



# Giorno 4-Nmap scan EPICODE

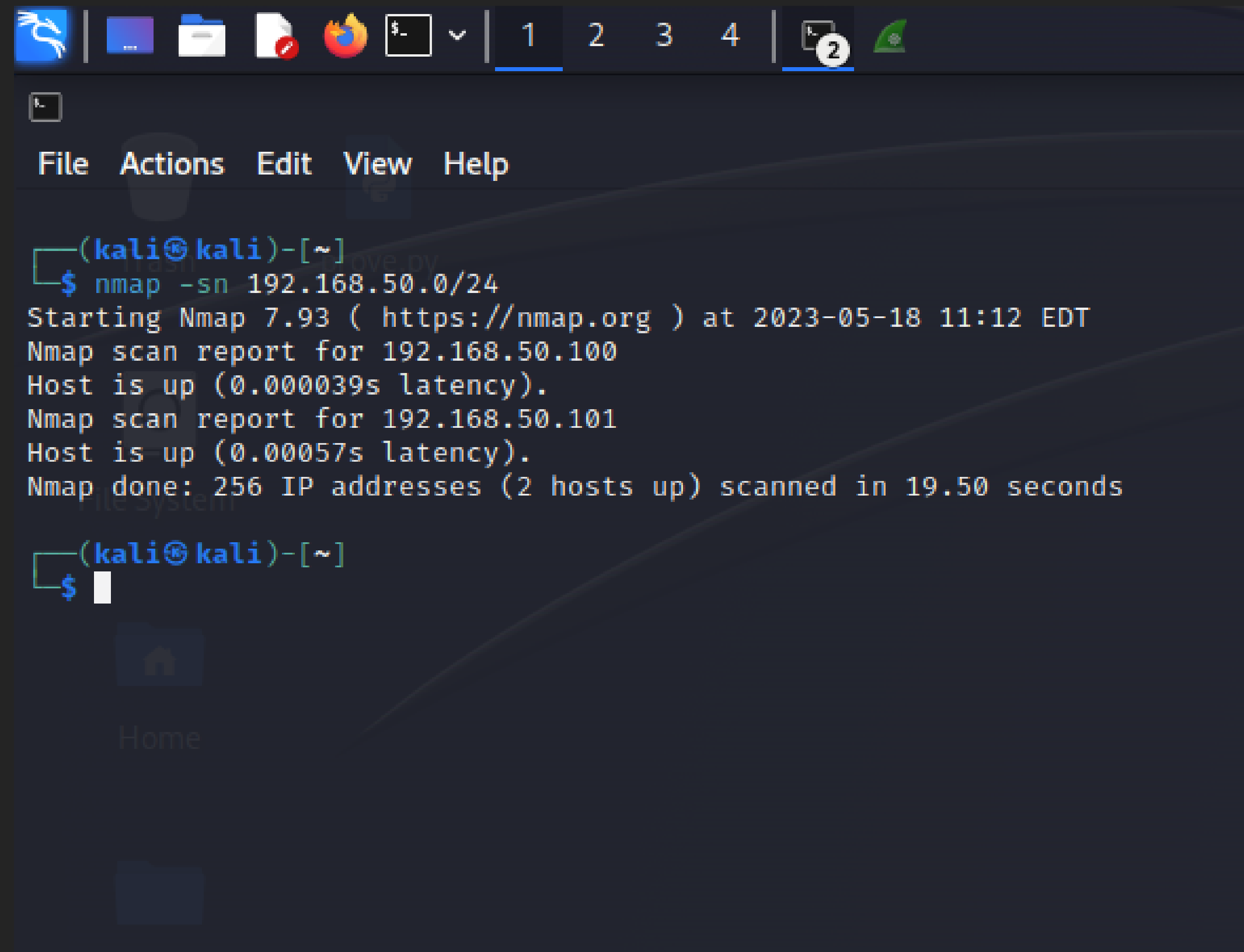
Giovanni Pisapia



# "HOST DISCOVERY"

Con il comando `-sn 192.168.5.101` andiamo individuare quali dispositivi vengono trovati su quella rete inviando un ping

