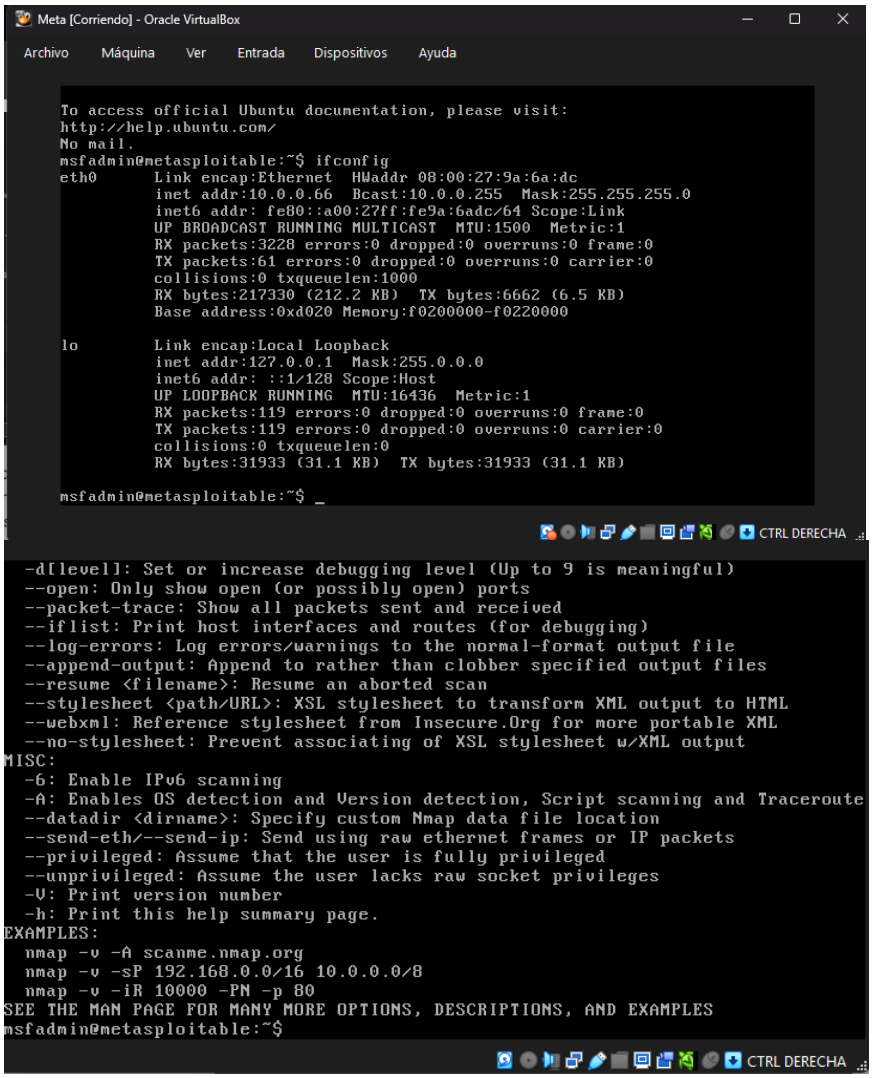
¿Cuál es la dirección IP de tu Metasploitable2? ¿Te aparece al hacer escaneo con nmap?

ip: 10.0.0.66, si te aparece activo.

¿Qué significa el parámetro -sn en Nmap?

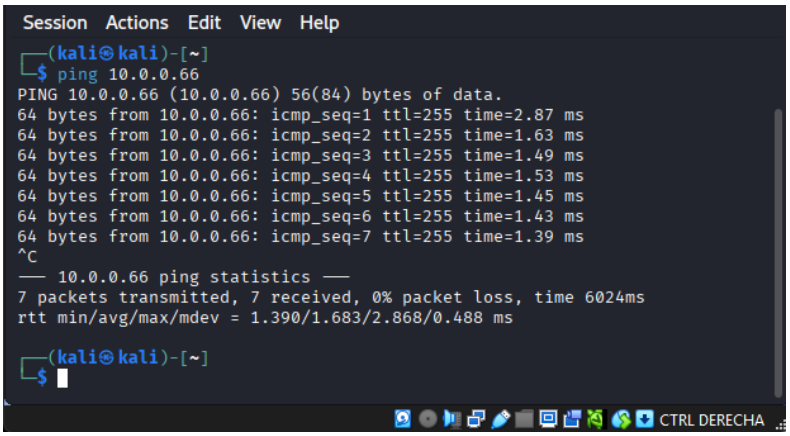
Hará ping y nos dará un listado de los ordenadores que están activos.



