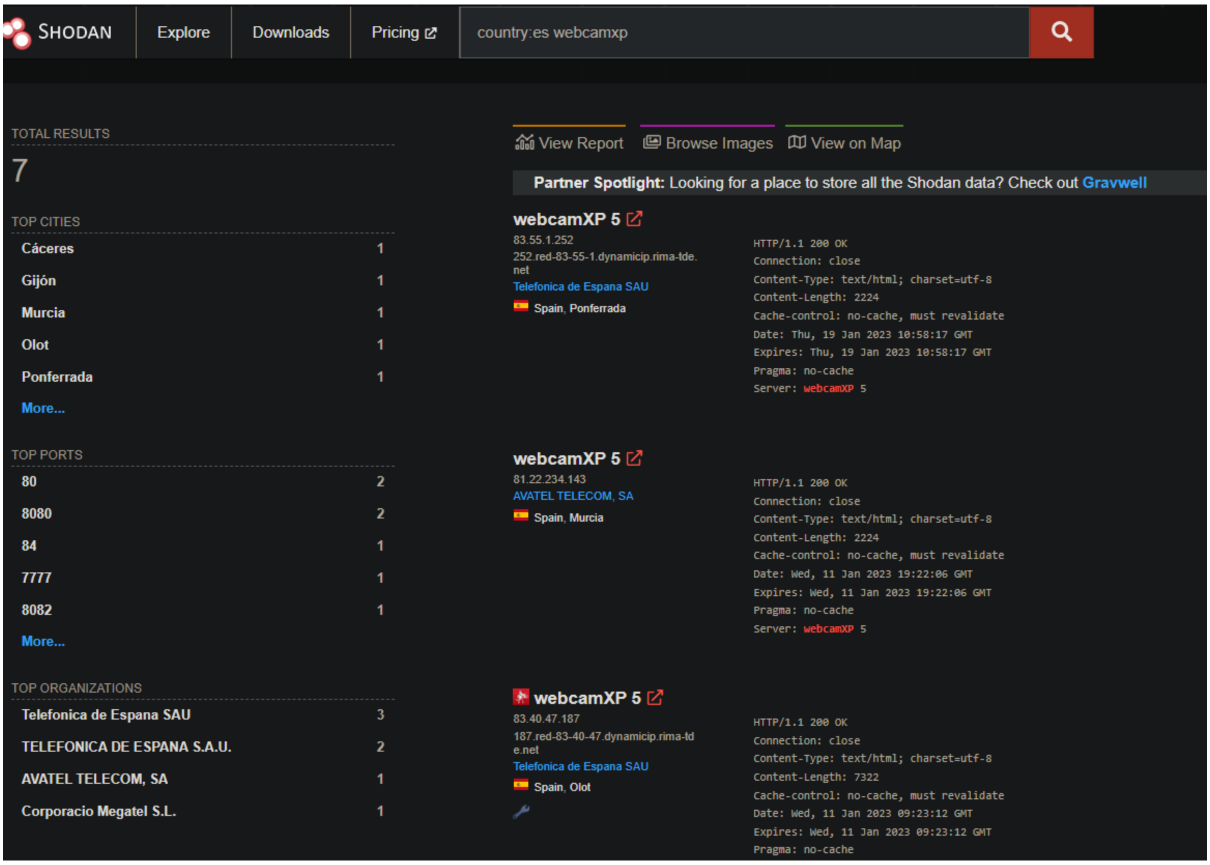
Practica Info Gathering

Shodan.

Hay multitud de filtros en shodan, **aquí unos cuantos.**

Aquí filtra por ordenadores con windowsxp(un programa para monitorizar cámaras) y que están en españa.



country:es webcamxp

TOTAL RESULTS

7

TOP CITIES	
Cáceres	1
Gijón	1
Murcia	1
Olot	1
Ponferrada	1
More...	

TOP PORTS	
80	2
8080	2
84	1
7777	1
8082	1
More...	

TOP ORGANIZATIONS	
Telefonica de Espana SAU	3
TELEFONICA DE ESPANA S.A.U.	2
AVATEL TELECOM, SA	1
Corporacio Megatel S.L.	1

Partner Spotlight: Looking for a place to store all the Shodan data? Check out Gravwell

webcamXP 5

83.55.1.252

252.red-83-55-1.dynamicip.rima-tde.net

Telefonica de Espana SAU

Spain, Ponferrada

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2224
Cache-control: no-cache, must revalidate
Date: Thu, 19 Jan 2023 10:58:17 GMT
Expires: Thu, 19 Jan 2023 10:58:17 GMT
Pragma: no-cache
Server: webcamXP 5
```

webcamXP 5

81.22.234.143

AVATEL TELECOM, SA

Spain, Murcia

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2224
Cache-control: no-cache, must revalidate
Date: Wed, 11 Jan 2023 19:22:06 GMT
Expires: Wed, 11 Jan 2023 19:22:06 GMT
Pragma: no-cache
Server: webcamXP 5
```

