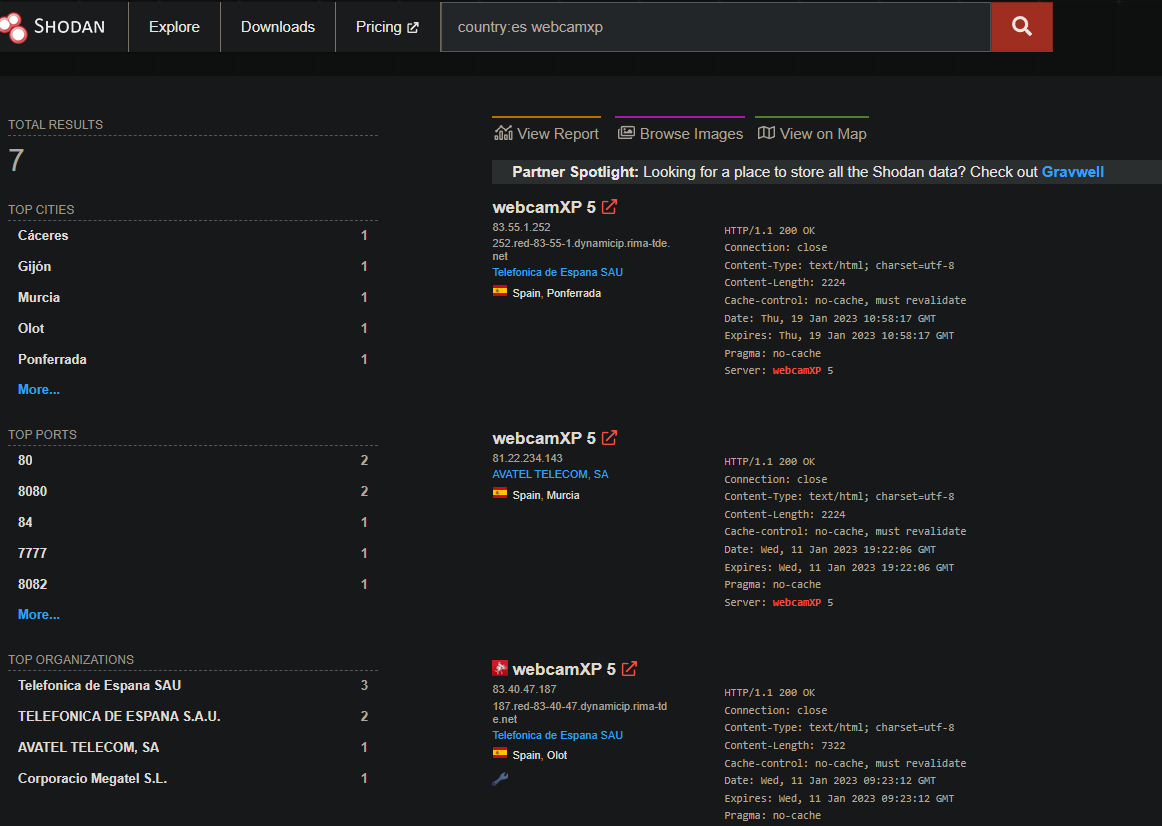
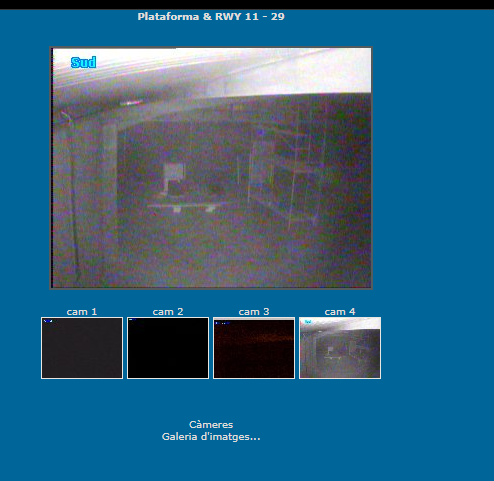
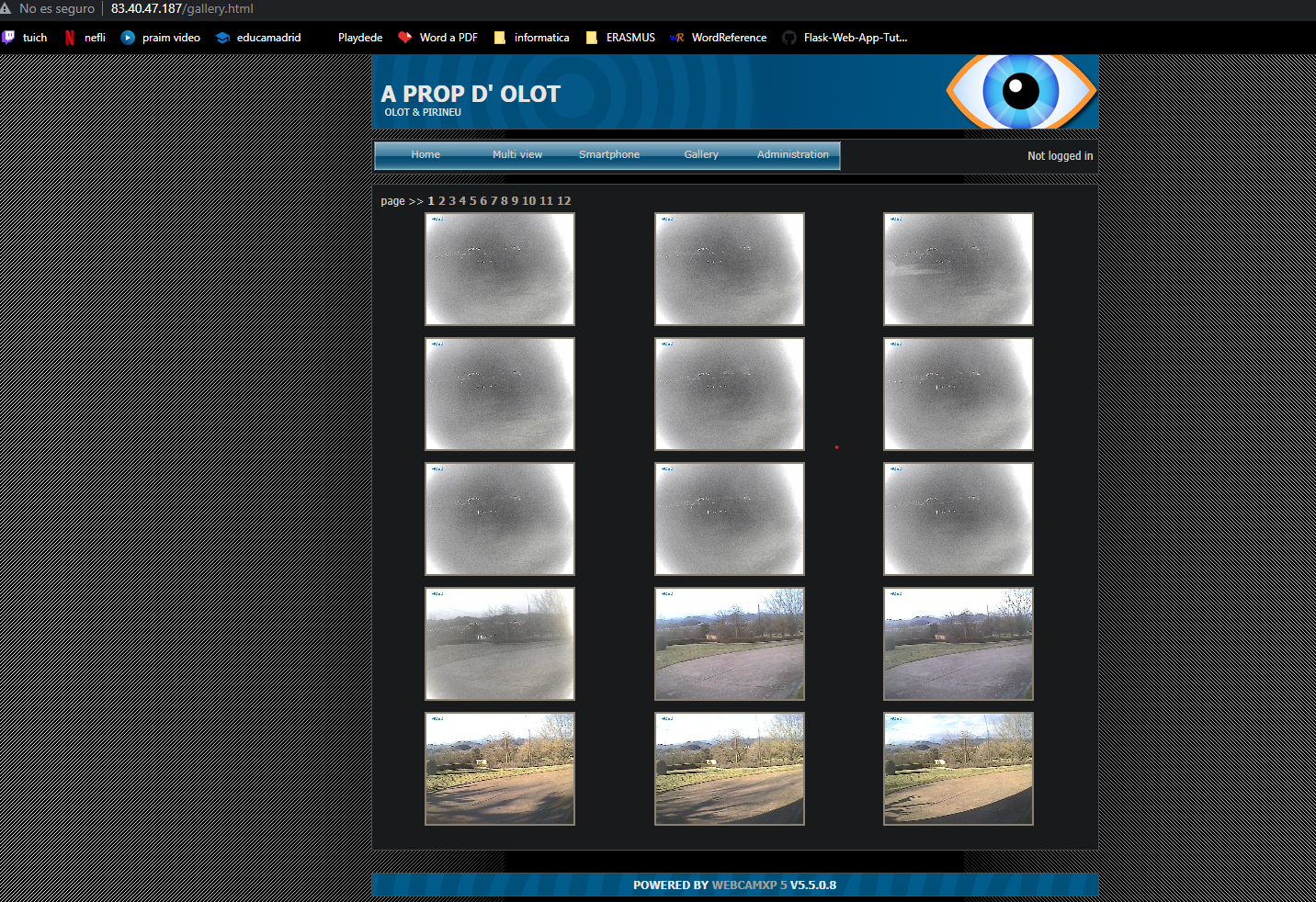
Practica Info Gathering