¿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



¿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.*

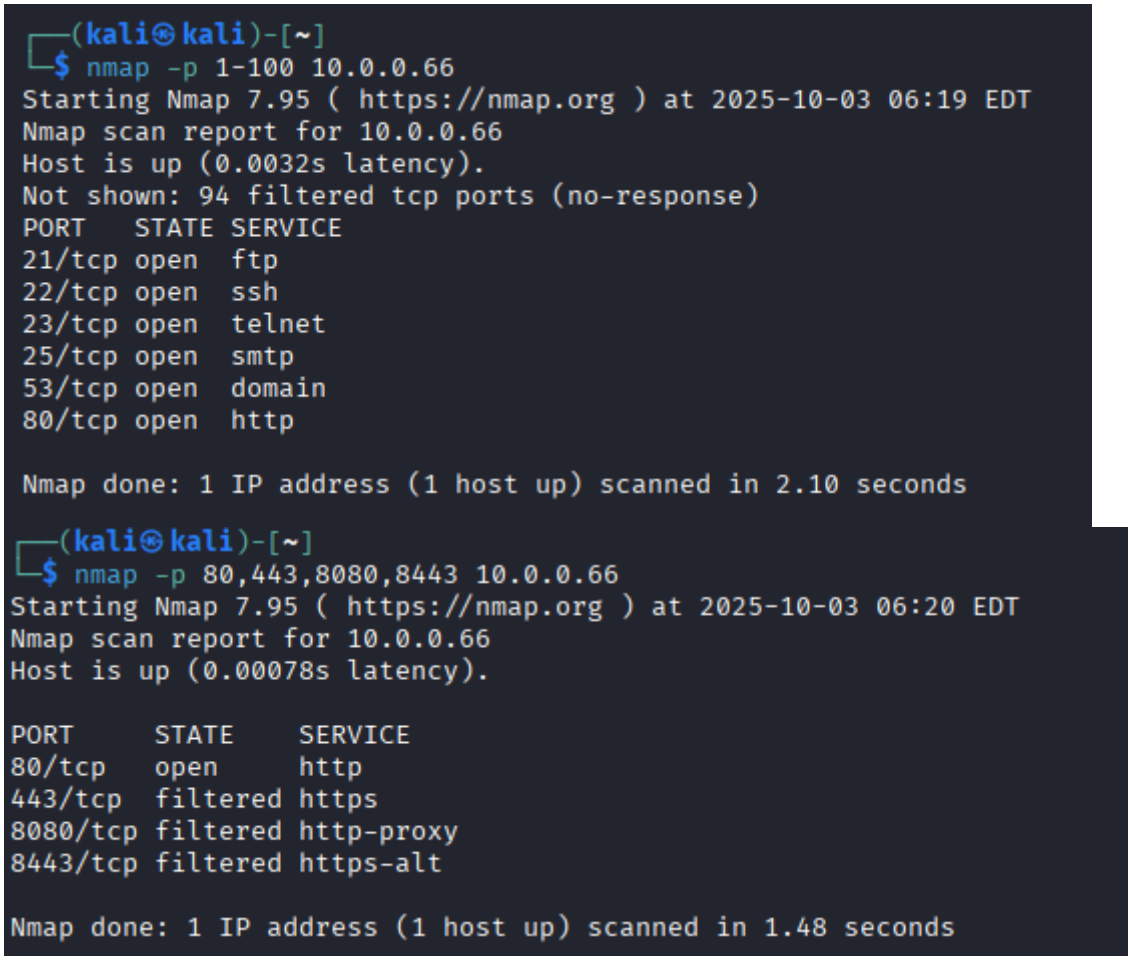
```
7 packets transmitted, 7 received, 0% packet loss, time 6024ms
rtt min/avg/max/mdev = 1.390/1.683/2.868/0.488 ms

┌──(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*



¿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

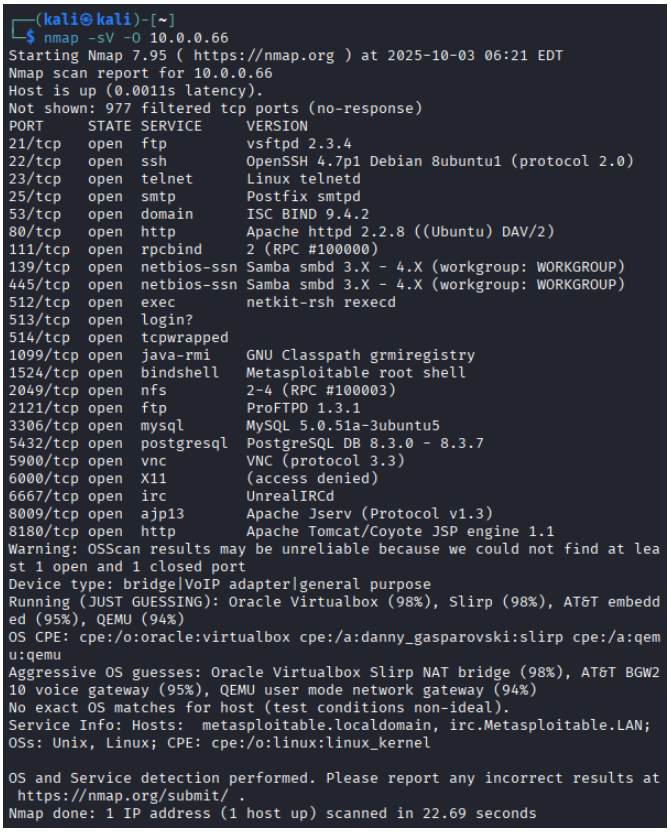
HTTP - Apache httpd 2.2.8 ((Ubuntu) DAV/2)

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

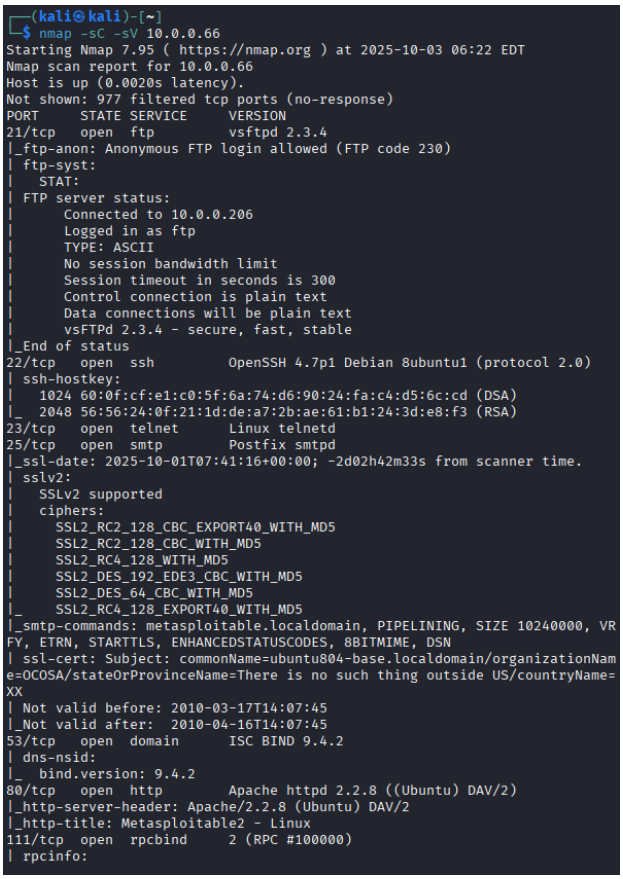
Bind Shell - Metasploitable root shell

MySQL - MySQL 5.0.51a-3ubuntu5

P*ostgreSQL - 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 (0.0011s 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 lea
st 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedd
ed (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qem
u:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW2
10 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 -sC -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:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d: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/organizationNam
e=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:
```

```
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationNam
e=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, Sup
portsCompression
|   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.localdomain/organizationNam
e=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.LA
N)
| 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.LA
N)
| 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.localdomain; OSs: Unix, Linux; CPE: cp
e:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -2d01h42m32s, deviation: 2h00m00s, median: -2d02h42m33
s
|_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: localdomain
|   FQDN: metasploitable.localdomain
|_  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. S
ee 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.*