

Esecuzione scansione sulla macchina metaspotable con nmap:

Scansione TCP:

```
(kali㉿kali)-[~]  
$ nmap -p 0-1023 192.168.50.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 06:04 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.000072s 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: 08:00:27:8C:6B:07 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```

Report:

Fonte dello scan: macchina kali linux con ip 192.168.50.100

Target dello scan: macchina metaspotable con ip 192.168.50.100

Tipo di scan: scansione TCP sulle porte well-known (dalla 0 alla 1023)

Risultati: 12 porte TCP aperte

Scansione SYN

```
(kali㉿kali)-[~]  
$ nmap -sS -p 0-1023 192.168.50.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 06:06 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.000074s 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: 08:00:27:8C:6B:07 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.53 seconds
```

Report:

Fonte dello scan: macchina kali linux con ip 192.168.50.100

Target dello scan: macchina metaspotable con ip 192.168.50.100

Tipo di scan: scansione SYN sulle porte well-known (dalla 0 alla 1023)

Risultati: 12 porte aperte

Scansione -A

```
└─$ nmap -sS -A -p 0-1023 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 06:07 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00016s 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,
BITMIME, 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_server_header: Apache/2.2.8 (Ubuntu) DAV/2
|_http_title: Metasploitable2 - Linux
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           36651/tcp  mountd
|   100005  1,2,3           41450/udp  mountd
|   100021  1,3,4           35507/tcp  nlockmgr
|   100021  1,3,4           37887/udp  nlockmgr
|   100024  1                48081/tcp  status
|   100024  1                54332/udp  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 rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
MAC Address: 08:00:27:8C:6B:07 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```

MAC Address: 08:00:27:8C:6B:07 (PCS Systemtechnik/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: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-09-08T06:10:02-04:00
|_ clock-skew: mean: 2h01m53s, deviation: 2h49m42s, median: 1m53s
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT      ADDRESS
1   0.16 ms  192.168.50.101

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 88.17 seconds

```

Report:

Fonte dello scan: macchina kali linux con ip 192.168.50.100

Target dello scan: macchina metaspotable con ip 192.168.50.100

Tipo di scan: scansione con switch «-A» sulle porte well-known (dalla 0 alla 1023)

Risultati: come da screen riportato qui sopra oltre ad aver intercettato le porte aperte con i relativi servizi in uso abbiamo altri risultati interessanti in quanto -A ci permette di intercettare il sistema operativo, i servizi e gli script.