

OS FINGERPRINT di META,

```
lucas@kali: ~  
File Azioni Modifica Visualizza Aiuto  
L$ sudo nmap -O 192.168.49.101  
[sudo] password di lucas:  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 20:46 CEST  
Nmap scan report for 192.168.49.101  
Host is up (0.049s 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:B1:AA:58 (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  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds  
  
(lucas@kali)-[~]  
$
```

SCAN con TCP connect

```
(lucas@kali)-[~]
$ sudo nmap -sT 192.168.49.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 20:51 CEST
Nmap scan report for 192.168.49.101
Host is up (0.015s 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
MAC Address: 08:00:27:B1:AA:58 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.10 seconds
(lucas@kali)-[~]
```

SCAN DI SOLO SYN

```
(lucas@kali)-[~]
$ sudo nmap -sS 192.168.49.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 20:54 CEST
Nmap scan report for 192.168.49.101
Host is up (0.074s 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:B1:AA:58 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.62 seconds
(lucas@kali)-[~]
```

La differenza tra le due scansione è:

TCP connect(-sT) stabilisce una connessione con il demone del servizio in ascolto, completando il 3-way-handshake (SYN-SYN/ACK-ACK), quindi la porta è aperta, invece lo Scan SYN(-sS) è una scansione furtiva in quanto non stabilisce una connessione completa con il demone in target (SYN-RST/ACK) non completa il 3-way-handshake in questo caso la porta risulta chiusa.

No.	Time	Source	Destination	Protocol	Length	Info
4	1.068502725	PcsCompu_08:db:a1	Broadcast	ARP	42	Who has 192.168.49.1? Tell 192.168.49.1
5	2.090807494	PcsCompu_08:db:a1	Broadcast	ARP	42	Who has 192.168.49.1? Tell 192.168.49.1
6	4.052442126	PcsCompu_08:db:a1	Broadcast	ARP	42	Who has 192.168.49.1? Tell 192.168.49.1
7	5.074919730	PcsCompu_08:db:a1	Broadcast	ARP	42	Who has 192.168.49.1? Tell 192.168.49.1
8	6.092309067	PcsCompu_08:db:a1	Broadcast	ARP	42	Who has 192.168.49.1? Tell 192.168.49.1
9	8.211163354	PcsCompu_08:db:a1	Broadcast	ARP	42	Who has 192.168.49.1? Tell 192.168.49.1
10	9.230280767	PcsCompu_08:db:a1	Broadcast	ARP	42	Who has 192.168.49.1? Tell 192.168.49.1
11	10.254812254	PcsCompu_08:db:a1	Broadcast	ARP	42	Who has 192.168.49.1? Tell 192.168.49.1
12	13.221656768	192.168.49.100	192.168.49.101	TCP	74	58820 → 113 [SYN] Seq=0 Win=64240 Len=0
13	13.223386022	192.168.49.100	192.168.49.101	TCP	74	56766 → 111 [SYN] Seq=0 Win=64240 Len=0
14	13.224413541	192.168.49.100	192.168.49.101	TCP	74	57980 → 8888 [SYN] Seq=0 Win=64240 Len=0
15	13.225105704	192.168.49.100	192.168.49.101	TCP	74	53650 → 80 [SYN] Seq=0 Win=64240 Len=0
16	13.225537622	192.168.49.100	192.168.49.101	TCP	74	43442 → 993 [SYN] Seq=0 Win=64240 Len=0
17	13.226627661	192.168.49.101	192.168.49.100	TCP	60	113 → 58820 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	13.226989190	192.168.49.100	192.168.49.101	TCP	74	38544 → 256 [SYN] Seq=0 Win=64240 Len=0
19	13.227574576	192.168.49.100	192.168.49.101	TCP	74	47016 → 21 [SYN] Seq=0 Win=64240 Len=0
20	13.228250081	192.168.49.100	192.168.49.101	TCP	74	45780 → 53 [SYN] Seq=0 Win=64240 Len=0
21	13.228899842	192.168.49.100	192.168.49.101	TCP	74	47654 → 1025 [SYN] Seq=0 Win=64240 Len=0
22	13.229278381	192.168.49.101	192.168.49.100	TCP	74	111 → 56766 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
23	13.229301246	192.168.49.100	192.168.49.101	TCP	66	56766 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0
24	13.229833394	192.168.49.101	192.168.49.100	TCP	60	8888 → 57980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	13.230138568	192.168.49.100	192.168.49.101	TCP	74	47158 → 139 [SYN] Seq=0 Win=64240 Len=0
26	13.230748533	192.168.49.101	192.168.49.100	TCP	74	80 → 53650 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
27	13.230768391	192.168.49.100	192.168.49.101	TCP	66	53650 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
28	13.232029150	192.168.49.101	192.168.49.100	TCP	60	993 → 43442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	13.232029592	192.168.49.101	192.168.49.100	TCP	60	256 → 38544 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	13.232029632	192.168.49.101	192.168.49.100	TCP	74	21 → 47016 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
31	13.232060746	192.168.49.100	192.168.49.101	TCP	66	47016 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0
32	13.230585232	192.168.49.100	192.168.49.101	TCP	66	56766 → 111 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	13.232667955	192.168.49.101	192.168.49.100	TCP	74	53 → 45780 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
34	13.230967380	192.168.49.100	192.168.49.101	TCP	66	45780 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0
35	13.231078467	192.168.49.100	192.168.49.101	TCP	66	53650 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36	13.231183610	192.168.49.100	192.168.49.101	TCP	66	47016 → 21 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	13.231282457	192.168.49.100	192.168.49.101	TCP	66	45780 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	13.231476394	192.168.49.100	192.168.49.101	TCP	74	50920 → 445 [SYN] Seq=0 Win=64240 Len=0

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_08:db:a1 (08:00:27:08:db:a1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

192.168.49.101 is neither a field nor a protocol name.

Pacchetti: 4194 - visualizzati: 4194 (100.0%) Profilo: Default

VERSION DETECTION

```
(lucas@kali)-[~]
$ sudo nmap -sV 192.168.49.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 20:56 CEST
Nmap scan report for 192.168.49.101
Host is up (0.044s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:B1:AA:58 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CP
E: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.90 seconds

(lucas@kali)-[~]
$
```

Report essenziale per identificare dati sensibili:

Nmap 7.93 scan initiated Tue May 2 21:36:37 2023 as: nmap -sV -oN report2 192.168.49.101

Nmap scan report for 192.168.49.101

Host is up (0.65s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

53/tcp open domain ISC BIND 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login?

514/tcp open shell Netkit rshd

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open vnc VNC (protocol 3.3)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

Service Info: Hosts: [metasploitable.localdomain](#), [irc.Metasploitable.LAN](#); OSs: [Unix, Linux](#); CPE: [cpe:/o:linux:linux_kernel](#)

Nmap done at Tue May 2 21:37:48 2023 -- 1 IP address (1 host up) scanned in 71.30 seconds

ABBIAMO IP, PORTE APERTE SERVIZI IN CUI POSSIAMO TENTARE DELLE VULNERABILITA CON DEGLI EXPLOIT TIPO SAMBA, APACHE ECC., E POSSIAMO VEDERE IL SISTEMA OPERATIVO CON LE VERSIONI ATTUALI.