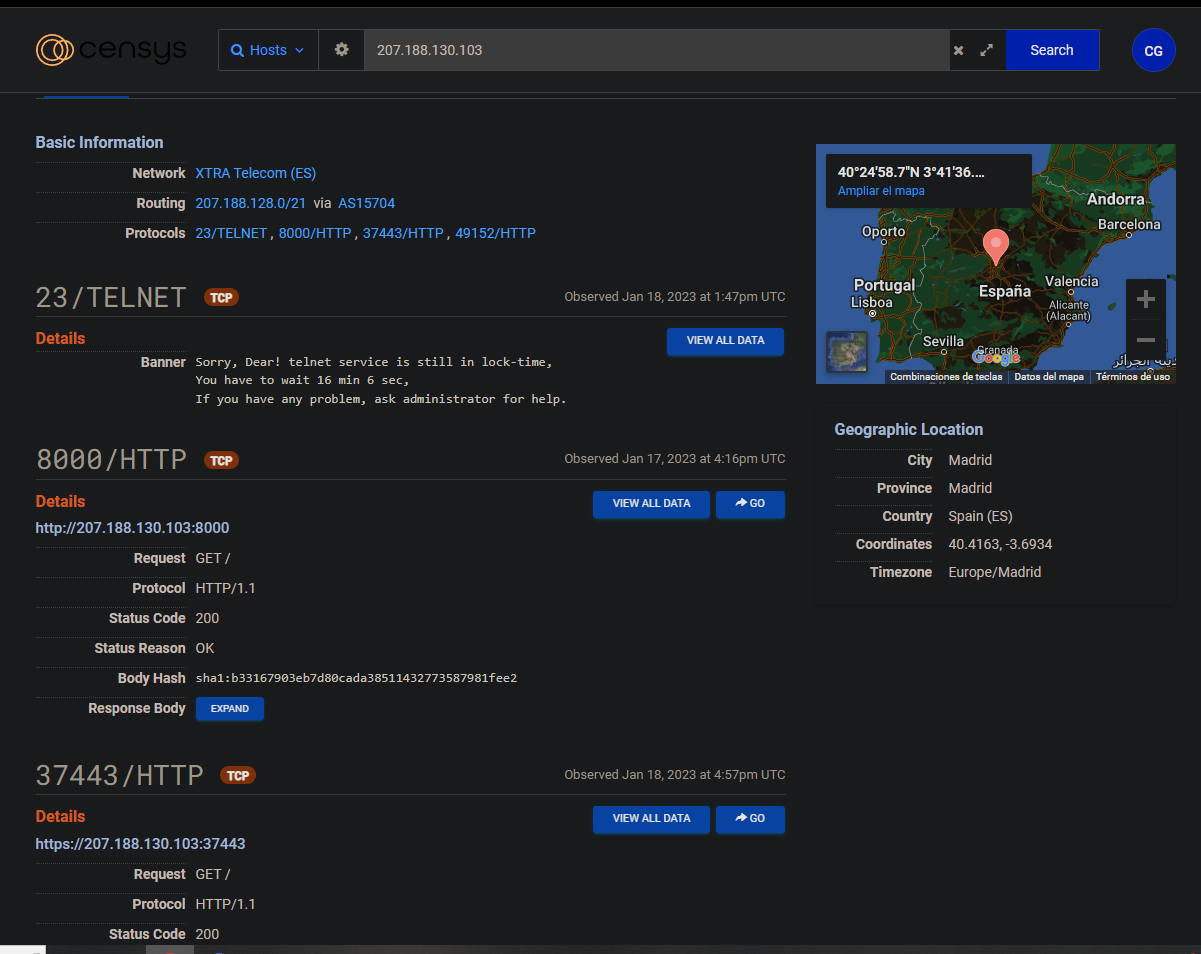
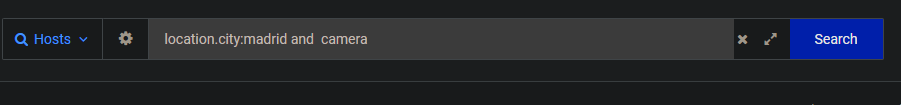
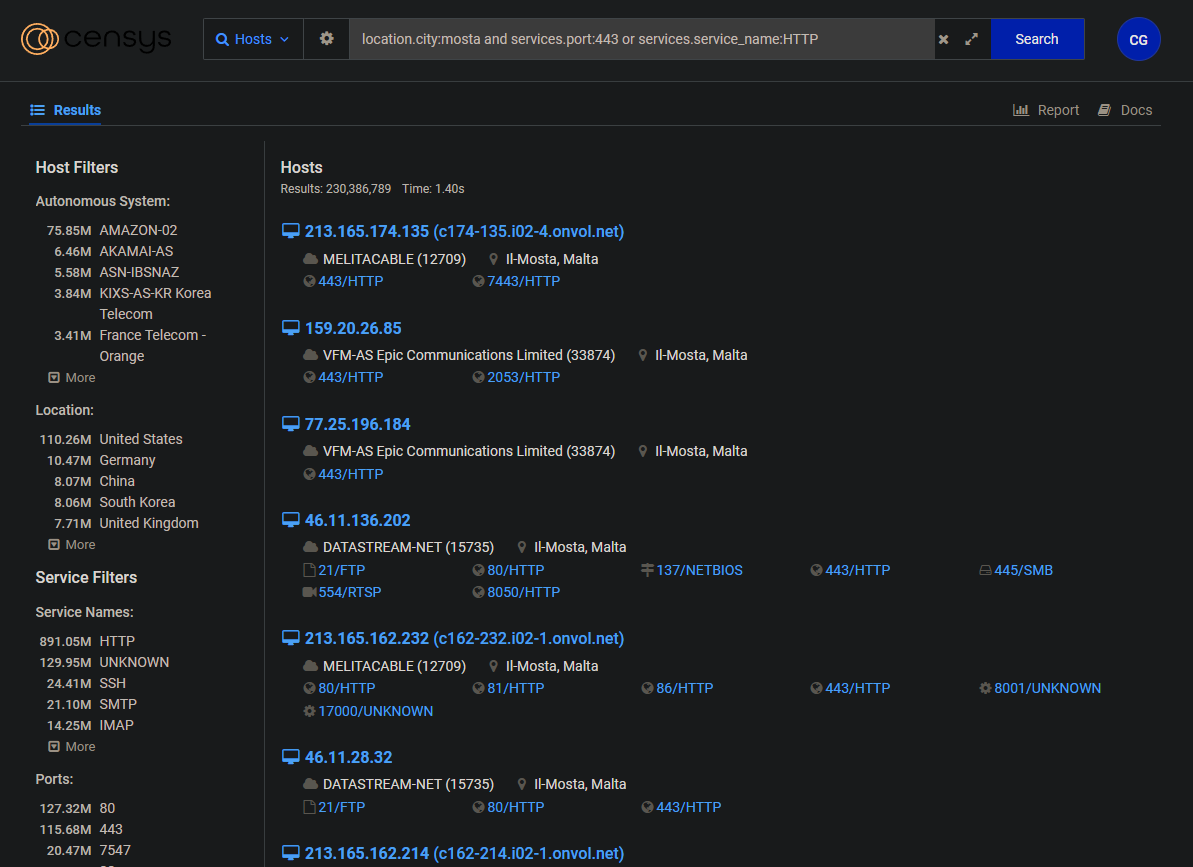
Extra Info Gathering

