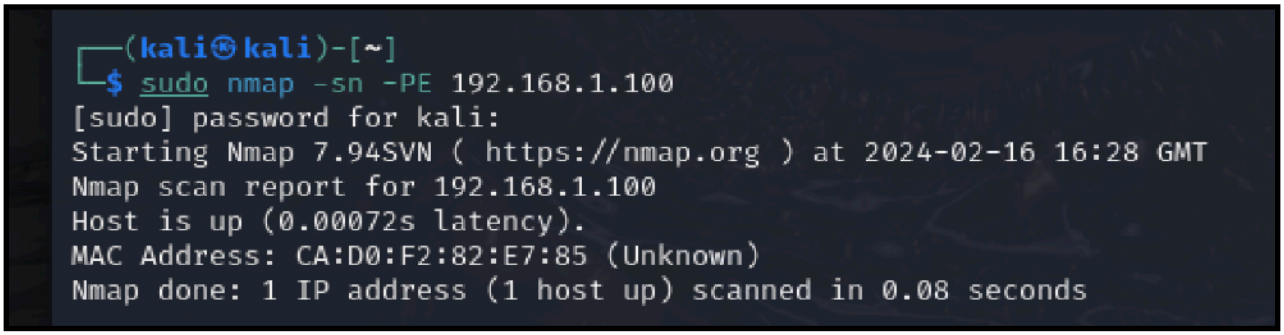
M3_W10D4

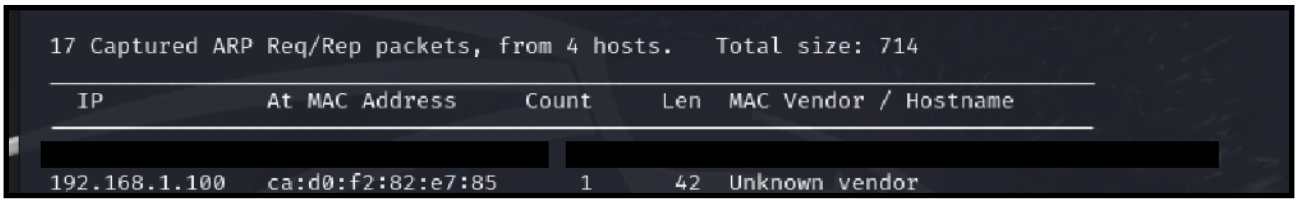
Utilizzo di alcuni strumenti per raccogliere informazioni sul target Metasploitable e produrre un report.

sudo nmap -sn -PE 192.168.1.100



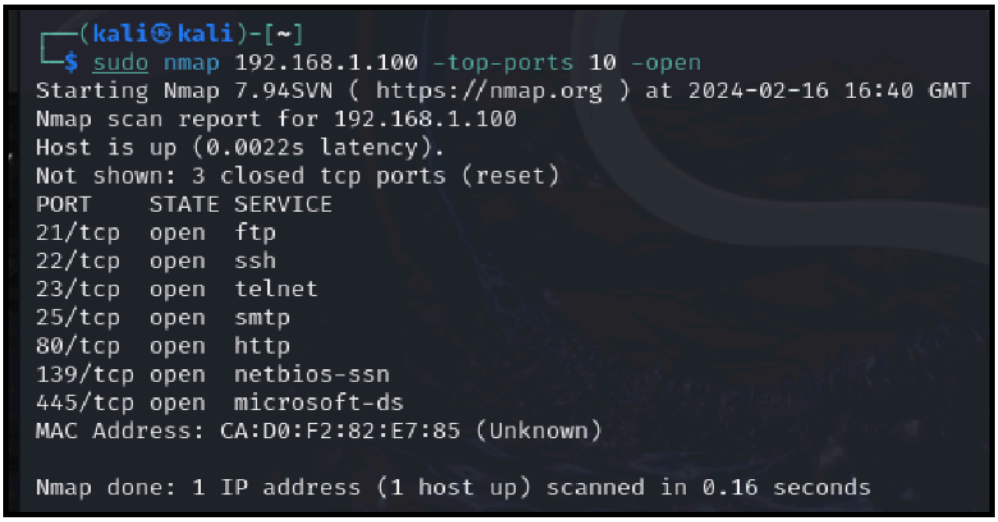
Con questo comando verifichiamo la presenza attiva di un host nell'indirizzo IP specificato, in questo caso quello di Metasploitable. Per la verifica Kali invierà un pacchetto ICMP.