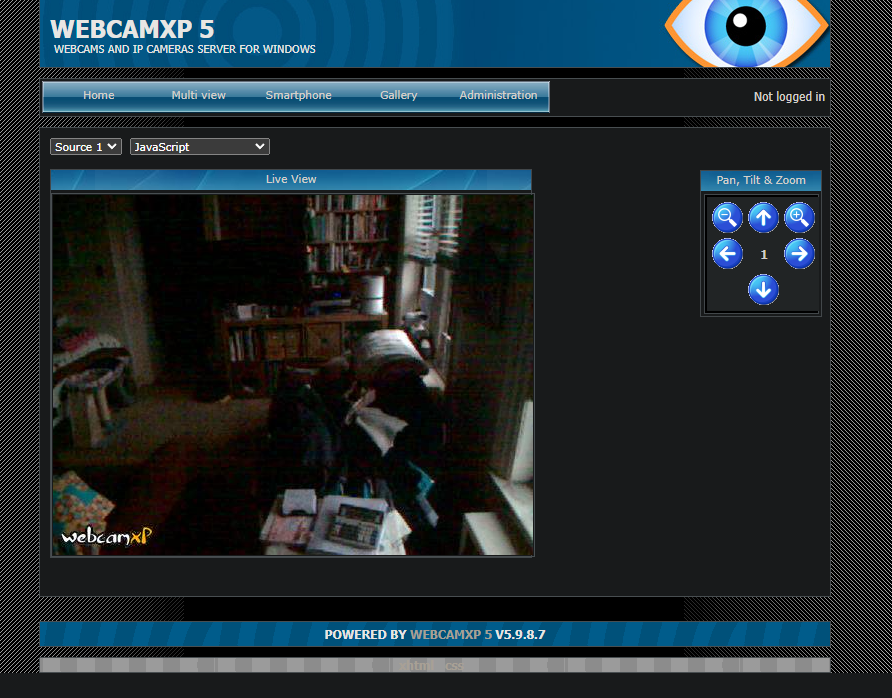
**Shodan.**

**Hay multitud de filtros en shodan, [aquí unos cuantos](https://cheatography.com/sir-slammington/cheat-sheets/shodan/).**

**Aquí filtra por ordenadores con windowsxp(un programa para monitorizar cámaras) y que están en españa.Aquí una de las cámaras que podemos ver sin iniciar sesión.**