webcamXP 5

83.40.47.187

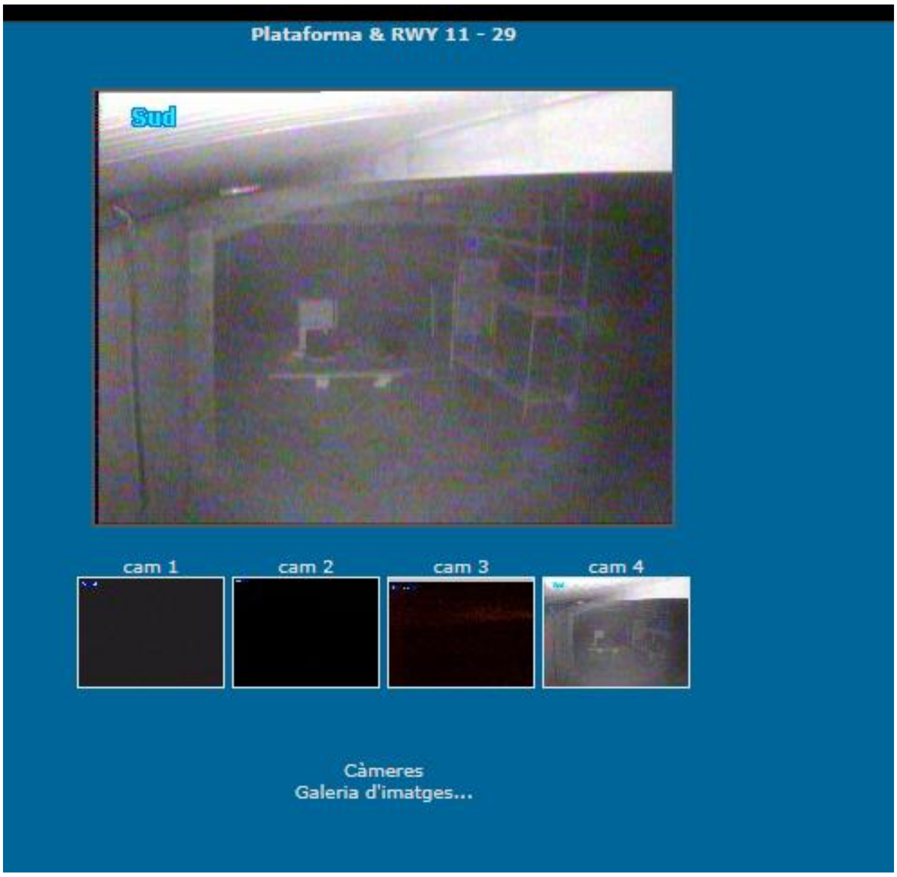
187.red-83-40-47.dynamicip.rima-tde.net

Telefonica de Espana SAU

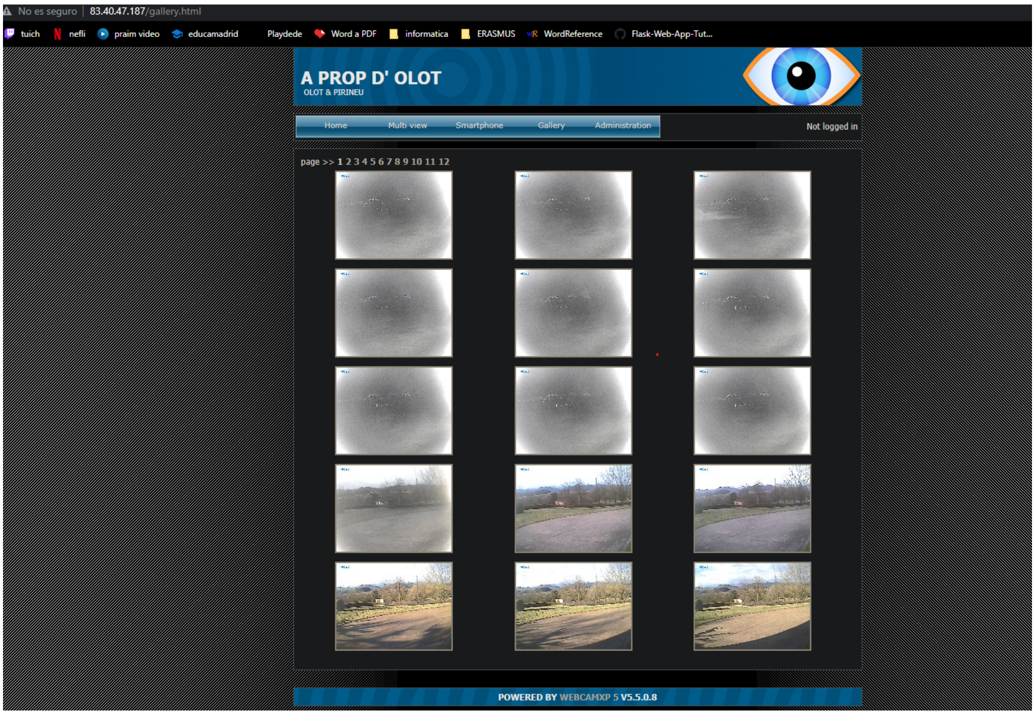
Spain, Olot

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7322
Cache-control: no-cache, must revalidate
Date: Wed, 11 Jan 2023 09:23:12 GMT
Expires: Wed, 11 Jan 2023 09:23:12 GMT
Pragma: no-cache
```

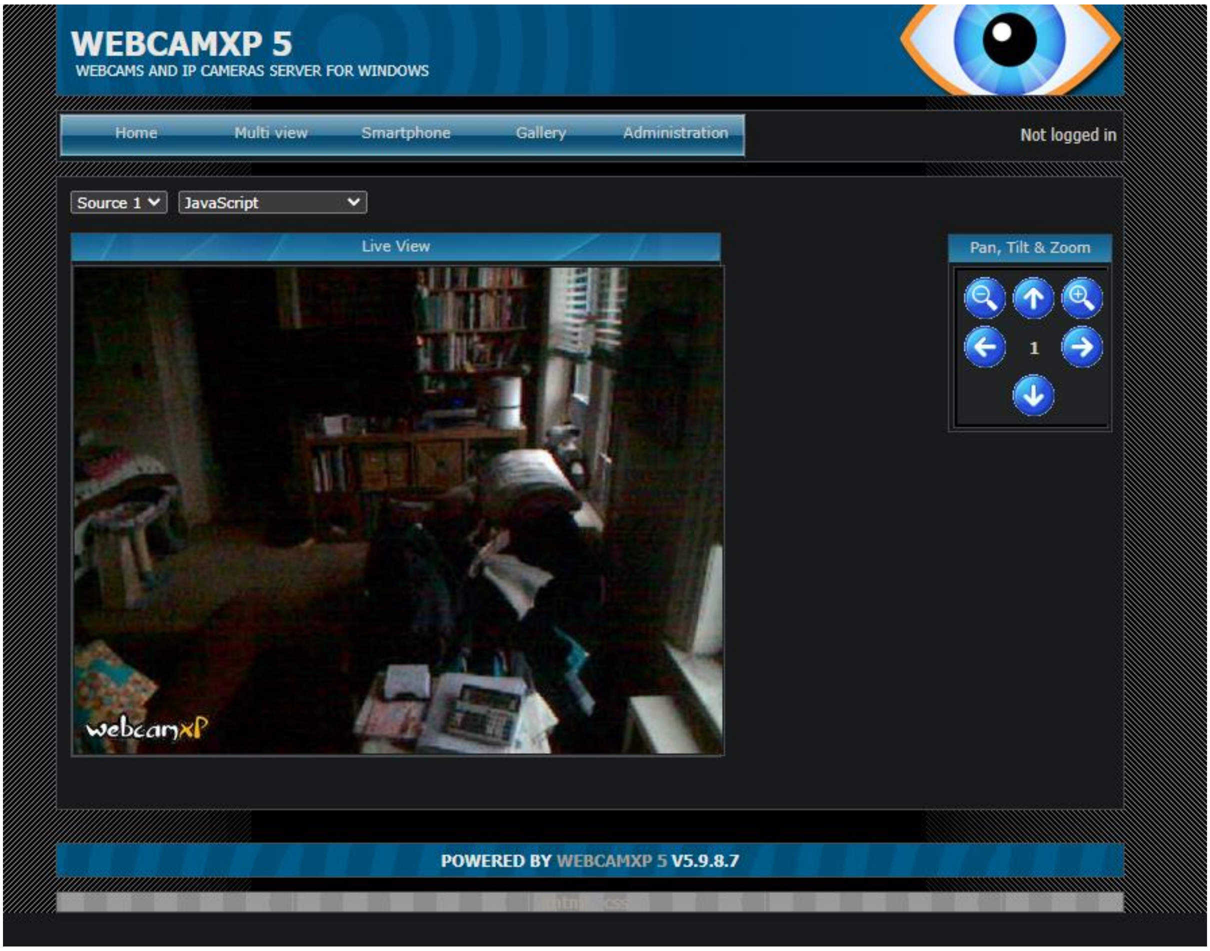
Aquí una de las cámaras que podemos ver sin iniciar sesión.



Aquí otro ejemplo.



Aquí una de la habitación de alguien.



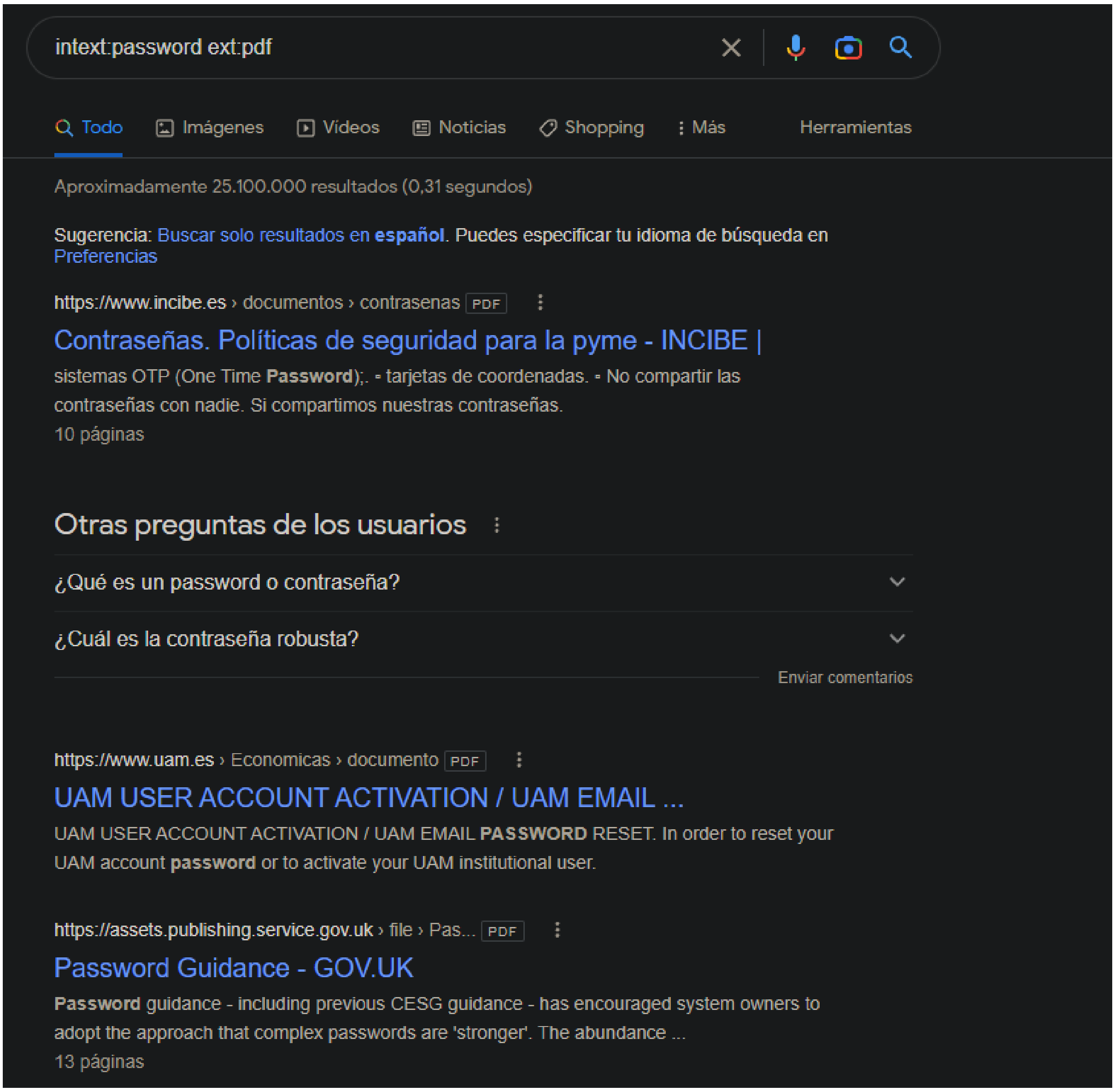
Claramente esto supone un gran riesgo ya que cualquiera puede saber donde estás geolocalizando tu ip y además ver lo que estas haciendo en tu casa. Cualquier atacante con un mínimo de conocimiento podría controlar cuando estas en casa y cunado no y entrar a robar por ejemplo.

Google dorks.

Google dorks sirve para hacer búsquedas avanzadas en Google, que no deja de ser el buscador mas grande del mundo sin incluir la dark web.

Al igual que shodan hay múltiples filtros para hacer las búsquedas mas precisas.

Aquí filtra por archivos pdf y que tienen la palabra password en ellos, lo cual puede servir a los atacantes para encontrar credenciales escritas por error en texto plano.



intext:password ext:pdf

Aproximadamente 25.100.000 resultados (0,31 segundos)

Sugerencia: Buscar solo resultados en **español**. Puedes especificar tu idioma de búsqueda en Preferencias

https://www.incibe.es › documentos › contrasenas PDF

Contraseñas. Políticas de seguridad para la pyme - INCIBE |

sistemas OTP (One Time **Password**);. ▪ tarjetas de coordenadas. ▪ No compartir las contraseñas con nadie. Si compartimos nuestras contraseñas.

10 páginas

Otras preguntas de los usuarios

¿Qué es un password o contraseña?

¿Cuál es la contraseña robusta?

Enviar comentarios

https://www.uam.es › Economicas › documento PDF

UAM USER ACCOUNT ACTIVATION / UAM EMAIL ...

UAM USER ACCOUNT ACTIVATION / UAM EMAIL **PASSWORD** RESET. In order to reset your UAM account **password** or to activate your UAM institutional user.

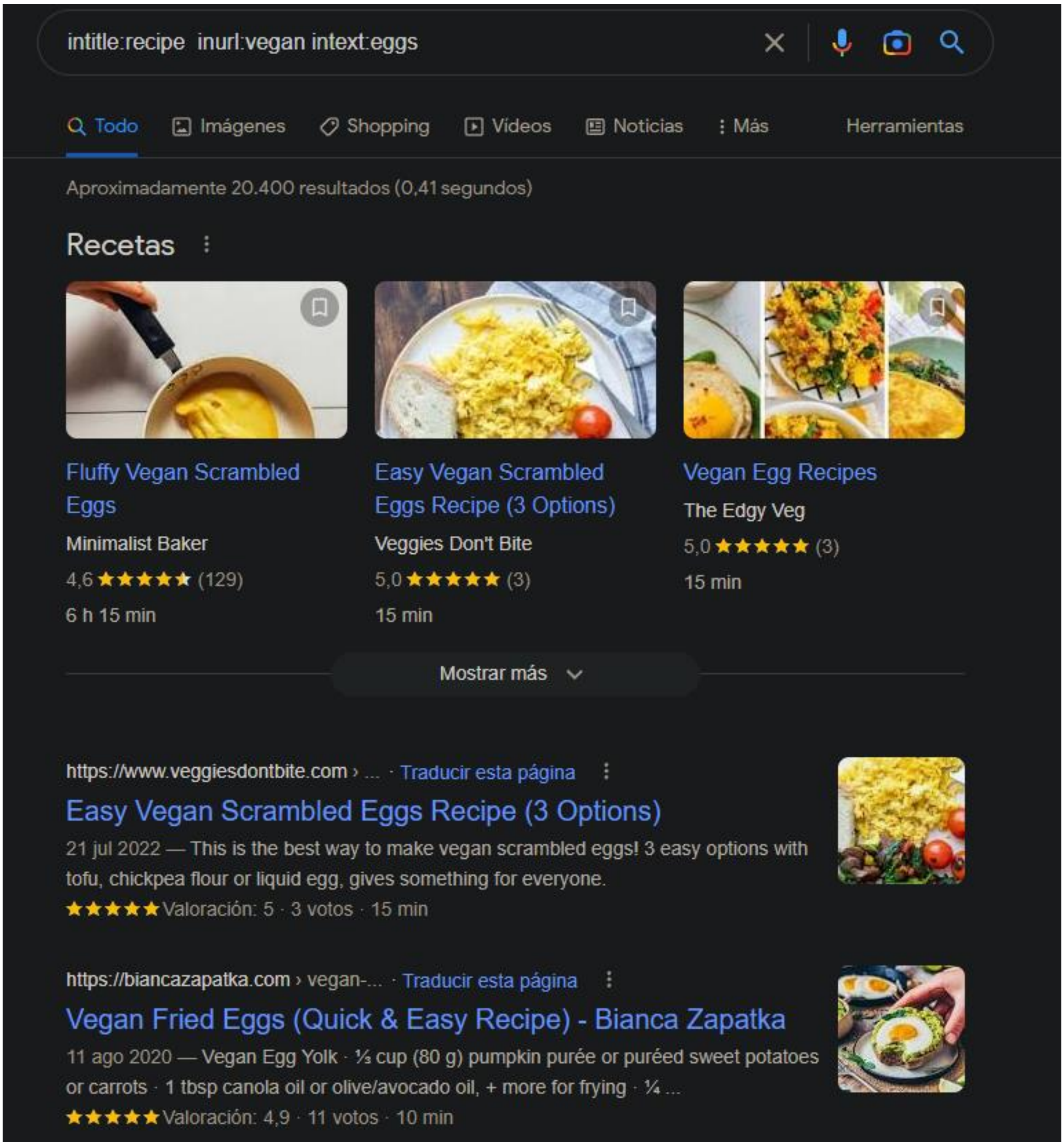
https://assets.publishing.service.gov.uk › file › Pas... PDF

Password Guidance - GOV.UK

Password guidance - including previous CESG guidance - has encouraged system owners to adopt the approach that complex passwords are 'stronger'. The abundance ...

13 páginas

Aquí filtra por paginas tituladas recipe, que incluyan la palabra vegan en la url y que en el texto este la palabra eggs.



intitle:recipe inurl:vegan intext:eggs

Aproximadamente 20.400 resultados (0,41 segundos)

Recetas

Fluffy Vegan Scrambled Eggs
Minimalist Baker
4,6 ★★★★★ (129)
6 h 15 min

Easy Vegan Scrambled Eggs Recipe (3 Options)
Veggies Don't Bite
5,0 ★★★★★ (3)
15 min

Vegan Egg Recipes
The Edgy Veg
5,0 ★★★★★ (3)
15 min

Mostrar más

https://www.veggiesdontbite.com › ... · Traducir esta página

Easy Vegan Scrambled Eggs Recipe (3 Options)

21 jul 2022 — This is the best way to make vegan scrambled eggs! 3 easy options with tofu, chickpea flour or liquid egg, gives something for everyone.
★★★★★ Valoración: 5 · 3 votos · 15 min

https://biancazapatka.com › vegan-... · Traducir esta página

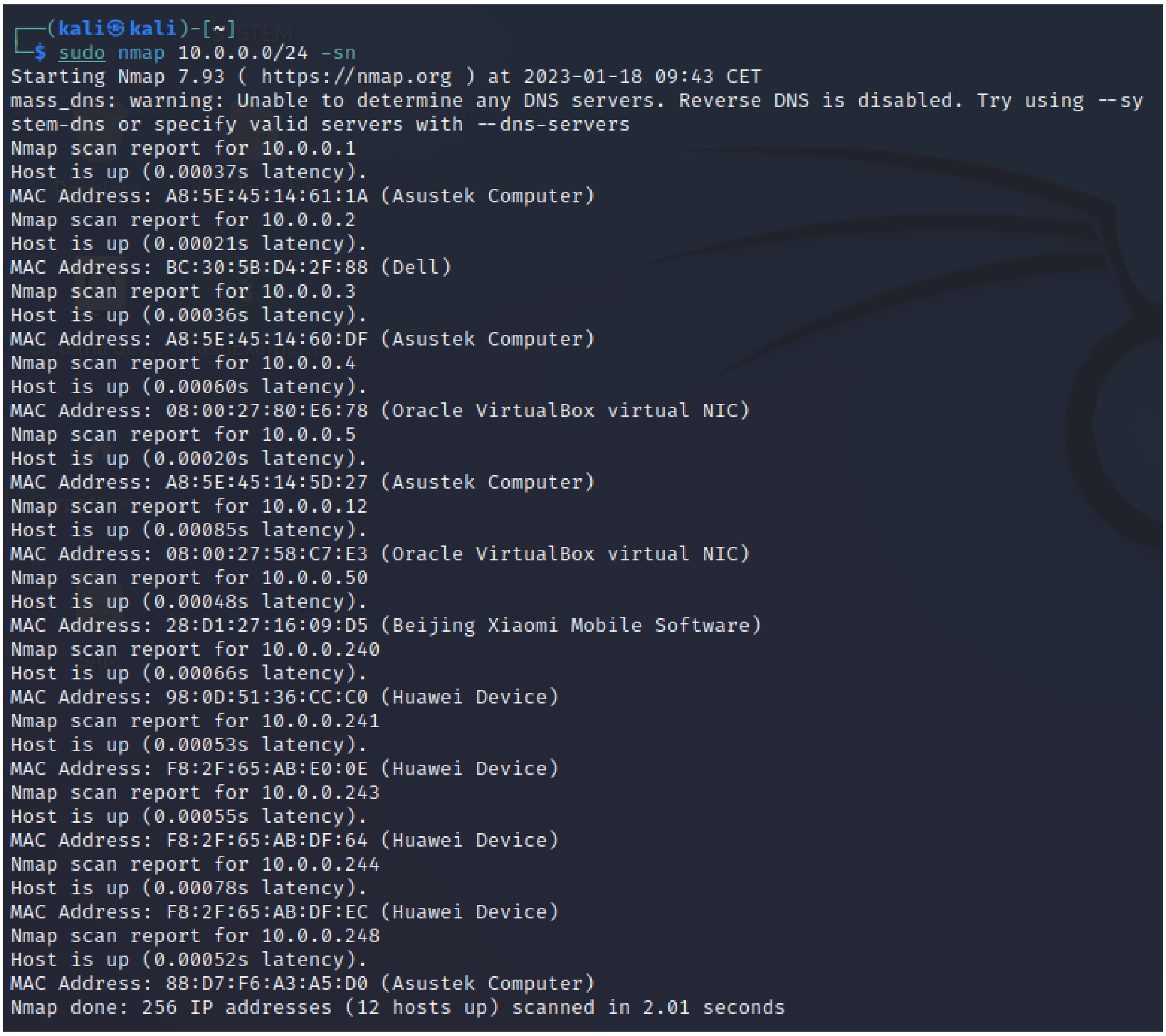
Vegan Fried Eggs (Quick & Easy Recipe) - Bianca Zapatka

11 ago 2020 — Vegan Egg Yolk · ⅓ cup (80 g) pumpkin purée or puréed sweet potatoes or carrots · 1 tbsp canola oil or olive/avocado oil, + more for frying · ¼ ...
★★★★★ Valoración: 4,9 · 11 votos · 10 min

nmap.

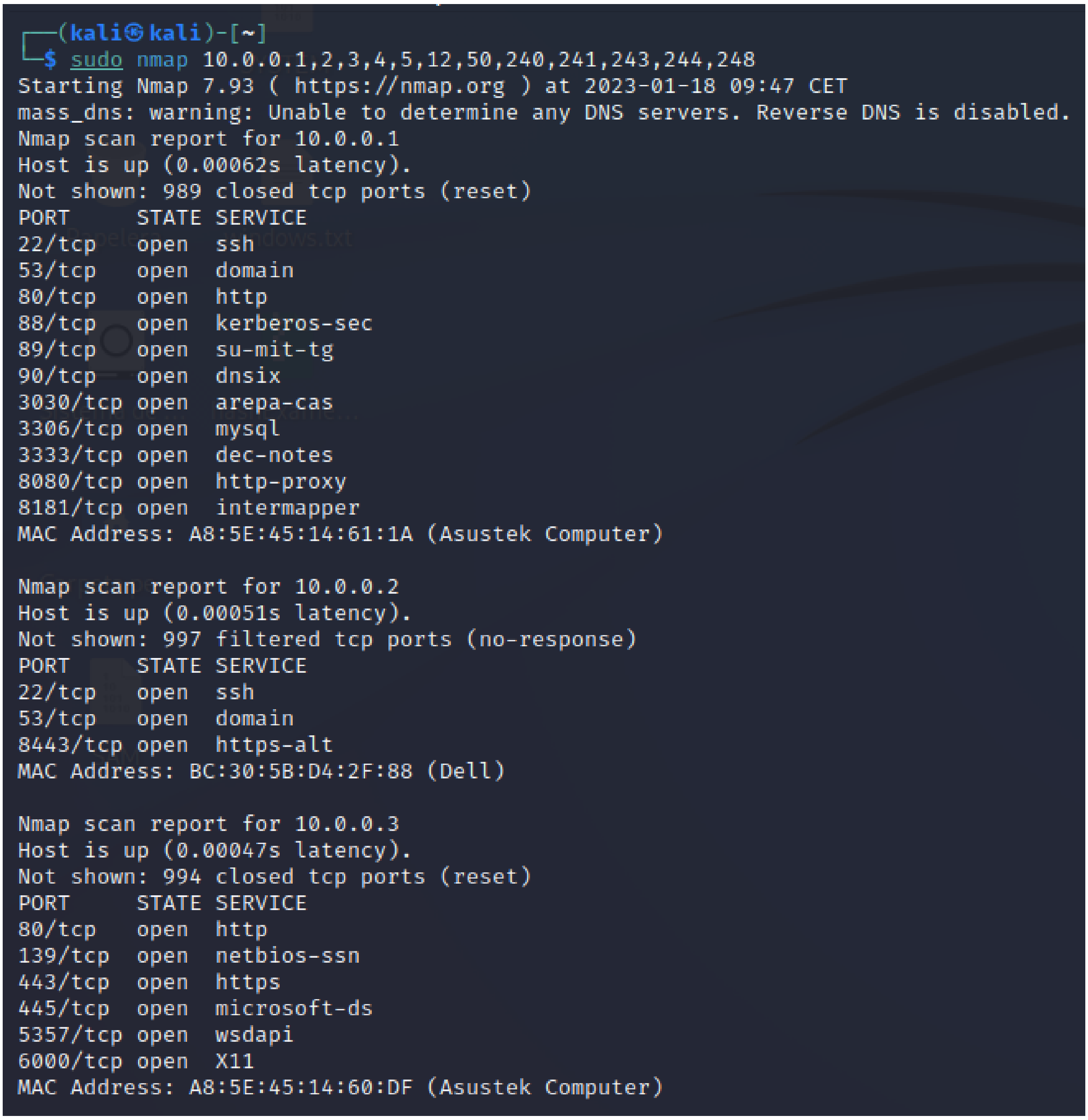
Red 10.0.0.0/24

Primero hacemos un host descovery para ver que maquinas están activas. Este paso puede fallar porque en caso de que las maquinas tengas cortafuegos o prohibido el ping, no contestarán y saldrán como desconectadas, aunque no esta de mas probar.

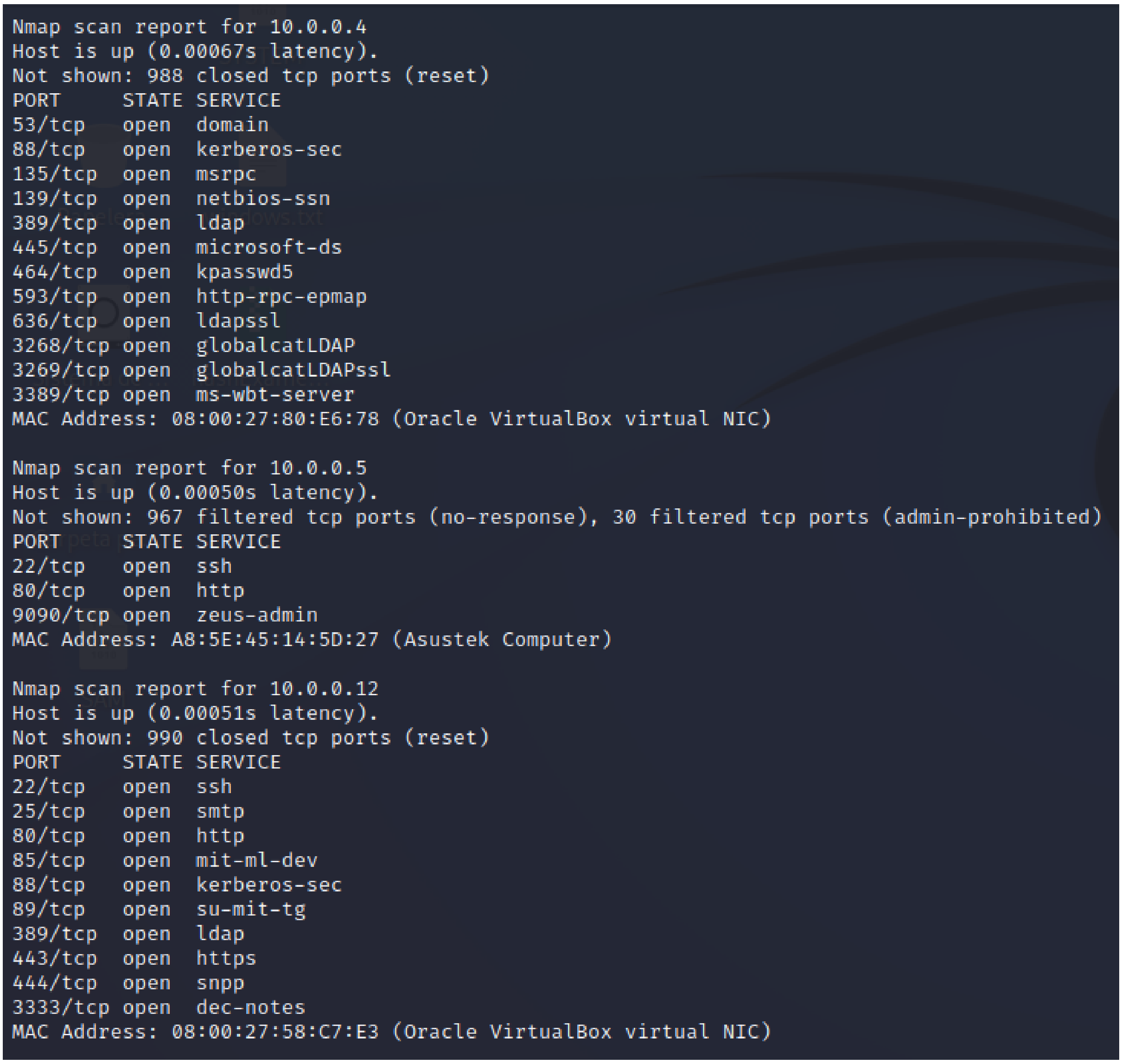


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.0.0/24 -sn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 09:43 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sy
stem-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.1
Host is up (0.00037s latency).
MAC Address: A8:5E:45:14:61:1A (Asustek Computer)
Nmap scan report for 10.0.0.2
Host is up (0.00021s latency).
MAC Address: BC:30:5B:D4:2F:88 (Dell)
Nmap scan report for 10.0.0.3
Host is up (0.00036s latency).
MAC Address: A8:5E:45:14:60:DF (Asustek Computer)
Nmap scan report for 10.0.0.4
Host is up (0.00060s latency).
MAC Address: 08:00:27:80:E6:78 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.0.5
Host is up (0.00020s latency).
MAC Address: A8:5E:45:14:5D:27 (Asustek Computer)
Nmap scan report for 10.0.0.12
Host is up (0.00085s latency).
MAC Address: 08:00:27:58:C7:E3 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.0.50
Host is up (0.00048s latency).
MAC Address: 28:D1:27:16:09:D5 (Beijing Xiaomi Mobile Software)
Nmap scan report for 10.0.0.240
Host is up (0.00066s latency).
MAC Address: 98:0D:51:36:CC:C0 (Huawei Device)
Nmap scan report for 10.0.0.241
Host is up (0.00053s latency).
MAC Address: F8:2F:65:AB:E0:0E (Huawei Device)
Nmap scan report for 10.0.0.243
Host is up (0.00055s latency).
MAC Address: F8:2F:65:AB:DF:64 (Huawei Device)
Nmap scan report for 10.0.0.244
Host is up (0.00078s latency).
MAC Address: F8:2F:65:AB:DF:EC (Huawei Device)
Nmap scan report for 10.0.0.248
Host is up (0.00052s latency).
MAC Address: 88:D7:F6:A3:A5:D0 (Asustek Computer)
Nmap done: 256 IP addresses (12 hosts up) scanned in 2.01 seconds
```

