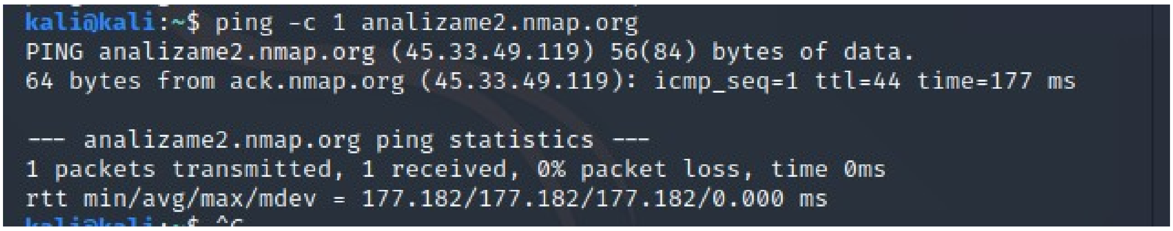
## TAREA 8 NMAP

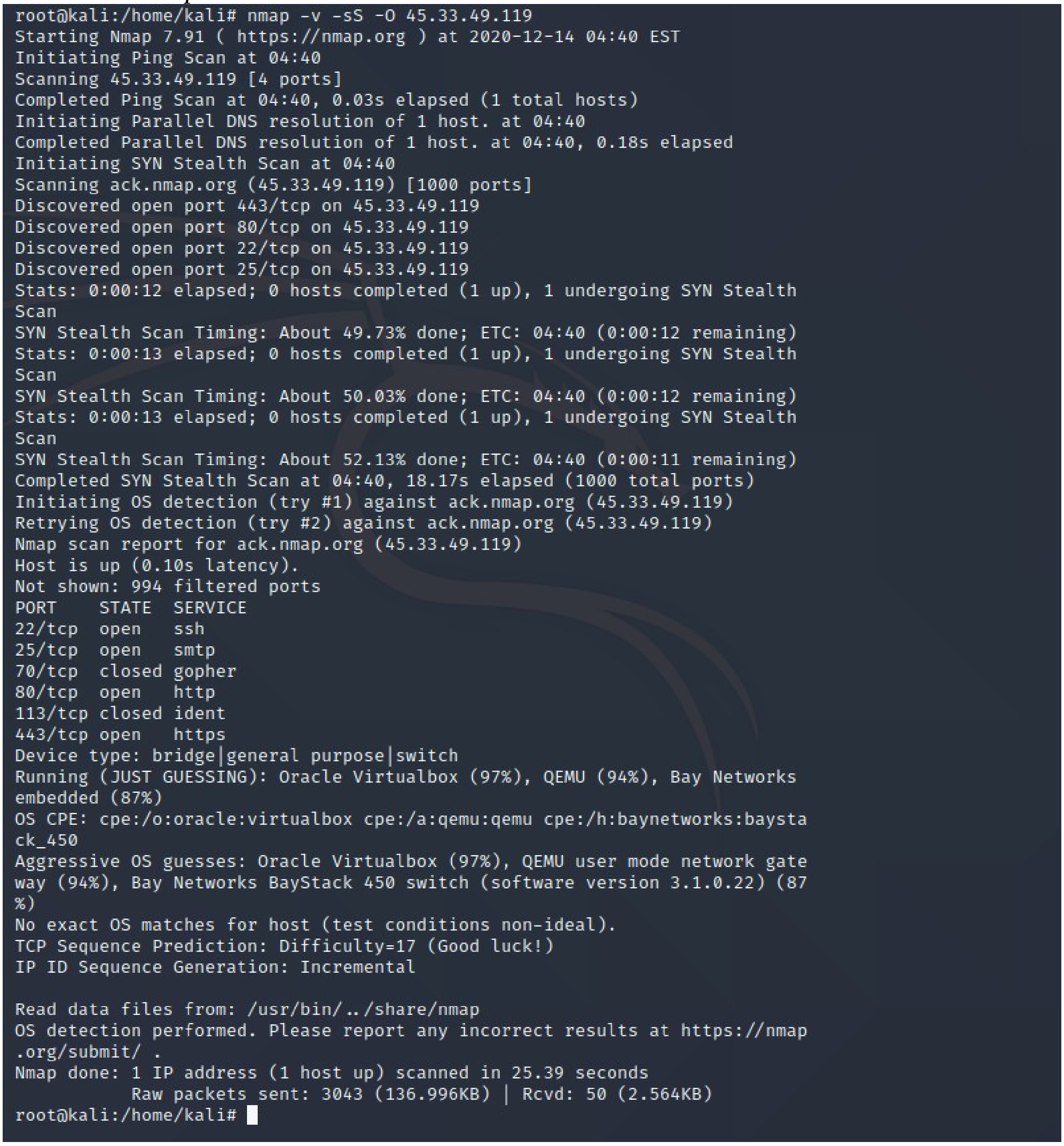
### 1. Anota las direcciones IP tres de sus vecinos y teclear “nmap -v -sS -O X.Y.Z.W” (X:Y.Z.W = una de las direcciones de arriba). Interprete la salida y anota puertos, servicios y sistema operativo.