**Aquí otro ejemplo.**

****

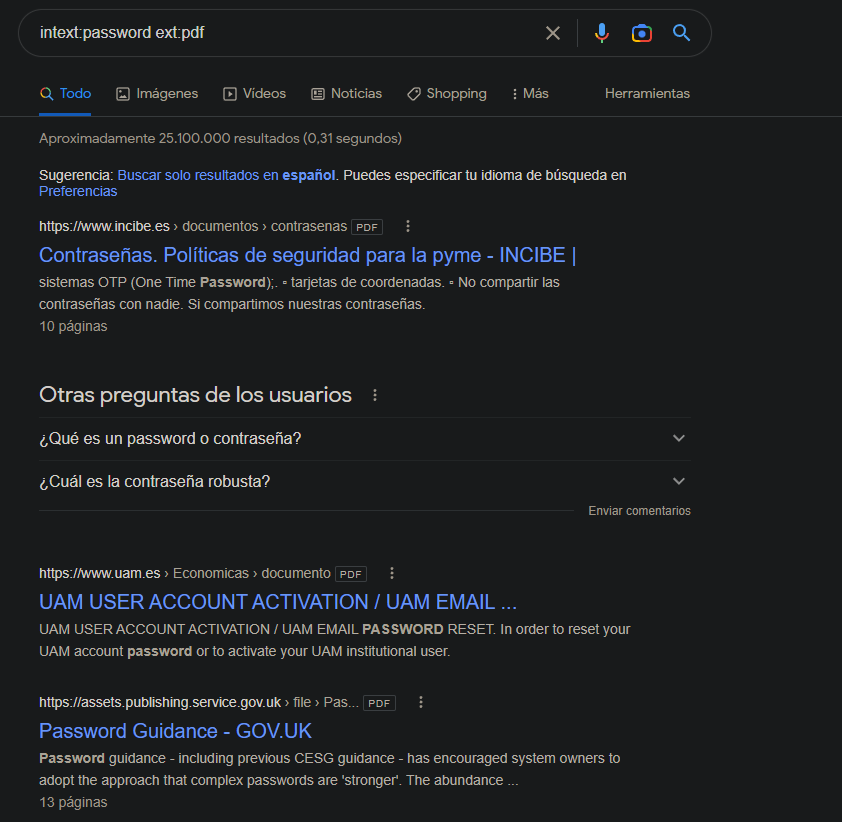
**Aquí una de la habitación de alguien.**

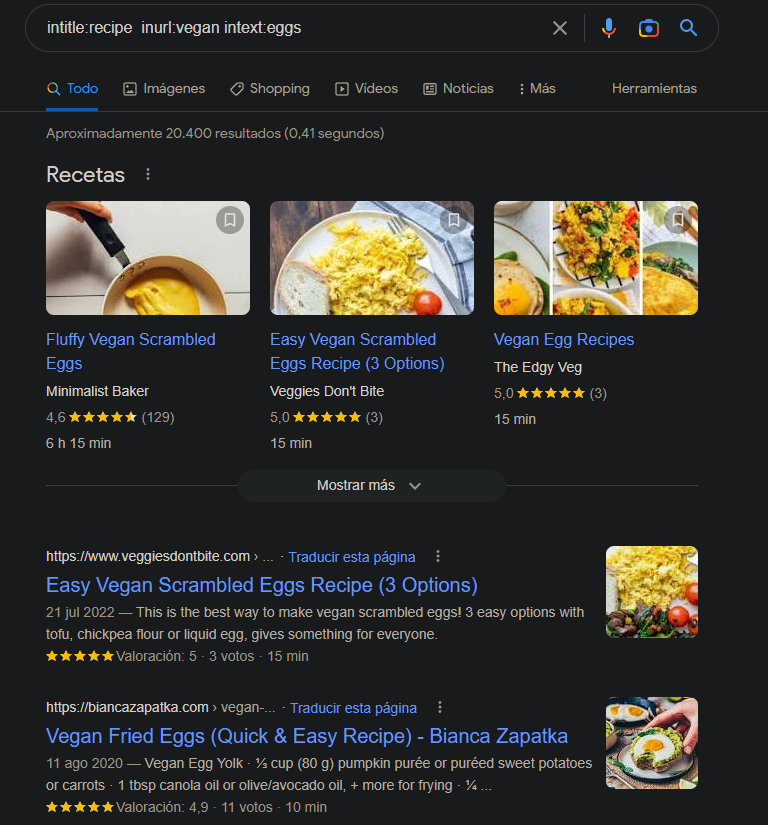
**Claramente esto supone un gran riesgo ya que cualquiera puede saber donde estás geolocalizando tu ip y además ver lo que estas haciendo en tu casa. Cualquier atacante con un mínimo de conocimiento podría controlar cuando estas en casa y cunado no y entrar a robar por ejemplo.**

**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.**

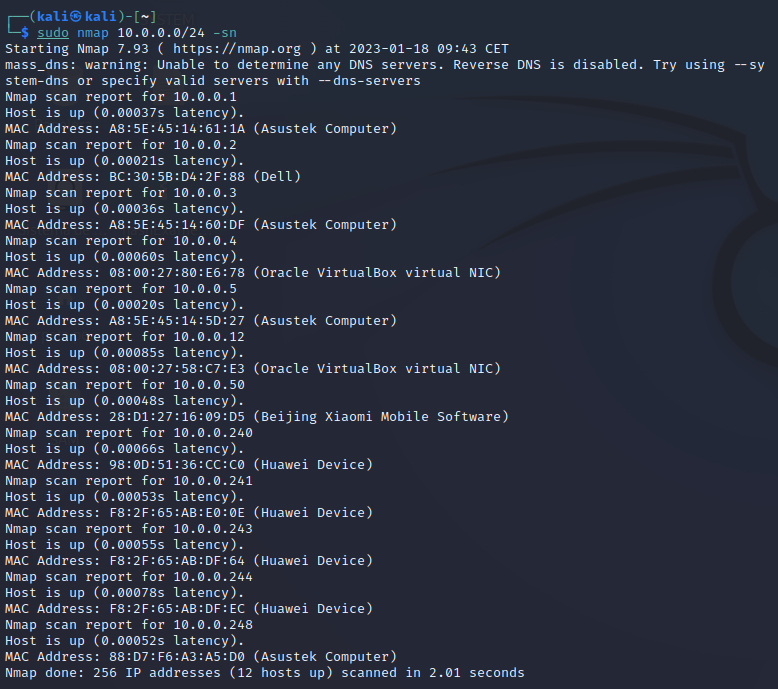
**Aquí filtra por archivos pdf y que tienen la palabra password en ellos, lo cual puede servir a los atacantes para encontrar credenciales escritas por error en texto plano.**

