Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake Questo esercizio può essere utile per lo studente per prendere dimestichezza con i vari comandi di nmap. Poiché su Linux è un potente tool di scansione della rete, si richiede di utilizzare i seguenti comandi e trascrivere i vari risultati su un report.

Ambiente:
VM Kali linux 192.168.1.100 scheda di rete bridged;
target VM Metasploitable 192.168.1.101 scheda di rete bridged

ES:

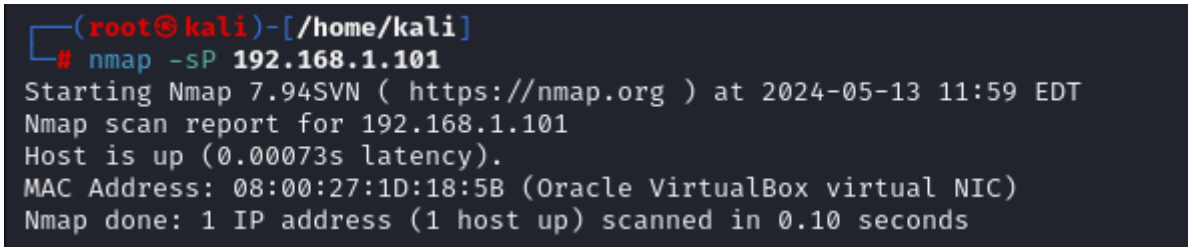
Svolgimento:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p 8080 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 11:20 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00057s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:1D:18:5B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 11:15 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00026s latency).
Not shown: 980 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
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
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
8180/tcp open  unknown
MAC Address: 08:00:27:1D:18:5B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 11:16 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00029s latency).
Not shown: 979 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
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  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
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: 08:00:27:1D:18:5B (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.64 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU -r -v 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 11:22 EDT
Initiating ARP Ping Scan at 11:22
Scanning 192.168.1.101 [1 port]
Completed ARP Ping Scan at 11:22, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:22
Completed Parallel DNS resolution of 1 host. at 11:22, 0.00s elapsed
Initiating UDP Scan at 11:22
Scanning 192.168.1.101 [1000 ports]
Discovered open port 111/udp on 192.168.1.101
Discovered open port 53/udp on 192.168.1.101
Increasing send delay for 192.168.1.101 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.1.101 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.1.101 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.1.101 from 200 to 400 due to max_successful_tryno increase to 7
Discovered open port 137/udp on 192.168.1.101
UDP Scan Timing: About 4.21% done; ETC: 11:34 (0:11:45 remaining)
Increasing send delay for 192.168.1.101 from 400 to 800 due to 11 out of 23 dropped probes since last increase.
UDP Scan Timing: About 7.00% done; ETC: 11:36 (0:13:44 remaining)
UDP Scan Timing: About 22.36% done; ETC: 11:38 (0:12:55 remaining)
UDP Scan Timing: About 28.63% done; ETC: 11:38 (0:12:03 remaining)
UDP Scan Timing: About 34.51% done; ETC: 11:39 (0:11:10 remaining)
UDP Scan Timing: About 40.18% done; ETC: 11:39 (0:10:16 remaining)
UDP Scan Timing: About 45.42% done; ETC: 11:39 (0:09:22 remaining)
UDP Scan Timing: About 50.80% done; ETC: 11:39 (0:08:30 remaining)
UDP Scan Timing: About 55.63% done; ETC: 11:39 (0:07:37 remaining)
UDP Scan Timing: About 61.27% done; ETC: 11:39 (0:06:43 remaining)
UDP Scan Timing: About 66.17% done; ETC: 11:39 (0:05:50 remaining)
UDP Scan Timing: About 69.02% done; ETC: 11:45 (0:07:21 remaining)
UDP Scan Timing: About 73.92% done; ETC: 11:45 (0:06:03 remaining)
UDP Scan Timing: About 78.67% done; ETC: 11:44 (0:04:53 remaining)
UDP Scan Timing: About 83.62% done; ETC: 11:44 (0:03:42 remaining)
UDP Scan Timing: About 88.68% done; ETC: 11:44 (0:02:32 remaining)
UDP Scan Timing: About 93.82% done; ETC: 11:44 (0:01:22 remaining)
Completed UDP Scan at 11:44, 1333.49s elapsed (1000 total ports)
Nmap scan report for 192.168.1.101
Host is up (0.00059s latency).
Not shown: 995 closed udp ports (port-unreach)
PORT    STATE         SERVICE
53/udp  open          domain
69/udp  open|filtered tftp
111/udp open          rpcbind
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
MAC Address: 08:00:27:1D:18:5B (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1333.72 seconds
           Raw packets sent: 1379 (66.021KB) | Rcvd: 1088 (79.385KB)
```



Risultati e Conclusioni:

- Le scansioni TCP e UDP hanno fornito una panoramica dettagliata delle porte aperte e dei servizi in esecuzione sull'host target.
- L'identificazione del sistema operativo ha permesso di determinare il tipo di sistema in esecuzione sull'host.
- La scansione della versione dei servizi ha fornito informazioni sulle versioni specifiche dei servizi in esecuzione.
- La scansione delle prime 100 porte comuni ha aiutato a identificare i servizi più rilevanti in esecuzione sull'host.
- La scansione tramite ARP ha fornito informazioni sulla presenza di altri dispositivi nella stessa rete.
- Le scansioni tramite PING sono state utili per identificare l'host attivo senza avviare una scansione completa.