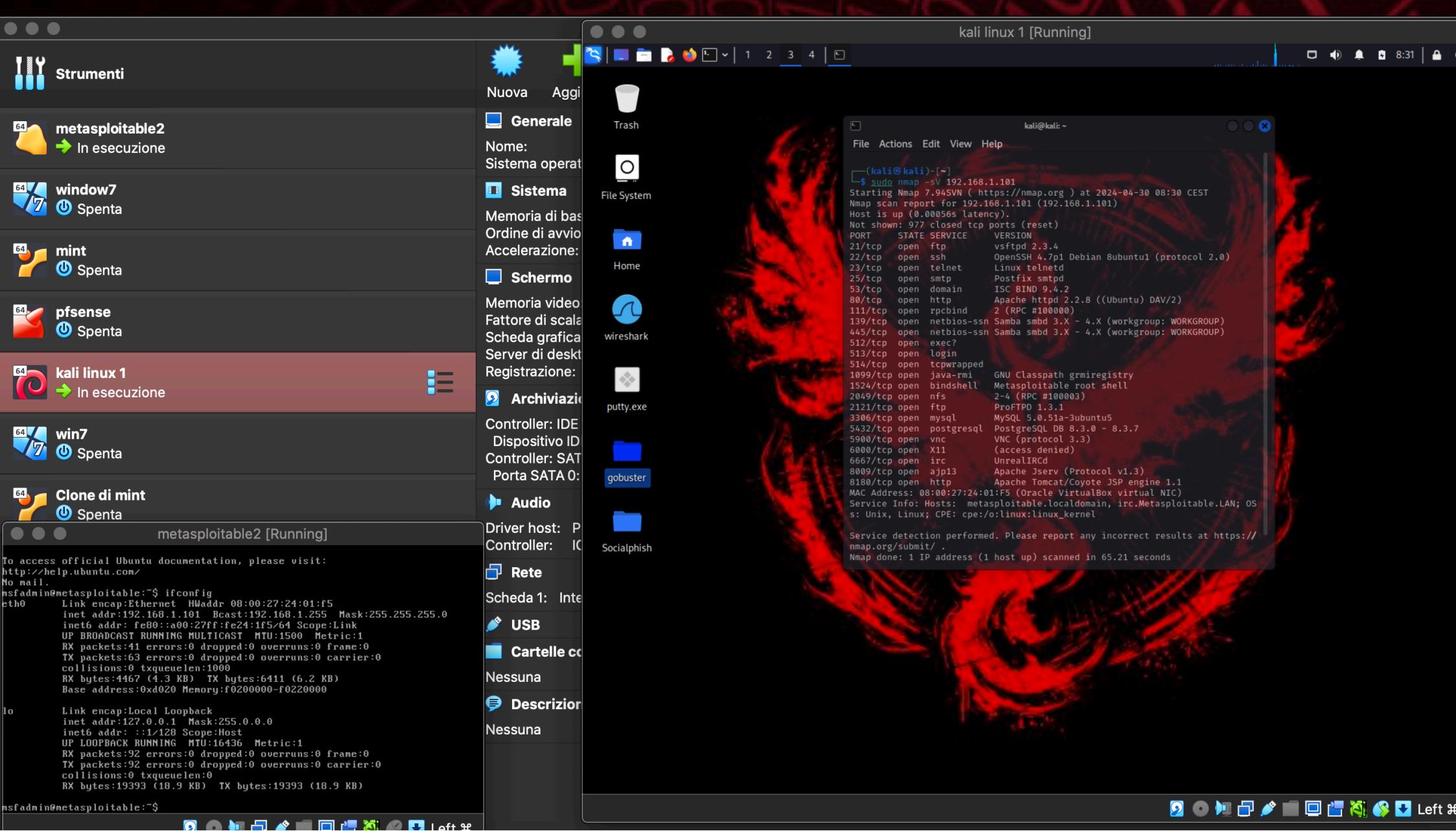
In sintesi, le differenze principali tra questi comandi risiedono nel tipo di scansione eseguita (OS detection, SYN scan, TCP connect scan, service version detection) e nel formato di output dei risultati. La scelta del comando dipende dalle esigenze specifiche di scansione e di analisi dei risultati.

