

# ESERCIZIO CONSEGNA W9D1

- Kali Linux > Metasploitable (TCP Scan):

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -p 1-1024 192.168.32.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 19:49 CET  
Nmap scan report for 192.168.32.101  
Host is up (0.012s latency).  
Not shown: 1012 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  
MAC Address: 08:00:27:8F:C3:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

- Kali Linux > Metasploitable (SYN Scan):

```
kali@kali: ~  
File Actions Edit View Help  
514/tcp open  shell  
MAC Address: 08:00:27:8F:C3:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds  
(kali@kali)-[~]  
$ sudo nmap -sS -p 1-1024 192.168.32.101  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 19:51 CET  
Nmap scan report for 192.168.32.101  
Host is up (0.00034s latency).  
Not shown: 1012 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  
MAC Address: 08:00:27:8F:C3:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds  
(kali@kali)-[~]  
$
```

- Kali Linux > Metasploitable (Scan invasivo -A):

```
(kali@kali)-[~]
$ sudo nmap -A -p 1-1024 192.168.32.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 19:55 CET
Nmap scan report for 192.168.32.101
Host is up (0.0054s latency).
Not shown: 1012 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 192.168.32.100
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_   program version  port/proto  service
|_   100000  2             111/tcp    rpcbind
|_   100000  2             111/udp    rpcbind
|_   100003  2,3,4         2049/tcp   nfs
|_   100003  2,3,4         2049/udp   nfs
|_   100005  1,2,3         57839/tcp  mountd
|_   100005  1,2,3         58418/udp  mountd
|_   100021  1,3,4         53134/tcp  nlockmgr
|_   100021  1,3,4         54840/udp  nlockmgr
|_   100024  1             39934/udp  status
|_   100024  1             42530/tcp  status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshcd
513/tcp   open  login?
```