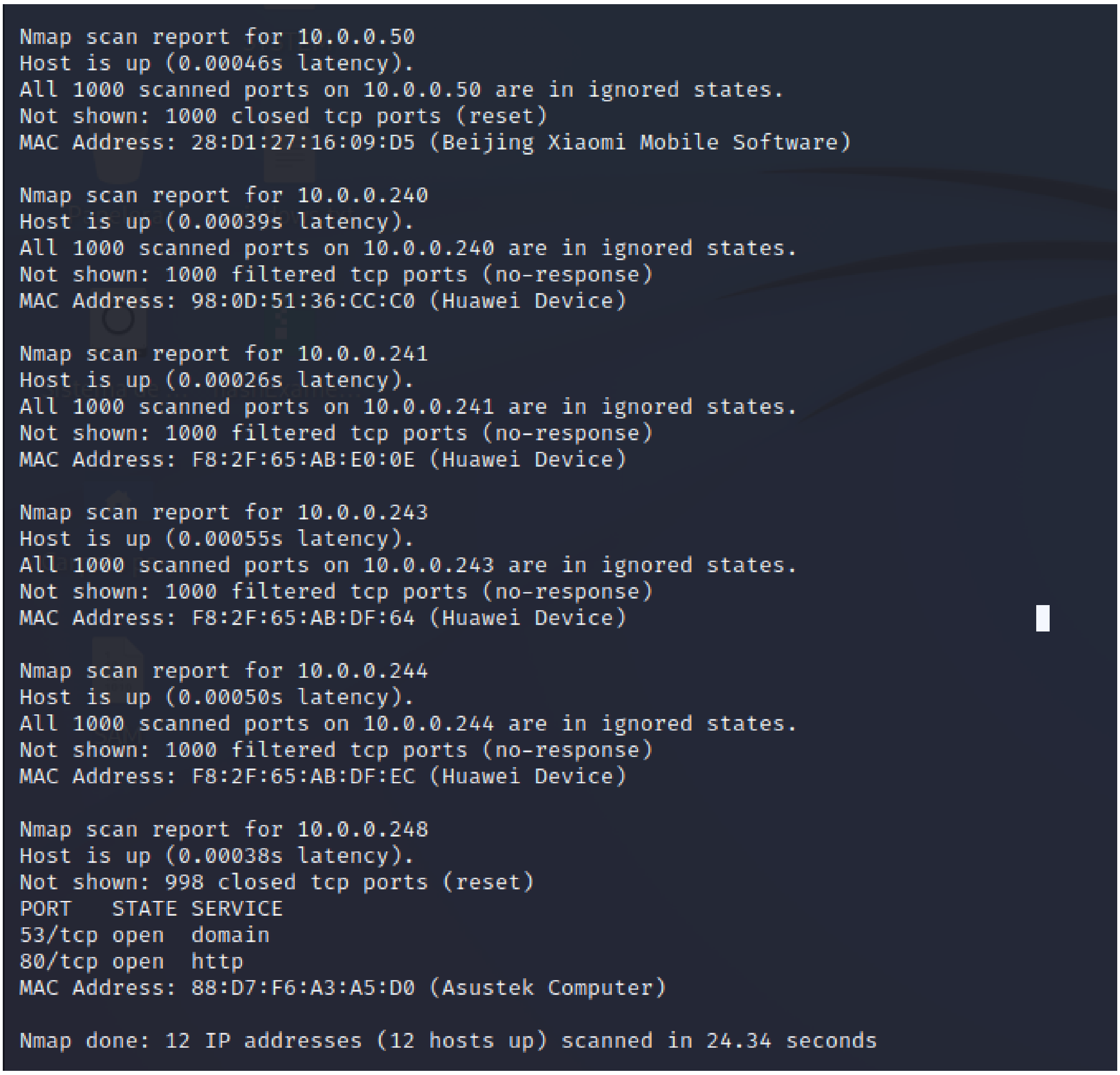
Ahora vamos a probar a ver que puertos tienen abiertos cada maquina.En la búsqueda por defecto buscara en los 1000 puertos conocidos y usando el protocolo TCP.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.0.1,2,3,4,5,12,50,240,241,243,244,248
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 09:47 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Nmap scan report for 10.0.0.1
Host is up (0.00062s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
89/tcp   open  su-mit-tg
90/tcp   open  dnsix
3030/tcp open  arepa-cas
3306/tcp open  mysql
3333/tcp open  dec-notes
8080/tcp open  http-proxy
8181/tcp open  intermapper
MAC Address: A8:5E:45:14:61:1A (Asustek Computer)

Nmap scan report for 10.0.0.2
Host is up (0.00051s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
8443/tcp open  https-alt
MAC Address: BC:30:5B:D4:2F:88 (Dell)

Nmap scan report for 10.0.0.3
Host is up (0.00047s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
6000/tcp open  X11
MAC Address: A8:5E:45:14:60:DF (Asustek Computer)
```



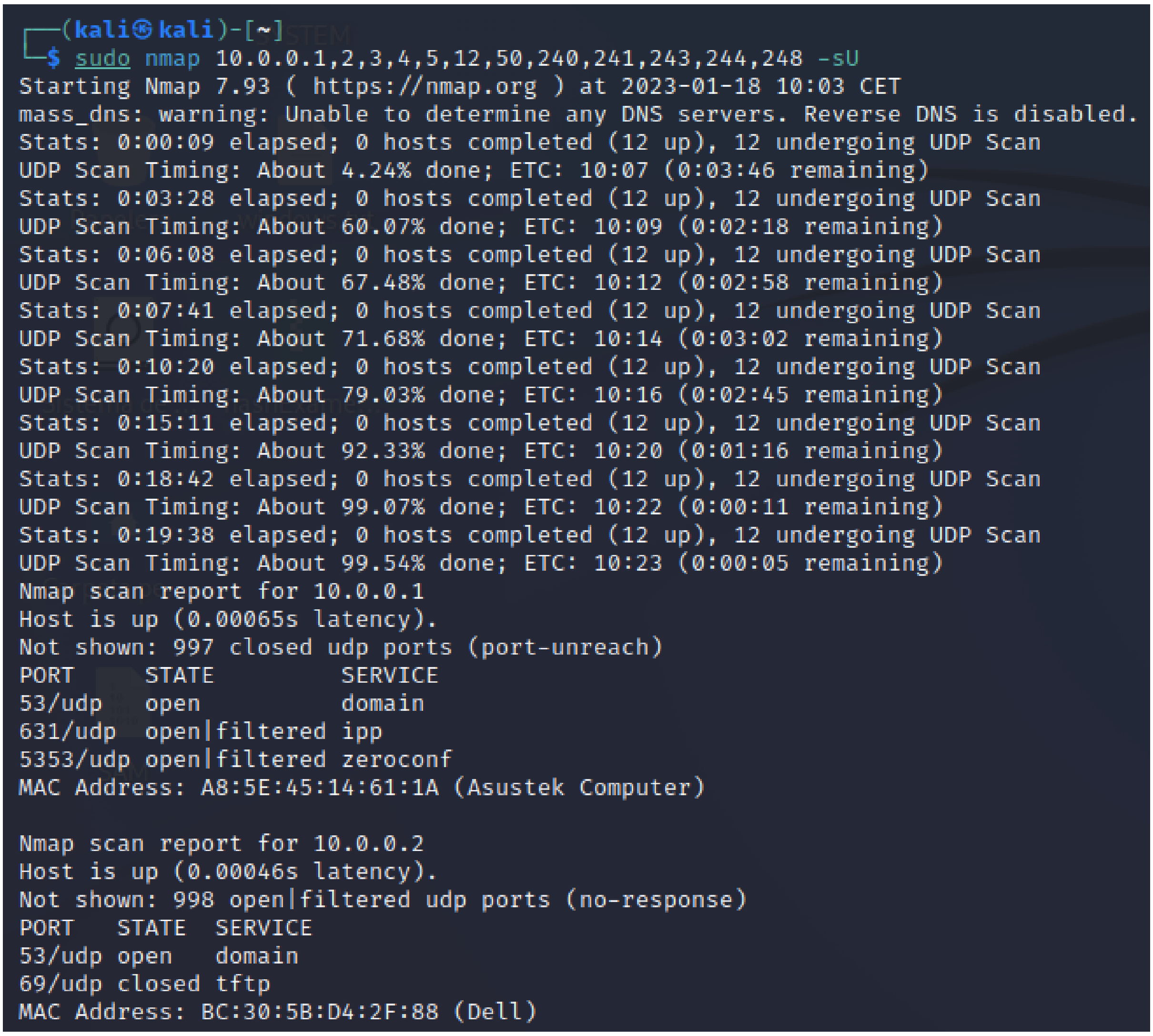
```
Nmap scan report for 10.0.0.4
Host is up (0.00067s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 08:00:27:80:E6:78 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.0.5
Host is up (0.00050s latency).
Not shown: 967 filtered tcp ports (no-response), 30 filtered tcp ports (admin-prohibited)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
9090/tcp open  zeus-admin
MAC Address: A8:5E:45:14:5D:27 (Asustek Computer)

Nmap scan report for 10.0.0.12
Host is up (0.00051s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
85/tcp   open  mit-ml-dev
88/tcp   open  kerberos-sec
89/tcp   open  su-mit-tg
389/tcp  open  ldap
443/tcp  open  https
444/tcp  open  snpp
3333/tcp open  dec-notes
MAC Address: 08:00:27:58:C7:E3 (Oracle VirtualBox virtual NIC)
```



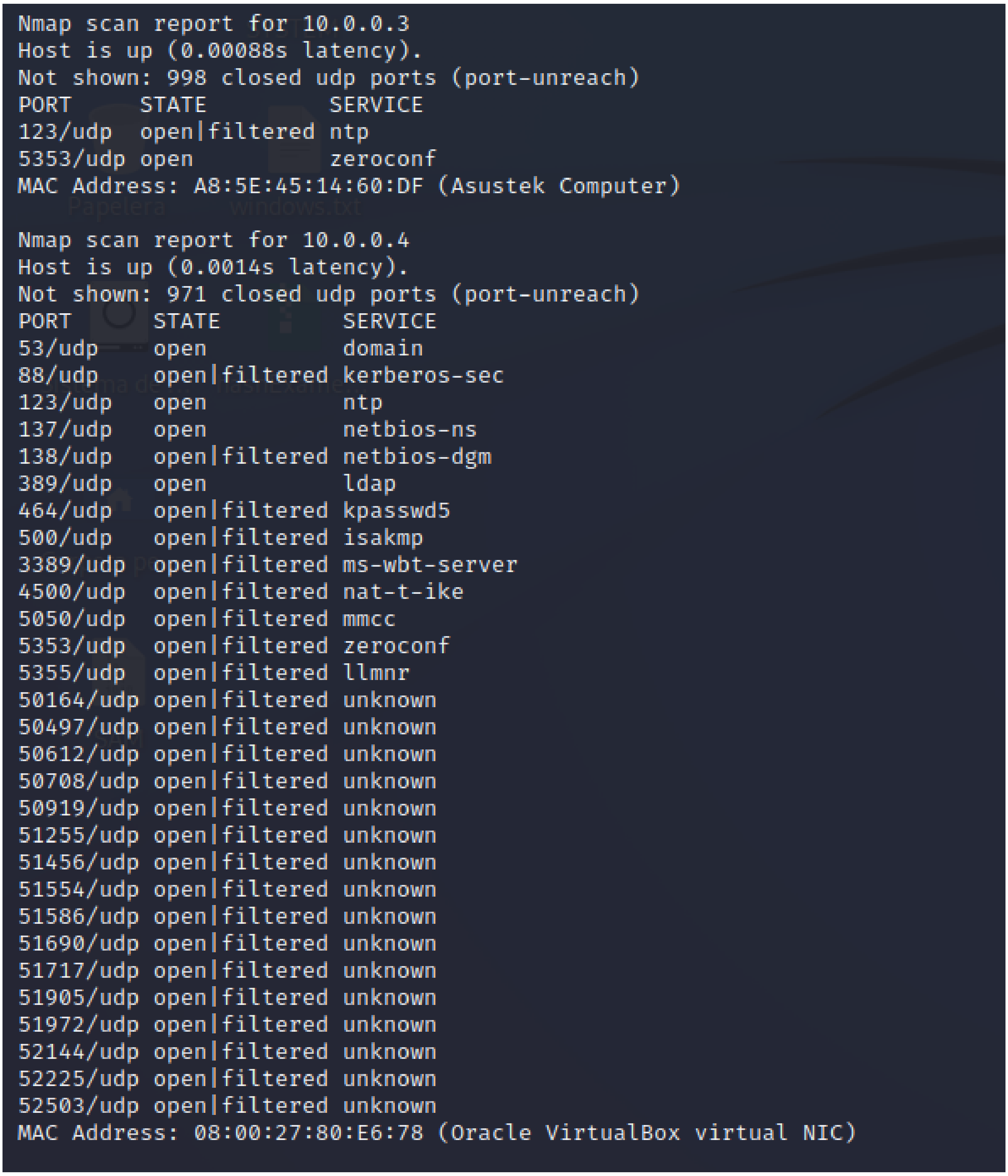
```
Nmap scan report for 10.0.0.50
Host is up (0.00046s latency).
All 1000 scanned ports on 10.0.0.50 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 28:D1:27:16:09:D5 (Beijing Xiaomi Mobile Software)