Voy a usar la página web que hay en los apuntes: *analizame2.nmap.org*
Al usar esta pagina web necesito extraerle la dirección Ip.



```
kali@kali:~$ ping -c 1 analizame2.nmap.org
PING analizame2.nmap.org (45.33.49.119) 56(84) bytes of data.
64 bytes from ack.nmap.org (45.33.49.119): icmp_seq=1 ttl=44 time=177 ms

--- analizame2.nmap.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 177.182/177.182/177.182/0.000 ms
```

Y me sale 45.33.49.119
Usamos *“nmap -v -sS -O 45.33.49.119”*



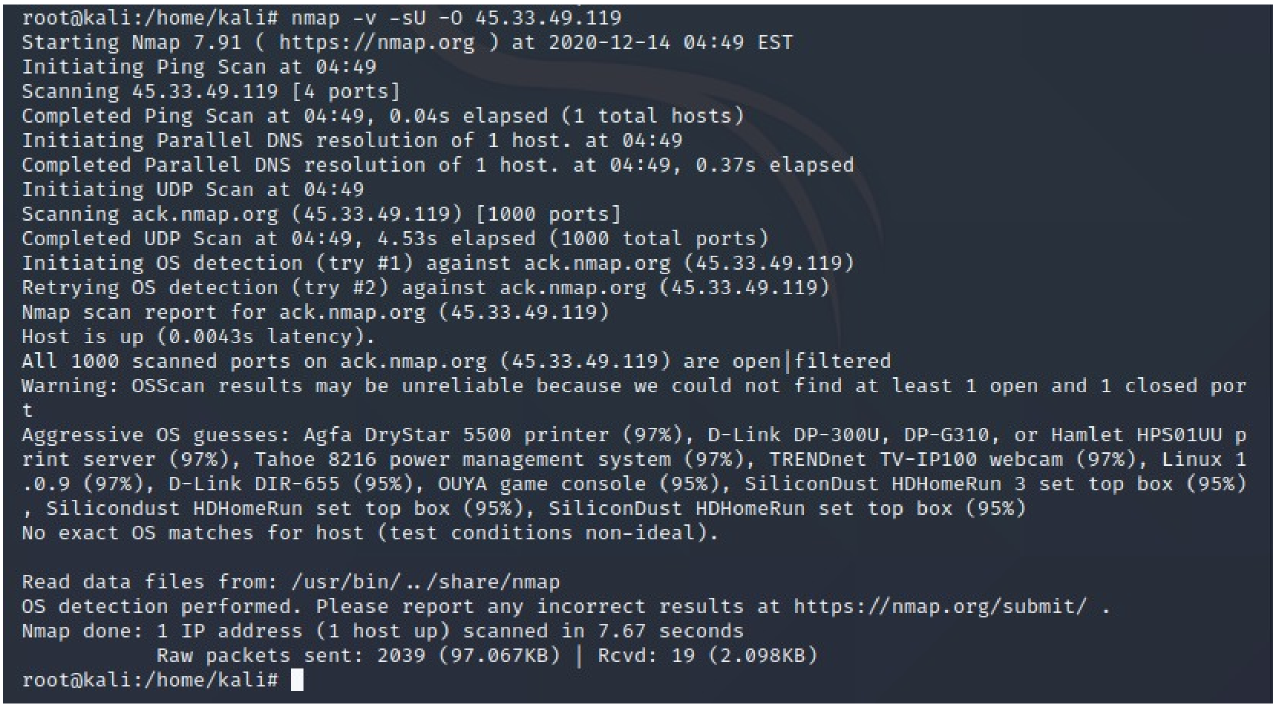
```
root@kali:/home/kali# nmap -v -sS -O 45.33.49.119
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-14 04:40 EST
Initiating Ping Scan at 04:40
Scanning 45.33.49.119 [4 ports]
Completed Ping Scan at 04:40, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:40
Completed Parallel DNS resolution of 1 host. at 04:40, 0.18s elapsed
Initiating SYN Stealth Scan at 04:40
Scanning ack.nmap.org (45.33.49.119) [1000 ports]
Discovered open port 443/tcp on 45.33.49.119
Discovered open port 80/tcp on 45.33.49.119
Discovered open port 22/tcp on 45.33.49.119
Discovered open port 25/tcp on 45.33.49.119
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 49.73% done; ETC: 04:40 (0:00:12 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 50.03% done; ETC: 04:40 (0:00:12 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 52.13% done; ETC: 04:40 (0:00:11 remaining)
Completed SYN Stealth Scan at 04:40, 18.17s elapsed (1000 total ports)
Initiating OS detection (try #1) against ack.nmap.org (45.33.49.119)
Retrying OS detection (try #2) against ack.nmap.org (45.33.49.119)
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.10s latency).
Not shown: 994 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
25/tcp  open   smtp
70/tcp  closed gopher
80/tcp  open   http
113/tcp closed ident
443/tcp open   https
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (94%), Bay Networks
embedded (87%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baysta
ck_450
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gate
way (94%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (87
%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.39 seconds
           Raw packets sent: 3043 (136.996KB) | Rcvd: 50 (2.564KB)
root@kali:/home/kali# 
```

Vemos que los ports y sus servicios abiertos son los siguientes:

| *PORT* | *STATE* | *SERVICE* |
|---|---|---|
| 22/tcp | open | ssh |
| 25/tcp | open | smtp |
| 70/tcp | closed | gopher |
| 80/tcp | open | http |
| 113/tcp | closed | ident |
| 443/tcp | open | https |

**2. En la línea de comandos teclear: “nmap -v -sU -O X.Y.Z.W”. Interprete la salida y anota puertos, servicios y sistema operativo.**