sudo netdiscover -r 192.168.1.100



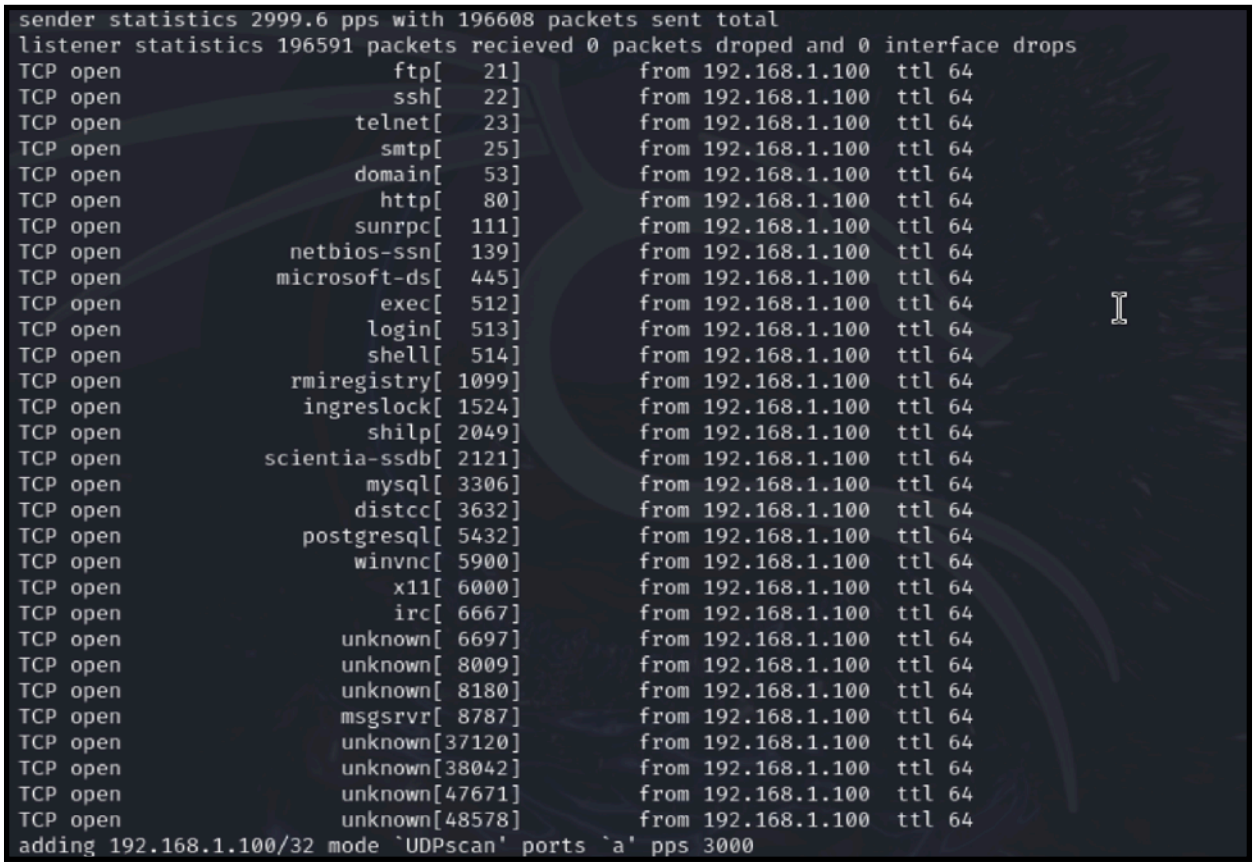
Netdiscover è uno strumento utile per trovare host su reti wireless o commutate. Può essere utilizzato sia in modalità attiva che passiva.

sudo nmap 192.168.1.100



Nmap per mezzo di questa sintassi scannerizzerà le 10 porte più comuni.

sudo us -mT -lv 192.168.1.100:a -r 3000 -R 3 && us -mU -lv 192.168.1.100:a -r 3000 -R 3



