

# W9D1

Scansione della rete di un IP tramite nmap.

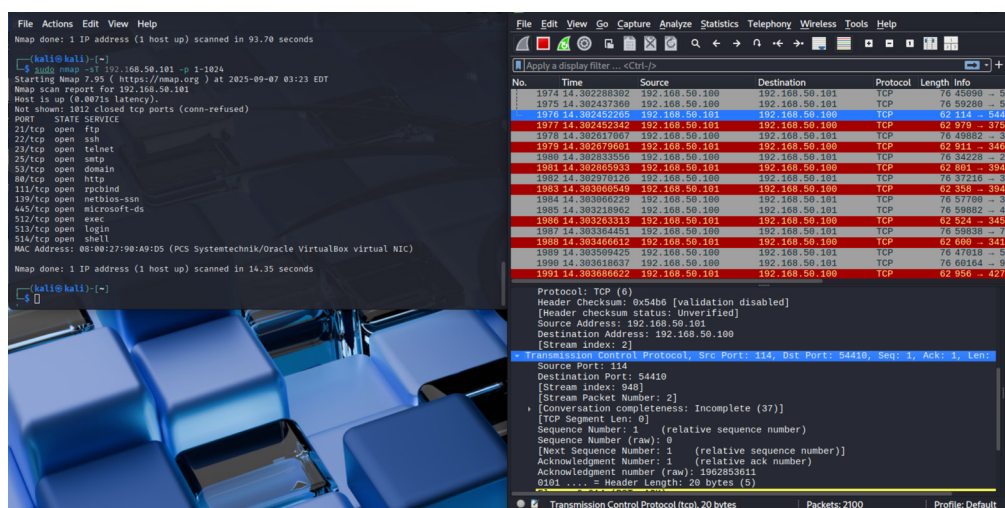
La scansione con nmap fornisce numerose informazioni iniziali per individuare potenziali vulnerabilità.

## nmap -sS

Metodo di scansione che permette di vedere le porte e il tipo. Si può vedere che le porte sono aperte in questo caso per cui potenzialmente vulnerabili

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sS 192.168.50.101 -p 1-1024  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-07 03:12 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00071s 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: 08:00:27:90:A9:D5 (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

Con Wireshark è possibile vedere le richieste e le risposte e catturarne il traffico



## nmap -A

Metodo di scansione che permette di vedere molte informazioni e potenziali vulnerabilità, il sistema operativo, servizi (ssh, https, http, mysql..), traceroute (tracciamento rotte) e script

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -A 192.168.50.101 -p 1-1024  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-07 03:14 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.0014s latency).  
Not shown: 1012 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
| ftp-syst:  
|   STAT:  
|   FTP server status:  
|   Connected to 192.168.50.100  
|   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  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
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         41852/udp  mountd  
|   100005  1,2,3         56463/tcp  mountd  
|   100021  1,3,4         46008/tcp  nlockmgr  
|   100021  1,3,4         52589/udp  nlockmgr  
|   100024  1             34765/udp  status  
|   100024  1             39566/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?  
514/tcp   open  shell        Netkit rshd  
MAC Address: 08:00:27:90:A9:D5 (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
Device type: general purpose  
Running: Linux 2.6.X
```