Nmap scan report for 10.0.0.240
Host is up (0.00039s latency).
All 1000 scanned ports on 10.0.0.240 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 98:0D:51:36:CC:C0 (Huawei Device)

Nmap scan report for 10.0.0.241
Host is up (0.00026s latency).
All 1000 scanned ports on 10.0.0.241 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F8:2F:65:AB:E0:0E (Huawei Device)

Nmap scan report for 10.0.0.243
Host is up (0.00055s latency).
All 1000 scanned ports on 10.0.0.243 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F8:2F:65:AB:DF:64 (Huawei Device)

Nmap scan report for 10.0.0.244
Host is up (0.00050s latency).
All 1000 scanned ports on 10.0.0.244 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F8:2F:65:AB:DF:EC (Huawei Device)

Nmap scan report for 10.0.0.248
Host is up (0.00038s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 88:D7:F6:A3:A5:D0 (Asustek Computer)

Nmap done: 12 IP addresses (12 hosts up) scanned in 24.34 seconds
```

Ahora la misma búsqueda, es decir los 1000 puertos conocidos, pero usando UDP.

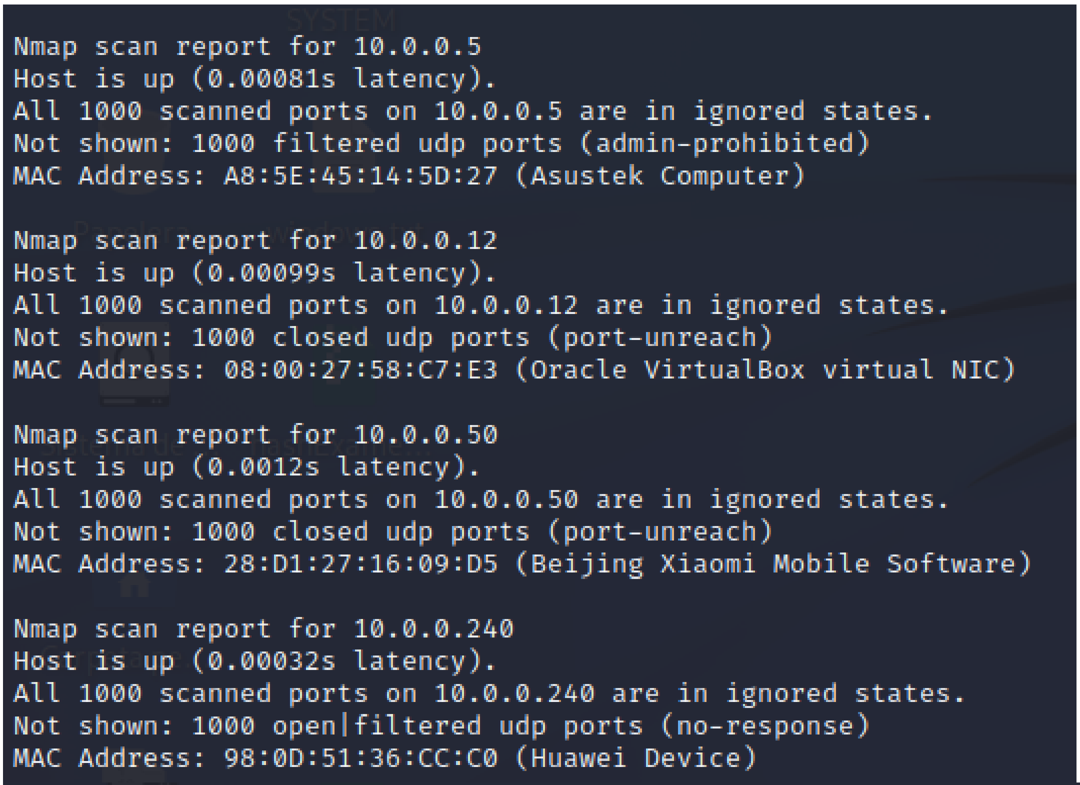
Podemos ver que hay bastantes mas puertos abiertos con el protocolo UDP que TCP y que algunos de estos puertos admiten tanto TCP como UDP.



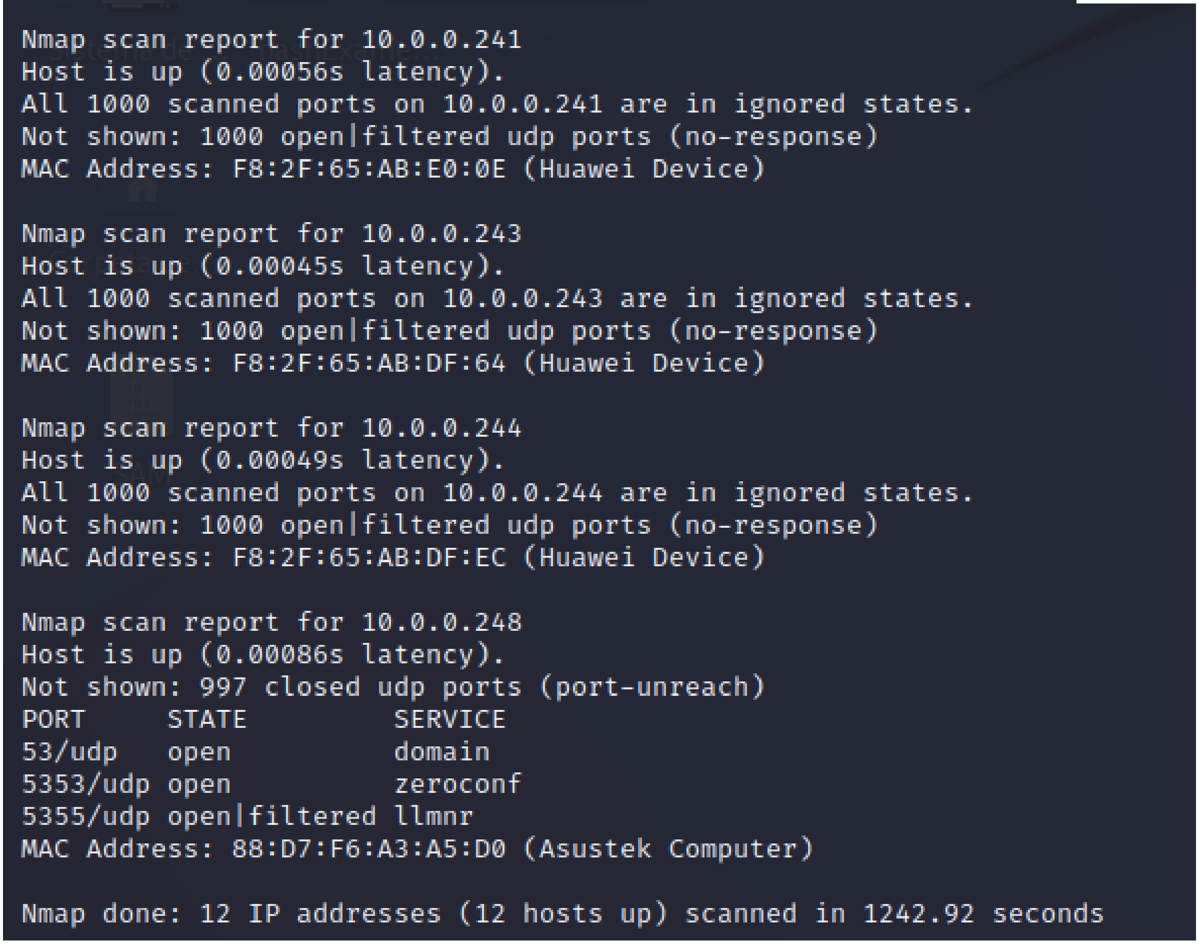
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.0.1,2,3,4,5,12,50,240,241,243,244,248 -sU
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 10:03 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Stats: 0:00:09 elapsed; 0 hosts completed (12 up), 12 undergoing UDP Scan
UDP Scan Timing: About 4.24% done; ETC: 10:07 (0:03:46 remaining)
Stats: 0:03:28 elapsed; 0 hosts completed (12 up), 12 undergoing UDP Scan
UDP Scan Timing: About 60.07% done; ETC: 10:09 (0:02:18 remaining)
Stats: 0:06:08 elapsed; 0 hosts completed (12 up), 12 undergoing UDP Scan
UDP Scan Timing: About 67.48% done; ETC: 10:12 (0:02:58 remaining)
Stats: 0:07:41 elapsed; 0 hosts completed (12 up), 12 undergoing UDP Scan
UDP Scan Timing: About 71.68% done; ETC: 10:14 (0:03:02 remaining)
Stats: 0:10:20 elapsed; 0 hosts completed (12 up), 12 undergoing UDP Scan
UDP Scan Timing: About 79.03% done; ETC: 10:16 (0:02:45 remaining)
Stats: 0:15:11 elapsed; 0 hosts completed (12 up), 12 undergoing UDP Scan
UDP Scan Timing: About 92.33% done; ETC: 10:20 (0:01:16 remaining)
Stats: 0:18:42 elapsed; 0 hosts completed (12 up), 12 undergoing UDP Scan
UDP Scan Timing: About 99.07% done; ETC: 10:22 (0:00:11 remaining)
Stats: 0:19:38 elapsed; 0 hosts completed (12 up), 12 undergoing UDP Scan
UDP Scan Timing: About 99.54% done; ETC: 10:23 (0:00:05 remaining)
Nmap scan report for 10.0.0.1
Host is up (0.00065s latency).
Not shown: 997 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf
MAC Address: A8:5E:45:14:61:1A (Asustek Computer)

Nmap scan report for 10.0.0.2
Host is up (0.00046s latency).
Not shown: 998 open|filtered udp ports (no-response)
PORT   STATE  SERVICE
53/udp open   domain
69/udp closed tftp
MAC Address: BC:30:5B:D4:2F:88 (Dell)
```



```
Nmap scan report for 10.0.0.3
Host is up (0.00088s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
5353/udp open          zeroconf
MAC Address: A8:5E:45:14:60:DF (Asustek Computer)

Nmap scan report for 10.0.0.4
Host is up (0.0014s latency).
Not shown: 971 closed udp ports (port-unreach)
PORT      STATE         SERVICE
53/udp    open          domain
88/udp    open|filtered kerberos-sec
123/udp   open          ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
389/udp   open          ldap
464/udp   open|filtered kpasswd5
500/udp   open|filtered isakmp
3389/udp  open|filtered ms-wbt-server
4500/udp  open|filtered nat-t-ike
5050/udp  open|filtered mmcc
5353/udp  open|filtered zeroconf
5355/udp  open|filtered llmnr
50164/udp open|filtered unknown
50497/udp open|filtered unknown
50612/udp open|filtered unknown
50708/udp open|filtered unknown
50919/udp open|filtered unknown
51255/udp open|filtered unknown
51456/udp open|filtered unknown
51554/udp open|filtered unknown
51586/udp open|filtered unknown
51690/udp open|filtered unknown
51717/udp open|filtered unknown
51905/udp open|filtered unknown
51972/udp open|filtered unknown
52144/udp open|filtered unknown
52225/udp open|filtered unknown
52503/udp open|filtered unknown
MAC Address: 08:00:27:80:E6:78 (Oracle VirtualBox virtual NIC)
```

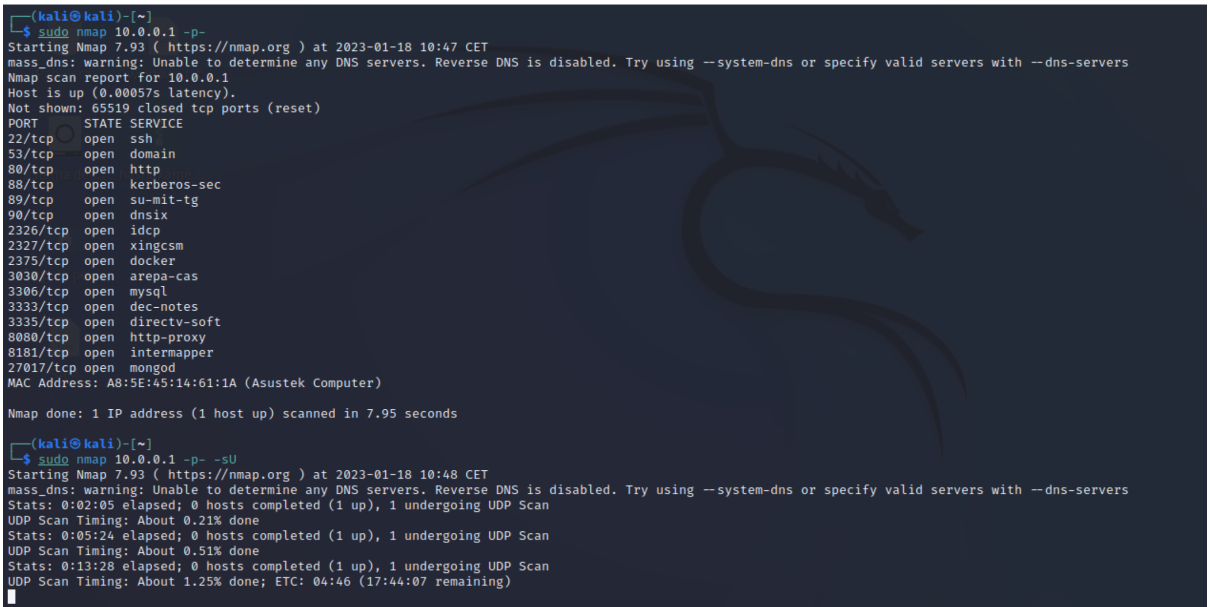


```
Nmap scan report for 10.0.0.5
Host is up (0.00081s latency).
All 1000 scanned ports on 10.0.0.5 are in ignored states.
Not shown: 1000 filtered udp ports (admin-prohibited)
MAC Address: A8:5E:45:14:5D:27 (Asustek Computer)

Nmap scan report for 10.0.0.12
Host is up (0.00099s latency).
All 1000 scanned ports on 10.0.0.12 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)
MAC Address: 08:00:27:58:C7:E3 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.0.50
Host is up (0.0012s latency).
All 1000 scanned ports on 10.0.0.50 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)
MAC Address: 28:D1:27:16:09:D5 (Beijing Xiaomi Mobile Software)

Nmap scan report for 10.0.0.240
Host is up (0.00032s latency).
All 1000 scanned ports on 10.0.0.240 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: 98:0D:51:36:CC:C0 (Huawei Device)
```

