

¿Cuál es la dirección IP de tu Metasploitable2? ¿Te aparece al hacer escaneo con nmap?

ip: 10.0.0.66, si te aparece activo.

¿Qué significa el parámetro -sn en Nmap?

Hará ping y nos dará un listado de los ordenadores que están activos.

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:9a:6a:dc  
          inet addr:10.0.0.66 Bcast:10.0.0.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe9a:6adc/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:3228 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:61 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:217330 (212.2 KB) TX bytes:6662 (6.5 KB)  
            Base address:0xd020 Memory:f0200000-f0220000  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING MTU:16436 Metric:1  
            RX packets:119 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:119 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:31933 (31.1 KB) TX bytes:31933 (31.1 KB)  
  
msfadmin@metasploitable:~$ _  
  
-d[level]: Set or increase debugging level (Up to 9 is meaningful)  
--open: Only show open (or possibly open) ports  
--packet-trace: Show all packets sent and received  
--iflist: Print host interfaces and routes (for debugging)  
--log-errors: Log errors/warnings to the normal-format output file  
--append-output: Append to rather than clobber specified output files  
--resume <filename>: Resume an aborted scan  
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML  
--webxml: Reference stylesheet from Insecure.Org for more portable XML  
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output  
MISC:  
-6: Enable IPv6 scanning  
-A: Enables OS detection and Version detection, Script scanning and Traceroute  
--datadir <dirname>: Specify custom Nmap data file location  
--send-eth/--send-ip: Send using raw ethernet frames or IP packets  
--privileged: Assume that the user is fully privileged  
--unprivileged: Assume the user lacks raw socket privileges  
-V: Print version number  
-h: Print this help summary page.  
EXAMPLES:  
nmap -v -A scanme.nmap.org  
nmap -v -sP 192.168.0.0/16 10.0.0.0/8  
nmap -v -iR 10000 -PN -p 80  
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES  
msfadmin@metasploitable:~$
```

¿Qué indican los tiempos de respuesta obtenidos? ¿Qué información puedes deducir sobre la conectividad entre tu máquina y Metasploitable?

Indican el tiempo que tardan los paquetes en ir a la dirección ip dada y regresar.

Como todos los paquetes que envía el ping han llegado, significa que he configurado bien Metasploitable

```
Session Actions Edit View Help
└─(kali㉿kali)-[~]
$ ping 10.0.0.66
PING 10.0.0.66 (10.0.0.66) 56(84) bytes of data.
64 bytes from 10.0.0.66: icmp_seq=1 ttl=255 time=2.87 ms
64 bytes from 10.0.0.66: icmp_seq=2 ttl=255 time=1.63 ms
64 bytes from 10.0.0.66: icmp_seq=3 ttl=255 time=1.49 ms
64 bytes from 10.0.0.66: icmp_seq=4 ttl=255 time=1.53 ms
64 bytes from 10.0.0.66: icmp_seq=5 ttl=255 time=1.45 ms
64 bytes from 10.0.0.66: icmp_seq=6 ttl=255 time=1.43 ms
64 bytes from 10.0.0.66: icmp_seq=7 ttl=255 time=1.39 ms
^C
--- 10.0.0.66 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6024ms
rtt min/avg/max/mdev = 1.390/1.683/2.868/0.488 ms

└─(kali㉿kali)-[~]
$
```

¿Cuántos puertos están abiertos en el escaneo básico? ¿Qué servicios identifica Nmap automáticamente?

23 puertos abiertos

Servicios:

- *HTTP: Identifica servidores web y sus versiones.*
- *FTP: Detecta servidores de transferencia de archivos y sus configuraciones.*
- *SSH: Reconoce servicios de acceso remoto seguro y sus versiones.*
- *SMTP: Identifica servidores de correo electrónico y sus configuraciones.*
- *DNS: Detecta servidores de nombres de dominio y sus versiones.*
- *RPC: Utiliza la herramienta de pruebas RPC para determinar programas y versiones si se descubren servicios.*
- *Telnet: Reconoce servicios de terminal remota.*

```
7 packets transmitted, 7 received, 0% packet loss, time 6024ms
rtt min/avg/max/mdev = 1.390/1.683/2.868/0.488 ms

└─(kali㉿kali)-[~]
$ nmap 10.0.0.66
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-03 06:18 EDT
Nmap scan report for 10.0.0.66
Host is up (0.0046s latency).
Not shown: 977 filtered tcp ports (no-response)
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 5.41 seconds
```

¿Cuál de los tres comandos ejecutó más rápido? ¿Por qué crees que es así? En el escaneo de puertos 1-100, ¿cuántos puertos abiertos encontraste comparado con el escaneo completo del ejercicio 3? ¿Por qué crees que es útil poder escanear rangos específicos de puertos?

nmap -p 80,443,8080,8443 [ip], ejecutó el escaneo más rápido porque escanea unos puertos específicos.

Se encontraron 6 puertos comparado a los 23 puertos encontrados en el escaneo completo.

Es útil si sabes que puertos estas buscando y no te interesa que salgan todos

```
(kali㉿kali)-[~]
└─$ nmap -p 1-100 10.0.0.66
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-03 06:19 EDT
Nmap scan report for 10.0.0.66
Host is up (0.0032s latency).
Not shown: 94 filtered tcp ports (no-response)
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

Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds

(kali㉿kali)-[~]
└─$ nmap -p 80,443,8080,8443 10.0.0.66
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-03 06:20 EDT
Nmap scan report for 10.0.0.66
Host is up (0.00078s latency).