Il comando `-Pn` in Nmap viene utilizzato per eseguire una scansione delle porte senza inviare ping al dispositivo di destinazione. Questo può essere utile quando la risposta ai ping è bloccata o disabilitata.



```
(kali㉿kali)-[~]  
$ nmap -sn 192.168.50.0/24  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 11:12 EDT  
Nmap scan report for 192.168.50.100  
Host is up (0.000039s latency).  
Nmap scan report for 192.168.50.101  
Host is up (0.00057s latency).  
Nmap done: 256 IP addresses (2 hosts up) scanned in 19.50 seconds  
  
(kali㉿kali)-[~]  
$
```

# "SCAN TECHNIQUES:"

Usiamo `-sT`, questo comando esegue una scansione delle porte utilizzando il metodo TCP Connect. Si connette attivamente alle porte specificate per verificare se sono aperte o chiuse. Il metodo TCP Connect richiede una connessione completa, rendendolo più evidente agli strumenti di monitoraggio di rete.

The image shows a Kali Linux terminal window on the left and a Wireshark network traffic capture on the right. The terminal window displays the output of the `nmap -sT 192.168.50.101` command, showing a list of open ports and services. The Wireshark window shows a packet capture on the `eth0` interface, with a display filter of `Apply a display filter ... <Ctrl-/>`. The packet list shows several TCP packets, with packet 3 highlighted in blue, indicating a successful connection to port 80. The packet details pane shows the structure of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.

**Terminal Output:**

```
(kali@kali)-[~]  
$ nmap -sT 192.168.50.101  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:00 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00057s 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  microsoft-ds  
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  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

**Wireshark Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	192.168.50.100	192.168.50.101	TCP	74	33794 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
2	0.0000000000	192.168.50.100	192.168.50.101	TCP	74	41516 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
3	0.000329882	192.168.50.101	192.168.50.100	TCP	74	80 → 33794 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS
4	0.000330140	192.168.50.101	192.168.50.100	TCP	60	443 → 41516 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.000359101	192.168.50.100	192.168.50.101	TCP	66	33794 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=7
6	0.000441400	192.168.50.100	192.168.50.101	TCP	66	33794 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
7	0.000738125	PcsCompu_c7:e1:36	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.100
8	1.028436037	PcsCompu_c7:e1:36	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.100
9	2.038958544	PcsCompu_c7:e1:36	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.100
10	4.017963229	PcsCompu_c7:e1:36	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.100
11	5.075675005	PcsCompu_c7:e1:36	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.100

**Wireshark Packet Details:**

- Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
- Ethernet II, Src: PcsCompu\_fa:f6:9a (08:00:27:fa:f6:9a), Dst: PcsCompu\_c7:e1:36 (08:00:27:c7:e1:36)
- Internet Protocol Version 4, Src: 192.168.50.101, Dst: 192.168.50.100
- Transmission Control Protocol, Src Port: 80, Dst Port: 33794, Seq: 0, Ack: 1, Len: 0

**Wireshark Packet Bytes:**

Offset	Bytes
0000	08 00 27 c7
0010	00 3c 00 00
0020	32 64 00 50
0030	16 a0 6d be
0040	68 1e 2a 29



# "SCAN TECHNIQUES:"

Usiamo -sS questo comando esegue una scansione delle porte utilizzando il metodo TCP SYN. Invia pacchetti SYN ai numeri di porta specificati per determinare quali porte sono aperte, chiuse o filtrate. Questa è una delle modalità di scansione più comuni utilizzate con Nmap.

The image displays two windows from a Kali Linux environment. The left window shows the output of an Nmap scan using the -sS option. The right window shows a Wireshark packet capture of the scan traffic on the eth0 interface.

**Nmap Scan Report for 192.168.50.101**

