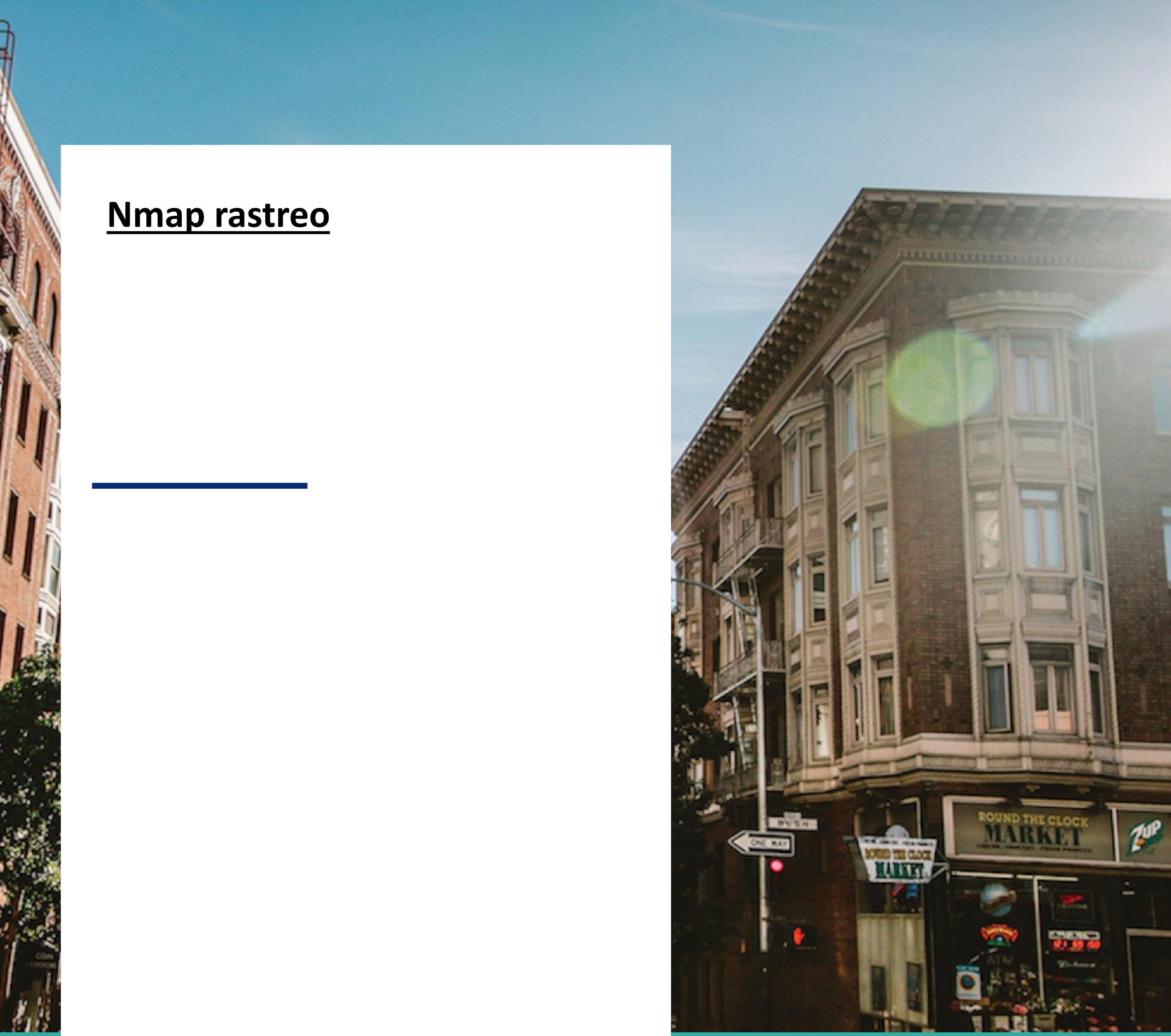


Nmap rastreo

21/11/2023

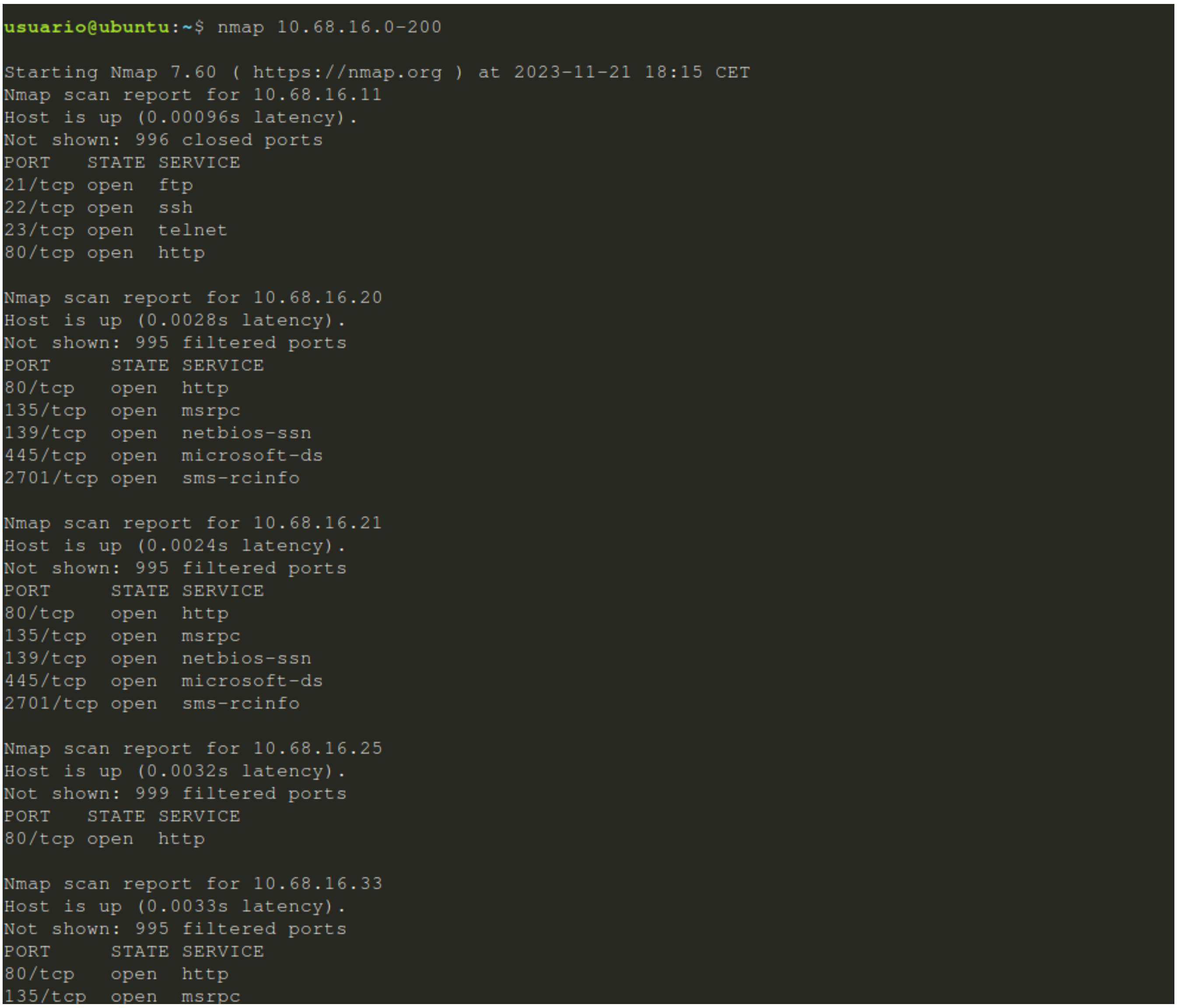
Guillermo Bellettini
Seguridad
Creado por: Nicolas Pavel Ballesteros Barrado