PORT      STATE      SERVICE
80/tcp    open       http
443/tcp   filtered  https
8080/tcp  filtered  http-proxy
8443/tcp  filtered  https-alt

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

¿Qué sistema operativo ejecuta Metasploitable2? Lista los 10 servicios principales con sus versiones exactas

SO: Unix, Linux

Servicios:

FTP - vsftpd 2.3.4

SSH - OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

Telnet - Linux telnetd

SMTP - Postfix smtpd

DNS - ISC BIND 9.4.2

HTTP - Apache httpd 2.2.8 ((Ubuntu) DAV/2)

NetBIOS-SSN - Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Bind Shell - Metasploitable root shell

MySQL - MySQL 5.0.51a-3ubuntu5

PostgreSQL - PostgreSQL DB 8.3.0 - 8.3.7

```
(kali㉿kali)-[~]
└─$ nmap -sV -O 10.0.0.66
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-03 06:21 EDT
Nmap scan report for 10.0.0.66
Host is up (0.001s latency).
Not shown: 977 filtered tcp ports (no-response)
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  tcpwrapped
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 22.69 seconds
```

```
(kali㉿kali)-[~]
└─$ nmap -sV 10.0.0.66
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-03 06:22 EDT
Nmap scan report for 10.0.0.66
Host is up (0.0020s latency).
Not shown: 977 filtered tcp ports (no-response)
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 10.0.0.206
|     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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6:c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3:d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-date: 2025-10-01T07:41:16+00:00; -2d02h42m33s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VR
FY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OC
SA/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
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:
```

```

| ssl-cert: Subject: commonName=ubuntu804-base.locldomain/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
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
| 100003 2,3,4 2049/tcp nfs
|_ 100003 2,3,4 2049/udp nfs
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 tcpwrapped
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
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 12
| Capabilities flags: 43564
| Some Capabilities: LongColumnFlag, Support41Auth, Speaks41ProtocolNew,
SupportsTransactions, SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsCompression
| Status: Autocommit
|_ Salt: "L8s[P\_G.Mz?k~VqYJ
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-10-01T07:41:16+00:00; -2d02h42m33s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.locldomain/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
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd (Admin email admin@Metasploitable.LAN)
| irc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd (Admin email admin@Metasploitable.LAN)
| irc-info:
| users: 1
| servers: 1
| lusers: 1
| lservers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 0 days, 0:33:42
| source ident: nmap
| source host: 311F67B4.D3975B40.7B559A54.IP
|_ error: Closing Link: njonosnat[10.0.0.206] (Quit: njonosnat)
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
Service Info: Host: metasploitable.locldomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -2d01h42m32s, deviation: 2h00m00s, median: -2d02h42m33s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS M
AC: <unknown> (unknown)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: locldomain
| FQDN: metasploitable.locldomain
| System time: 2025-10-01T03:40:37-04:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.42 seconds

```

¿Qué servicios aparecen en ejecución en la máquina Metasploitable según la salida? ¿Qué versiones identifica nmap para al menos dos de esos servicios? ¿Hay algún servicio que muestre advertencias o mensajes de seguridad en la salida de los scripts? ¿Cuál y qué significa?

Solo aparece el servicio de DHCP (UDP) y no sale su versión.

Advertencias:

hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See <https://www.robtex.com/api/>

http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See <https://www.robtex.com/api/>

Significado: Los scripts de nmap que consultan la API de Robtex están deshabilitados temporalmente porque la API de Robtex cambió. nmap no pudo usar esas comprobaciones externas, por lo que faltará la información que esos scripts habrían aportado.

```
(kali㉿kali)-[~]
$ nmap -sV --script=default,safe 10.0.0.66
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-03 06:27 EDT
No profinet devices in the subnet
Pre-scan script results:
|_ hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_ http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
| broadcast-listener:
|_ udp
|   DHCP
|     srv ip      cli ip      mask          gw          dns
|     vendor
|_ 10.0.2.2  10.0.2.16  255.255.255.0  10.0.2.2  192.168.0.253, 8.8.8.8
|_ multicast-profinet-discovery: 0
|_ eap-info: please specify an interface with -e
| broadcast-dhcp-discover:
| Response 1 of 1:
|   Interface: eth0
|   IP Offered: 10.0.2.16
|   Server Identifier: 10.0.2.2
|   Subnet Mask: 255.255.255.0
|   Router: 10.0.2.2
|   Domain Name Server: 192.168.0.253, 8.8.8.8
|_ Domain Name: CALASANZSALAMANCA.local
```

Selecciona una de las vulnerabilidades que hayas visto, y busca su código CVE en google.

MySQL < 5.6.35 / < 5.7.17 - Integer Overflow

CVE asociada: CVE-2017-3599

Qué hace la vulnerabilidad:

- *Es un integer overflow en el parseo del handshake/conexión del servidor MySQL que puede desencadenar un buffer overflow y provocar que mysqld se cuelgue o crashee. La explotación puede realizarse de forma remota y sin autenticación.*

```
(kali㉿kali)-[~]
$ searchsploit mysql MySQL 5.0.51

-----
```

Exploit Title	Path
MySQL < 5.6.35 / < 5.7.17 - Integer Over	multiple/dos/41954.py
MySQL < 5.6.35 / < 5.7.17 - Integer Over	multiple/dos/41954.py
Oracle MySQL < 5.1.49 - 'DDL' Statements	linux/dos/34522.txt
Oracle MySQL < 5.1.49 - 'WITH ROLLUP' De	multiple/dos/15467.txt
Oracle MySQL < 5.1.49 - Malformed 'BINLO	linux/dos/34521.txt
Oracle MySQL < 5.1.50 - Privilege Escala	multiple/remote/34796.txt

```
-----
```

Shellcodes: No Results