Scansioni Nmap

```
┌──(kali_alex㉿kali)-[~]
└─$ sudo nmap -sT 192.168.1.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 19:25 CEST
Nmap scan report for 192.168.1.60
Host is up (0.00092s latency).
Not shown: 978 closed tcp ports (conn-refused)
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
8180/tcp open  unknown
MAC Address: 08:00:27:88:06:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.27 seconds

┌──(kali_alex㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 19:26 CEST
Nmap scan report for 192.168.1.60
Host is up (0.00013s 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  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: 08:00:27:88:06:6A (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 63.95 seconds

┌──(kali_alex㉿kali)-[~]

└─$ sudo nmap -sV -O 192.168.1.60

Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 19:28 CEST

Nmap scan report for 192.168.1.60

Host is up (0.00048s 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 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: 08:00:27:88:06:6A (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

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 65.21 seconds

┌──(kali_alex㉿kali)-[~]

└─$ sudo nmap -sV -oN meta.txt 192.168.1.60

Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 19:31 CEST

Nmap scan report for 192.168.1.60

Host is up (0.00017s 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 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: 08:00:27:88:06:6A (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 63.67 seconds

┌──(kali_alex㉿kali)-[~]

└─$ ls

a.out Ddosattack.py meta.txt Port-scanner.py report1 Scaricati studenti

backdoor.py documenti Modelli programmazione report2 Scrivania Video

client.py Immagini Nessus-10.5.1-debian10_amd64.deb Pubblici report3 Socket.py windows

┌──(kali_alex㉿kali)-[~]

└─$ nano meta.txt

┌──(kali_alex㉿kali)-[~]

└─$ sudo nmap -sS -p 8080 192.168.1.60

Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 19:35 CEST

Nmap scan report for 192.168.1.60

Host is up (0.00027s latency).

PORT STATE SERVICE

8080/tcp closed http-proxy

MAC Address: 08:00:27:88:06:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.21 seconds

┌──(kali_alex㉿kali)-[~]

└─$ sudo nmap -sS -p 80 192.168.1.60

Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 19:35 CEST

Nmap scan report for 192.168.1.60

Host is up (0.00030s latency).

PORT STATE SERVICE

80/tcp open http

MAC Address: 08:00:27:88:06:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.21 seconds

┌──(kali_alex㉿kali)-[~]

└─$ sudo nmap -sS -p 192.168.1.60

Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 19:36 CEST

Error #487: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"

QUITTING!

┌──(kali_alex㉿kali)-[~]

└─$ sudo nmap -sS -p1-65535 192.168.1.60

Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 19:37 CEST

Nmap scan report for 192.168.1.60

Host is up (0.00017s latency).

Not shown: 65505 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

3632/tcp open distccd

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

6697/tcp open ircs-u

8009/tcp open ajp13

8180/tcp open unknown

8787/tcp open msgsrvr

44891/tcp open unknown

54107/tcp open unknown

56260/tcp open unknown

60857/tcp open unknown

MAC Address: 08:00:27:88:06:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds

┌──(kali_alex㉿kali)-[~]

└─$ sudo nmap -sU -r -v 192.168.1.60

Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 19:38 CEST

Initiating ARP Ping Scan at 19:38

Scanning 192.168.1.60 [1 port]

Completed ARP Ping Scan at 19:38, 0.05s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 19:38

Completed Parallel DNS resolution of 1 host. at 19:38, 11.02s elapsed

Initiating UDP Scan at 19:38

Scanning 192.168.1.60 [1000 ports]

Discovered open port 53/udp on 192.168.1.60

Discovered open port 111/udp on 192.168.1.60

Increasing send delay for 192.168.1.60 from 0 to 50 due to max_successful_tryno increase to 4

Discovered open port 137/udp on 192.168.1.60

Increasing send delay for 192.168.1.60 from 50 to 100 due to 11 out of 12 dropped probes since last increase.

Increasing send delay for 192.168.1.60 from 100 to 200 due to 11 out of 12 dropped probes since last increase.

UDP Scan Timing: About 9.45% done; ETC: 19:44 (0:04:57 remaining)