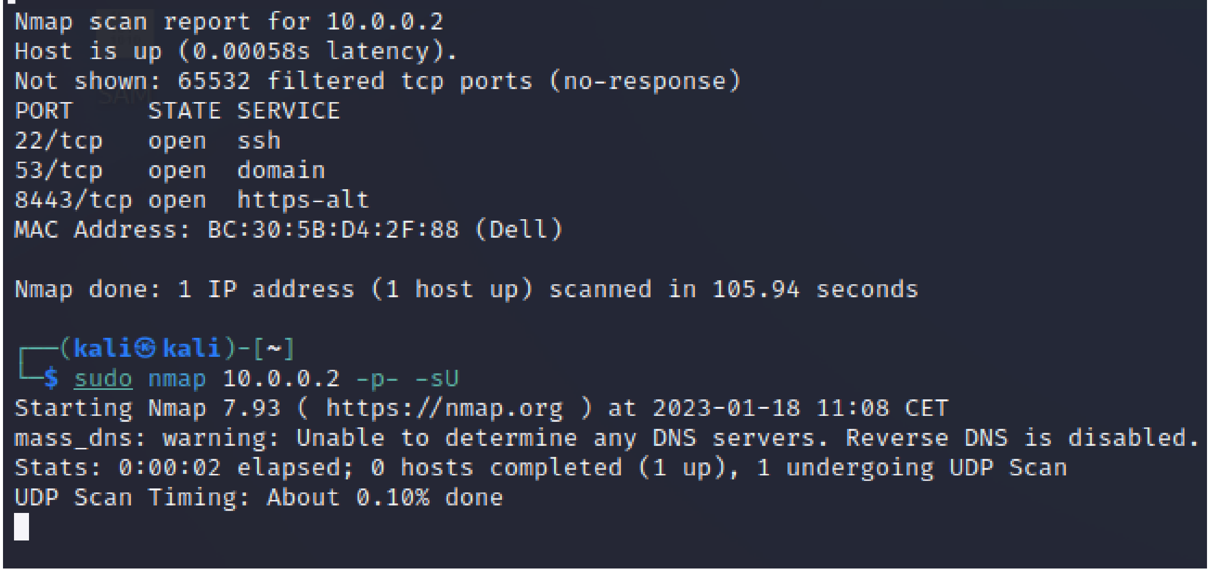


```
Nmap scan report for 10.0.0.241
Host is up (0.00056s latency).
All 1000 scanned ports on 10.0.0.241 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: F8:2F:65:AB:E0:0E (Huawei Device)

Nmap scan report for 10.0.0.243
Host is up (0.00045s latency).
All 1000 scanned ports on 10.0.0.243 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: F8:2F:65:AB:DF:64 (Huawei Device)

Nmap scan report for 10.0.0.244
Host is up (0.00049s latency).
All 1000 scanned ports on 10.0.0.244 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: F8:2F:65:AB:DF:EC (Huawei Device)

Nmap scan report for 10.0.0.248
Host is up (0.00086s latency).
Not shown: 997 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
5353/udp open          zeroconf
5355/udp open|filtered llmnr
MAC Address: 88:D7:F6:A3:A5:D0 (Asustek Computer)

Nmap done: 12 IP addresses (12 hosts up) scanned in 1242.92 seconds
```

Ahora vamos a escanear no solo los 1000 puertos conocidos, sino los 65535 puertos que hay en total. Primero mediante TCP y luego UDP. Nos centraremos solo en una ip para que la busqueda no se haga eterna.Primero con la 10.0.0.1 y despues con la 10.0.0.2.



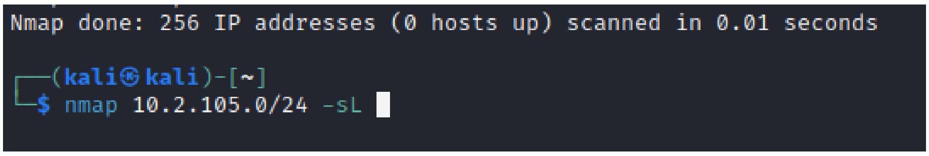
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.0.1 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 10:47 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.1
Host is up (0.00057s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
89/tcp    open  su-mit-tg
90/tcp    open  dnsix
2326/tcp  open  idcp
2327/tcp  open  xingcsm
2375/tcp  open  docker
3030/tcp  open  arepa-cas
3306/tcp  open  mysql
3333/tcp  open  dec-notes
3335/tcp  open  directv-soft
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
27017/tcp open  mongod
MAC Address: A8:5E:45:14:61:1A (Asustek Computer)

Nmap done: 1 IP address (1 host up) scanned in 7.95 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.0.1 -p- -sU
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 10:48 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:02:05 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 0.21% done
Stats: 0:05:24 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 0.51% done
Stats: 0:13:28 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 1.25% done; ETC: 04:46 (17:44:07 remaining)
█
```



```
Nmap scan report for 10.0.0.2
Host is up (0.00058s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
8443/tcp open  https-alt
MAC Address: BC:30:5B:D4:2F:88 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 105.94 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.0.2 -p- -sU
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 11:08 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 0.10% done
█
```

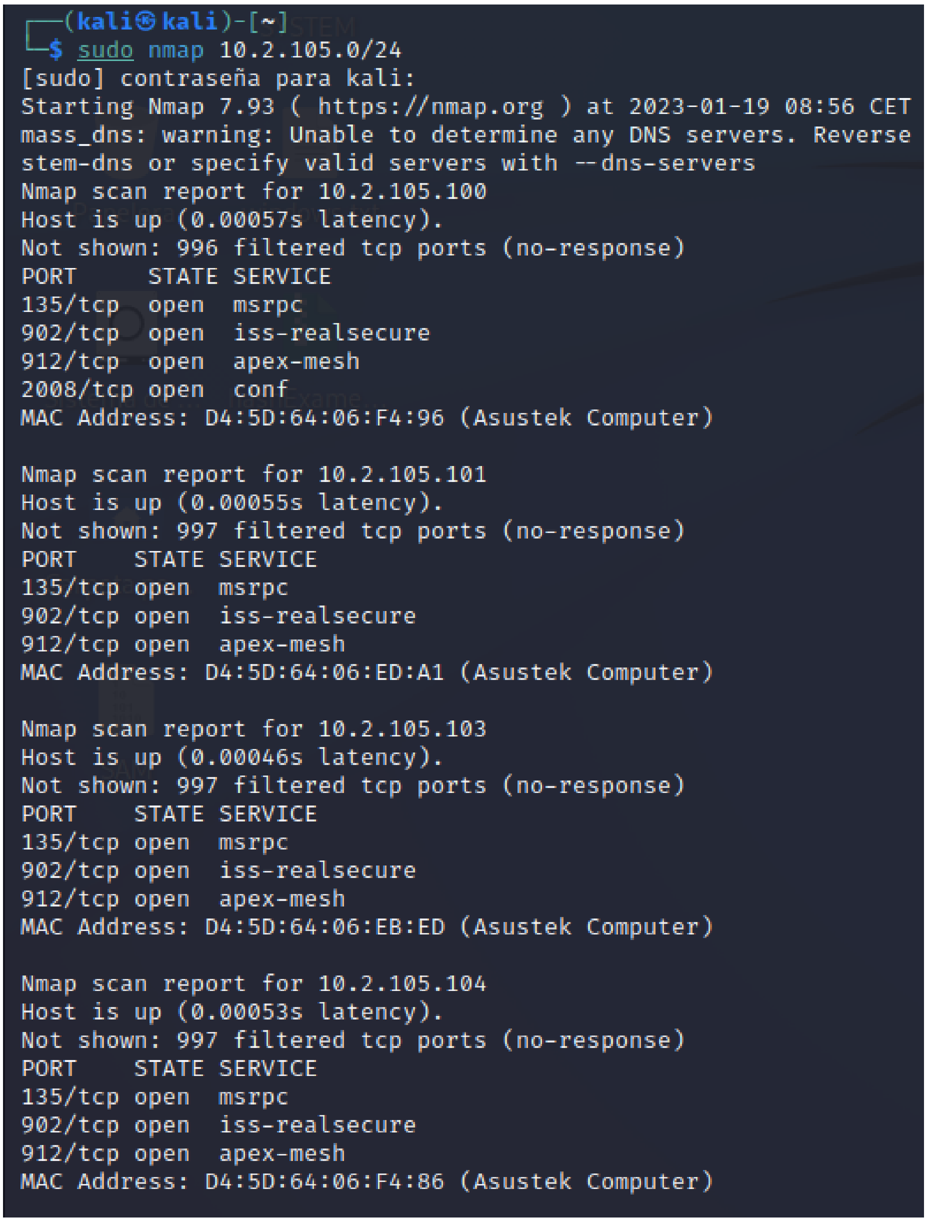
Red 10.2.105.0/24

Al igual que antes empezaremos por probar a hacer ping a las maquinas. En este caso todas son Windows y por lo tanto tienen por defecto un cortafuegos que impide el ping(ICMP). El resto de comandos son también los mismo que en el ejercicio anterior.

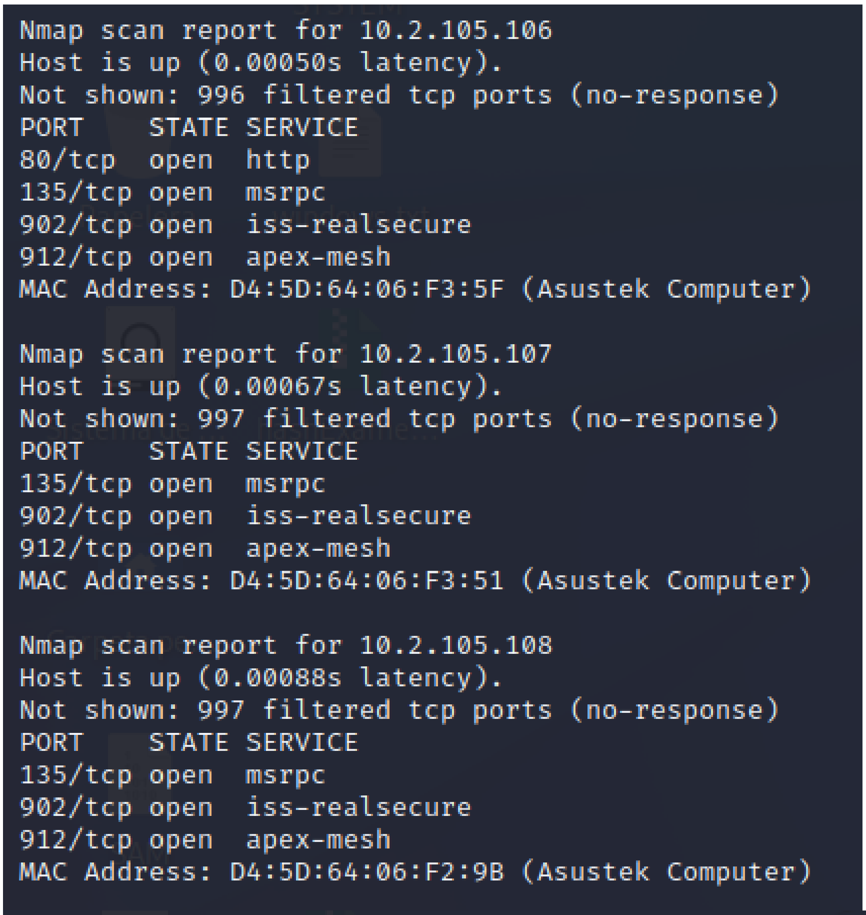


```
Nmap done: 256 IP addresses (0 hosts up) scanned in 0.01 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 10.2.105.0/24 -sL
```

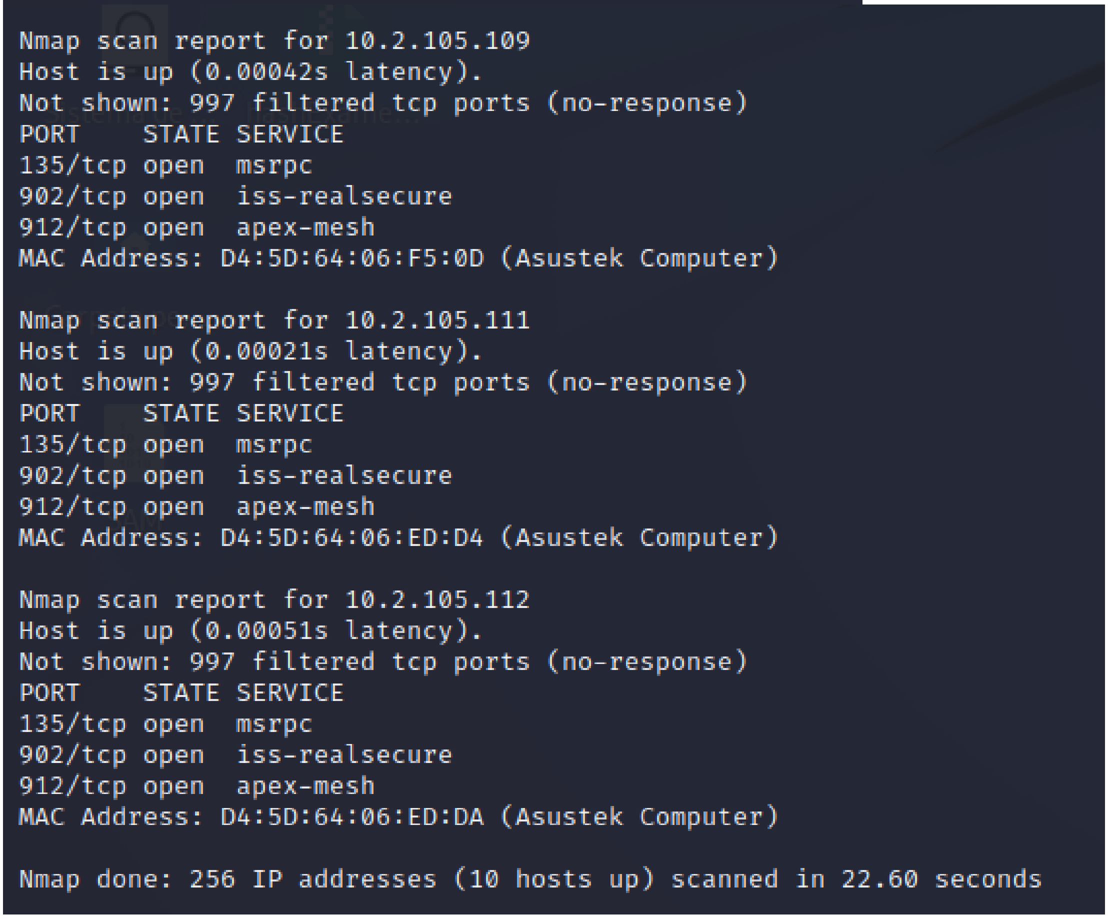
TCP



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.2.105.0/24
[sudo] contraseña para kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 08:56 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse
stem-dns or specify valid servers with --dns-servers
Nmap scan report for 10.2.105.100
Host is up (0.00057s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2008/tcp open  conf
MAC Address: D4:5D:64:06:F4:96 (Asustek Computer)

Nmap scan report for 10.2.105.101
Host is up (0.00055s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: D4:5D:64:06:ED:A1 (Asustek Computer)

Nmap scan report for 10.2.105.103
Host is up (0.00046s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: D4:5D:64:06:EB:ED (Asustek Computer)

Nmap scan report for 10.2.105.104
Host is up (0.00053s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: D4:5D:64:06:F4:86 (Asustek Computer)
```