Escribimos *“nmap -v -sU -O 45.33.49.119”:*

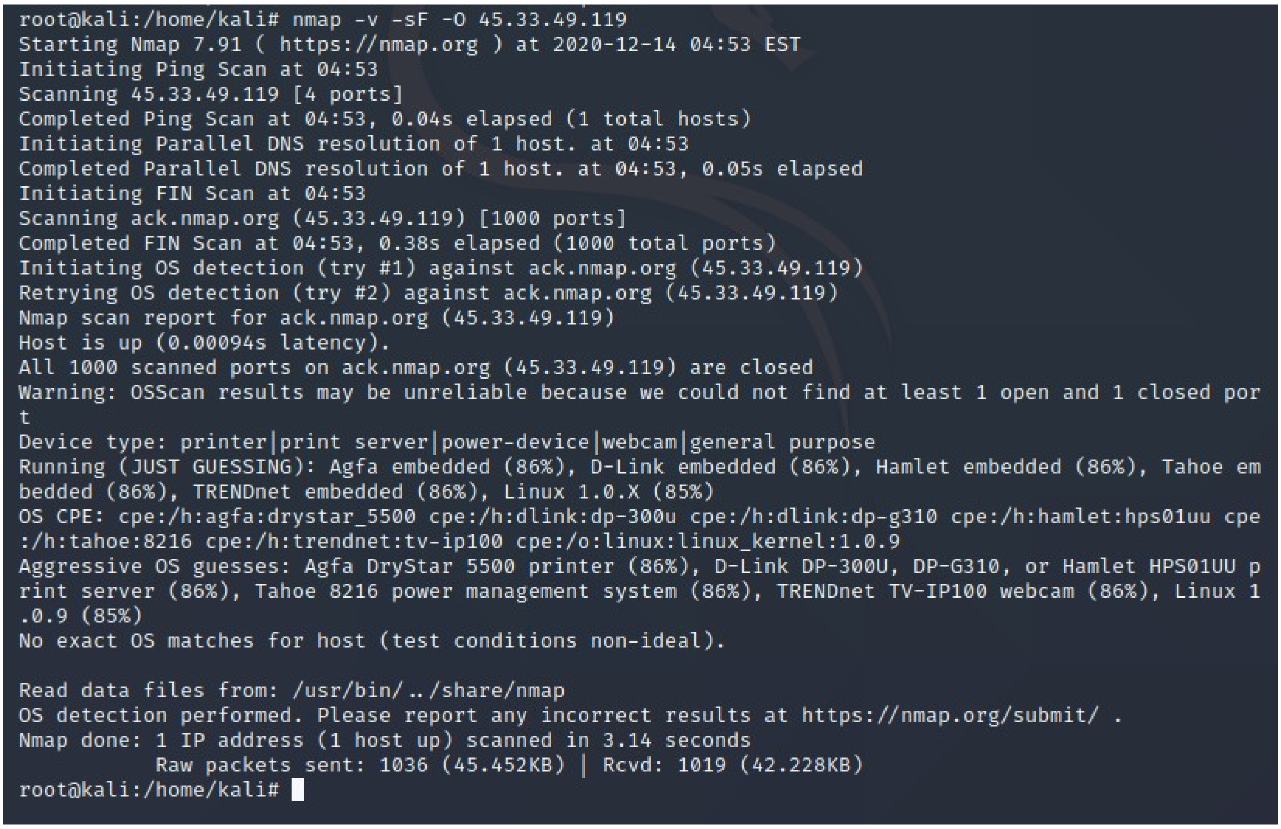


```
root@kali:/home/kali# nmap -v -sU -O 45.33.49.119
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-14 04:49 EST
Initiating Ping Scan at 04:49
Scanning 45.33.49.119 [4 ports]
Completed Ping Scan at 04:49, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:49
Completed Parallel DNS resolution of 1 host. at 04:49, 0.37s elapsed
Initiating UDP Scan at 04:49
Scanning ack.nmap.org (45.33.49.119) [1000 ports]
Completed UDP Scan at 04:49, 4.53s elapsed (1000 total ports)
Initiating OS detection (try #1) against ack.nmap.org (45.33.49.119)
Retrying OS detection (try #2) against ack.nmap.org (45.33.49.119)
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.0043s latency).
All 1000 scanned ports on ack.nmap.org (45.33.49.119) are open|filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
t
Aggressive OS guesses: Agfa DryStar 5500 printer (97%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU p
rint server (97%), Tahoe 8216 power management system (97%), TRENDnet TV-IP100 webcam (97%), Linux 1
.0.9 (97%), D-Link DIR-655 (95%), OUYA game console (95%), SiliconDust HDHomeRun 3 set top box (95%)
, Silicondust HDHomeRun set top box (95%), SiliconDust HDHomeRun set top box (95%)
No exact OS matches for host (test conditions non-ideal).

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.67 seconds
           Raw packets sent: 2039 (97.067KB) | Rcvd: 19 (2.098KB)
root@kali:/home/kali# 
```

No encontramos respuesta del servidor.

**3. En la línea de comandos teclear “nmap -v -sF -O X.Y.Z.W”. Interpretar la salida y diga cual es la diferencia con los comandos tecleados en los puntos uno y dos:**

Usamos *“nmap -v -sF -O 45.33.49.119”*:

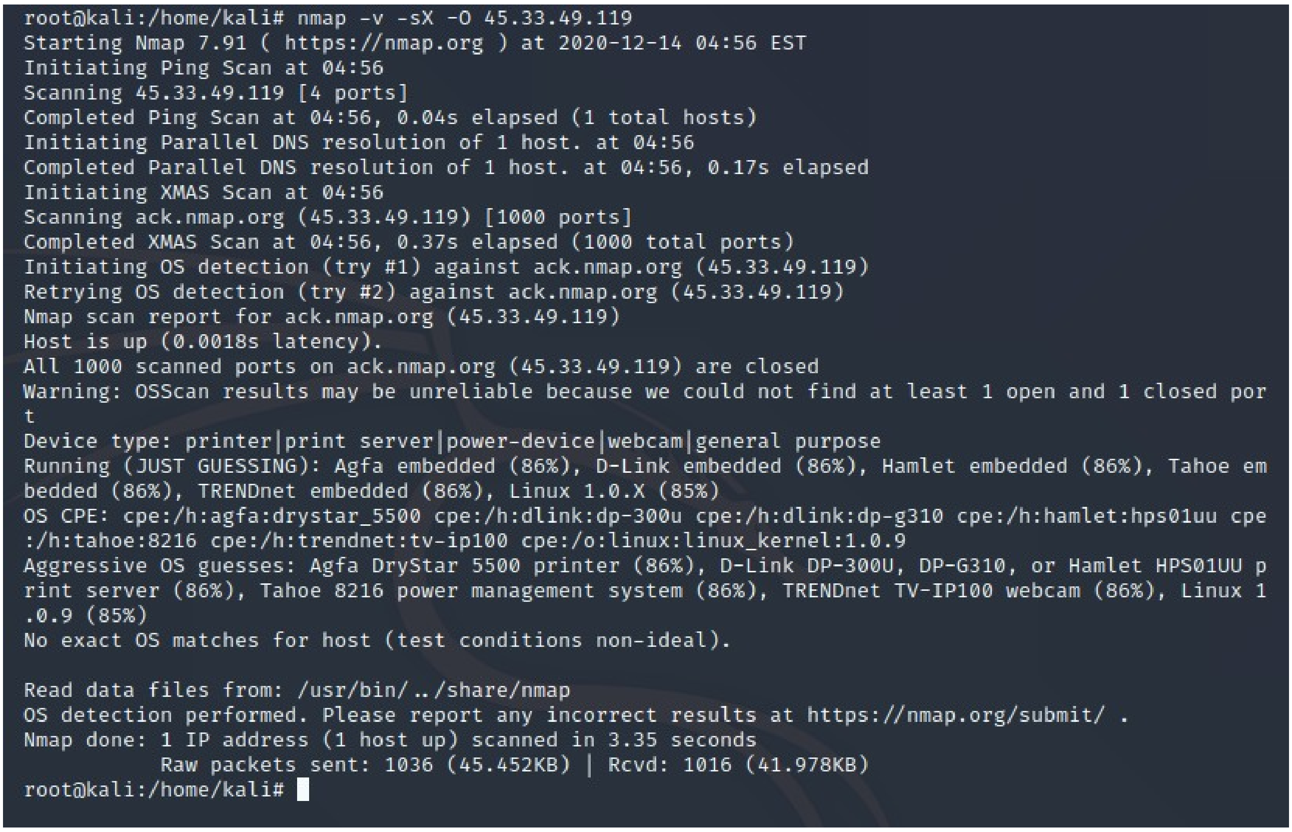


```
root@kali:/home/kali# nmap -v -sF -O 45.33.49.119
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-14 04:53 EST
Initiating Ping Scan at 04:53
Scanning 45.33.49.119 [4 ports]
Completed Ping Scan at 04:53, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:53
Completed Parallel DNS resolution of 1 host. at 04:53, 0.05s elapsed
Initiating FIN Scan at 04:53
Scanning ack.nmap.org (45.33.49.119) [1000 ports]
Completed FIN Scan at 04:53, 0.38s elapsed (1000 total ports)
Initiating OS detection (try #1) against ack.nmap.org (45.33.49.119)
Retrying OS detection (try #2) against ack.nmap.org (45.33.49.119)
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.00094s latency).
All 1000 scanned ports on ack.nmap.org (45.33.49.119) are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
t
Device type: printer|print server|power-device|webcam|general purpose
Running (JUST GUESSING): Agfa embedded (86%), D-Link embedded (86%), Hamlet embedded (86%), Tahoe em
bedded (86%), TRENDnet embedded (86%), Linux 1.0.X (85%)
OS CPE: cpe:/h:agfa:drystar_5500 cpe:/h:dlink:dp-300u cpe:/h:dlink:dp-g310 cpe:/h:hamlet:hps01uu cpe
:/h:tahoe:8216 cpe:/h:trendnet:tv-ip100 cpe:/o:linux:linux_kernel:1.0.9
Aggressive OS guesses: Agfa DryStar 5500 printer (86%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU p
rint server (86%), Tahoe 8216 power management system (86%), TRENDnet TV-IP100 webcam (86%), Linux 1
.0.9 (85%)
No exact OS matches for host (test conditions non-ideal).

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.14 seconds
           Raw packets sent: 1036 (45.452KB) | Rcvd: 1019 (42.228KB)
root@kali:/home/kali# 
```

No encontramos respuesta del servidor.

### 4. En la línea de comandos tecelar: “nmap -v -sX -O X.Y.Z.W”

Usamos *“nmap -v -sX -O 45.33.49.119”*



```
root@kali:/home/kali# nmap -v -sX -O 45.33.49.119
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-14 04:56 EST
Initiating Ping Scan at 04:56
Scanning 45.33.49.119 [4 ports]
Completed Ping Scan at 04:56, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:56
Completed Parallel DNS resolution of 1 host. at 04:56, 0.17s elapsed
Initiating XMAS Scan at 04:56
Scanning ack.nmap.org (45.33.49.119) [1000 ports]
Completed XMAS Scan at 04:56, 0.37s elapsed (1000 total ports)
Initiating OS detection (try #1) against ack.nmap.org (45.33.49.119)
Retrying OS detection (try #2) against ack.nmap.org (45.33.49.119)
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.0018s latency).
All 1000 scanned ports on ack.nmap.org (45.33.49.119) are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
t
Device type: printer|print server|power-device|webcam|general purpose
Running (JUST GUESSING): Agfa embedded (86%), D-Link embedded (86%), Hamlet embedded (86%), Tahoe em
bedded (86%), TRENDnet embedded (86%), Linux 1.0.X (85%)
OS CPE: cpe:/h:agfa:drystar_5500 cpe:/h:dlink:dp-300u cpe:/h:dlink:dp-g310 cpe:/h:hamlet:hps01uu cpe
:/h:tahoe:8216 cpe:/h:trendnet:tv-ip100 cpe:/o:linux:linux_kernel:1.0.9
Aggressive OS guesses: Agfa DryStar 5500 printer (86%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU p
rint server (86%), Tahoe 8216 power management system (86%), TRENDnet TV-IP100 webcam (86%), Linux 1
.0.9 (85%)
No exact OS matches for host (test conditions non-ideal).

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.35 seconds
           Raw packets sent: 1036 (45.452KB) | Rcvd: 1016 (41.978KB)
root@kali:/home/kali# 
```

