Scansioni con Nmap

```
__(kali⊛kali)-[~/Desktop]
s nmap 192.168.50.101 --script smb-os-discovery
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 03:53 CST
Nmap scan report for 192.168.50.101
Host is up (0.00079s latency).
Not shown: 977 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 microsof0
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 mysal
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Host script results:
 smb-os-discovery:
   OS: Unix (Samba 3.0.20-Debian)
   Computer name: metasploitable
   NetBIOS computer name:
   Domain name: localdomain
   FQDN: metasploitable.localdomain
   System time: 2023-12-20T04:53:22-05:00
Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

Porte aperte e SO Metasploitable

disponendo di un basso livello di sicurezza Nmap riesce a fare una scansione completa di tutte le porte e ci mostra quali sono aperte.

In basso si possono notare info riguardo OS

Scansione SYN e scansione TCP

```
—(kali⊛kali)-[~]
                                                                                                                    __(kali@kali)-[~/Desktop]
$ nmap 192.168.50.101
                                                                                                                   ___s nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 04:24 CST
                                                                                                                   Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 04:24 CST
Nmap scan report for 192.168.50.101
                                                                                                                   Nmap scan report for 192.168.50.101
Host is up (0.00057s latency).
                                                                                                                   Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (conn-refused)
                                                                                                                   Not shown: 977 closed tcp ports (conn-refused)
       STATE SERVICE
                                                                                                                           STATE SERVICE
21/tcp open ftp
                                                                                                                   21/tcp open ftp
22/tcp open ssh
                                                                                                                   22/tcp
                                                                                                                           open ssh
23/tcp open telnet
                                                                                                                   23/tcp open telnet
25/tcp open smtp
                                                                                                                   25/tcp open smtp
       open domain
                                                                                                                           open domain
                                                                                                                   80/tcp open http
80/tcp open http
111/tcp open
                                                                                                                   111/tcp open rpcbind
              rpcbind
139/tcp open netbios-ssn
                                                                                                                   139/tcp open netbios-ssn
445/tcp open microsoft-ds
                                                                                                                   445/tcp open microsoft-ds
512/tcp open exec
                                                                                                                   512/tcp open exec
513/tcp open login
                                                                                                                   513/tcp open login
514/tcp open shell
                                                                                                                   514/tcp open shell
1099/tcp open rmiregistry
                                                                                                                   1099/tcp open rmiregistry
1524/tcp open ingreslock
                                                                                                                   1524/tcp open ingreslock
2049/tcp open nfs
                                                                                                                   2049/tcp open nfs
2121/tcp open ccproxy-ftp
                                                                                                                   2121/tcp open ccproxy-ftp
3306/tcp open mysql
                                                                                                                   3306/tcp open mysql
5432/tcp open postgresql
                                                                                                                   5432/tcp open postgresal
                                                                                                                   5900/tcp open vnc
5900/tcp open vnc
6000/tcp open X11
                                                                                                                   6000/tcp open X11
6667/tcp open irc
                                                                                                                   6667/tcp open irc
8009/tcp open ajp13
                                                                                                                   8009/tcp open ajp13
8180/tcp open unknown
                                                                                                                   8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
                                                                                                                   Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
                                                                                                                   (kali⊛ kali)-[~/Desktop]
__(kali⊛kali)-[~]
_$∏
```

Sembrerebbe che la scansione SYN sia più lenta e quindi meno aggressiva

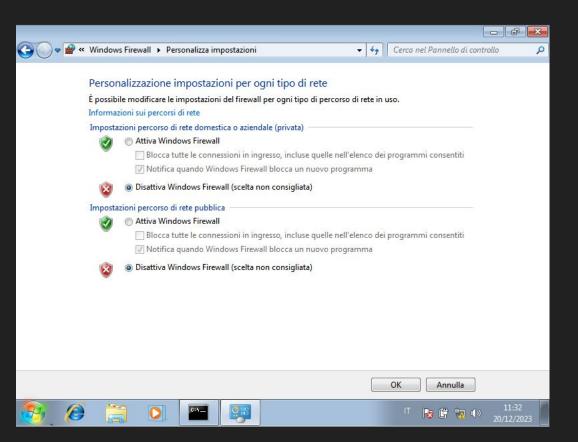
Servizi attivi e Versione

```
__(kali⊕kali)-[~]
_$ nmap -sV 192.168.50.101
Starting Nmap 7.94 (https://nmap.org) at 2023-12-20 03:48 CST
Nmap scan report for 192.168.50.101
Host is up (0.00053s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT
         STATE SERVICE
                          VERSTON
21/tcp open ftp
                          vsftpd 2.3.4
                          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/tcp open ssh
23/tcp open telnet
                          Linux telnetd
25/tcp open smtp
                          Postfix smtpd
                          ISC BIND 9.4.2
53/tcp open domain
                          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp open http
                          2 (RPC #100000)
111/tcp open rpcbind
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
                          Metasploitable root shell
1524/tcp open bindshell
2049/tcp open nfs
                          2-4 (RPC #100003)
2121/tcp open ftp
                          ProFTPD 1.3.1
3306/tcp open mysql
                          MvSOL 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
                          Apache Jserv (Protocol v1.3)
8009/tcp open ajp13
8180/tcp open unknown
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ke
rnel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.71 seconds
```

Porte filtrate Windows

Disponendo di un livello di sicurezza più elevato i firewall di windows bloccano sia il ping sia lo scan delle porte; per ovviare al primo problema basta aggiungere -Pn nel comando della shell, nel secondo invece bisogna disattivare i firewall direttamente da windows

Firewall disattivati



Andando su Pannello di Controllo>Windows Firewall>Personalizza impostazioni è possibile disattivare i firewall per reti private e pubbliche

Porte aperte e SO Windows

```
—(kali®kali)-[~]
s nmap -Pn 192.168.32.101 --script smb-os-discovery
Starting Nmap 7.94 (https://nmap.org) at 2023-12-20 04:34 CST
Nmap scan report for 192.168.32.101
Host is up (0.00054s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT
         STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
         open microsof0
445/tcp
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown
Host script results:
  smb-os-discovery:
   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
   OS CPE: cpe:/o:microsoft:windows_7::sp1
   Computer name: Windows-PC
   NetBIOS computer name: WINDOWS-PC\x00
   Workgroup: WORKGROUP\x00
   System time: 2023-12-20T11:34:52+01:00
Nmap done: 1 IP address (1 host up) scanned in 14.85 seconds
  —(kali⊛kali)-[~]
```

Ecco ora rese visibili le porte aperte di windows con relativo sistema operativo in basso.

Nonostante le modifiche sulla sicurezza alcune delle porte restano chiuse o filtrate (ad esempio la porta 80)