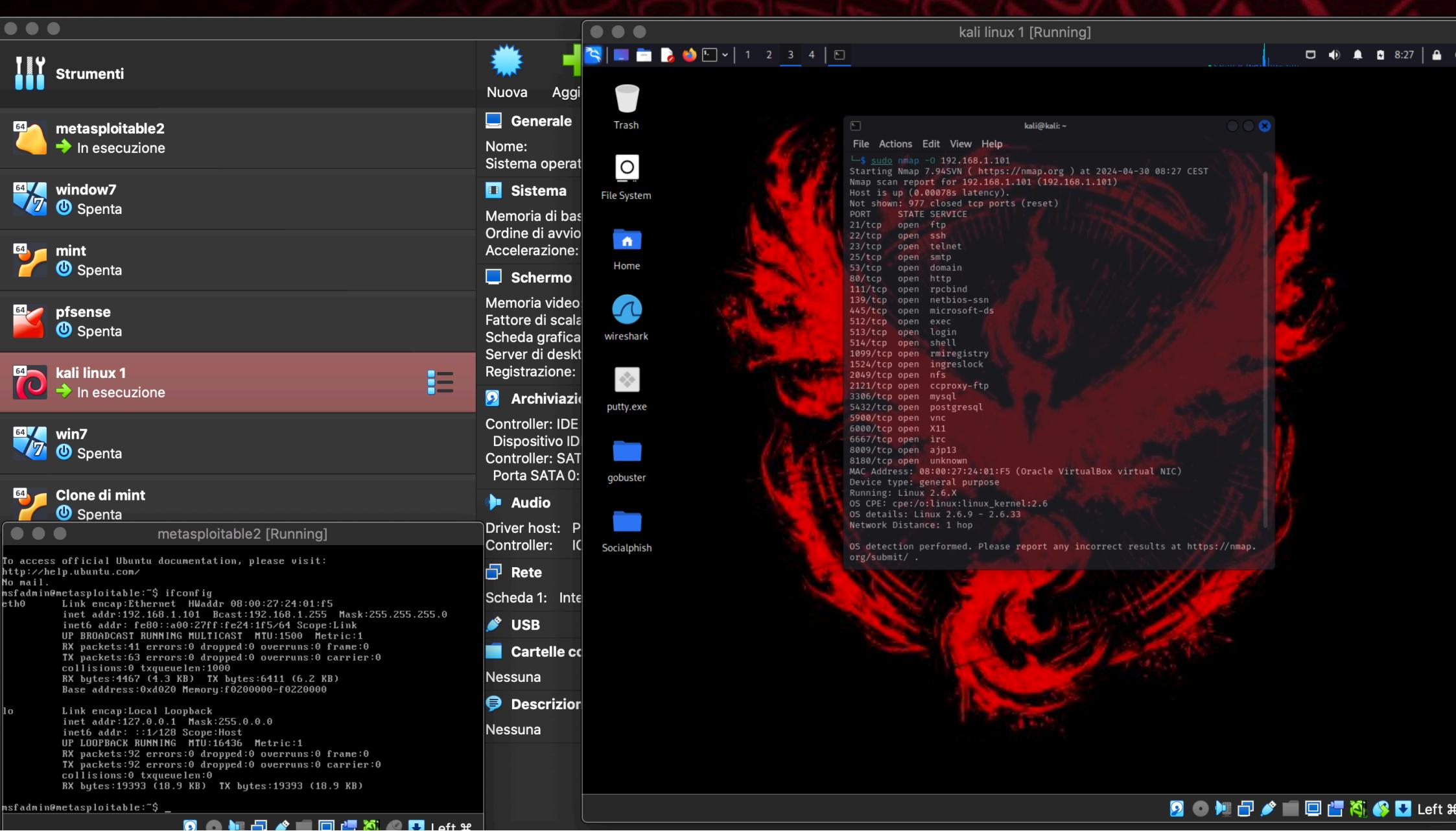
Le differenze principali tra la scansione TCP SYN e la scansione TCP connect risiedono nel modo in cui vengono stabiliti i contatti con le porte del target e nel livello di furtività della scansione.