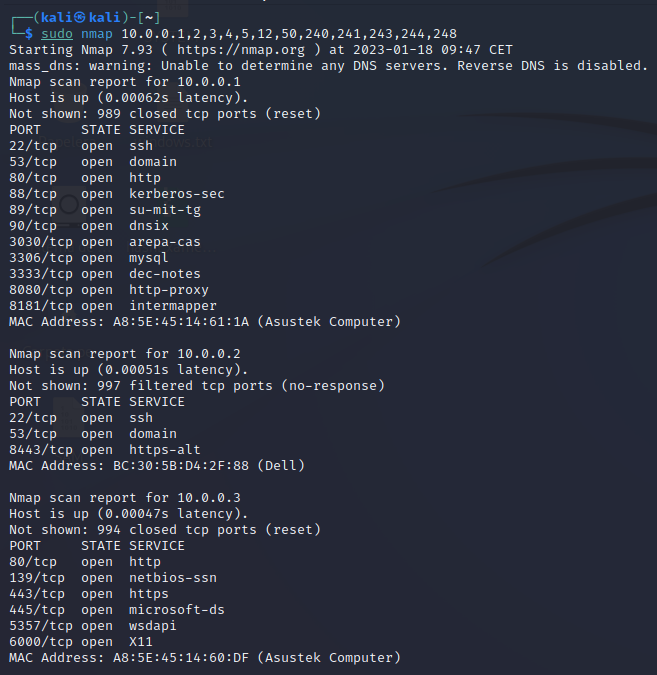
**Aquí filtra por paginas tituladas recipe, que incluyan la palabra vegan en la url y que en el texto este la palabra eggs.**

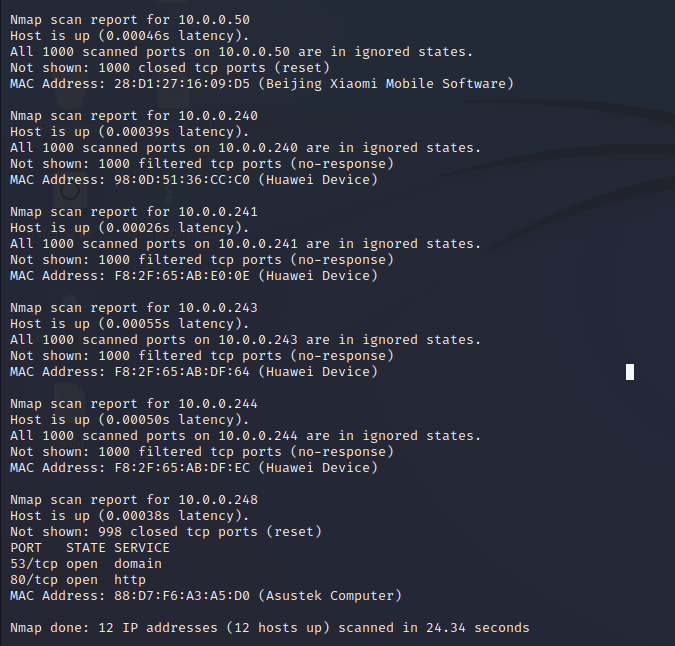
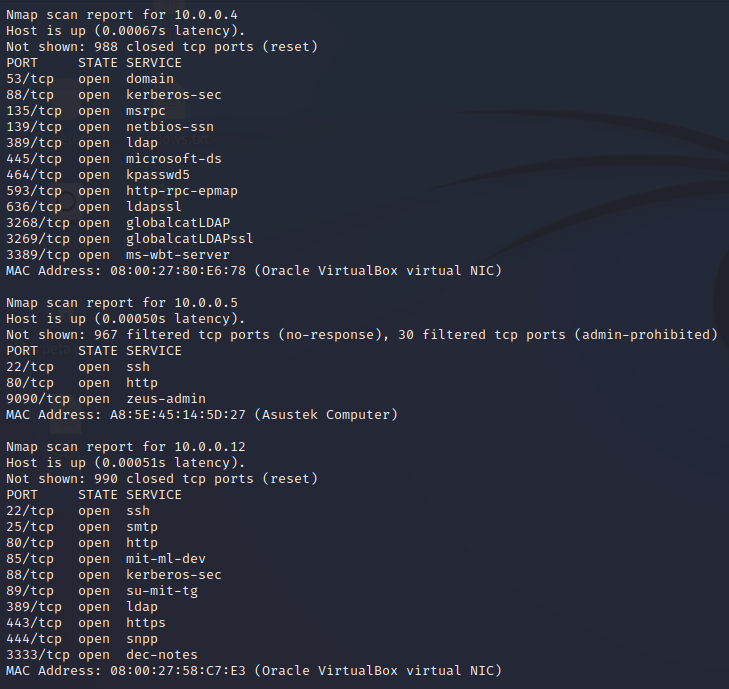
**nmap.**

**Red 10.0.0.0/24**

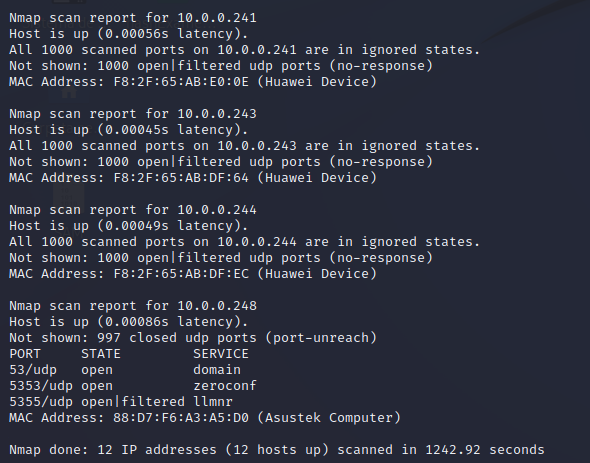
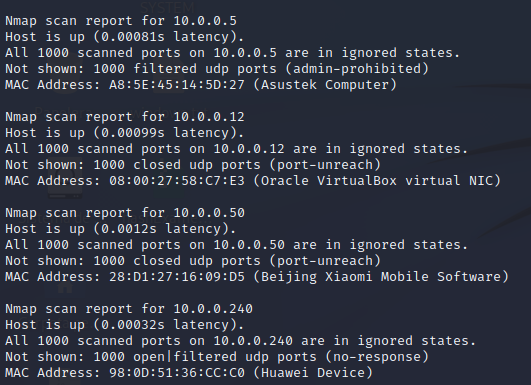
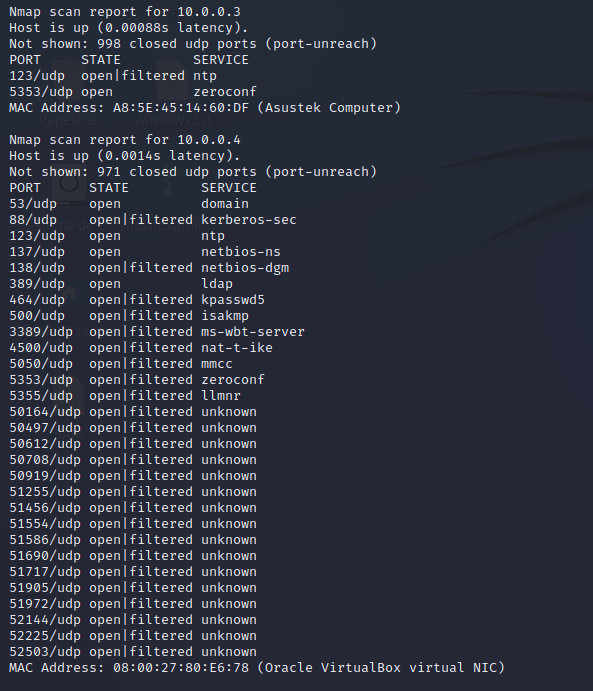
**Primero hacemos un host descovery para ver que maquinas están activas. Este paso puede fallar porque en caso de que las maquinas tengas cortafuegos o prohibido el ping, no contestarán y saldrán como desconectadas, aunque no esta de mas probar.**

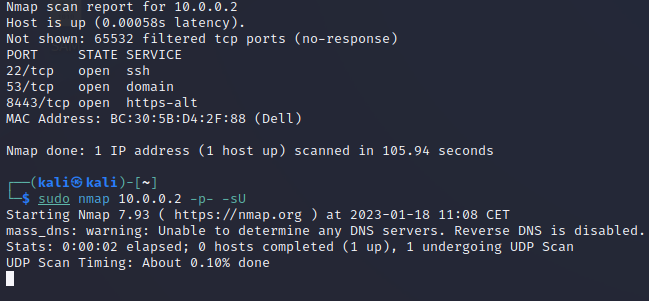
****

**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.**

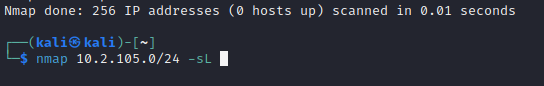
****

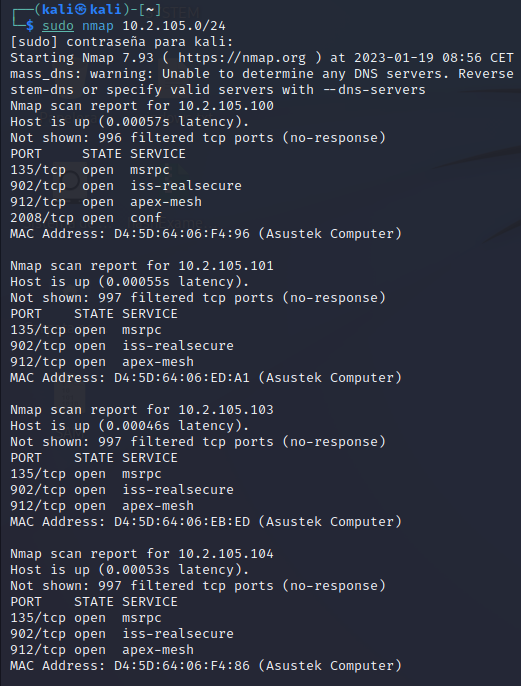
**Ahora la misma búsqueda, es decir los 1000 puertos conocidos, pero usando UDP.**

