



INTRODUZIONE

In questo report si illustra l'utilizzo del tool di NMAP per scan di vario tipo.

Configurazione METASLOITABLE

```
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 06:5d:44:32:84:a0 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.5.101/24 brd 192.168.5.255 scope global eth0  
    inet6 fde1:e8f0:e255:14f0:45d:44ff:fe32:84a0/64 scope global dynamic  
        valid_lft 2591982sec preferred_lft 604782sec  
    inet6 fe80::45d:44ff:fe32:84a0/64 scope link  
        valid_lft forever preferred_lft forever  
msfadmin@metasploitable:~$ _
```

OS fingerprinting - Meta

```
(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.5.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:36 CEST
Nmap scan report for 192.168.5.101
Host is up (0.0025s latency).
Not shown: 979 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    filtered http
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
8009/tcp  open  ajp13
8180/tcp  open  unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.29 (Gentoo)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.97 seconds
```

SYN SCAN - META

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.5.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:38 CEST
Nmap scan report for 192.168.5.101
Host is up (0.0055s latency).
Not shown: 979 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    filtered http
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
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

TCP connect - Metasploitable

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.5.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:45 CEST
Nmap scan report for 192.168.5.101
Host is up (0.0045s latency).
Not shown: 979 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    filtered  http
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
8009/tcp  open      ajp13
8180/tcp  open      unknown

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

VERSION DETECTION

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.5.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:48 CEST
Nmap scan report for 192.168.5.101
Host is up (0.0073s 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
80/tcp    filtered  http
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
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS:
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.89 seconds
```


CONFIGURAZIONE WINDOWS 7

```
CA Prompt dei comandi

C:\Users\Eleonora>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN) 2:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : fde1:e8f0:e255:14f0:28f2:5
876:ef29:8221
    Indirizzo IPv6 temporaneo. . . . . : fde1:e8f0:e255:14f0:795c:a
bd7:bfb4:696d
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::28f2:5876:ef29:8221%
13
    Indirizzo IPv4. . . . . : 192.168.50.102
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.50.1

Scheda Tunnel isatap.{AEDCD081-77E6-4B07-B258-F76D596BE00A}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\Eleonora>
```

OS FINGERPRINTING FIREWALL ATTIVO

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 15:57 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0048s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: E6:BD:6D:37:4E:BF (Unknown)
Too many fingerprints match this host to give specific OS details
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 24.70 seconds
```

FIREWALL SPENTO

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 15:17 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0022s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: E6:BD:6D:37:4E:BF (Unknown)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
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 6.42 seconds
```