Contenido

Nmap rastreo 1

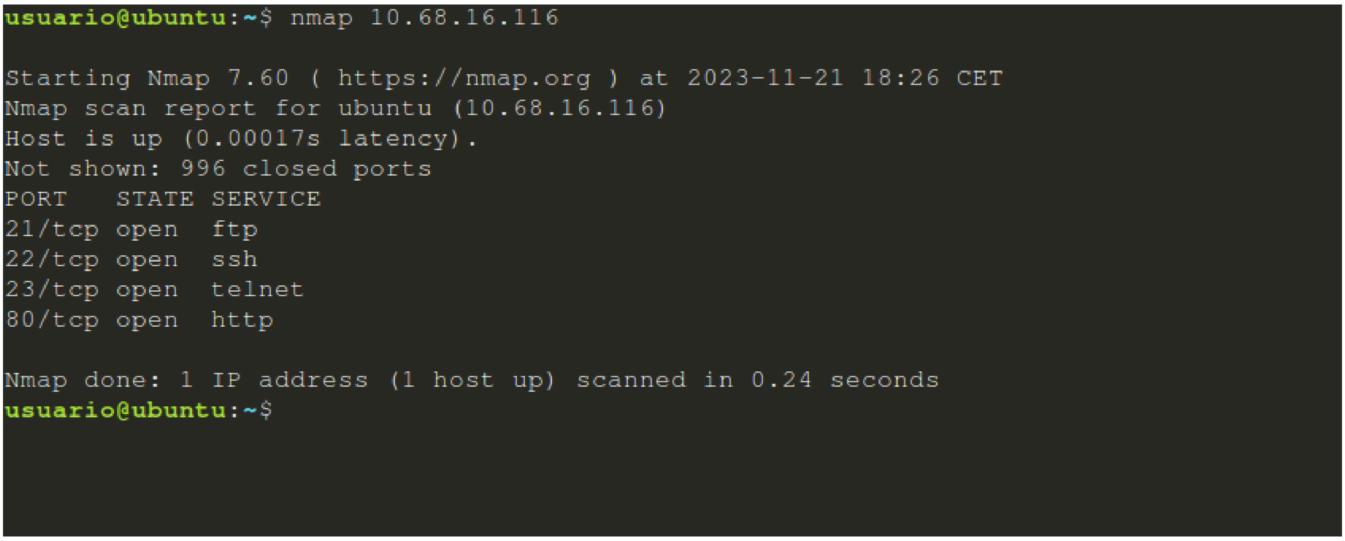
- Escaneo de un Rango de IPs: 3
- Escaneo de una Dirección IP: 3
- Escaneo de una Subred: 4
- Escaneo de un Rango de Puertos: 4
- Escaneo de un puerto especifico 5
- Escaneo de Puertos con Servicio y Versión: 5
- Escaneo Agresivo (Sin DNS): 5
- Escaneo de Versiones y Scripts de Vulnerabilidad: 6
- Escaneo de Hosts Vivos (Ping Scan): 7
- Escaneo UDP: 7
- Escaneo de un Archivo de Hosts: 8
- Escaneo en Modo Sigiloso (Sin Salida a la Pantalla): 8
- Escaneo de Firewall para Puertos Abiertos y Filtrados: 9
- Escaneo de Red Completa con Registro en Archivo XML: 9

Escaneo de un Rango de IPs:



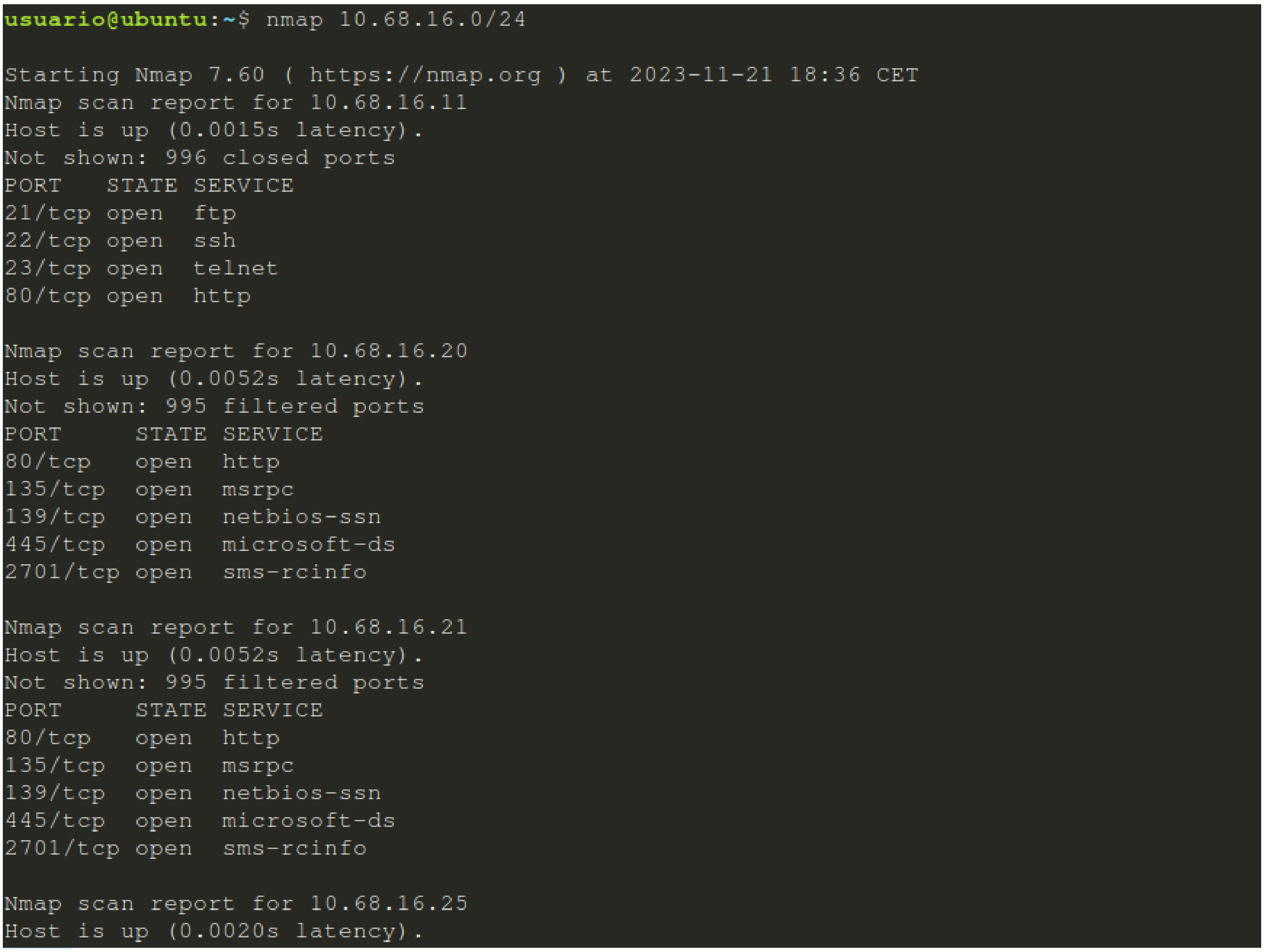
```
usuario@ubuntu:~$ nmap 10.68.16.0-200

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 18:15 CET
Nmap scan report for 10.68.16.11
Host is up (0.00096s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap scan report for 10.68.16.20
Host is up (0.0028s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2701/tcp open  sms-rcinfo

Nmap scan report for 10.68.16.21
Host is up (0.0024s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2701/tcp open  sms-rcinfo

Nmap scan report for 10.68.16.25
Host is up (0.0032s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 10.68.16.33
Host is up (0.0033s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
```