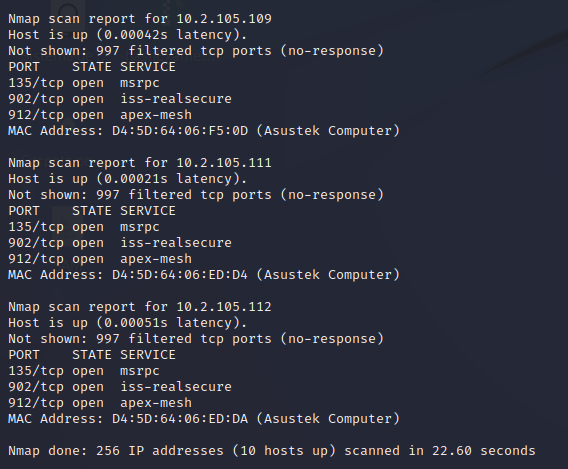
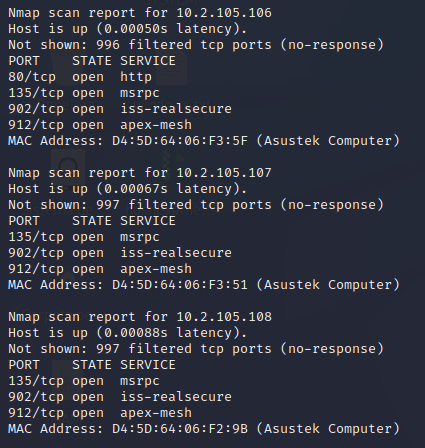
**Podemos ver que hay bastantes mas puertos abiertos con el protocolo UDP que TCP y que algunos de estos puertos admiten tanto TCP como UDP.**

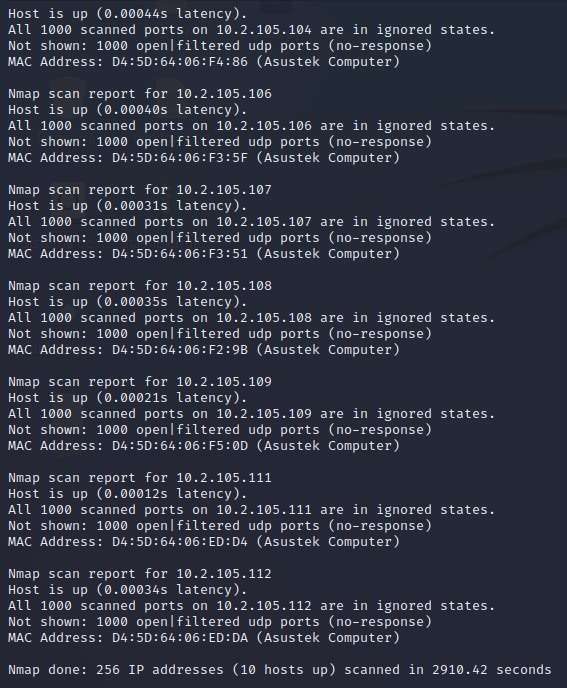
**Ahora vamos a escanear no solo los 1000 puertos conocidos, sino los 65535 puertos que hay en total. Primero mediante TCP y luego UDP. Nos centraremos solo en una ip para que la busqueda no se haga eterna.Primero con la 10.0.0.1 y despues con la 10.0.0.2.**