Increasing send delay for 192.168.1.60 from 200 to 400 due to 11 out of 11 dropped probes since last increase.

Increasing send delay for 192.168.1.60 from 400 to 800 due to 11 out of 11 dropped probes since last increase.

UDP Scan Timing: About 13.22% done; ETC: 19:46 (0:06:41 remaining)

UDP Scan Timing: About 16.03% done; ETC: 19:48 (0:07:57 remaining)

UDP Scan Timing: About 18.97% done; ETC: 19:49 (0:08:37 remaining)

Discovered open port 2049/udp on 192.168.1.60

Stats: 0:03:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan

UDP Scan Timing: About 23.93% done; ETC: 19:50 (0:09:07 remaining)

Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan

UDP Scan Timing: About 23.95% done; ETC: 19:50 (0:09:06 remaining)

UDP Scan Timing: About 40.05% done; ETC: 19:53 (0:08:29 remaining)

UDP Scan Timing: About 46.95% done; ETC: 19:53 (0:07:46 remaining)

UDP Scan Timing: About 53.22% done; ETC: 19:53 (0:07:00 remaining)

UDP Scan Timing: About 58.88% done; ETC: 19:53 (0:06:11 remaining)

UDP Scan Timing: About 64.72% done; ETC: 19:54 (0:05:23 remaining)

UDP Scan Timing: About 70.47% done; ETC: 19:54 (0:04:33 remaining)

UDP Scan Timing: About 75.90% done; ETC: 19:54 (0:03:45 remaining)

UDP Scan Timing: About 81.25% done; ETC: 19:54 (0:02:57 remaining)

UDP Scan Timing: About 86.47% done; ETC: 19:54 (0:02:08 remaining)

UDP Scan Timing: About 91.68% done; ETC: 19:54 (0:01:19 remaining)

Completed UDP Scan at 19:55, 1025.17s elapsed (1000 total ports)

Nmap scan report for 192.168.1.60

Host is up (0.00041s latency).

Not shown: 954 closed udp ports (port-unreach)

PORT STATE SERVICE

21/udp open|filtered ftp

37/udp open|filtered time

38/udp open|filtered rap

49/udp open|filtered tacacs

53/udp open domain

67/udp open|filtered dhcps

68/udp open|filtered dhcpc

69/udp open|filtered tftp

80/udp open|filtered http

111/udp open rpcbind

112/udp open|filtered mcidas

113/udp open|filtered auth

120/udp open|filtered cfdptkt

136/udp open|filtered profile

137/udp open netbios-ns

138/udp open|filtered netbios-dgm

139/udp open|filtered netbios-ssn

161/udp open|filtered snmp

162/udp open|filtered snmptrap

192/udp open|filtered osu-nms

199/udp open|filtered smux

207/udp open|filtered at-7

363/udp open|filtered rsvp_tunnel

389/udp open|filtered ldap

407/udp open|filtered timbuktu

427/udp open|filtered svrloc

434/udp open|filtered mobileip-agent

445/udp open|filtered microsoft-ds

464/udp open|filtered kpasswd5

497/udp open|filtered retrospect

502/udp open|filtered mbap

512/udp open|filtered biff

514/udp open|filtered syslog

515/udp open|filtered printer

518/udp open|filtered ntalk

539/udp open|filtered apertus-ldp

593/udp open|filtered http-rpc-epmap

626/udp open|filtered serialnumberd

639/udp open|filtered msdp

657/udp open|filtered rmc

682/udp open|filtered xfr

684/udp open|filtered corba-iiop-ssl

686/udp open|filtered hcp-wismar

688/udp open|filtered realm-rusd

764/udp open|filtered omserv

2049/udp open   nfs

MAC Address: 08:00:27:88:06:6A (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 1036.36 seconds

Raw packets sent: 1698 (75.193KB) | Rcvd: 1045 (76.182KB)

┌──(kali_alex㉿kali)-[~]

└─$ sudo nmap -F 192.168.1.60

[sudo] password di kali_alex:

Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 19:57 CEST

Nmap scan report for 192.168.1.60

Host is up (0.00027s 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: 08:00:27:88:06:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.23 seconds


┌──(kali_alex㉿kali)-[~]
└─$ sudo nmap -PR 192.168.1.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 19:59 CEST
Nmap scan report for 192.168.1.60
Host is up (0.00038s 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: 08:00:27:88:06:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.26 seconds


┌──(kali_alex㉿kali)-[~]
└─$ sudo nmap -sP 192.168.1.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 20:00 CEST
Nmap scan report for 192.168.1.60
Host is up (0.00030s latency).
```

MAC Address: 08:00:27:88:06:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.12 seconds

┌──(kali_alex㉿kali)-[~]

└─$ sudo nmap -Pn 192.168.1.60

Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 20:02 CEST

Nmap scan report for 192.168.1.60

Host is up (0.00022s 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: 08:00:27:88:06:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds