Traccia 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. Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

Nmap con -sn e -PE ci permette di capire se il target è up o down.

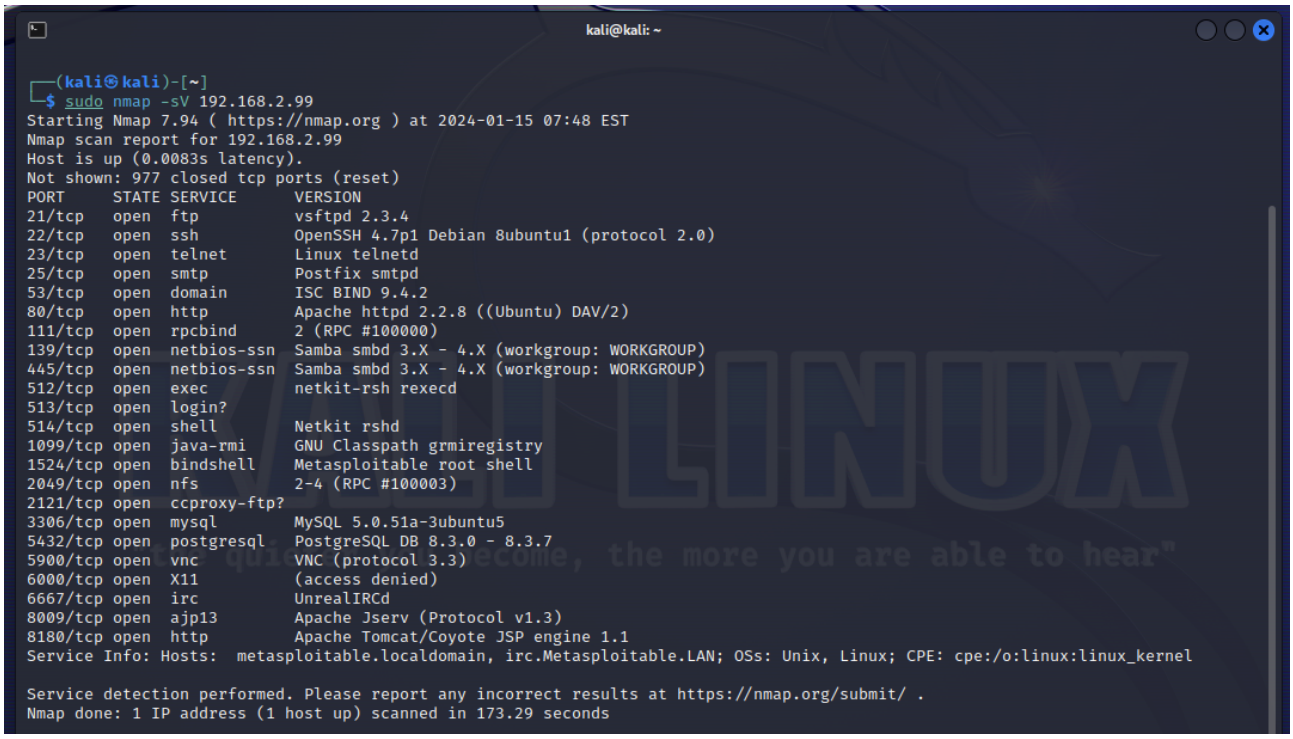
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.2.99
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 07:37 EST
Nmap scan report for 192.168.2.99
Host is up (0.0052s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Netdiscover con il -r target ci offre una cattura dei pacchetti

```
kali@kali: ~
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.2.1     08:00:27:92:fd:69      1      60  PCS Systemtechnik GmbH
192.168.2.99    08:00:27:9c:24:72      2     120  PCS Systemtechnik GmbH
```

Nmap con opzione -sV globale di porte e servizi aperti su un target con anche la descrizione della versione



Con l'utilizzo di unicorn scan sono state identificate porte alte aperte in TCP come la 34844 e la 48655