Escaneo de una Dirección IP:



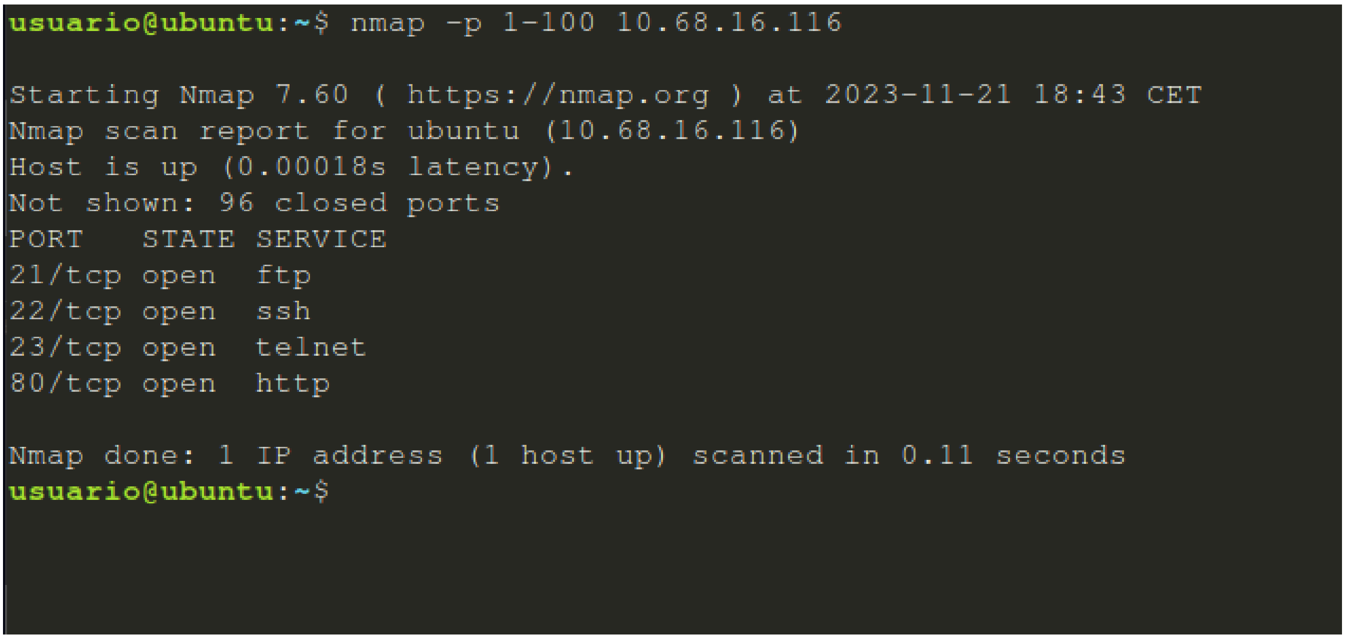
```
usuario@ubuntu:~$ nmap 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 18:26 CET
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.00017s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
usuario@ubuntu:~$
```

Escaneo de una Subred:



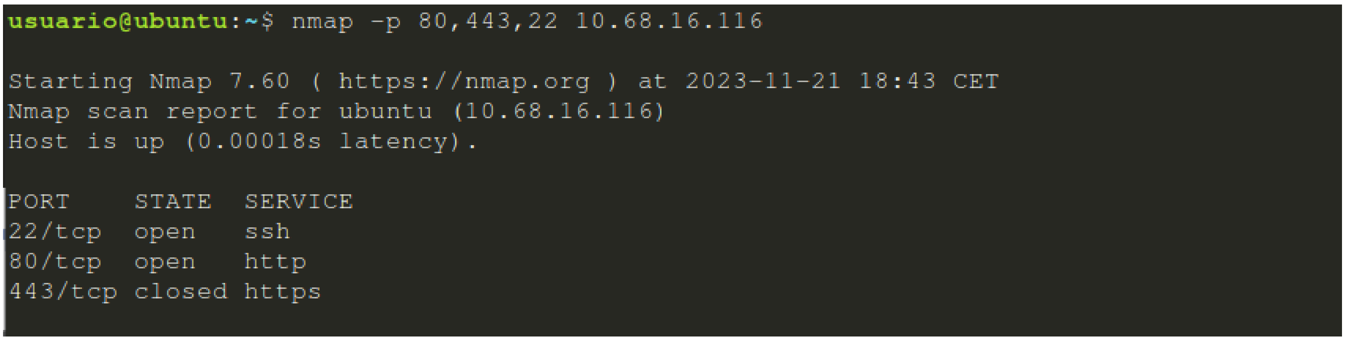
```
usuario@ubuntu:~$ nmap 10.68.16.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 18:36 CET
Nmap scan report for 10.68.16.11
Host is up (0.0015s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap scan report for 10.68.16.20
Host is up (0.0052s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2701/tcp open  sms-rcinfo

Nmap scan report for 10.68.16.21
Host is up (0.0052s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2701/tcp open  sms-rcinfo

Nmap scan report for 10.68.16.25
Host is up (0.0020s latency).
```

Escaneo de un Rango de Puertos:



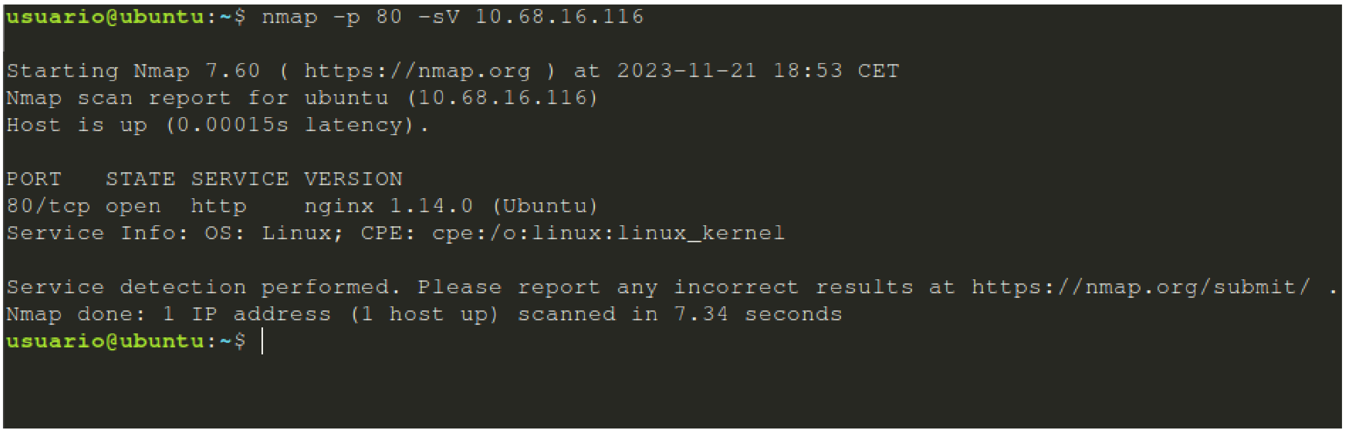
```
usuario@ubuntu:~$ nmap -p 1-100 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 18:43 CET
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.00018s latency).
Not shown: 96 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
usuario@ubuntu:~$
```

