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:

TCP: #	nmap -sS ip address
scansione completa: #	nmap -sV ip address
output su file: #	nmap -sV -oN file.txt ip address
scansione su porta: #	nmap -sS -p 8080 ip address
scansione tutte le porte: #	nmap -sS -p ip address
scansione UDP: #	nmap -sU -r -v ip address
scansione sistema operativo: #	nmap -O ip address
scansione versione servizi: #	nmap -sV ip address
scansione common 100 ports: #	nmap -F ip address
scansione tramite ARP: #	nmap -PR ip address
scansione tramite PING: #	nmap -sP ip address

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -sV -oN file.txt 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:06 CET
Nmap scan report for 192.168.50.101
Host is up (0.00038s 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  shell       Netkit rshd
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: 08:00:27:1F:AC:80 (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 25.34 seconds
```

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -FR 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:35 CET
Nmap scan report for 192.168.50.101
Host is up (0.00092s latency).
Not shown: 82 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
513/tcp  open  login
514/tcp  open  shell
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
8009/tcp open  ajp13
MAC Address: 08:00:27:1F:AC:80 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.36 seconds
```

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -sS -p 8080 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:08 CET
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:1F:AC:80 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -sP 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:37 CET
Nmap scan report for 192.168.50.101
Host is up (0.00059s latency).
MAC Address: 08:00:27:1F:AC:80 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
```

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -sS -P 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:10 CET
Nmap scan report for 192.168.50.101
Host is up (0.00032s 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: 08:00:27:1F:AC:80 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds
```

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -PN 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:37 CET
Nmap scan report for 192.168.50.101
Host is up (0.00031s 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: 08:00:27:1F:AC:80 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds
```

```
└─# nmap -sU -r -v 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:11 CET
Initiating ARP Ping Scan at 21:11
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 21:11, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:11
Completed Parallel DNS resolution of 1 host. at 21:11, 13.02s elapsed
Initiating UDP Scan at 21:11
Scanning 192.168.50.101 [1000 ports]
Discovered open port 111/udp on 192.168.50.101
Discovered open port 53/udp on 192.168.50.101
Increasing send delay for 192.168.50.101 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.50.101 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.50.101 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.50.101 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.50.101 from 400 to 800 due to 11 out of 12 dropped probes since last increase.
Discovered open port 137/udp on 192.168.50.101
UDP Scan Timing: About 3.64% done; ETC: 21:26 (0:13:40 remaining)
UDP Scan Timing: About 8.66% done; ETC: 21:27 (0:14:25 remaining)
Stats: 0:03:27 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 19.11% done; ETC: 21:28 (0:13:41 remaining)
Discovered open port 2049/udp on 192.168.50.101
UDP Scan Timing: About 25.07% done; ETC: 21:29 (0:12:48 remaining)
UDP Scan Timing: About 31.23% done; ETC: 21:29 (0:11:51 remaining)
UDP Scan Timing: About 37.21% done; ETC: 21:29 (0:10:56 remaining)
Stats: 0:07:32 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 41.92% done; ETC: 21:29 (0:10:08 remaining)
Stats: 0:07:35 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 42.23% done; ETC: 21:29 (0:10:06 remaining)
UDP Scan Timing: About 47.59% done; ETC: 21:29 (0:09:11 remaining)
UDP Scan Timing: About 52.83% done; ETC: 21:29 (0:08:17 remaining)
UDP Scan Timing: About 57.60% done; ETC: 21:29 (0:07:23 remaining)
UDP Scan Timing: About 63.03% done; ETC: 21:29 (0:06:26 remaining)
UDP Scan Timing: About 68.59% done; ETC: 21:29 (0:05:29 remaining)
UDP Scan Timing: About 73.73% done; ETC: 21:29 (0:04:36 remaining)
UDP Scan Timing: About 79.18% done; ETC: 21:29 (0:03:39 remaining)
UDP Scan Timing: About 84.42% done; ETC: 21:29 (0:02:44 remaining)
UDP Scan Timing: About 89.57% done; ETC: 21:29 (0:01:50 remaining)
UDP Scan Timing: About 94.80% done; ETC: 21:29 (0:00:55 remaining)
Completed UDP Scan at 21:30, 1091.56s elapsed (1000 total ports)
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).
Not shown: 994 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
2049/udp open          nfs
MAC Address: 08:00:27:1F:AC:80 (Oracle VirtualBox virtual NIC)
```

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:04 CET
Nmap scan report for 192.168.50.101
Host is up (0.00040s 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  shell       Netkit rshd
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: 08:00:27:1F:AC:80 (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 25.67 seconds
```

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -O 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:32 CET
Nmap scan report for 192.168.50.101
Host is up (0.0012s 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: 08:00:27:1F:AC:80 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.80 seconds
```

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:00 CET
Nmap scan report for 192.168.50.101
Host is up (0.00041s 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: 08:00:27:1F:AC:80 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.53 seconds
```

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:33 CET
Nmap scan report for 192.168.50.101
Host is up (0.00066s 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  shell       Netkit rshd
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: 08:00:27:1F:AC:80 (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 25.44 seconds
```

```
┌──(root㉿kali)-[/home/giovanni]
└─# nmap -F 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 21:35 CET
Nmap scan report for 192.168.50.101
Host is up (0.00072s latency).
Not shown: 82 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
513/tcp  open  login
514/tcp  open  shell
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
8009/tcp open  ajp13
MAC Address: 08:00:27:1F:AC:80 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```