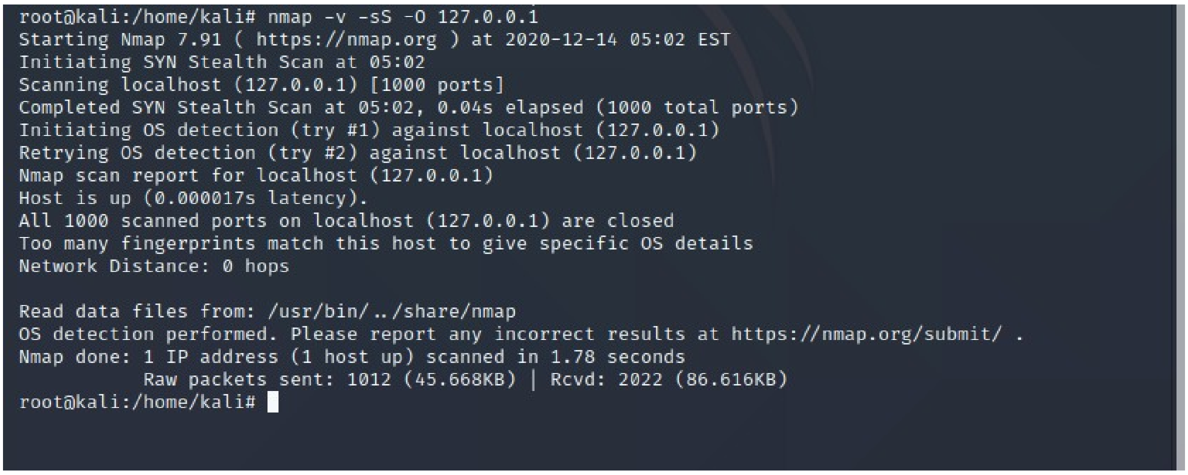
No encontramos respuesta del servidor

**5. Interpretar la salida y explica las diferencias con los comandos de los puntos anteriores:**

Depende del comando que usemos envía una respuesta o otra muy diferente y dependiendo de esa repuesta; nmap detecta los servicios y los ports del servidor.

**6. Ejecute nmap sobre su misma máquina (Linux) “nmap -v -sS -O 127.0.0.1” y escriba los servicios (no los puertos) que tiene arriba. Cierre uno de los servicios anteriores. Para cerrar un servicio en Linux**

Usamos *“nmap -v -sS -O 127.0.0.1”*

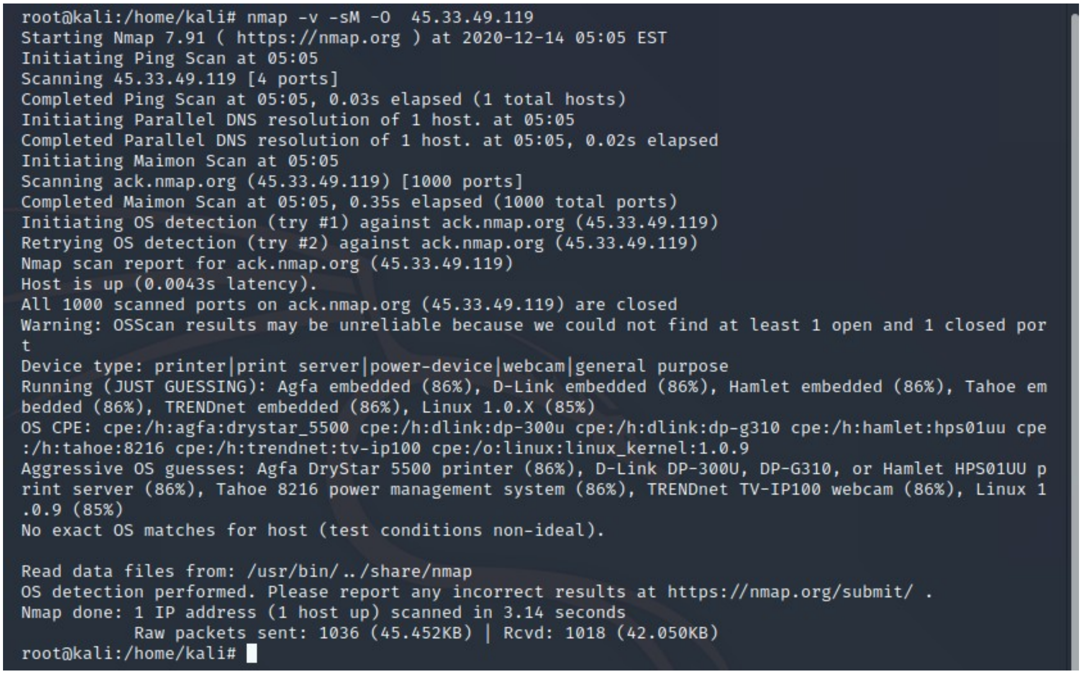


```
root@kali:/home/kali# nmap -v -sS -O 127.0.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-14 05:02 EST
Initiating SYN Stealth Scan at 05:02
Scanning localhost (127.0.0.1) [1000 ports]
Completed SYN Stealth Scan at 05:02, 0.04s elapsed (1000 total ports)
Initiating OS detection (try #1) against localhost (127.0.0.1)
Retrying OS detection (try #2) against localhost (127.0.0.1)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000017s latency).
All 1000 scanned ports on localhost (127.0.0.1) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
           Raw packets sent: 1012 (45.668KB) | Rcvd: 2022 (86.616KB)
root@kali:/home/kali# 
```

No he podido encontrar respuesta del servidor otra vez.

