

Host discovery

```
(kali㉿kali)-[~]
└─$ sudo nmap -F -sS
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 12:50 CET
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds

(kali㉿kali)-[~]
└─$ sudo nmap -F -sS 192.168.50.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 12:50 CET
Nmap scan report for 192.168.50.101
Host is up (0.000097s latency).
Not shown: 82 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
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13
MAC Address: 08:00:27:C7:41:A5 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.50.100
Host is up (0.000050s latency).
All 100 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 100 closed tcp ports (reset)

Nmap done: 256 IP addresses (2 hosts up) scanned in 30.50 seconds
```

Ho scannerizzato la rete con nmap ed è stata correttamente individuata la macchina metaesplorable. Utilizzando lo switch -F, nmap testa le 100 porte di solito più utilizzate , e in questo caso sono state trovate 18 aperte.

Sys scan su porte well-know

```
(kali@kali)-[~]
└─$ sudo nmap -sS -p 0-1023 192.168.50.101
[sudo] password di kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 14:39 CET
Nmap scan report for 192.168.50.101
Host is up (0.00024s 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:C7:41:A5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds

(kali@kali)-[~]
└─$
```

Applica un filtro di visualizzazione ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
33	268.167369283	192.168.50.100	192.168.50.101	TCP	58	49432 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	268.167432704	192.168.50.101	192.168.50.100	TCP	60	445 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
35	268.167432934	192.168.50.101	192.168.50.100	TCP	60	113 → 49432 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36	268.167432996	192.168.50.101	192.168.50.100	TCP	60	135 → 49432 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	268.167458302	192.168.50.100	192.168.50.101	TCP	54	49432 → 445 [RST] Seq=1 Win=0 Len=0
38	268.167523719	192.168.50.101	192.168.50.100	TCP	60	995 → 49432 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
39	268.167523800	192.168.50.101	192.168.50.100	TCP	60	21 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
40	268.167523823	192.168.50.101	192.168.50.100	TCP	60	143 → 49432 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41	268.167523850	192.168.50.101	192.168.50.100	TCP	60	23 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
42	268.167523877	192.168.50.101	192.168.50.100	TCP	60	80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
43	268.167523900	192.168.50.101	192.168.50.100	TCP	60	22 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
44	268.167523928	192.168.50.101	192.168.50.100	TCP	60	111 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
45	268.167538013	192.168.50.100	192.168.50.101	TCP	54	49432 → 21 [RST] Seq=1 Win=0 Len=0
46	268.167540573	192.168.50.100	192.168.50.101	TCP	54	49432 → 23 [RST] Seq=1 Win=0 Len=0
47	268.167552629	192.168.50.100	192.168.50.101	TCP	54	49432 → 80 [RST] Seq=1 Win=0 Len=0
48	268.167558066	192.168.50.100	192.168.50.101	TCP	54	49432 → 22 [RST] Seq=1 Win=0 Len=0
49	268.167565826	192.168.50.100	192.168.50.101	TCP	54	49432 → 111 [RST] Seq=1 Win=0 Len=0
50	268.16779597	192.168.50.100	192.168.50.101	TCP	58	49432 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51	268.167604044	192.168.50.100	192.168.50.101	TCP	58	49432 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 45: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on 0
Ethernet II, Src: PcsCompu_ba:47:e7 (08:00:27:ba:47:e7), Dst: PcsC 00:00:00:28:00:00
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
Transmission Control Protocol, Src Port: 49432, Dst Port: 21, Seq: 1, Win: 0, Len: 0

Fonte	Target	Tipo Scan	Risultato
Kali(192.168.50.100)	Metasploitable(192.168.50.101)	sS	12 servizi attivi su porte 0-1023

Tcp Scan su porte well-know

```
(kali@kali)-[~]
└─$ sudo nmap -sT -p 0-1023 192.168.50.101
[sudo] password di kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 14:49 CET
Nmap scan report for 192.168.50.101
Host is up (0.00026s latency).
Not shown: 1012 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  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
MAC Address: 08:00:27:C7:41:A5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds

(kali@kali)-[~]
└─$
```

ip.addr == 192.168.50.101 and tcp.port in {80..83}

No.	Time	Source	Destination	Protocol	Length	Info
41	13.136392440	192.168.50.100	192.168.50.101	TCP	74	42728 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536375794
62	13.136852346	192.168.50.101	192.168.50.100	TCP	74	80 → 42728 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK
64	13.136852021	192.168.50.100	192.168.50.101	TCP	66	42728 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2536375794
67	13.136912919	192.168.50.100	192.168.50.101	TCP	66	42728 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2536375794
282	13.140632719	192.168.50.100	192.168.50.101	TCP	74	39052 → 83 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536375794
312	13.141495627	192.168.50.101	192.168.50.100	TCP	60	83 → 39052 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
471	13.198960384	192.168.50.100	192.168.50.101	TCP	74	53008 → 82 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536375794
483	13.198140580	192.168.50.101	192.168.50.100	TCP	60	82 → 53008 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1974	13.231924701	192.168.50.100	192.168.50.101	TCP	74	37284 → 91 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536375794
1981	13.232065211	192.168.50.101	192.168.50.100	TCP	60	81 → 37284 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 67: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on 0
Ethernet II, Src: PcsCompu_ba:47:e7 (08:00:27:ba:47:e7), Dst: PcsC 00:00:00:28:00:00
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
... = Version: 4
... = Header Length: 20 bytes (5)
Total Length: 52
Identification: 0xb3eb (46059)
... = Flags: 0x2, Don't fragment
... = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xa0be [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.50.100
Destination Address: 192.168.50.101
Transmission Control Protocol, Src Port: 42728, Dst Port: 80, Seq: 1, Win: 0, Len: 0
Source Port: 42728
Destination Port: 80
[Stream Index: 13]
[Conversation completeness: Complete, NO DATA (39)]