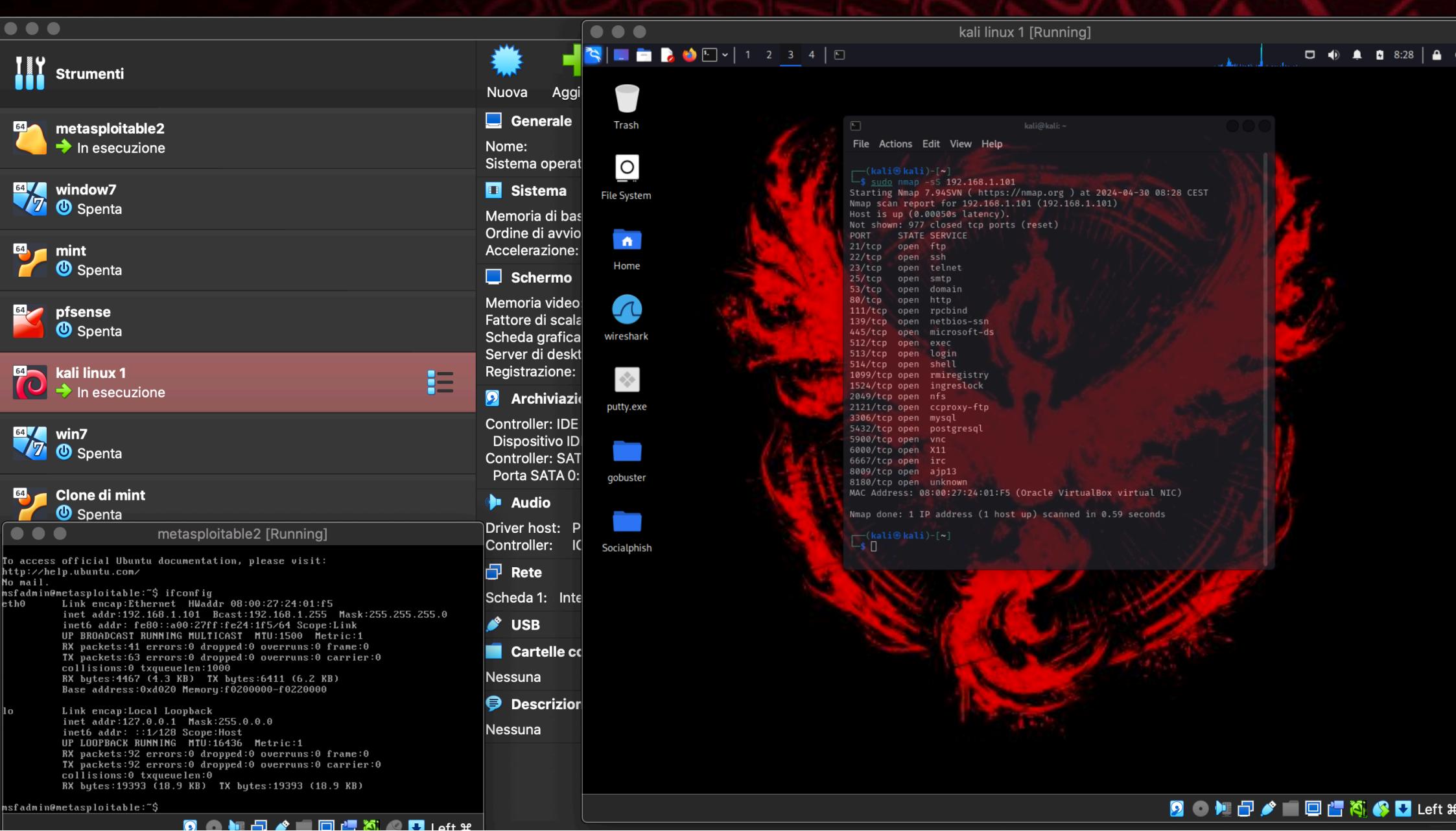
1. **Scansione TCP SYN (sS o -sS):**
  - Questo tipo di scansione invia pacchetti SYN al target per verificare lo stato delle porte.
  - Se una porta risponde con un pacchetto SYN/ACK, significa che la porta è aperta.
  - Se una porta risponde con un pacchetto RST, significa che la porta è chiusa.
  - Questa scansione non completa mai la connessione TCP, il che la rende stealth e meno probabile che venga rilevata dai sistemi di sicurezza.
  - È utile per identificare le porte aperte sul target in modo discreto.
2. **Scansione TCP connect (sT o -sT):**
  - Questo tipo di scansione si comporta come una connessione TCP normale.
  - Il comando tenta di stabilire una connessione TCP completa con le porte del target.
  - Se la connessione viene stabilita, significa che la porta è aperta.
  - Se la connessione viene respinta (ad esempio, con un pacchetto RST), significa che la porta è chiusa.
  - Questo metodo di scansione è meno stealth rispetto alla scansione SYN, poiché completa la connessione TCP e può essere più facilmente rilevato dai sistemi di sicurezza.
  - Tuttavia, può fornire risultati più accurati in quanto stabilisce effettivamente se una porta è aperta o chiusa.