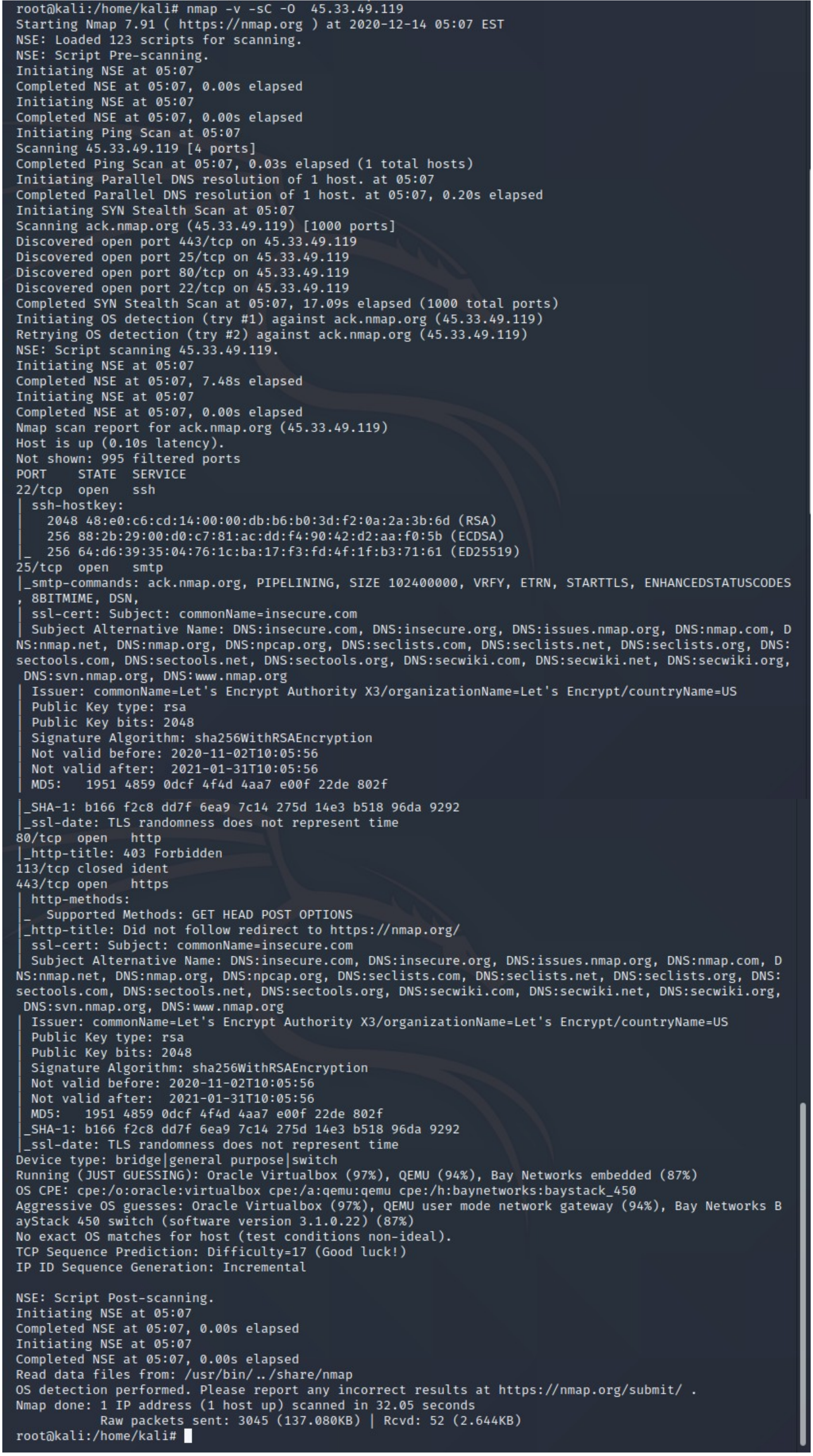
**7. Investiga tres pruebas además de las obtenidas aquí en las que realices búsquedas concretas y anota los resultados obtenidos. Interpreta los resultados y explica si has obtenido los resultados que esperabas:**

PRIMERA PRUEBA: *“nmap -v -sM -O  45.33.49.119”*:



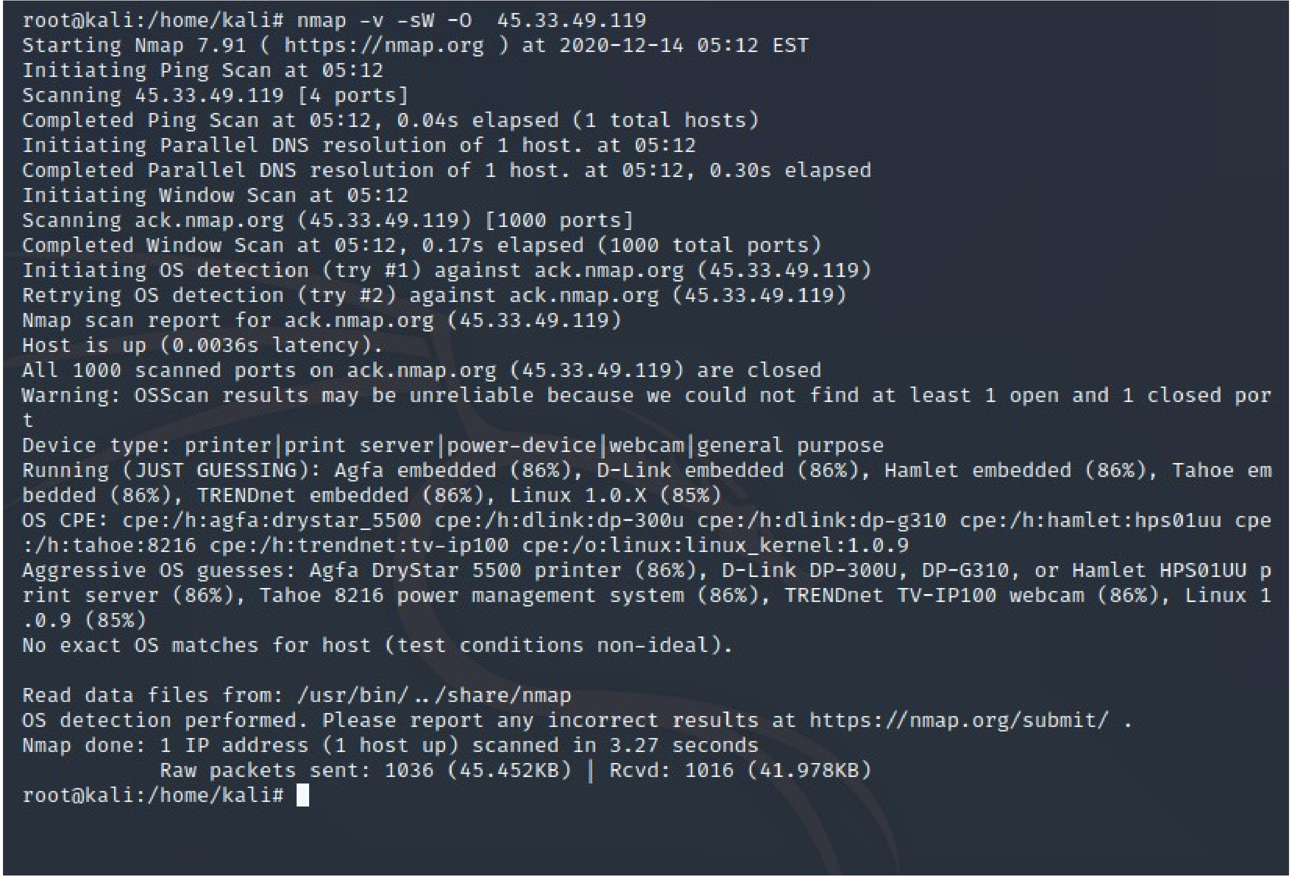
```
root@kali:/home/kali# nmap -v -sM -O  45.33.49.119
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-14 05:05 EST
Initiating Ping Scan at 05:05
Scanning 45.33.49.119 [4 ports]
Completed Ping Scan at 05:05, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:05
Completed Parallel DNS resolution of 1 host. at 05:05, 0.02s elapsed
Initiating Maimon Scan at 05:05
Scanning ack.nmap.org (45.33.49.119) [1000 ports]
Completed Maimon Scan at 05:05, 0.35s elapsed (1000 total ports)
Initiating OS detection (try #1) against ack.nmap.org (45.33.49.119)
Retrying OS detection (try #2) against ack.nmap.org (45.33.49.119)
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.0043s latency).
All 1000 scanned ports on ack.nmap.org (45.33.49.119) are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
t
Device type: printer|print server|power-device|webcam|general purpose
Running (JUST GUESSING): Agfa embedded (86%), D-Link embedded (86%), Hamlet embedded (86%), Tahoe em
bedded (86%), TRENDnet embedded (86%), Linux 1.0.X (85%)
OS CPE: cpe:/h:agfa:drystar_5500 cpe:/h:dlink:dp-300u cpe:/h:dlink:dp-g310 cpe:/h:hamlet:hps01uu cpe
:/h:tahoe:8216 cpe:/h:trendnet:tv-ip100 cpe:/o:linux:linux_kernel:1.0.9
Aggressive OS guesses: Agfa DryStar 5500 printer (86%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU p
rint server (86%), Tahoe 8216 power management system (86%), TRENDnet TV-IP100 webcam (86%), Linux 1
.0.9 (85%)
No exact OS matches for host (test conditions non-ideal).

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.14 seconds
           Raw packets sent: 1036 (45.452KB) | Rcvd: 1018 (42.050KB)
root@kali:/home/kali# 
```