Escaneo de un puerto especifico



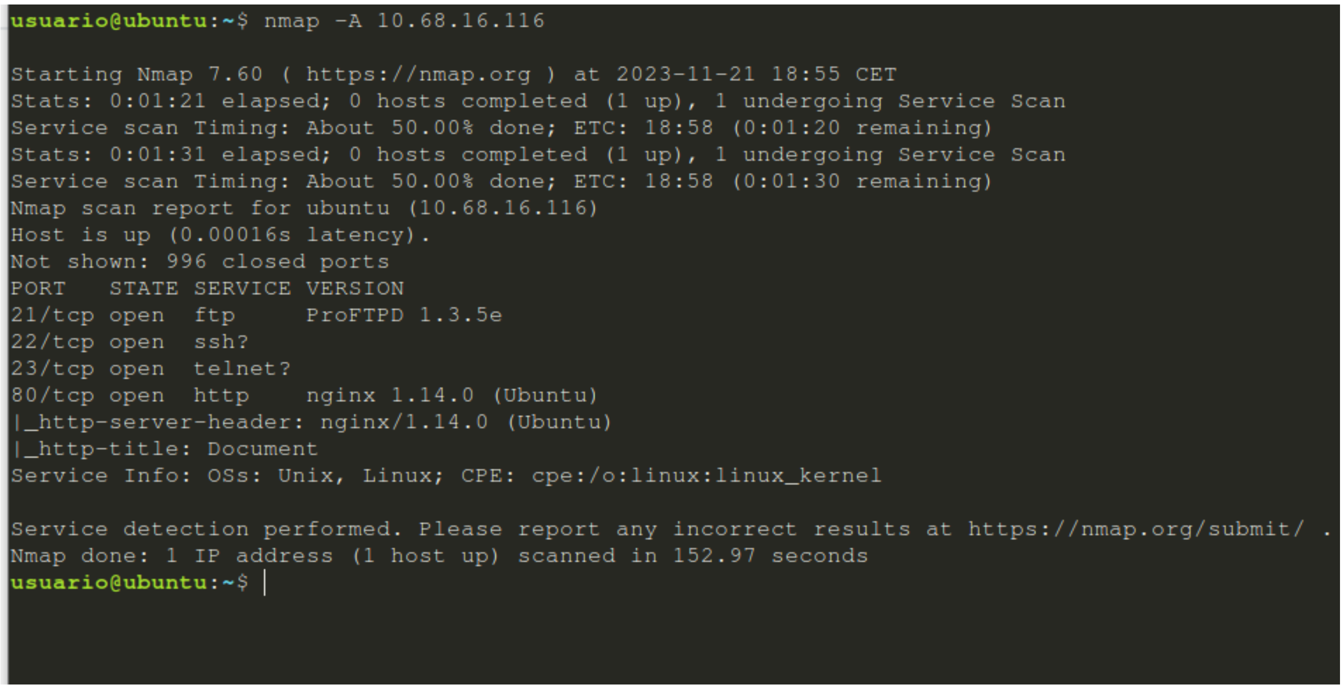
```
usuario@ubuntu:~$ nmap -p 80,443,22 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 18:43 CET
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.00018s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https
```

Escaneo de Puertos con Servicio y Versión:



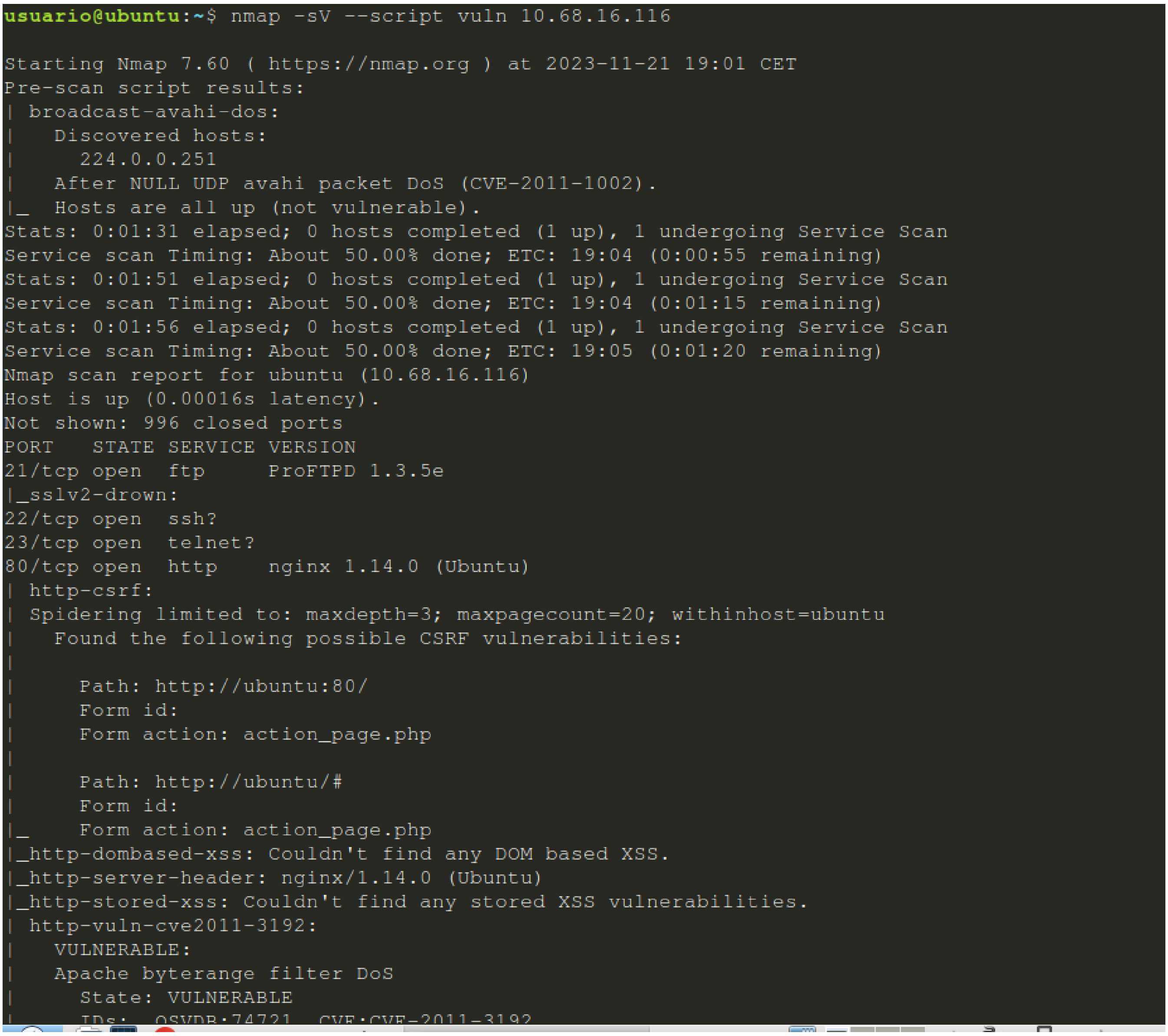
```
usuario@ubuntu:~$ nmap -p 80 -sV 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 18:53 CET
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.00015s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.0 (Ubuntu)
Service Info: OS: 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 7.34 seconds
usuario@ubuntu:~$ |
```

Escaneo Agresivo (Sin DNS):