Fonte	Target	Tipo Scan	Risultato
Kali(192.168.50.100)	Metasploitable(192.168.50.101)	sT	12 servizi attivi su porte 0-1023

Scan con switch -A

File Azioni Modifica Visualizza Aiuto

Starting Nmap 7.93 (https://nmap.org) at 2023-02-09 15:50 CET
Nmap scan report for 192.168.50.101
Host is up (0.00023s latency).
Not shown: 1012 closed tcp ports (conn-refused)
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 Subuntul (protocol 2.0)
|_ssh-hostkey:
|_1024 600fcfe1c05f64d69024fac4d56ccd (DSA)
|_2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp open telnet?
25/tcp open smtp?
|_smtp-command: Metasploitable.localdomain, PIPELINING, SIZE 102400
00, 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 38670/udp mountd
|_100005 1,2,3 48028/tcp mountd
|_100021 1,3,4 41750/udp nlockmgr
|_100021 1,3,4 57030/tcp nlockmgr
|_100024 1 37501/udp status
|_100024 1 57842/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?

File Modifica Visualizza Vaj Cattura Analizza Statistiche Telefonja Wireless Strumenti Aiuto

ip.addr == 192.168.50.101 and tcp.port in {80,110}

No.	Time	Source	Destination	Protocol	Length	Info
3732	178.401786170	192.168.50.101	192.168.50.100	TCP	66	80 - 33414 [ACK] Seq=1 Ack=215 Win=6912 Len=0 TSval=494747 TSe
3733	178.401724109	192.168.50.100	192.168.50.101	HTTP	604	POST /sdk HTTP/1.1
3734	178.401741903	192.168.50.100	192.168.50.101	HTTP	84	GET / HTTP/1.0
3735	178.401780122	192.168.50.101	192.168.50.100	TCP	66	80 - 33370 [ACK] Seq=1 Ack=157 Win=6912 Len=0 TSval=494747 TSe
3736	178.401780262	192.168.50.101	192.168.50.100	TCP	66	80 - 33340 [ACK] Seq=1 Ack=163 Win=6912 Len=0 TSval=494747 TSe
3737	178.401825088	192.168.50.101	192.168.50.100	TCP	66	80 - 33320 [ACK] Seq=1 Ack=619 Win=7040 Len=0 TSval=494747 TSe
3738	178.401864091	192.168.50.101	192.168.50.100	TCP	66	80 - 33378 [ACK] Seq=1 Ack=19 Win=5888 Len=0 TSval=494747 TSe
3739	178.401873279	192.168.50.100	192.168.50.101	HTTP	233	PROPFIND / HTTP/1.1
3740	178.401807094	192.168.50.100	192.168.50.101	HTTP	227	GET /.git/HEAD HTTP/1.1
3742	178.401937111	192.168.50.100	192.168.50.101	HTTP	218	GET / HTTP/1.1
3743	178.401950371	192.168.50.100	192.168.50.101	HTTP	222	OPTIONS / HTTP/1.1
3744	178.402110752	192.168.50.101	192.168.50.100	TCP	66	80 - 33386 [ACK] Seq=1 Ack=168 Win=6912 Len=0 TSval=494747 TSe
3745	178.402110820	192.168.50.101	192.168.50.100	TCP	66	80 - 33398 [ACK] Seq=1 Ack=162 Win=6912 Len=0 TSval=494747 TSe
3746	178.402110851	192.168.50.101	192.168.50.100	TCP	66	80 - 33318 [ACK] Seq=1 Ack=153 Win=6912 Len=0 TSval=494747 TSe
3747	178.402110877	192.168.50.101	192.168.50.100	TCP	66	80 - 33416 [ACK] Seq=1 Ack=157 Win=6912 Len=0 TSval=494747 TSe
3748	178.402163819	192.168.50.101	192.168.50.100	HTTP	558	HTTP/1.1 404 Not Found (text/html)
3749	178.402163072	192.168.50.101	192.168.50.100	TCP	66	80 - 33334 [FIN, ACK] Seq=493 Ack=177 Win=6912 Len=0 TSval=494
3750	178.402170088	192.168.50.100	192.168.50.101	TCP	66	33334 - 80 [ACK] Seq=177 Ack=493 Win=64128 Len=0 TSval=2540190
3753	178.403385114	192.168.50.100	192.168.50.100	HTTP	544	HTTP/1.1 404 Not Found (text/html)

Frame 3732: 66 bytes on wire (528 bits), 66 bytes captured (528 b

Ethernet II, Src: PcsCompu_c7:41:a5 (08:00:27:c7:41:a5), Dst: Pcs

Internet Protocol Version 4, Src: 192.168.50.101, Dst: 192.168.50

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 52

Identification: 0x392f (14639)

010 = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: TCP (6)

Header Checksum: 0x1b7b [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.50.101

Destination Address: 192.168.50.100

Transmission Control Protocol, Src Port: 80, Dst Port: 33414, Seq

Source Port: 80

Destination Port: 33414

[Stream index: 1208]

[Conversation completeness: Complete, WITH DATA (31)]

Header Checksum (ip.checksum), 2 byte

Pacchetti: 4962 - visualizzati: 403 (8.1%)

Profilo: Default

Fonte	Target	Tipo Scan	Risultato
Kali(192.168.50.100)	Metasploitable(192.168.50.101)	sT -A	12 servizi attivi su porte 0-1023, incluse versioni e info sui servizi e S.O.