```
Nmap scan report for 192.168.50.101
Host is up (0.00073s latency).
Not shown: 977 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
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
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
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:FA:F6:9A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.51 seconds
```

**Wireshark Packet Capture (eth0)**

No.	Time	Source	Destination	Protocol	Length	Info
49	19.323584857	192.168.50.100	192.168.50.101	TCP	54	60857 → 111 [RST] Seq=1 Win=0 Len=0
50	19.323795337	192.168.50.100	192.168.50.101	TCP	58	60857 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51	19.323848354	192.168.50.101	192.168.50.100	TCP	60	22 → 60857 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
52	19.323871249	192.168.50.100	192.168.50.101	TCP	54	60857 → 22 [RST] Seq=1 Win=0 Len=0
53	19.324194324	192.168.50.100	192.168.50.101	TCP	58	60857 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
54	19.324263183	192.168.50.100	192.168.50.101	TCP	58	60857 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55	19.324312824	192.168.50.100	192.168.50.101	TCP	58	60857 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
56	19.324427304	192.168.50.101	192.168.50.100	TCP	60	256 → 60857 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57	19.324502646	192.168.50.100	192.168.50.101	TCP	58	60857 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
58	19.324558101	192.168.50.100	192.168.50.101	TCP	58	60857 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
59	19.324749029	192.168.50.101	192.168.50.100	TCP	60	113 → 60857 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

**Packet Details (Frame 57):**

- Frame 57: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
- Ethernet II, Src: PcsCompu\_c7:e1:36 (08:00:27:c7:e1:36), Dst: PcsCompu\_fa:f6:9a (08:00:27:fa:f6:9a)
- Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
- Transmission Control Protocol, Src Port: 60857, Dst Port: 80, Seq: 0, Len: 0

**Packet Bytes:**

Offset	Hex	ASCII
0000	08 00 27 fa	
0010	00 2c c6 d9	
0020	32 65 ed b9	
0030	04 00 88 b2	

**Wireshark Status:** eth0: <live capture in progress> Packets: 2040 · Displayed: 2040 (100.0%) Profile: Default

# "SCAN AGGRESSIVE"

-A 192.168.50.101 Questo comando esegue una scansione completa che include diverse tecniche di scansione combinate in un'unica scansione. Include la scansione delle porte , la rilevazione delle versioni dei servizi e il rilevamento del sistema operativo. Questo tipo di scansione fornisce un'analisi più completa e dettagliata della macchina di destinazione.

```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_clock-skew: mean: -47m20s, deviation: 2h18m33s, median: -2h07m20s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2023-05-18T07:40:07-04:00
```

```
TRACEROUTE
HOP RTT      ADDRESS
1   0.89 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 45.33 seconds

```
—(kali@kali)-[~]
```

```
—(kali@kali)-[~]
$ sudo nmap -A -p 1-1023 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:47 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00089s latency).
Not shown: 1011 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 192.168.50.100
|   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
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211dde72bae61b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-05-18T11:40:26+00:00; -2h07m20s from scanner time.
|_ssl-v2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
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
```



fonte dello scan	target dello scan	tipo scan	risultato	comando
nmap	192.168.50.101	SCAN TECHNIQUES: synk	12 porte/Servizi attivi che potrebbero portare vulnerabilità	<code>nmap -sS 192.168.50.101</code>
nmap	192.168.50.101	SCAN TECHNIQUES: tcp	12 porte/Servizi attivi che potrebbero portare vulnerabilità	<code>nmap -sT 192.168.50.101</code>
nmap	192.168.50.101	scanner operation system	Linux 2.6.9 – 2.6.33	<code>nmap -O 192.168.50.101</code>
namap	192.168.50.101	"SCAN AGGRESSIVE"	scanner aggressiva dove si vedono servizi porte e sistemi operativi attivi	<code>nmap -A 192.168.50.101</code>
nmap	192.168.50.0/24	host discovery	2 host attivi: 192.168.50.100–192.168.50.10	<code>nmap -sn 192.168.50.0/24</code>
namp	192.168.50.0/24	host discovery senza ping	2 host attivi: 192.168.50.100–192.168.50.101	<code>nmap -Pn 192.168.50.0/24</code>