


A decorative graphic in the top-left corner consisting of two overlapping parallelograms. The front one is blue and the back one is light green. They are set against a dark navy blue background with faint, lighter blue diagonal stripes.


Consegna S5L3



```
(root@kali)-[/home/kali/Desktop]
# nmap -O 192.168.32.102 --script smb-os-discovery
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 04:59 EST
Nmap scan report for 192.168.32.102
Host is up (0.00026s 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  microsoftsmb
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:B9:10:DA (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
```


```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-12-20T05:00:11-05:00
```

```
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.08 seconds
```




```
(root@kali)-[/home/kali/Desktop]
# nmap -sS 192.168.32.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 05:49 EST
Nmap scan report for 192.168.32.102
Host is up (0.000086s 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:B9:10:DA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```



```
(root@kali)-[/home/kali/Desktop]
# nmap -sT 192.168.32.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 04:44 EST
Nmap scan report for 192.168.32.102
Host is up (0.00052s 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:B9:10:DA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
```



(root@kali)-[/home/kali/Desktop]

# nmap -sV 192.168.32.102

Starting Nmap 7.94 ( <https://nmap.org> ) at 2023-12-20 04:46 EST

Nmap scan report for 192.168.32.102

Host is up (0.000089s 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:B9:10:DA (Oracle VirtualBox virtual NIC)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: 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 24.62 seconds

**(root@kali)~[/home/kali/Desktop]**

**# nmap -O 192.168.32.101**

Starting Nmap 7.94 ( <https://nmap.org> ) at 2023-12-20 04:50 EST

Nmap scan report for 192.168.32.101

Host is up (0.00037s latency).

All 1000 scanned ports on 192.168.32.101 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:37:08:76 (Oracle VirtualBox virtual NIC)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: specialized|VoIP phone|general purpose|phone

Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XPL2012, Palmmicro embedded, VMware Player

OS CPE: cpe:/h:allen-bradley:micrologix\_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows\_7 cpe:/o:microsoft:windows\_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows\_xp::sp3 cpe:/o:microsoft:windows\_server\_2012 cpe:/a:vmware:player

OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server

2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device

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 36.37 seconds

**(root@kali)~[/home/kali/Desktop]**

**# nmap -sT 192.168.32.101**

Starting Nmap 7.94 ( <https://nmap.org> ) at 2023-12-20 04:52 EST

Nmap scan report for 192.168.32.101

Host is up (0.00026s latency).

All 1000 scanned ports on 192.168.32.101 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:37:08:76 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 36.38 seconds

**(root@kali)~[/home/kali/Desktop]**

**# nmap -sS 192.168.32.101**

Starting Nmap 7.94 ( <https://nmap.org> ) at 2023-12-20 04:54 EST

Nmap scan report for 192.168.32.101

Host is up (0.00030s latency).

All 1000 scanned ports on 192.168.32.101 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:37:08:76 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 36.02 seconds

# Conclusioni

Macchina Kali Ip: 192.168.32.100

Macchina Metasploitable Ip: 192.168.32.102

Porte aperte:

21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

Macchina Windows 7 Ip: 192.168.32.101

Come possiamo notare su Windows 7 non troviamo porte aperte perché non ci sono regole sul Firewall che permettano il passaggio dei pacchetti tcp/udp

Scansioni effettuate su Meta:

Os fingerprint, Syn Scan, TCP connect, Version detection

La differenza tra syn e TCP è che la prima è di tipo Reset quindi si ferma al SYN-ACK mandando poi un reset per non

lasciare tracce, la seconda è conn-refused perché il Three-Way-Handshake non va a buon fine per via delle regole del firewall

Scansioni a windows 7:

Os fingerprint , Apertura TCP/UDP nelle regole firewall in entrata, Apertura TCP/UDP nelle regole firewall in uscita