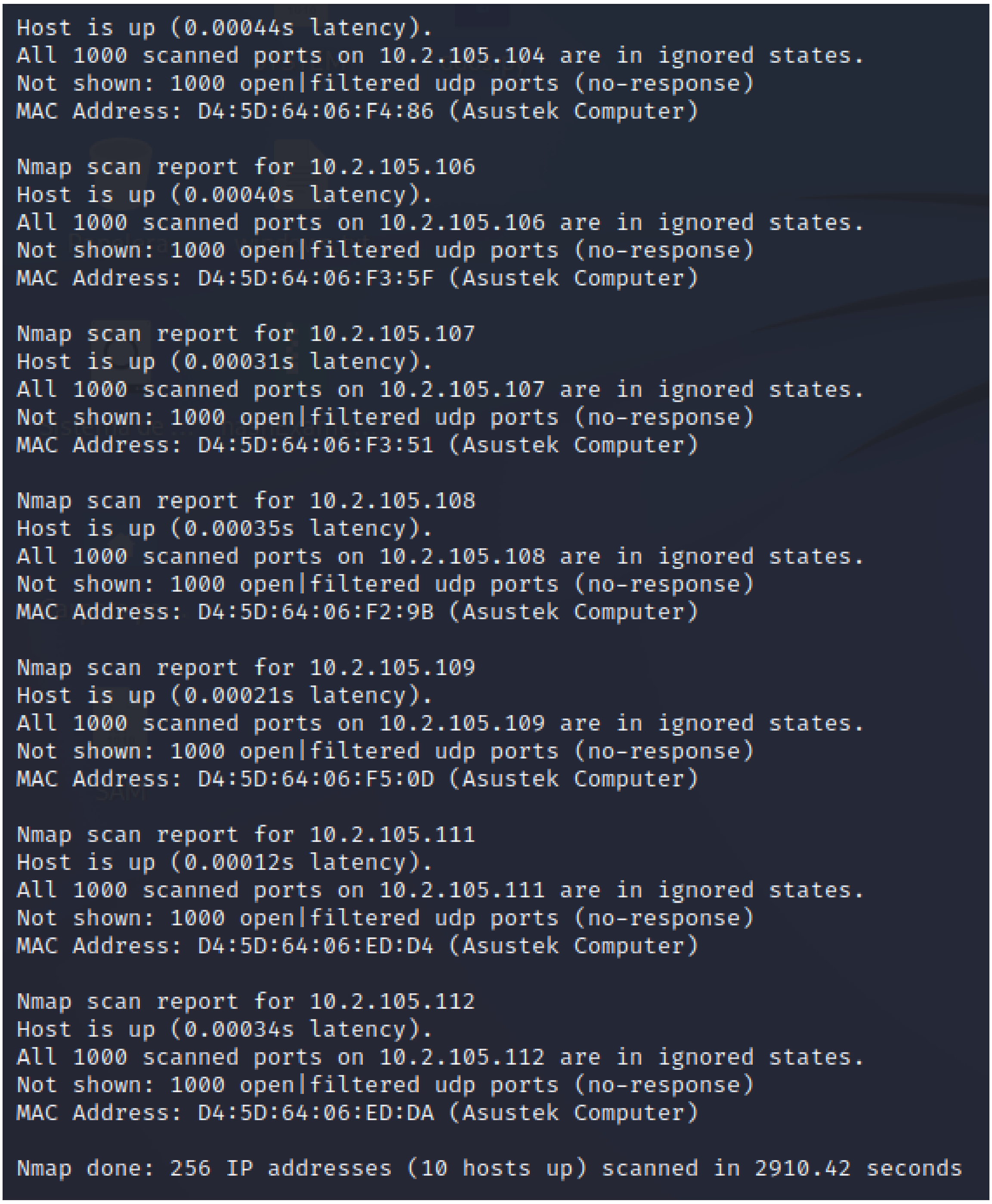


```
Nmap scan report for 10.2.105.106
Host is up (0.00050s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp open  msrpc
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: D4:5D:64:06:F3:5F (Asustek Computer)

Nmap scan report for 10.2.105.107
Host is up (0.00067s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp open  msrpc
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: D4:5D:64:06:F3:51 (Asustek Computer)

Nmap scan report for 10.2.105.108
Host is up (0.00088s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp open  msrpc
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: D4:5D:64:06:F2:9B (Asustek Computer)
```



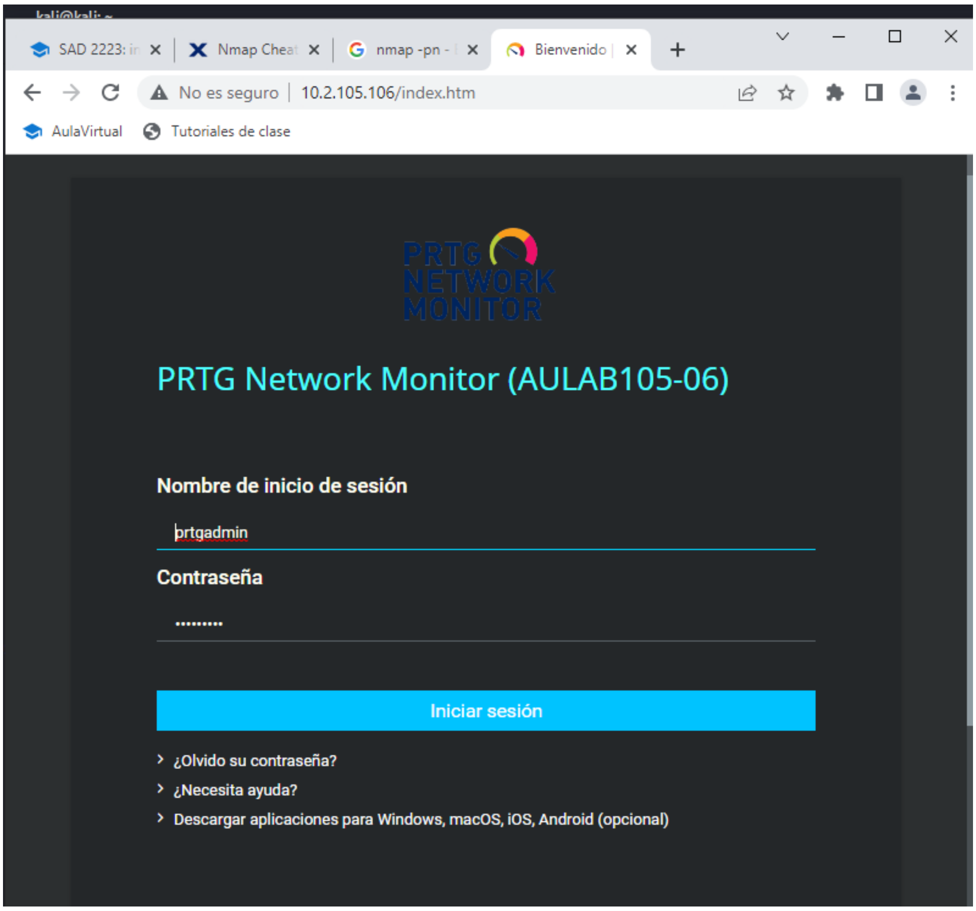
```
Nmap scan report for 10.2.105.109
Host is up (0.00042s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp open  msrpc
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: D4:5D:64:06:F5:0D (Asustek Computer)

Nmap scan report for 10.2.105.111
Host is up (0.00021s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp open  msrpc
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: D4:5D:64:06:ED:D4 (Asustek Computer)

Nmap scan report for 10.2.105.112
Host is up (0.00051s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp open  msrpc
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: D4:5D:64:06:ED:DA (Asustek Computer)

Nmap done: 256 IP addresses (10 hosts up) scanned in 22.60 seconds
```

UDP



```
Host is up (0.00044s latency).
All 1000 scanned ports on 10.2.105.104 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: D4:5D:64:06:F4:86 (Asustek Computer)

Nmap scan report for 10.2.105.106
Host is up (0.00040s latency).
All 1000 scanned ports on 10.2.105.106 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: D4:5D:64:06:F3:5F (Asustek Computer)

Nmap scan report for 10.2.105.107
Host is up (0.00031s latency).
All 1000 scanned ports on 10.2.105.107 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: D4:5D:64:06:F3:51 (Asustek Computer)

Nmap scan report for 10.2.105.108
Host is up (0.00035s latency).
All 1000 scanned ports on 10.2.105.108 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: D4:5D:64:06:F2:9B (Asustek Computer)

Nmap scan report for 10.2.105.109
Host is up (0.00021s latency).
All 1000 scanned ports on 10.2.105.109 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: D4:5D:64:06:F5:0D (Asustek Computer)

Nmap scan report for 10.2.105.111
Host is up (0.00012s latency).
All 1000 scanned ports on 10.2.105.111 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: D4:5D:64:06:ED:D4 (Asustek Computer)

Nmap scan report for 10.2.105.112
Host is up (0.00034s latency).
All 1000 scanned ports on 10.2.105.112 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: D4:5D:64:06:ED:DA (Asustek Computer)

Nmap done: 256 IP addresses (10 hosts up) scanned in 2910.42 seconds
```

Por ejemplo en la 10.2.105.106 hay una conexión HTTP abierta.



PRTG Network Monitor (AULAB105-06)

Nombre de inicio de sesión

prtgadmin

Contraseña

•••••••••

Iniciar sesión

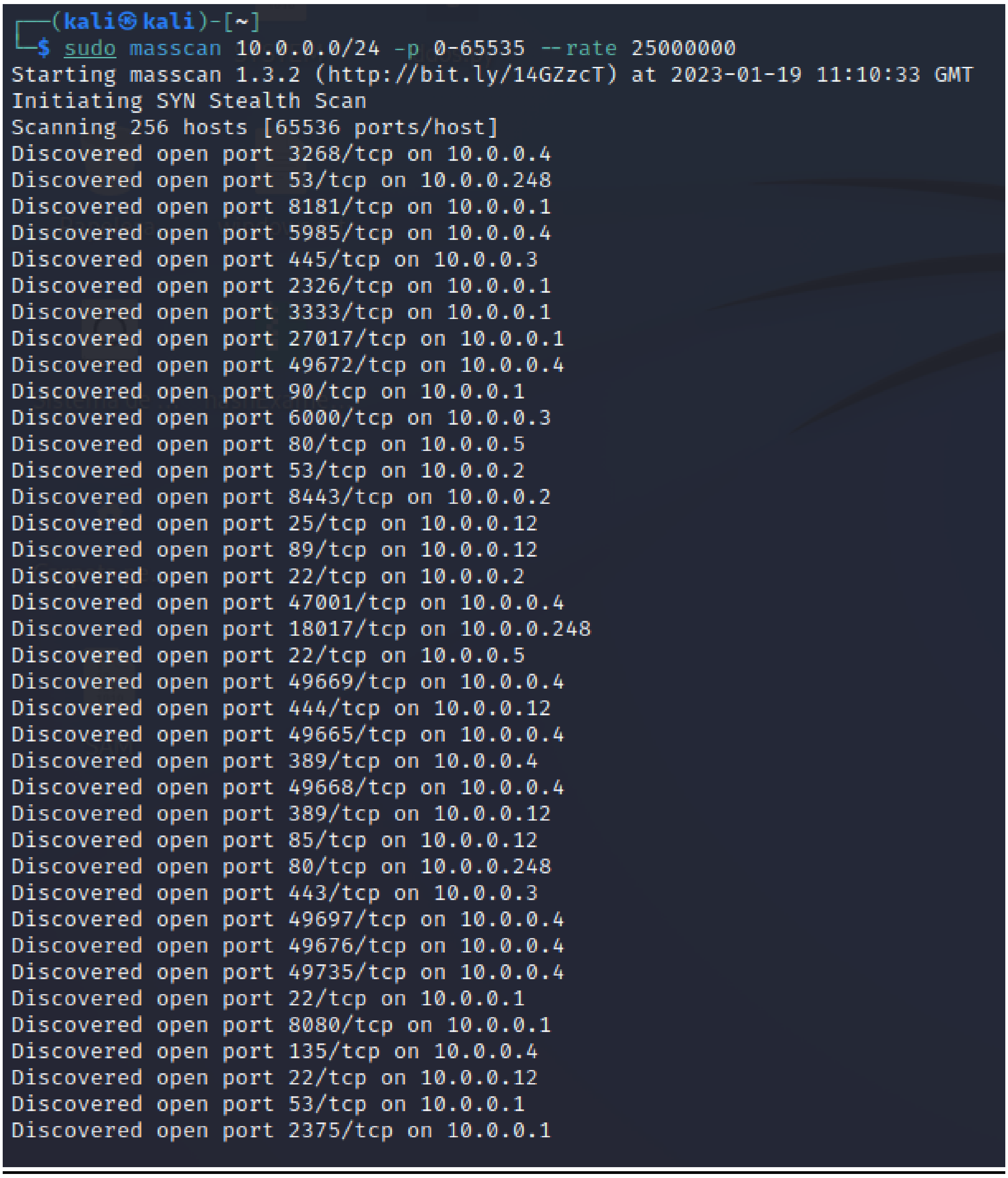
- ¿Olvido su contraseña?
- ¿Necesita ayuda?
- Descargar aplicaciones para Windows, macOS, iOS, Android (opcional)

masscan.

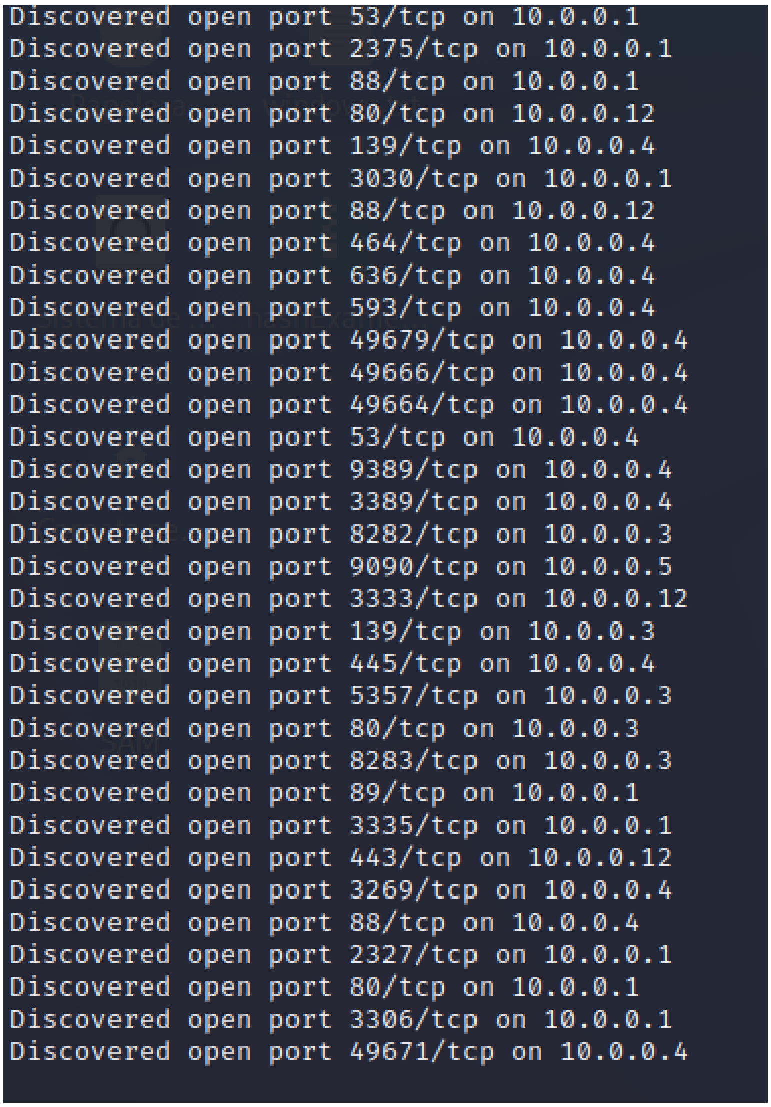
La única diferencia entre masscan y nmap es que en masscan puedes elegir cuantos paquetes mandar por segundo entre 0-25000000, siendo 100 los paquetes por defecto. Esto se declara mediante la variable rate. Lo que no me gusta tanto de masscan es que no te ordena los resultados , sino que te los va mostrando a medida que los descubre.