SEGUNDA PRUEBA: *“nmap -v -sC -O  45.33.49.119”*:



```
root@kali:/home/kali# nmap -v -sC -O  45.33.49.119
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-14 05:07 EST
NSE: Loaded 123 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:07
Completed NSE at 05:07, 0.00s elapsed
Initiating NSE at 05:07
Completed NSE at 05:07, 0.00s elapsed
Initiating Ping Scan at 05:07
Scanning 45.33.49.119 [4 ports]
Completed Ping Scan at 05:07, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:07
Completed Parallel DNS resolution of 1 host. at 05:07, 0.20s elapsed
Initiating SYN Stealth Scan at 05:07
Scanning ack.nmap.org (45.33.49.119) [1000 ports]
Discovered open port 443/tcp on 45.33.49.119
Discovered open port 25/tcp on 45.33.49.119
Discovered open port 80/tcp on 45.33.49.119
Discovered open port 22/tcp on 45.33.49.119
Completed SYN Stealth Scan at 05:07, 17.09s elapsed (1000 total ports)
Initiating OS detection (try #1) against ack.nmap.org (45.33.49.119)
Retrying OS detection (try #2) against ack.nmap.org (45.33.49.119)
NSE: Script scanning 45.33.49.119.
Initiating NSE at 05:07
Completed NSE at 05:07, 7.48s elapsed
Initiating NSE at 05:07
Completed NSE at 05:07, 0.00s elapsed
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.10s latency).
Not shown: 995 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
| ssh-hostkey: 
|   2048 48:e0:c6:cd:14:00:00:db:b6:b0:3d:f2:0a:2a:3b:6d (RSA)
|   256 88:2b:29:00:d0:c7:81:ac:dd:f4:90:42:d2:aa:f0:5b (ECDSA)
|_  256 64:d6:39:35:04:76:1c:ba:17:f3:fd:4f:1f:b3:71:61 (ED25519)
25/tcp  open   smtp
|_smtp-commands: ack.nmap.org, PIPELINING, SIZE 102400000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES
, 8BITMIME, DSN, 
| ssl-cert: Subject: commonName=insecure.com
| Subject Alternative Name: DNS:insecure.com, DNS:insecure.org, DNS:issues.nmap.org, DNS:nmap.com, D
NS:nmap.net, DNS:nmap.org, DNS:npcap.org, DNS:seclists.com, DNS:seclists.net, DNS:seclists.org, DNS:
sectools.com, DNS:sectools.net, DNS:sectools.org, DNS:secwiki.com, DNS:secwiki.net, DNS:secwiki.org,
 DNS:svn.nmap.org, DNS:www.nmap.org
| Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-11-02T10:05:56
| Not valid after:  2021-01-31T10:05:56
| MD5:   1951 4859 0dcf 4f4d 4aa7 e00f 22de 802f
|_SHA-1: b166 f2c8 dd7f 6ea9 7c14 275d 14e3 b518 96da 9292
|_ssl-date: TLS randomness does not represent time
80/tcp  open   http
|_http-title: 403 Forbidden
113/tcp closed ident
443/tcp open   https
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://nmap.org/
| ssl-cert: Subject: commonName=insecure.com
| Subject Alternative Name: DNS:insecure.com, DNS:insecure.org, DNS:issues.nmap.org, DNS:nmap.com, D
NS:nmap.net, DNS:nmap.org, DNS:npcap.org, DNS:seclists.com, DNS:seclists.net, DNS:seclists.org, DNS:
sectools.com, DNS:sectools.net, DNS:sectools.org, DNS:secwiki.com, DNS:secwiki.net, DNS:secwiki.org,
 DNS:svn.nmap.org, DNS:www.nmap.org
| Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-11-02T10:05:56
| Not valid after:  2021-01-31T10:05:56
| MD5:   1951 4859 0dcf 4f4d 4aa7 e00f 22de 802f
|_SHA-1: b166 f2c8 dd7f 6ea9 7c14 275d 14e3 b518 96da 9292
|_ssl-date: TLS randomness does not represent time
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (94%), Bay Networks embedded (87%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (94%), Bay Networks B
ayStack 450 switch (software version 3.1.0.22) (87%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

NSE: Script Post-scanning.
Initiating NSE at 05:07
Completed NSE at 05:07, 0.00s elapsed
Initiating NSE at 05:07
Completed NSE at 05:07, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.05 seconds
           Raw packets sent: 3045 (137.080KB) | Rcvd: 52 (2.644KB)
root@kali:/home/kali# 
```

TERCERA PRUEBA: *“nmap -v -sW -O  45.33.49.119”*:



```
root@kali:/home/kali# nmap -v -sW -O  45.33.49.119
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-14 05:12 EST
Initiating Ping Scan at 05:12
Scanning 45.33.49.119 [4 ports]
Completed Ping Scan at 05:12, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:12
Completed Parallel DNS resolution of 1 host. at 05:12, 0.30s elapsed
Initiating Window Scan at 05:12
Scanning ack.nmap.org (45.33.49.119) [1000 ports]
Completed Window Scan at 05:12, 0.17s elapsed (1000 total ports)
Initiating OS detection (try #1) against ack.nmap.org (45.33.49.119)
Retrying OS detection (try #2) against ack.nmap.org (45.33.49.119)
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.0036s latency).
All 1000 scanned ports on ack.nmap.org (45.33.49.119) are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
t
Device type: printer|print server|power-device|webcam|general purpose
Running (JUST GUESSING): Agfa embedded (86%), D-Link embedded (86%), Hamlet embedded (86%), Tahoe em
bedded (86%), TRENDnet embedded (86%), Linux 1.0.X (85%)
OS CPE: cpe:/h:agfa:drystar_5500 cpe:/h:dlink:dp-300u cpe:/h:dlink:dp-g310 cpe:/h:hamlet:hps01uu cpe
:/h:tahoe:8216 cpe:/h:trendnet:tv-ip100 cpe:/o:linux:linux_kernel:1.0.9
Aggressive OS guesses: Agfa DryStar 5500 printer (86%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU p
rint server (86%), Tahoe 8216 power management system (86%), TRENDnet TV-IP100 webcam (86%), Linux 1
.0.9 (85%)
No exact OS matches for host (test conditions non-ideal).

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.27 seconds
           Raw packets sent: 1036 (45.452KB) | Rcvd: 1016 (41.978KB)
root@kali:/home/kali# █
```

**8. Busca tres direcciones de Internet interesantes de nmap donde hayas consultado alguna información:**

https://nmap.org/man/es/index.html
https://www.networkcomputing.com/networking/nmap-tutorial-common-commands
http://www.cursodehackers.com/nmap.html