**Censys.**

**Lo guay de censys es que puedes hacer filtros booleanos, es decir usar and y or. De forma que si queremos buscar ip con http o https podríamos. Shodan solo permite añadir mas filtros como si fuera un and.**

**Aquí buscamos cámaras en madrid**

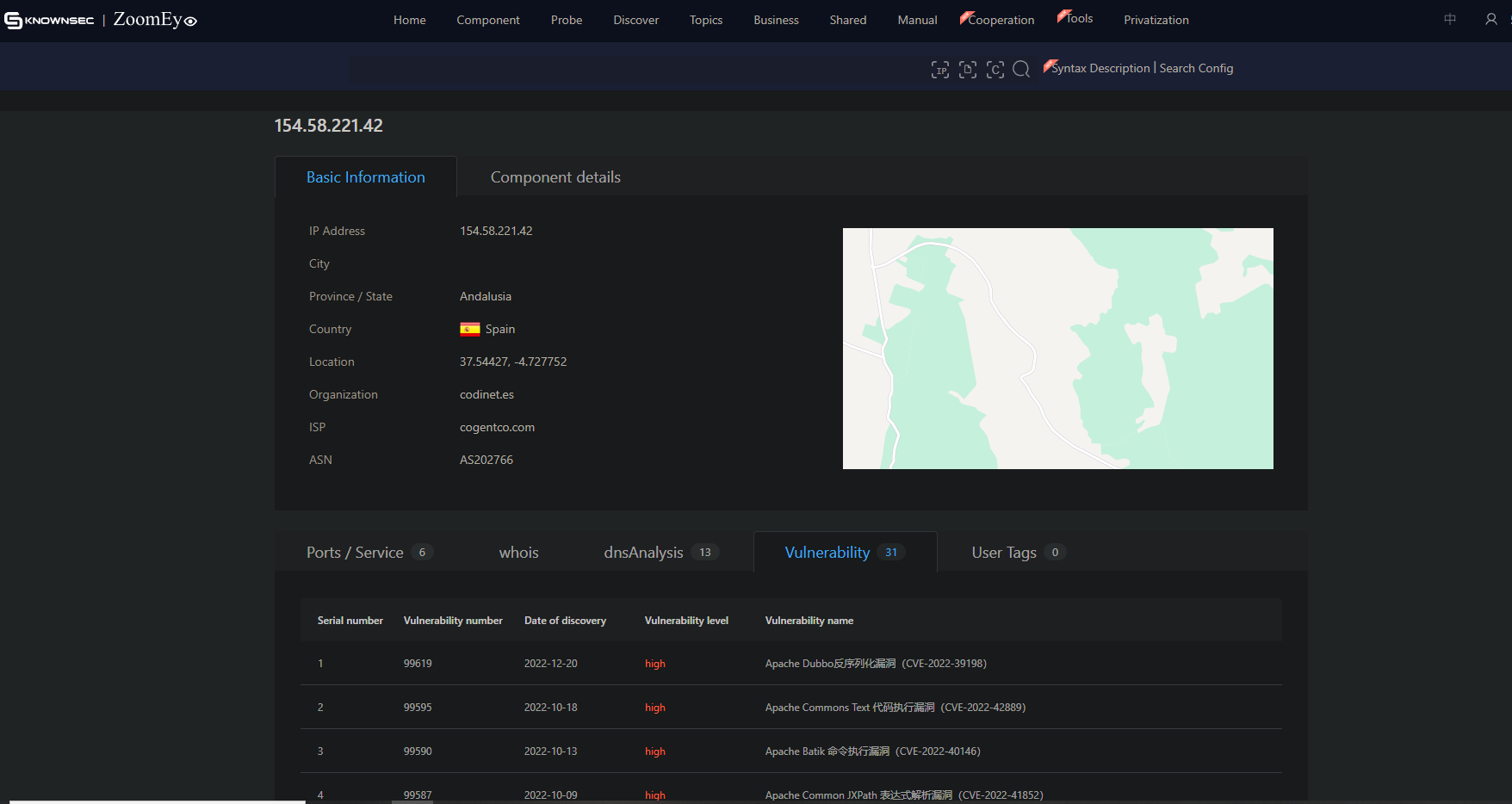
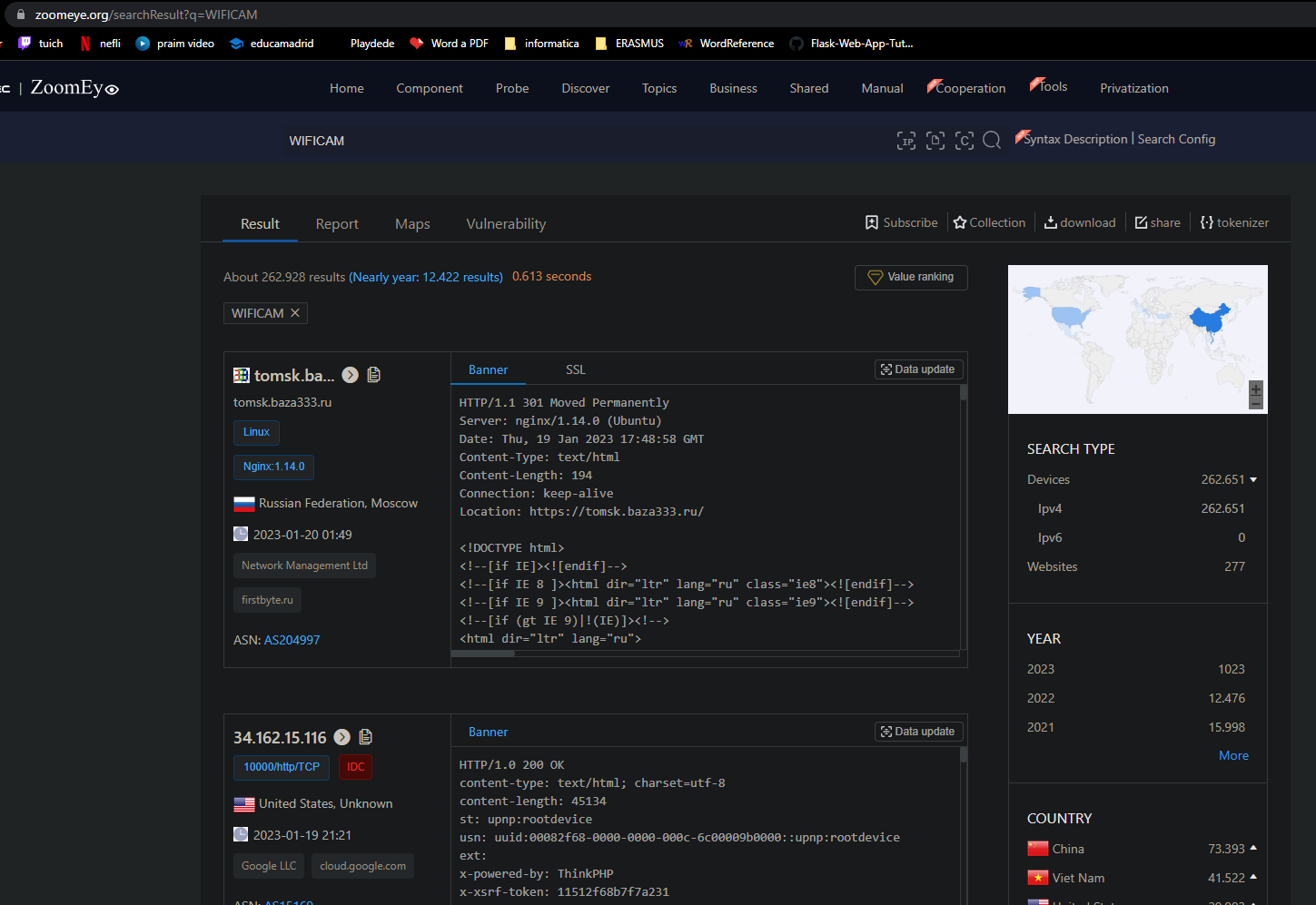