Red 10.0.0.0/24

TCP

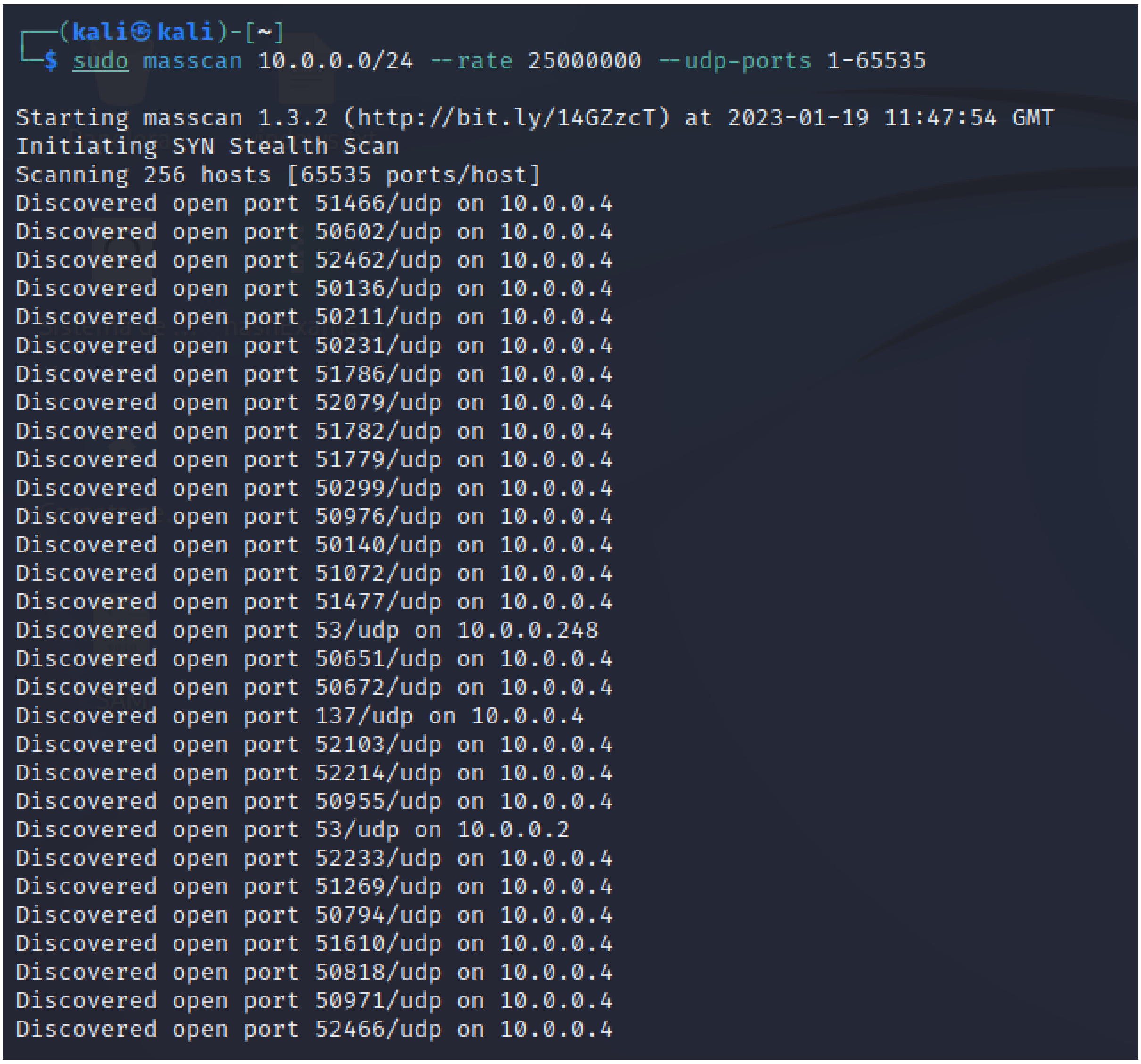


```
┌──(kali㉿kali)-[~]
└─$ sudo masscan 10.0.0.0/24 -p 0-65535 --rate 25000000
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-01-19 11:10:33 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [65536 ports/host]
Discovered open port 3268/tcp on 10.0.0.4
Discovered open port 53/tcp on 10.0.0.248
Discovered open port 8181/tcp on 10.0.0.1
Discovered open port 5985/tcp on 10.0.0.4
Discovered open port 445/tcp on 10.0.0.3
Discovered open port 2326/tcp on 10.0.0.1
Discovered open port 3333/tcp on 10.0.0.1
Discovered open port 27017/tcp on 10.0.0.1
Discovered open port 49672/tcp on 10.0.0.4
Discovered open port 90/tcp on 10.0.0.1
Discovered open port 6000/tcp on 10.0.0.3
Discovered open port 80/tcp on 10.0.0.5
Discovered open port 53/tcp on 10.0.0.2
Discovered open port 8443/tcp on 10.0.0.2
Discovered open port 25/tcp on 10.0.0.12
Discovered open port 89/tcp on 10.0.0.12
Discovered open port 22/tcp on 10.0.0.2
Discovered open port 47001/tcp on 10.0.0.4
Discovered open port 18017/tcp on 10.0.0.248
Discovered open port 22/tcp on 10.0.0.5
Discovered open port 49669/tcp on 10.0.0.4
Discovered open port 444/tcp on 10.0.0.12
Discovered open port 49665/tcp on 10.0.0.4
Discovered open port 389/tcp on 10.0.0.4
Discovered open port 49668/tcp on 10.0.0.4
Discovered open port 389/tcp on 10.0.0.12
Discovered open port 85/tcp on 10.0.0.12
Discovered open port 80/tcp on 10.0.0.248
Discovered open port 443/tcp on 10.0.0.3
Discovered open port 49697/tcp on 10.0.0.4
Discovered open port 49676/tcp on 10.0.0.4
Discovered open port 49735/tcp on 10.0.0.4
Discovered open port 22/tcp on 10.0.0.1
Discovered open port 8080/tcp on 10.0.0.1
Discovered open port 135/tcp on 10.0.0.4
Discovered open port 22/tcp on 10.0.0.12
Discovered open port 53/tcp on 10.0.0.1
Discovered open port 2375/tcp on 10.0.0.1
```



```
Discovered open port 53/tcp on 10.0.0.1
Discovered open port 2375/tcp on 10.0.0.1
Discovered open port 88/tcp on 10.0.0.1
Discovered open port 80/tcp on 10.0.0.12
Discovered open port 139/tcp on 10.0.0.4
Discovered open port 3030/tcp on 10.0.0.1
Discovered open port 88/tcp on 10.0.0.12
Discovered open port 464/tcp on 10.0.0.4
Discovered open port 636/tcp on 10.0.0.4
Discovered open port 593/tcp on 10.0.0.4
Discovered open port 49679/tcp on 10.0.0.4
Discovered open port 49666/tcp on 10.0.0.4
Discovered open port 49664/tcp on 10.0.0.4
Discovered open port 53/tcp on 10.0.0.4
Discovered open port 9389/tcp on 10.0.0.4
Discovered open port 3389/tcp on 10.0.0.4
Discovered open port 8282/tcp on 10.0.0.3
Discovered open port 9090/tcp on 10.0.0.5
Discovered open port 3333/tcp on 10.0.0.12
Discovered open port 139/tcp on 10.0.0.3
Discovered open port 445/tcp on 10.0.0.4
Discovered open port 5357/tcp on 10.0.0.3
Discovered open port 80/tcp on 10.0.0.3
Discovered open port 8283/tcp on 10.0.0.3
Discovered open port 89/tcp on 10.0.0.1
Discovered open port 3335/tcp on 10.0.0.1
Discovered open port 443/tcp on 10.0.0.12
Discovered open port 3269/tcp on 10.0.0.4
Discovered open port 88/tcp on 10.0.0.4
Discovered open port 2327/tcp on 10.0.0.1
Discovered open port 80/tcp on 10.0.0.1
Discovered open port 3306/tcp on 10.0.0.1
Discovered open port 49671/tcp on 10.0.0.4
```

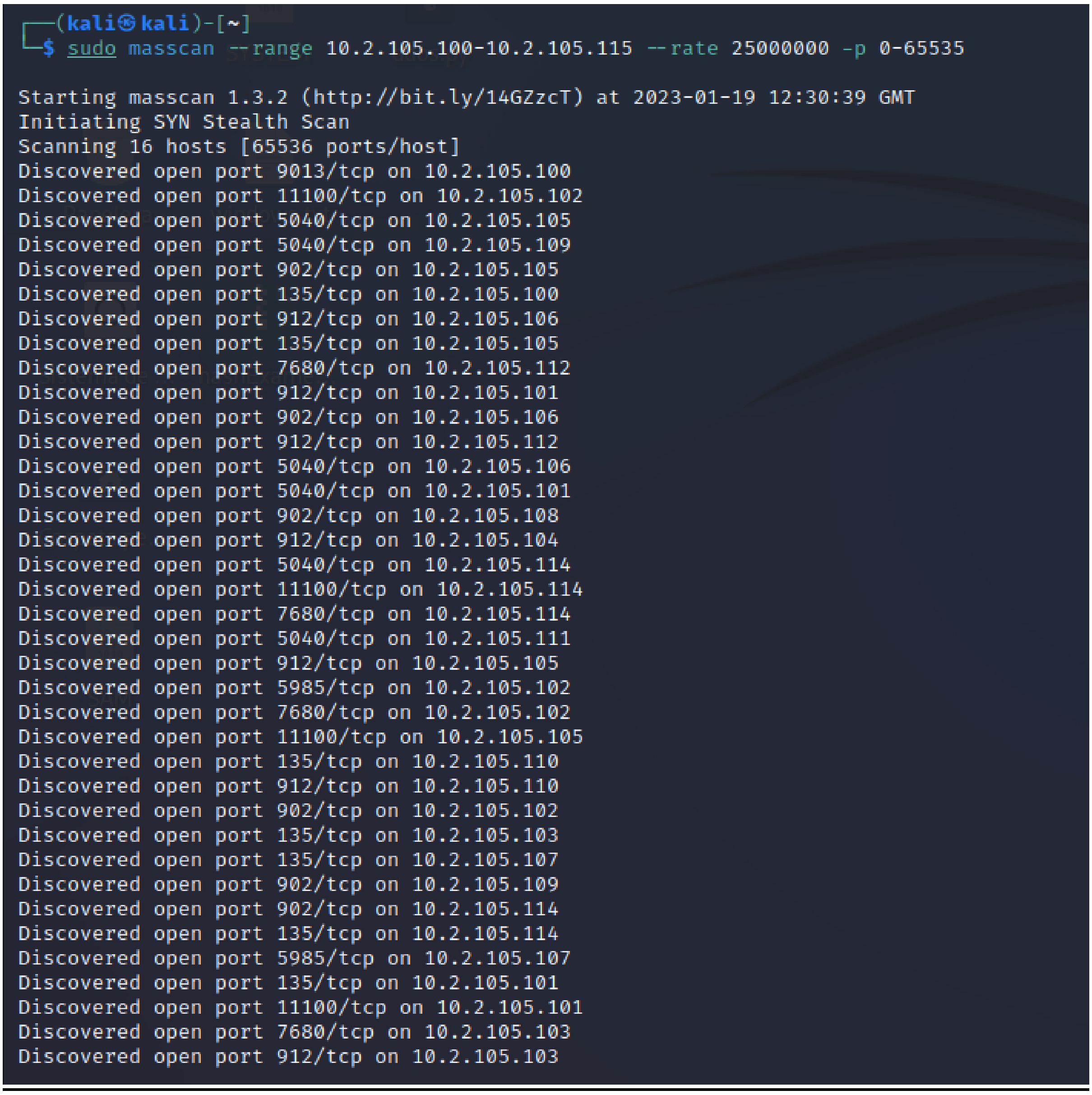
UDP



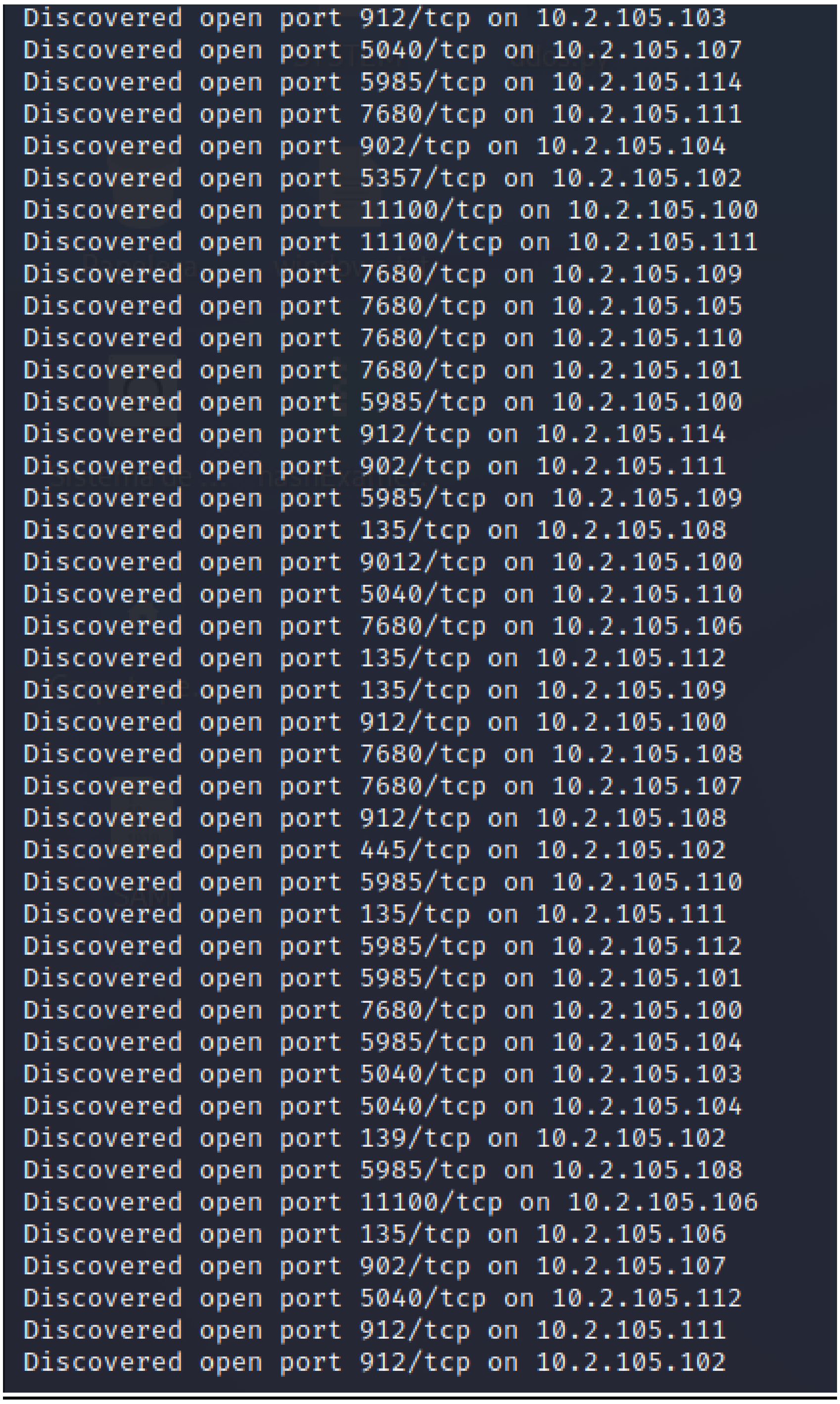
```
┌──(kali㉿kali)-[~]
└─$ sudo masscan 10.0.0.0/24 --rate 25000000 --udp-ports 1-65535

Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-01-19 11:47:54 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [65535 ports/host]
Discovered open port 51466/udp on 10.0.0.4
Discovered open port 50602/udp on 10.0.0.4
Discovered open port 52462/udp on 10.0.0.4
Discovered open port 50136/udp on 10.0.0.4
Discovered open port 50211/udp on 10.0.0.4
Discovered open port 50231/udp on 10.0.0.4
Discovered open port 51786/udp on 10.0.0.4
Discovered open port 52079/udp on 10.0.0.4
Discovered open port 51782/udp on 10.0.0.4
Discovered open port 51779/udp on 10.0.0.4
Discovered open port 50299/udp on 10.0.0.4
Discovered open port 50976/udp on 10.0.0.4
Discovered open port 50140/udp on 10.0.0.4
Discovered open port 51072/udp on 10.0.0.4
Discovered open port 51477/udp on 10.0.0.4
Discovered open port 53/udp on 10.0.0.248
Discovered open port 50651/udp on 10.0.0.4
Discovered open port 50672/udp on 10.0.0.4
Discovered open port 137/udp on 10.0.0.4
Discovered open port 52103/udp on 10.0.0.4
Discovered open port 52214/udp on 10.0.0.4
Discovered open port 50955/udp on 10.0.0.4
Discovered open port 53/udp on 10.0.0.2
Discovered open port 52233/udp on 10.0.0.4
Discovered open port 51269/udp on 10.0.0.4
Discovered open port 50794/udp on 10.0.0.4
Discovered open port 51610/udp on 10.0.0.4
Discovered open port 50818/udp on 10.0.0.4
Discovered open port 50971/udp on 10.0.0.4
Discovered open port 52466/udp on 10.0.0.4
```