Unicornscan è predefinito per una scansione TCP/UDP. Il comando in questo caso farà una scansione del nostro IP (192.168.1.100), cercando tutte le porte e inviando 3000 pacchetti al secondo intervallando le due scansioni con un timeout di 3 secondi.

sudo nmap -sS -sV -T4 192.168.1.100

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -T4 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 17:06 GMT
Nmap scan report for 192.168.1.100
Host is up (0.00065s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: CA:D0:F2:82:E7:85 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
 cpe:/o:linux:linux_kernel
```

Nmap con questo comando effettua uno scan stealth dei servizi di Metasploitable indicando la loro versione attuale.

nc -nvz 192.168.1.100 1-1024

```
┌──(kali㉿kali)-[~]
└─$ nc -nvz 192.168.1.100 1-1024
(UNKNOWN) [192.168.1.100] 514 (shell) open
(UNKNOWN) [192.168.1.100] 513 (login) open
(UNKNOWN) [192.168.1.100] 512 (exec) open
(UNKNOWN) [192.168.1.100] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.100] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.100] 111 (sunrpc) open
(UNKNOWN) [192.168.1.100] 80 (http) open
(UNKNOWN) [192.168.1.100] 53 (domain) open
(UNKNOWN) [192.168.1.100] 25 (smtp) open
(UNKNOWN) [192.168.1.100] 23 (telnet) open
(UNKNOWN) [192.168.1.100] 22 (ssh) open
(UNKNOWN) [192.168.1.100] 21 (ftp) open
```

Netcat effettuerà una scansione delle porte aperte nell'intervallo 1-1024

nc -nv 192.168.1.100 22

```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.1.100 22
(UNKNOWN) [192.168.1.100] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Netcat con questo comando effettua una scansione completa della porta 22 (ssh) andando a rilevare la versione del sistema target.

sudo nmap -sV 192.168.1.100

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 17:18 GMT
Nmap scan report for 192.168.1.100
Host is up (0.00064s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: CA:D0:F2:82:E7:85 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
 cpe:/o:linux:linux_kernel
```

Nmap scansione le porte attive e ne definisce le versioni.

Report

REPORT			
SCAN SOURCE	**SCAN TARGET**	**SCAN TYPE**	**RESULTS**
KALI LINUX	METASPLOITABLE (192.168.1.100)	Tool: Nmap / Command: sudo nmap -sn -PE 192.168.1.100	1 host attivo / MAC Address: CA:D0:F2:82:E7:85
KALI LINUX	METASPLOITABLE (192.168.1.100)	Tool: Netdiscover / Command: sudo netdiscover -r 192.168.1.100	1 Indirizzo IP attivo in rete / MAC Address: CA:D0:F2:82:E7:85
KALI LINUX	METASPLOITABLE (192.168.1.100)	Tool: Nmap / Command: sudo nmap 192.168.1.100	Scansione TCP 10 porte comuni: 21/ftp , 22/ssh , 23/ telnet , 25/smtp , 80/http , 139/ netbios-ssn , 445/microsoft-ds
KALI LINUX	METASPLOITABLE (192.168.1.100)	Tool: Unicornsarn / Command: sudo us -mT -Iv 192.168.1.100:a -r 3000 -R 3 && us -mU -Iv 192.168.1.100:a -r 3000 -R 3	Scansione porte TCP/UDP
KALI LINUX	METASPLOITABLE (192.168.1.100)	Tool: Nmap / Command: sudo nmap -sS -sV -T4 192.168.1.100	Scansione porte TCP / Versione porte
KALI LINUX	METASPLOITABLE (192.168.1.100)	Tool: Netcat / Command: nc -nvz 192.168.1.100 1-1024	Scansione stealth porte attive nel range 1-1024
KALI LINUX	METASPLOITABLE (192.168.1.100)	Tool: Netcat / Command: nc -nv 192.168.1.100 22	Scansione completa porta 22/ ssh / Versione sistema target
KALI LINUX	METASPLOITABLE (192.168.1.100)	Tool: Nmap / Command: sudo nmap -sV 192.168.1.100	Scansione TCP porte attive / Versione porte