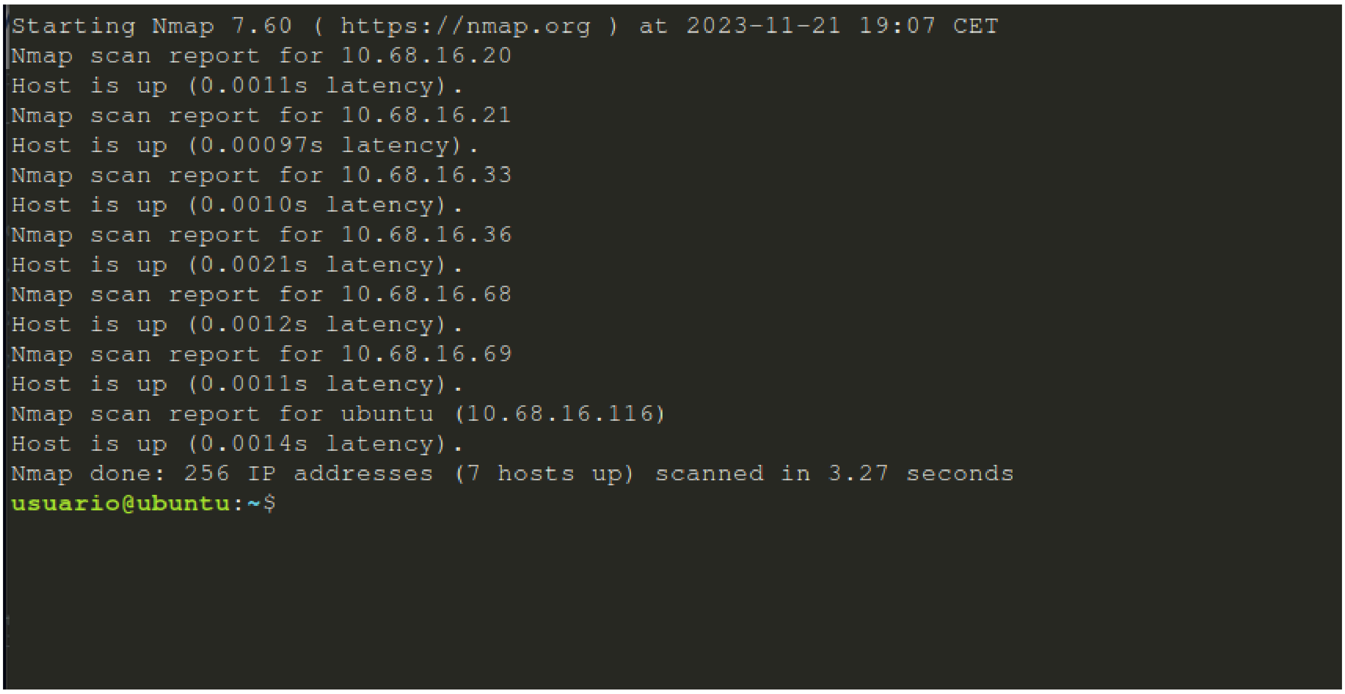
```
usuario@ubuntu:~$ nmap -A 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 18:55 CET
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 18:58 (0:01:20 remaining)
Stats: 0:01:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 18:58 (0:01:30 remaining)
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.00016s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5e
22/tcp open  ssh?
23/tcp open  telnet?
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Document
Service Info: 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 152.97 seconds
usuario@ubuntu:~$ |
```

Escaneo de Versiones y Scripts de Vulnerabilidad:



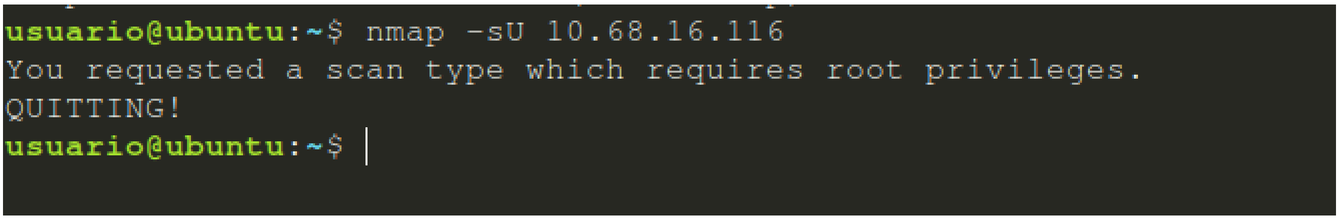
```
usuario@ubuntu:~$ nmap -sV --script vuln 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 19:01 CET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:01:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 19:04 (0:00:55 remaining)
Stats: 0:01:51 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 19:04 (0:01:15 remaining)
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 19:05 (0:01:20 remaining)
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.00016s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5e
|_sslv2-drown:
22/tcp open  ssh?
23/tcp open  telnet?
80/tcp open  http    nginx 1.14.0 (Ubuntu)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=ubuntu
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://ubuntu:80/
|     Form id:
|     Form action: action_page.php
|
|     Path: http://ubuntu/#
|     Form id:
|_    Form action: action_page.php
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  OSVDB:74721  CVE:CVE-2011-3192
```

Escaneo de Hosts Vivos (Ping Scan):



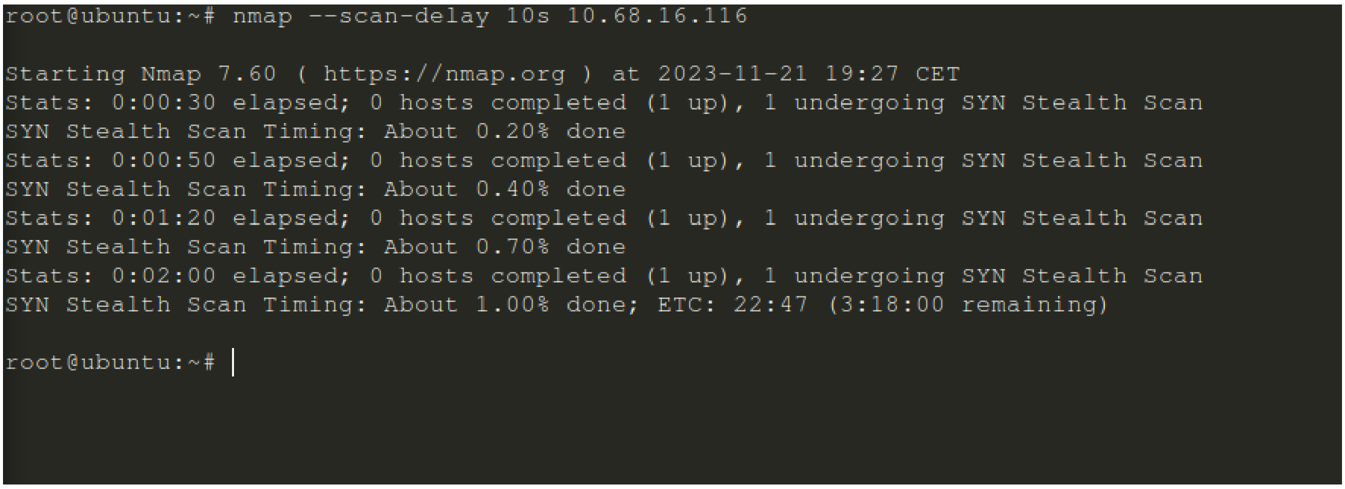
```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 19:07 CET
Nmap scan report for 10.68.16.20
Host is up (0.0011s latency).
Nmap scan report for 10.68.16.21
Host is up (0.00097s latency).
Nmap scan report for 10.68.16.33
Host is up (0.0010s latency).
Nmap scan report for 10.68.16.36
Host is up (0.0021s latency).
Nmap scan report for 10.68.16.68
Host is up (0.0012s latency).
Nmap scan report for 10.68.16.69
Host is up (0.0011s latency).
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.0014s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 3.27 seconds
usuario@ubuntu:~$
```