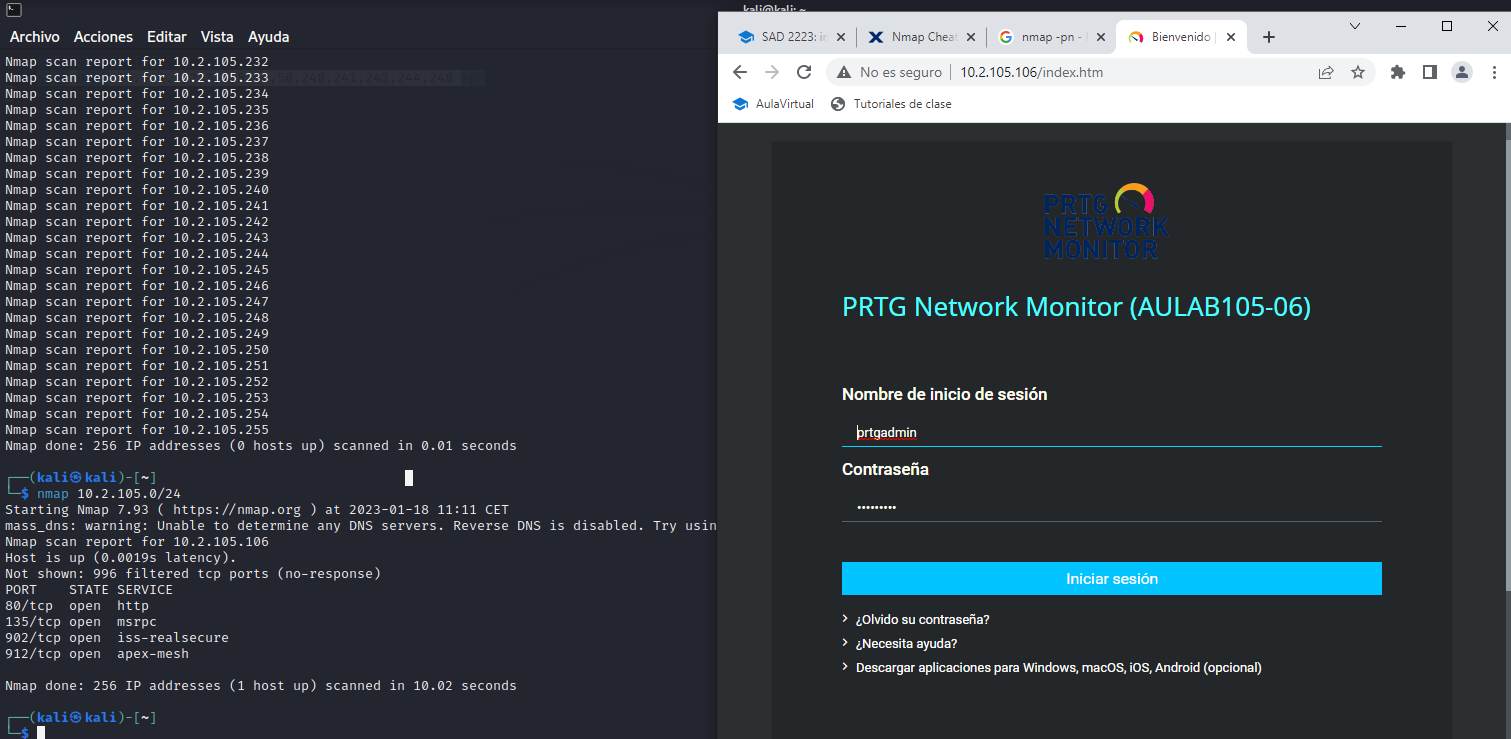
**Red 10.2.105.0/24**

**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.  
**

**TCP  
**

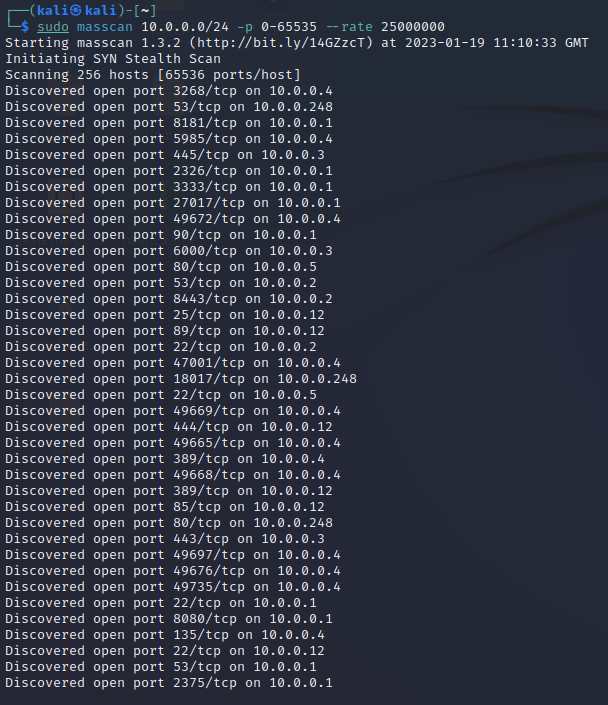
****

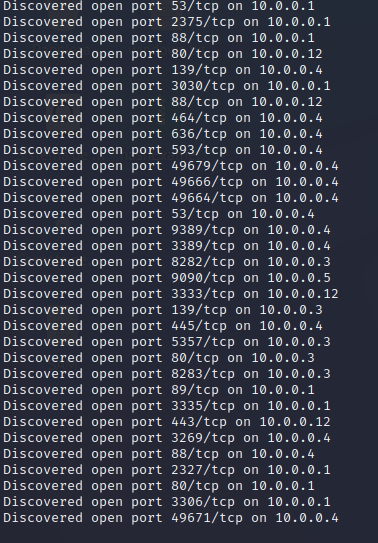
**UDP  
**

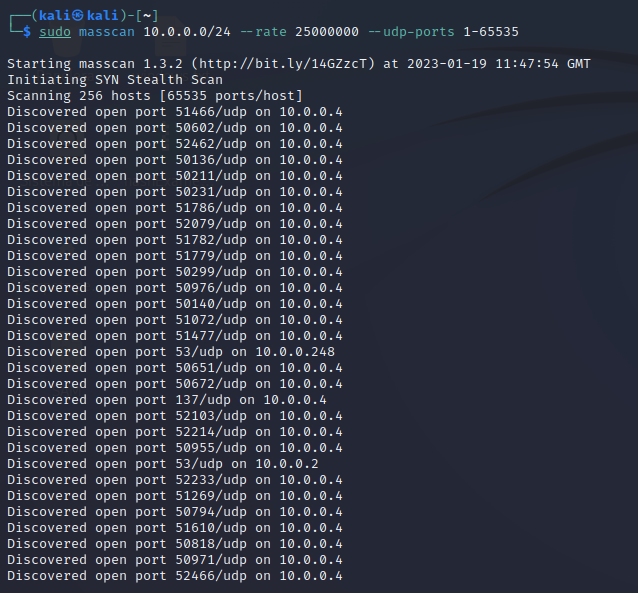
**Por ejemplo en la 10.2.105.106 hay una conexión HTTP abierta.**