Red 10.2.105.0/24

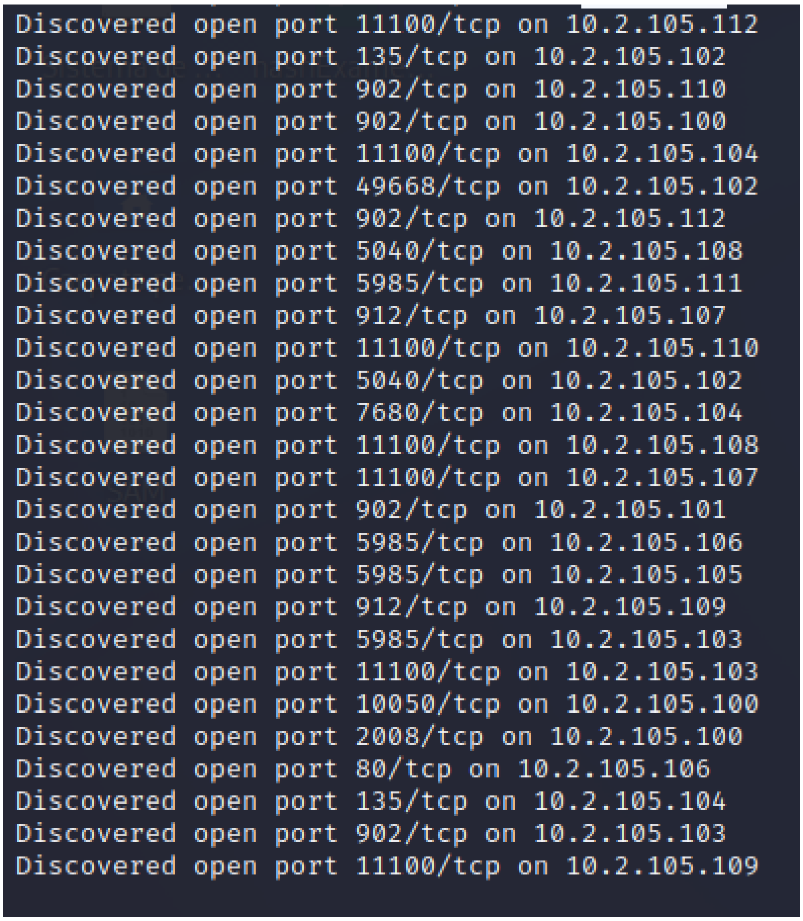
TCP



```
┌──(kali㉿kali)-[~]
└─$ sudo masscan --range 10.2.105.100-10.2.105.115 --rate 25000000 -p 0-65535

Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-01-19 12:30:39 GMT
Initiating SYN Stealth Scan
Scanning 16 hosts [65536 ports/host]
Discovered open port 9013/tcp on 10.2.105.100
Discovered open port 11100/tcp on 10.2.105.102
Discovered open port 5040/tcp on 10.2.105.105
Discovered open port 5040/tcp on 10.2.105.109
Discovered open port 902/tcp on 10.2.105.105
Discovered open port 135/tcp on 10.2.105.100
Discovered open port 912/tcp on 10.2.105.106
Discovered open port 135/tcp on 10.2.105.105
Discovered open port 7680/tcp on 10.2.105.112
Discovered open port 912/tcp on 10.2.105.101
Discovered open port 902/tcp on 10.2.105.106
Discovered open port 912/tcp on 10.2.105.112
Discovered open port 5040/tcp on 10.2.105.106
Discovered open port 5040/tcp on 10.2.105.101
Discovered open port 902/tcp on 10.2.105.108
Discovered open port 912/tcp on 10.2.105.104
Discovered open port 5040/tcp on 10.2.105.114
Discovered open port 11100/tcp on 10.2.105.114
Discovered open port 7680/tcp on 10.2.105.114
Discovered open port 5040/tcp on 10.2.105.111
Discovered open port 912/tcp on 10.2.105.105
Discovered open port 5985/tcp on 10.2.105.102
Discovered open port 7680/tcp on 10.2.105.102
Discovered open port 11100/tcp on 10.2.105.105
Discovered open port 135/tcp on 10.2.105.110
Discovered open port 912/tcp on 10.2.105.110
Discovered open port 902/tcp on 10.2.105.102
Discovered open port 135/tcp on 10.2.105.103
Discovered open port 135/tcp on 10.2.105.107
Discovered open port 902/tcp on 10.2.105.109
Discovered open port 902/tcp on 10.2.105.114
Discovered open port 135/tcp on 10.2.105.114
Discovered open port 5985/tcp on 10.2.105.107
Discovered open port 135/tcp on 10.2.105.101
Discovered open port 11100/tcp on 10.2.105.101
Discovered open port 7680/tcp on 10.2.105.103
Discovered open port 912/tcp on 10.2.105.103
```

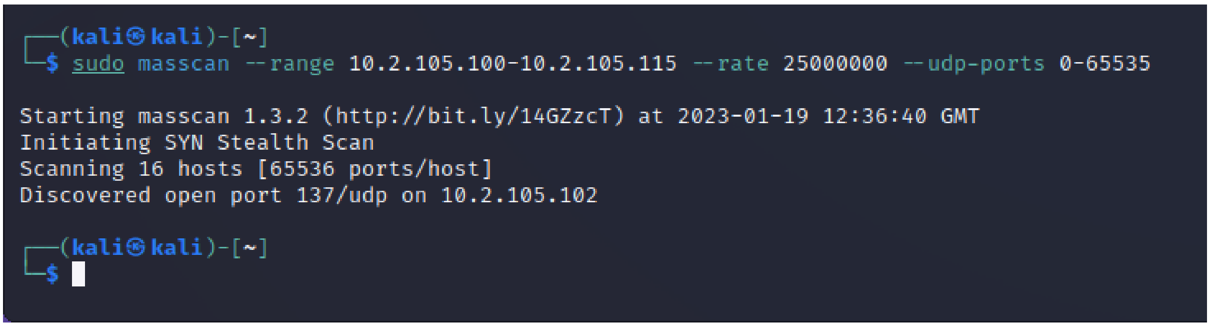


```
Discovered open port 912/tcp on 10.2.105.103
Discovered open port 5040/tcp on 10.2.105.107
Discovered open port 5985/tcp on 10.2.105.114
Discovered open port 7680/tcp on 10.2.105.111
Discovered open port 902/tcp on 10.2.105.104
Discovered open port 5357/tcp on 10.2.105.102
Discovered open port 11100/tcp on 10.2.105.100
Discovered open port 11100/tcp on 10.2.105.111
Discovered open port 7680/tcp on 10.2.105.109
Discovered open port 7680/tcp on 10.2.105.105
Discovered open port 7680/tcp on 10.2.105.110
Discovered open port 7680/tcp on 10.2.105.101
Discovered open port 5985/tcp on 10.2.105.100
Discovered open port 912/tcp on 10.2.105.114
Discovered open port 902/tcp on 10.2.105.111
Discovered open port 5985/tcp on 10.2.105.109
Discovered open port 135/tcp on 10.2.105.108
Discovered open port 9012/tcp on 10.2.105.100
Discovered open port 5040/tcp on 10.2.105.110
Discovered open port 7680/tcp on 10.2.105.106
Discovered open port 135/tcp on 10.2.105.112
Discovered open port 135/tcp on 10.2.105.109
Discovered open port 912/tcp on 10.2.105.100
Discovered open port 7680/tcp on 10.2.105.108
Discovered open port 7680/tcp on 10.2.105.107
Discovered open port 912/tcp on 10.2.105.108
Discovered open port 445/tcp on 10.2.105.102
Discovered open port 5985/tcp on 10.2.105.110
Discovered open port 135/tcp on 10.2.105.111
Discovered open port 5985/tcp on 10.2.105.112
Discovered open port 5985/tcp on 10.2.105.101
Discovered open port 7680/tcp on 10.2.105.100
Discovered open port 5985/tcp on 10.2.105.104
Discovered open port 5040/tcp on 10.2.105.103
Discovered open port 5040/tcp on 10.2.105.104
Discovered open port 139/tcp on 10.2.105.102
Discovered open port 5985/tcp on 10.2.105.108
Discovered open port 11100/tcp on 10.2.105.106
Discovered open port 135/tcp on 10.2.105.106
Discovered open port 902/tcp on 10.2.105.107
Discovered open port 5040/tcp on 10.2.105.112
Discovered open port 912/tcp on 10.2.105.111
Discovered open port 912/tcp on 10.2.105.102
```



```
Discovered open port 11100/tcp on 10.2.105.112
Discovered open port 135/tcp on 10.2.105.102
Discovered open port 902/tcp on 10.2.105.110
Discovered open port 902/tcp on 10.2.105.100
Discovered open port 11100/tcp on 10.2.105.104
Discovered open port 49668/tcp on 10.2.105.102
Discovered open port 902/tcp on 10.2.105.112
Discovered open port 5040/tcp on 10.2.105.108
Discovered open port 5985/tcp on 10.2.105.111
Discovered open port 912/tcp on 10.2.105.107
Discovered open port 11100/tcp on 10.2.105.110
Discovered open port 5040/tcp on 10.2.105.102
Discovered open port 7680/tcp on 10.2.105.104
Discovered open port 11100/tcp on 10.2.105.108
Discovered open port 11100/tcp on 10.2.105.107
Discovered open port 902/tcp on 10.2.105.101
Discovered open port 5985/tcp on 10.2.105.106
Discovered open port 5985/tcp on 10.2.105.105
Discovered open port 912/tcp on 10.2.105.109
Discovered open port 5985/tcp on 10.2.105.103
Discovered open port 11100/tcp on 10.2.105.103
Discovered open port 10050/tcp on 10.2.105.100
Discovered open port 2008/tcp on 10.2.105.100
Discovered open port 80/tcp on 10.2.105.106
Discovered open port 135/tcp on 10.2.105.104
Discovered open port 902/tcp on 10.2.105.103
Discovered open port 11100/tcp on 10.2.105.109
```

UDP

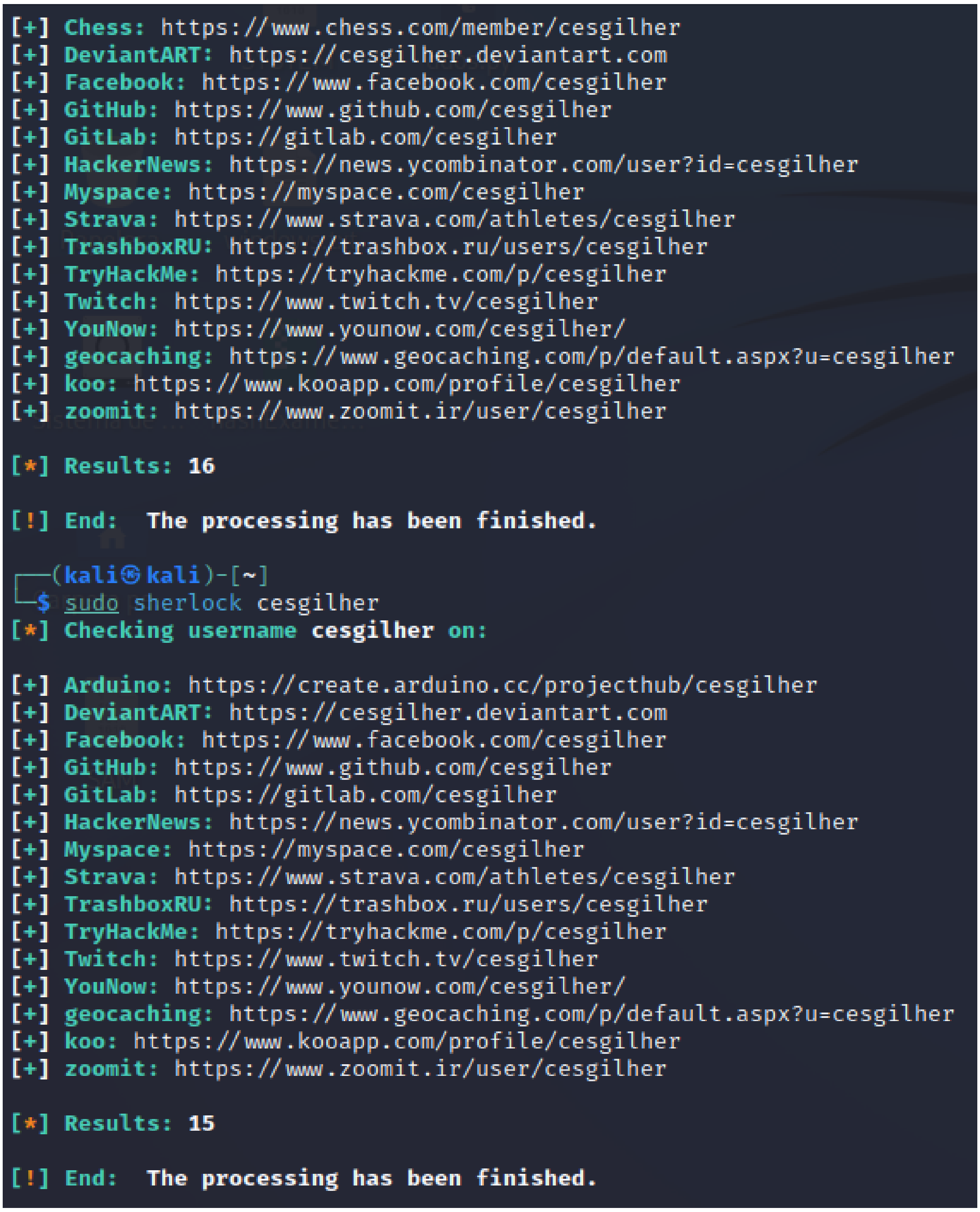


```
┌──(kali㉿kali)-[~]
└─$ sudo masscan --range 10.2.105.100-10.2.105.115 --rate 25000000 --udp-ports 0-65535

Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-01-19 12:36:40 GMT
Initiating SYN Stealth Scan
Scanning 16 hosts [65536 ports/host]
Discovered open port 137/udp on 10.2.105.102

┌──(kali㉿kali)-[~]
└─$ 
```

Sherlock.

Sherlock sirve para buscar gente en redes sociales mediante nombre de usuario. Me parece una herramienta muy incompleta porque en caso de que una persona no use siempre el mismo nombre de usuario, no nos aparecerán esos perfiles en la búsqueda. Considero que seria mas útil poder buscar por correo electrónico. Otra cosa que no me gusta demasiado es que busques lo que busques siempre encuentra perfiles que sabemos que no existen. Aquí hay un hilo en github donde dan ejemplos.

Luego yo he realizado la misma búsqueda dos veces y no me ha dado los mismos resultados. Lo cual no da mucha fiabilidad.



```
[+] Chess: https://www.chess.com/member/cesgilher
[+] DeviantART: https://cesgilher.deviantart.com
[+] Facebook: https://www.facebook.com/cesgilher
[+] GitHub: https://www.github.com/cesgilher
[+] GitLab: https://gitlab.com/cesgilher
[+] HackerNews: https://news.ycombinator.com/user?id=cesgilher
[+] Myspace: https://myspace.com/cesgilher
[+] Strava: https://www.strava.com/athletes/cesgilher
[+] TrashboxRU: https://trashbox.ru/users/cesgilher
[+] TryHackMe: https://tryhackme.com/p/cesgilher
[+] Twitch: https://www.twitch.tv/cesgilher
[+] YouNow: https://www.younow.com/cesgilher/
[+] geocaching: https://www.geocaching.com/p/default.aspx?u=cesgilher
[+] koo: https://www.kooapp.com/profile/cesgilher
[+] zoomit: https://www.zoomit.ir/user/cesgilher

[*] Results: 16

[!] End:  The processing has been finished.

┌──(kali㉿kali)-[~]
└─$ sudo sherlock cesgilher
[*] Checking username cesgilher on:

[+] Arduino: https://create.arduino.cc/projecthub/cesgilher
[+] DeviantART: https://cesgilher.deviantart.com
[+] Facebook: https://www.facebook.com/cesgilher
[+] GitHub: https://www.github.com/cesgilher
[+] GitLab: https://gitlab.com/cesgilher
[+] HackerNews: https://news.ycombinator.com/user?id=cesgilher
[+] Myspace: https://myspace.com/cesgilher
[+] Strava: https://www.strava.com/athletes/cesgilher
[+] TrashboxRU: https://trashbox.ru/users/cesgilher
[+] TryHackMe: https://tryhackme.com/p/cesgilher
[+] Twitch: https://www.twitch.tv/cesgilher
[+] YouNow: https://www.younow.com/cesgilher/
[+] geocaching: https://www.geocaching.com/p/default.aspx?u=cesgilher
[+] koo: https://www.kooapp.com/profile/cesgilher
[+] zoomit: https://www.zoomit.ir/user/cesgilher

[*] Results: 15

[!] End:  The processing has been finished.
```