Escaneo UDP:



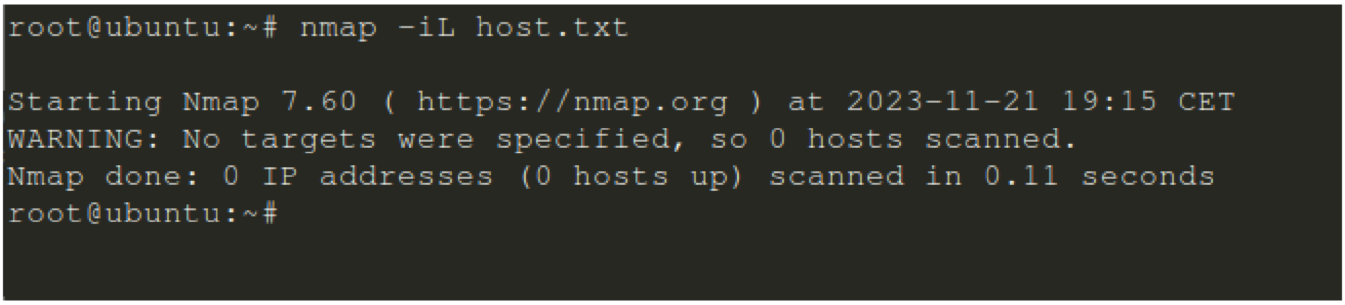
```
usuario@ubuntu:~$ nmap -sU 10.68.16.116
You requested a scan type which requires root privileges.
QUITTING!
usuario@ubuntu:~$
```

Escaneo con Tiempo de Retraso Personalizado:



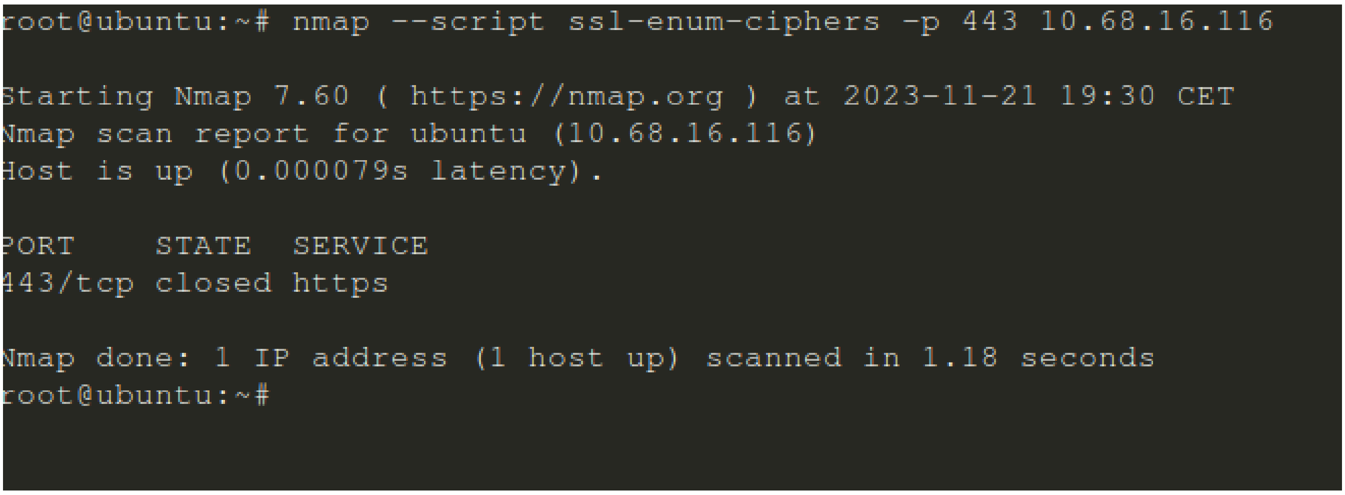
```
root@ubuntu:~# nmap --scan-delay 10s 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 19:27 CET
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.20% done
Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.40% done
Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.70% done
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.00% done; ETC: 22:47 (3:18:00 remaining)

root@ubuntu:~#
```

Escaneo de un Archivo de Hosts:



```
root@ubuntu:~# nmap -iL host.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 19:15 CET
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.11 seconds
root@ubuntu:~#
```

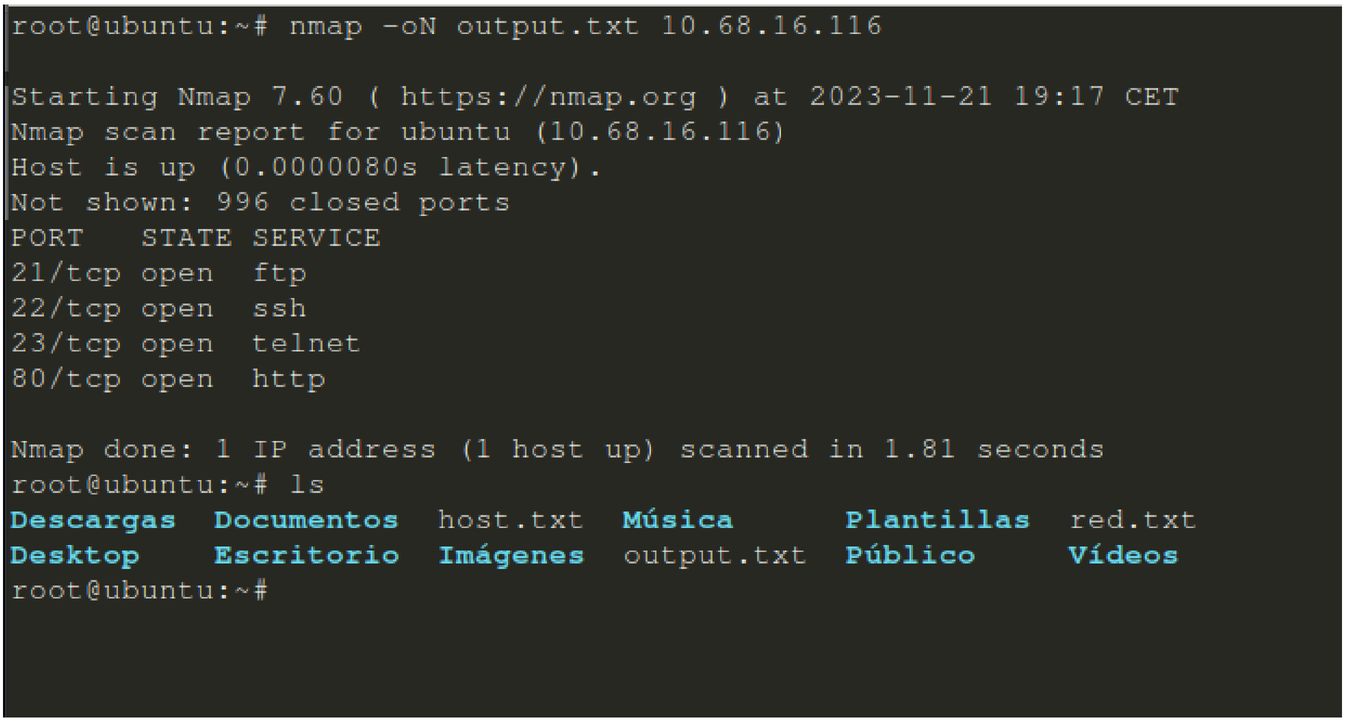
Escaneo con Fingerprinting de SSL:



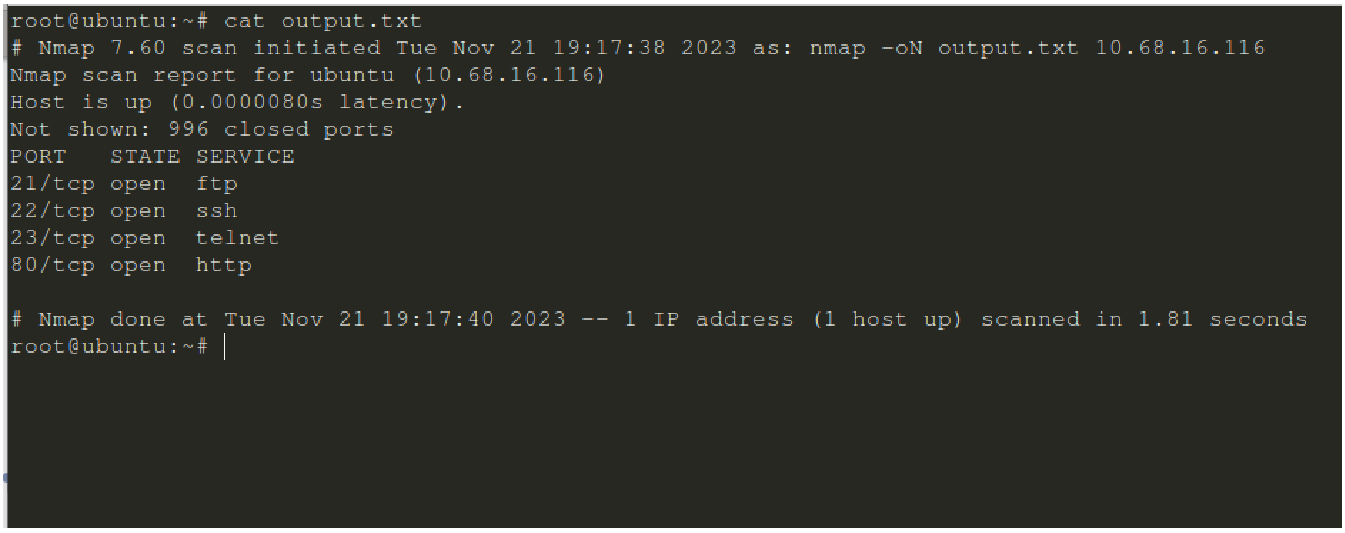
```
root@ubuntu:~# nmap --script ssl-enum-ciphers -p 443 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 19:30 CET
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.000079s latency).

PORT    STATE  SERVICE
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
root@ubuntu:~#
```

Escanea y enumera los cifrados SSL disponibles en el puerto 443.

Escaneo en Modo Sigiloso (Sin Salida a la Pantalla):

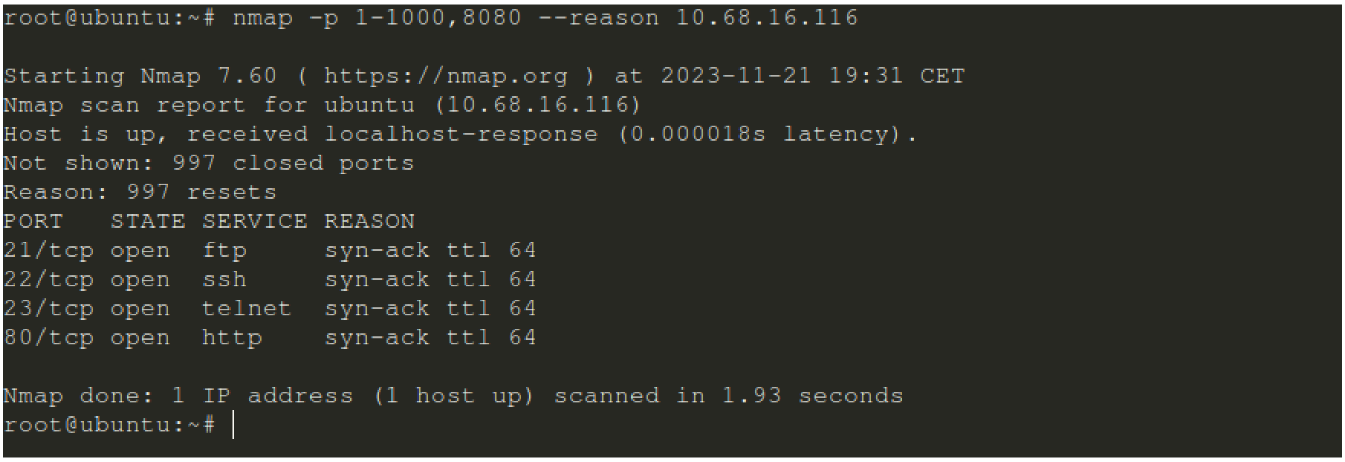


```
root@ubuntu:~# nmap -oN output.txt 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 19:17 CET
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.0000080s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
root@ubuntu:~# ls
Descargas  Documentos  host.txt  Música      Plantillas  red.txt
Desktop    Escritorio  Imágenes  output.txt  Público     Vídeos
root@ubuntu:~#
```



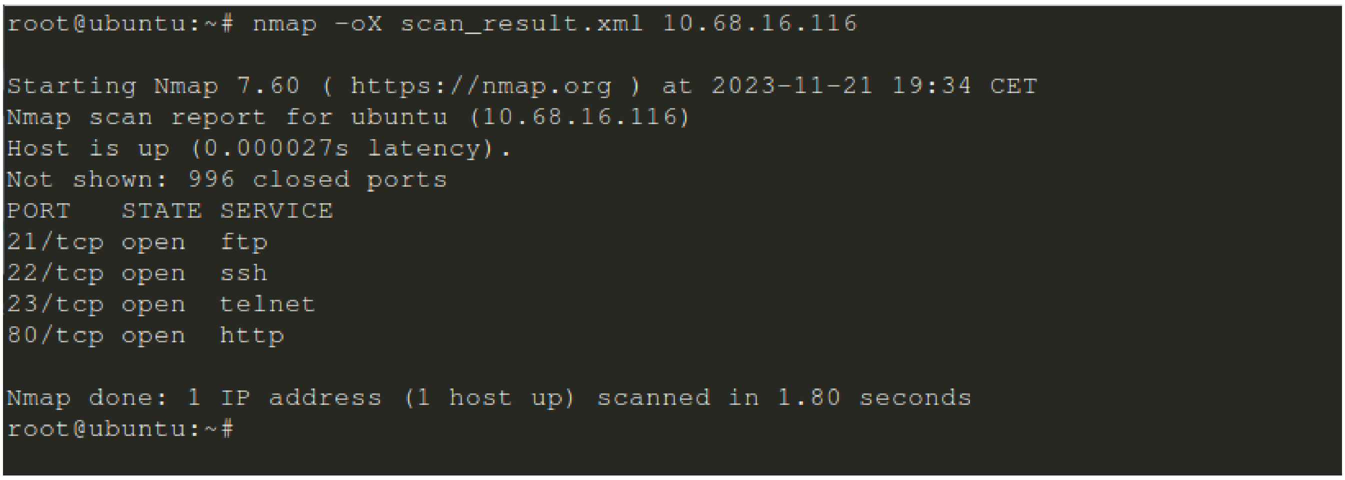
```
root@ubuntu:~# cat output.txt
# Nmap 7.60 scan initiated Tue Nov 21 19:17:38 2023 as: nmap -oN output.txt 10.68.16.116
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.0000080s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

# Nmap done at Tue Nov 21 19:17:40 2023 -- 1 IP address (1 host up) scanned in 1.81 seconds
root@ubuntu:~# 
```