**masscan.**

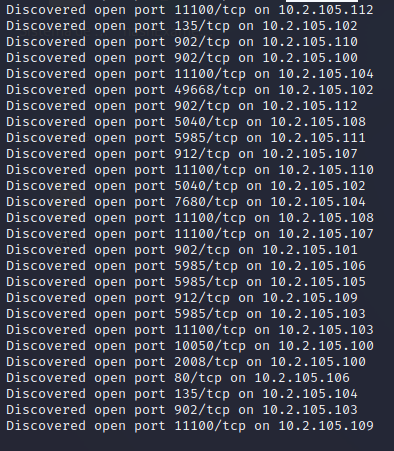
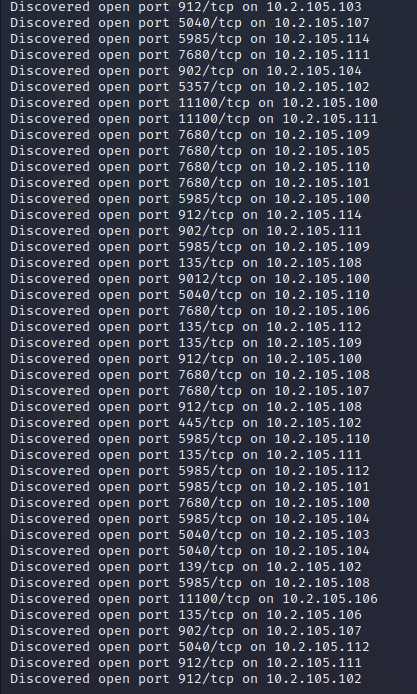
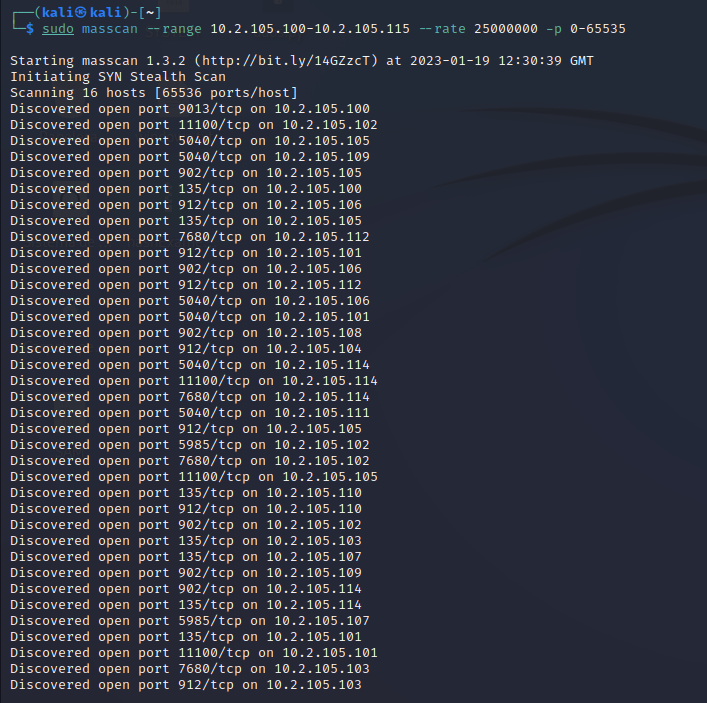
**La única diferencia entre masscan y nmap es que en masscan puedes elegir cuantos paquetes mandar por segundo entre 0-25000000, siendo 100 los paquetes por defecto. Esto se declara mediante la variable rate. Lo que no me gusta tanto de masscan es que no te ordena los resultados , sino que te los va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

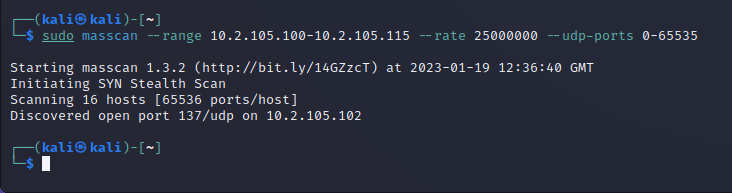
**Red 10.0.0.0/24  
TCP  
**

****

**UDP**

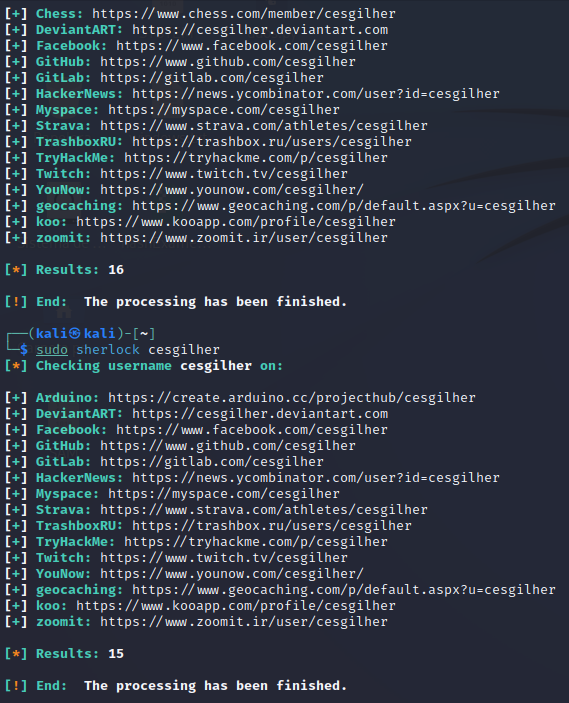
**Red 10.2.105.0/24**

**TCP  
**

**UDP**

**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.](https://github.com/sherlock-project/sherlock/issues/541)**

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

****