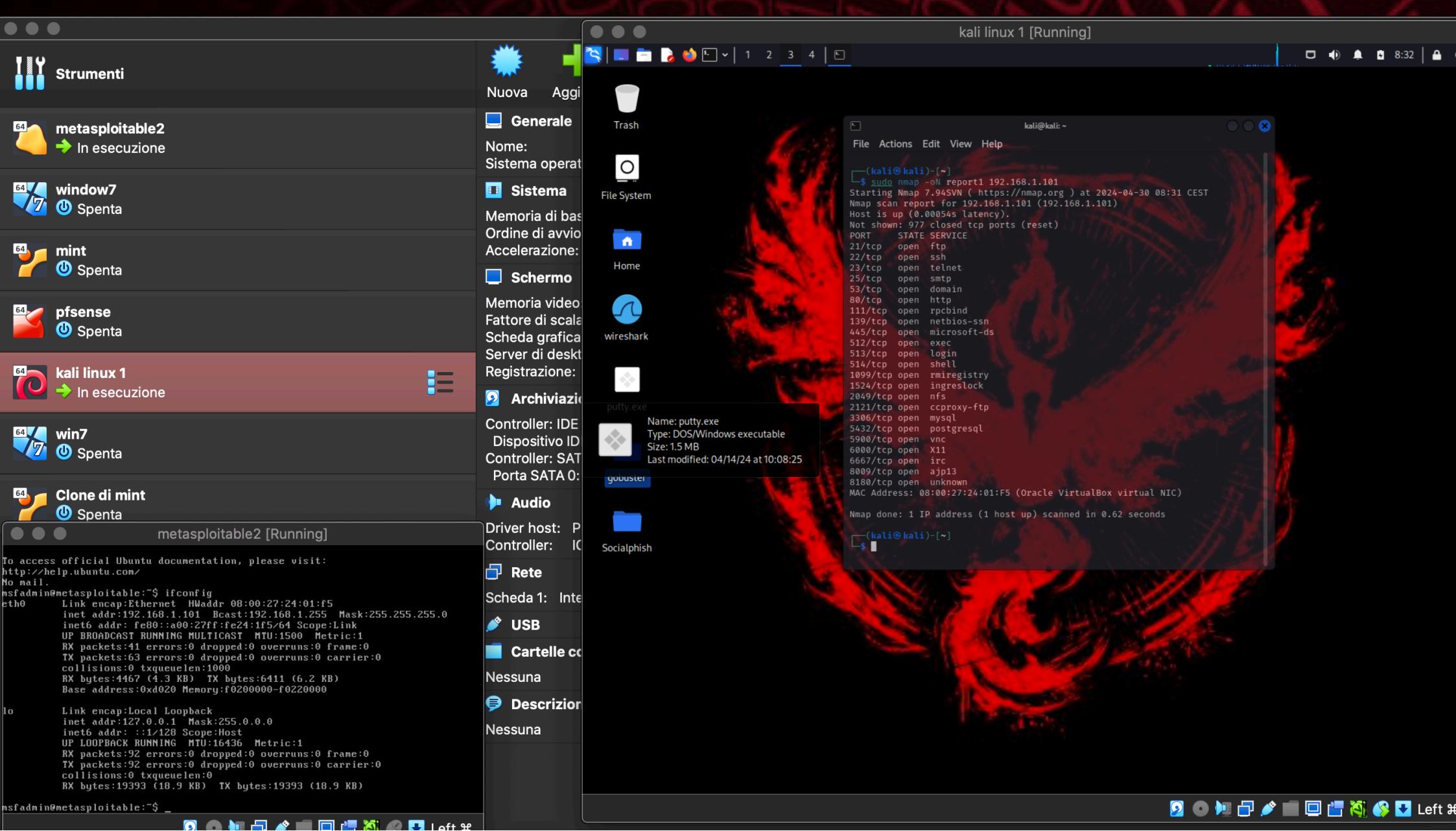
In breve, la scansione TCP SYN è più stealth e meno intrusiva perché non completa la connessione TCP, mentre la scansione TCP connect è più simile a una connessione TCP normale e può essere più facilmente rilevata. La scelta tra i due metodi dipende dalle esigenze specifiche di scansione e dal livello di stealth richiesto.



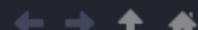




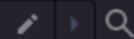




File Edit View Go Bookmarks Help



kali



### Places

Computer

kali

Desktop

Recent

Trash

Documents

Music

Pictures

Videos

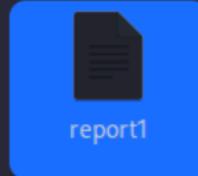
Downloads

### Devices

File System

### Network

Browse the file system go1.14.1.linux-  
31.6 GiB used (55%) | 26.2 GiB free (45%)



"report1" | 900 bytes | plain text document

Socialphish



armitage-tmp

Desktop

Documents

Downloads



evilginx2

loic

Music

Pictures



Public

Shellter\_Backups

Templates

Videos

```
Shell No. 1
File Actions Edit View Help
File Edit Options Buffers Tools Help
# Nmap 7.94SVN scan initiated Tue Apr 30 08:31:52 2024 as: nmap -oN report1\
192.168.1.101
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00054s 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: 08:00:27:24:01:F5 (Oracle VirtualBox virtual NIC)

# Nmap done at Tue Apr 30 08:31:53 2024 -- 1 IP address (1 host up) scanned\
in 0.62 seconds

-UU-:%%- F1 report1 All L1 (Fundamental) -
Note: file is write protected
```