Escaneo de Firewall para Puertos Abiertos y Filtrados:

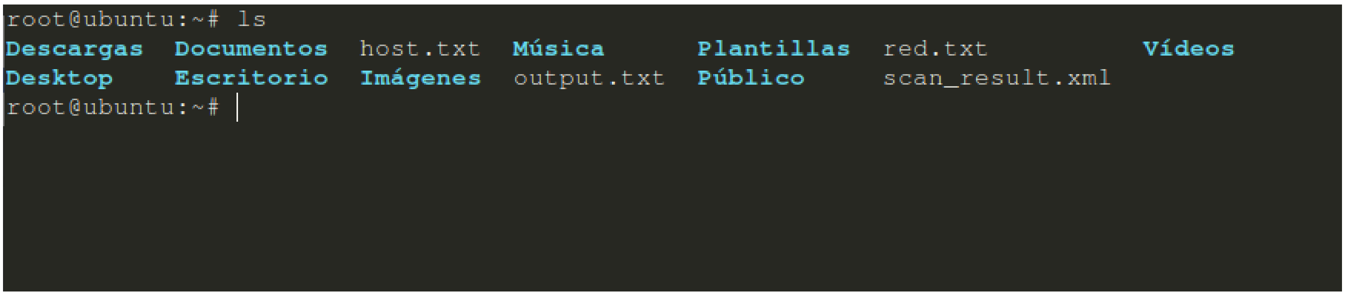


```
root@ubuntu:~# nmap -p 1-1000,8080 --reason 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 19:31 CET
Nmap scan report for ubuntu (10.68.16.116)
Host is up, received localhost-response (0.000018s latency).
Not shown: 997 closed ports
Reason: 997 resets
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
22/tcp open  ssh     syn-ack ttl 64
23/tcp open  telnet  syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64

Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
root@ubuntu:~# 
```

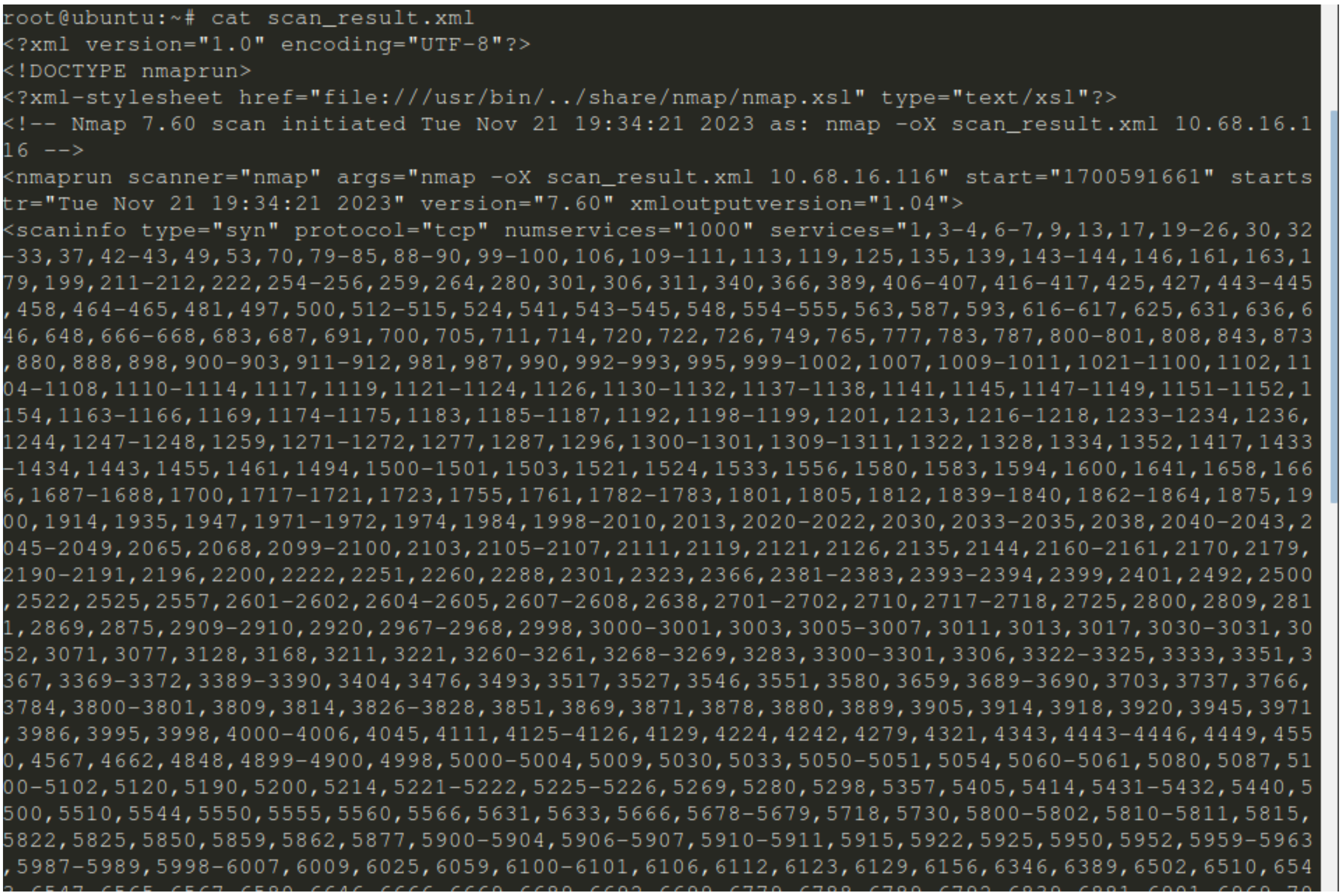
Escaneo de Red Completa con Registro en Archivo XML:



```
root@ubuntu:~# nmap -oX scan_result.xml 10.68.16.116

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-21 19:34 CET
Nmap scan report for ubuntu (10.68.16.116)
Host is up (0.000027s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
root@ubuntu:~#
```



```
root@ubuntu:~# ls
Descargas  Documentos  host.txt  Música      Plantillas  red.txt          Vídeos
Desktop    Escritorio  Imágenes  output.txt  Público     scan_result.xml
root@ubuntu:~# 
```



```
root@ubuntu:~# cat scan_result.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.60 scan initiated Tue Nov 21 19:34:21 2023 as: nmap -oX scan_result.xml 10.68.16.1
16 -->
<nmaprun scanner="nmap" args="nmap -oX scan_result.xml 10.68.16.116" start="1700591661" starts
tr="Tue Nov 21 19:34:21 2023" version="7.60" xmloutputversion="1.04">
<scaninfo type="syn" protocol="tcp" numservices="1000" services="1,3-4,6-7,9,13,17,19-26,30,32
-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,1
79,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445
,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,6
46,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873
,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,11
04-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1
154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,
1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433
-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,166
6,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,19
00,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2
045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,
2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500
,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,281
1,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,30
52,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3
367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,
3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971
,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,455
0,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,51
00-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5
500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,
5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963
,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,654
```

Escanea toda la red y guarda los resultados en un archivo XML.