****

**Aquí buscamos por ciudad: mosta,malta y que tenga abierto el puerto 443(https) o use HTTP**

**Alternativas a Censys.**

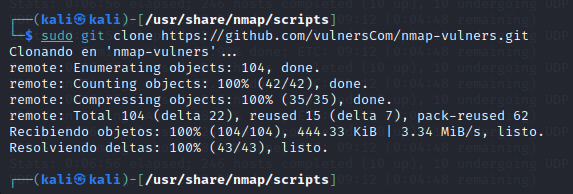
**Alternativas a Shodan y Censys hay muchas, como Zoom Eye, IVRE,FOFA.**

**Yo he probado Zoom Eye. No es tan completo como los demás pero supongo que si sabes que buscar cumple su función.**

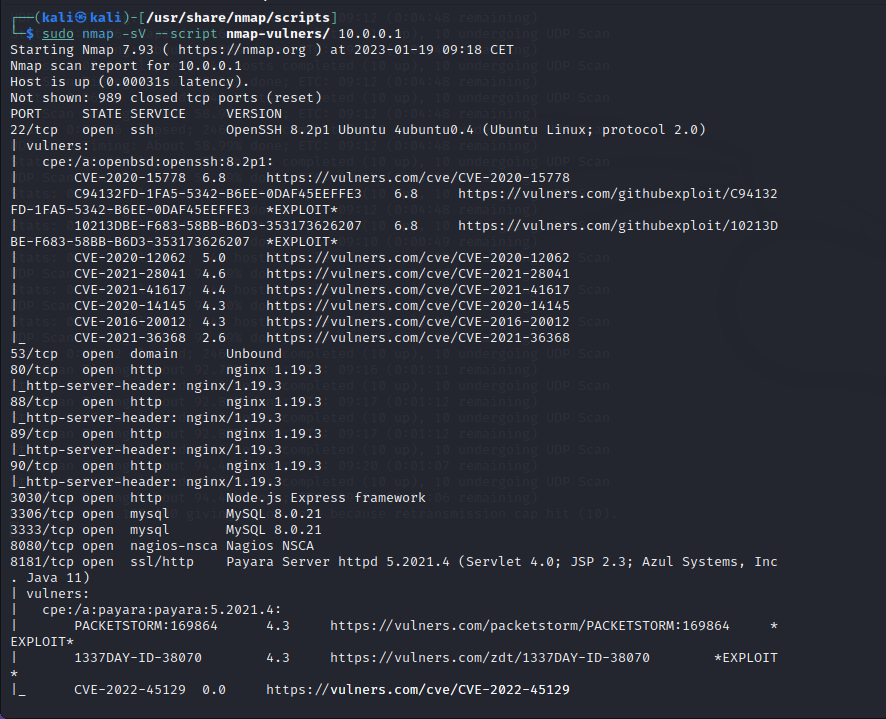
****

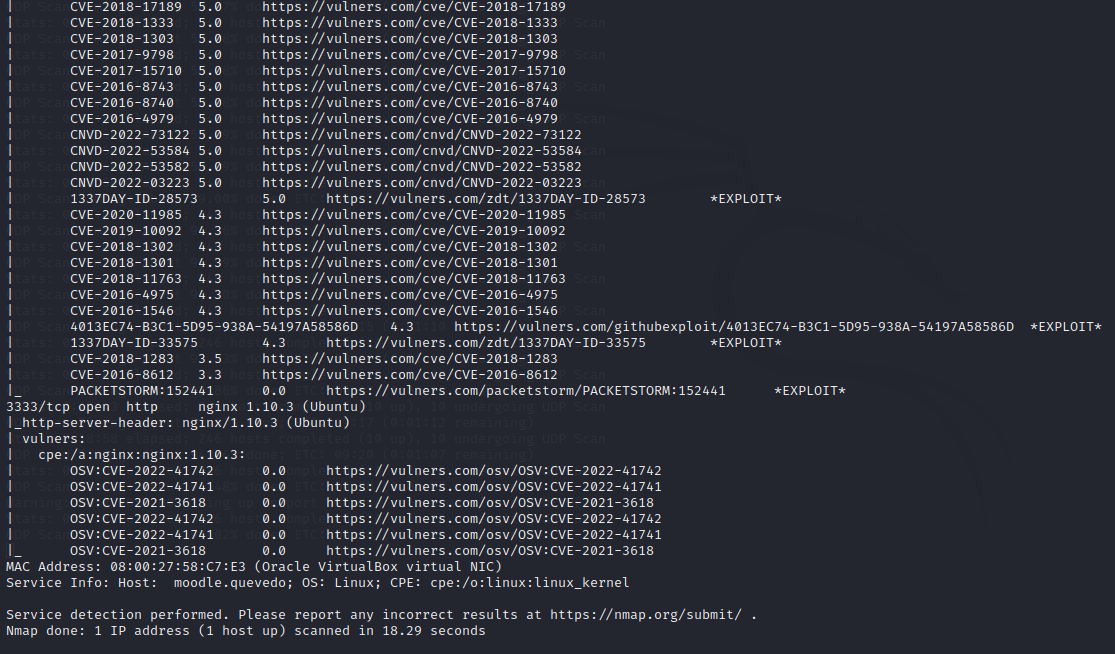
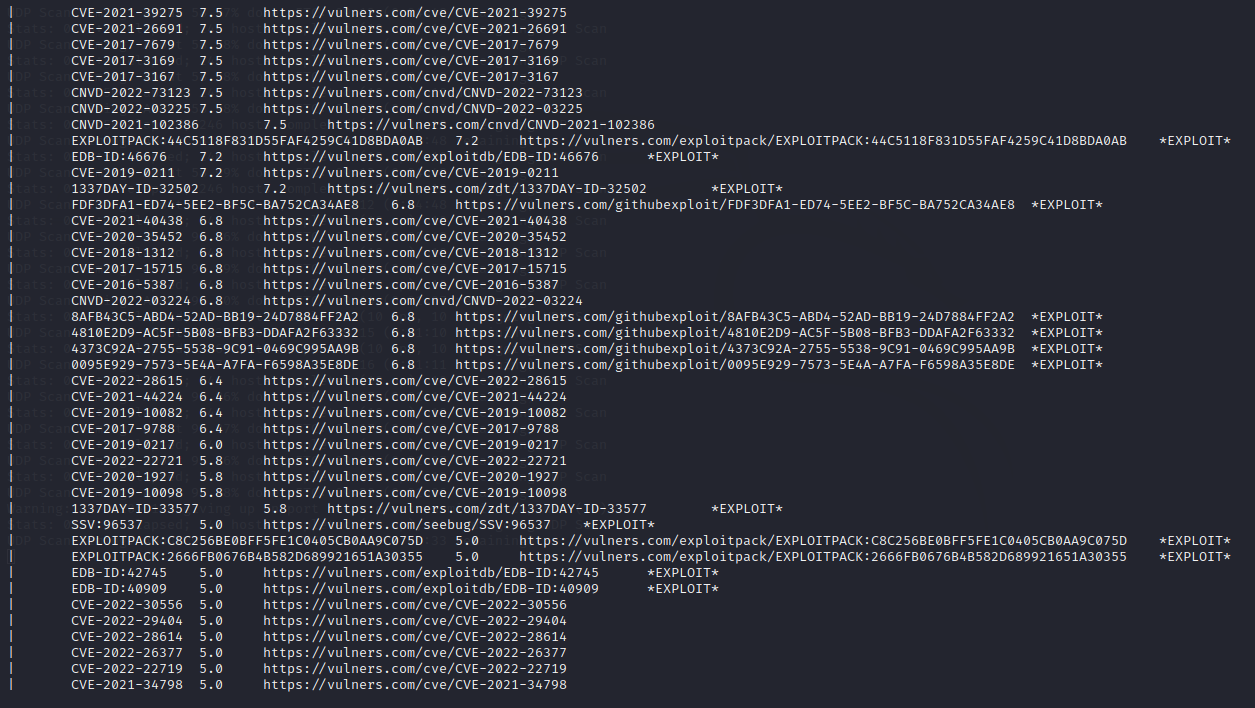
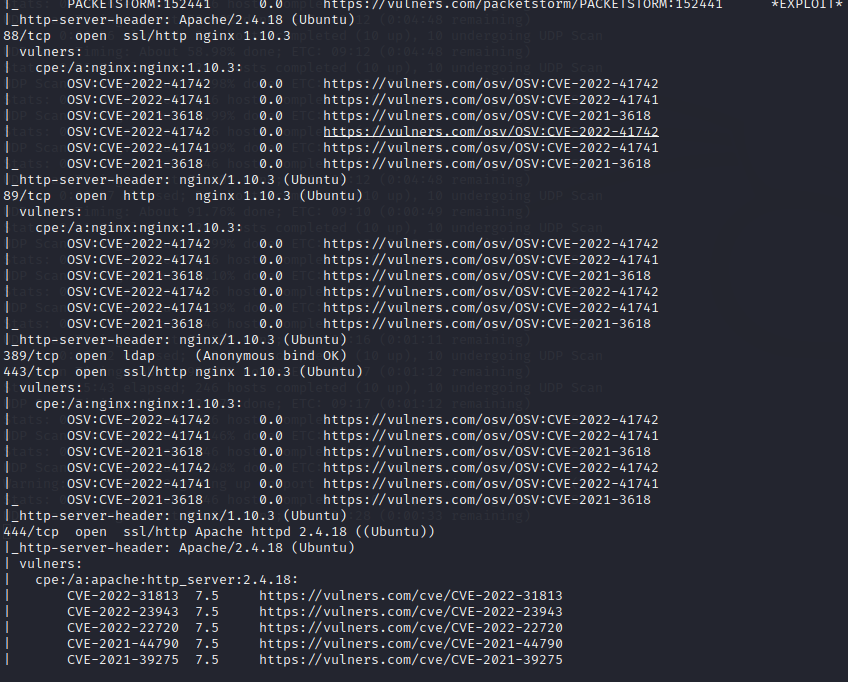
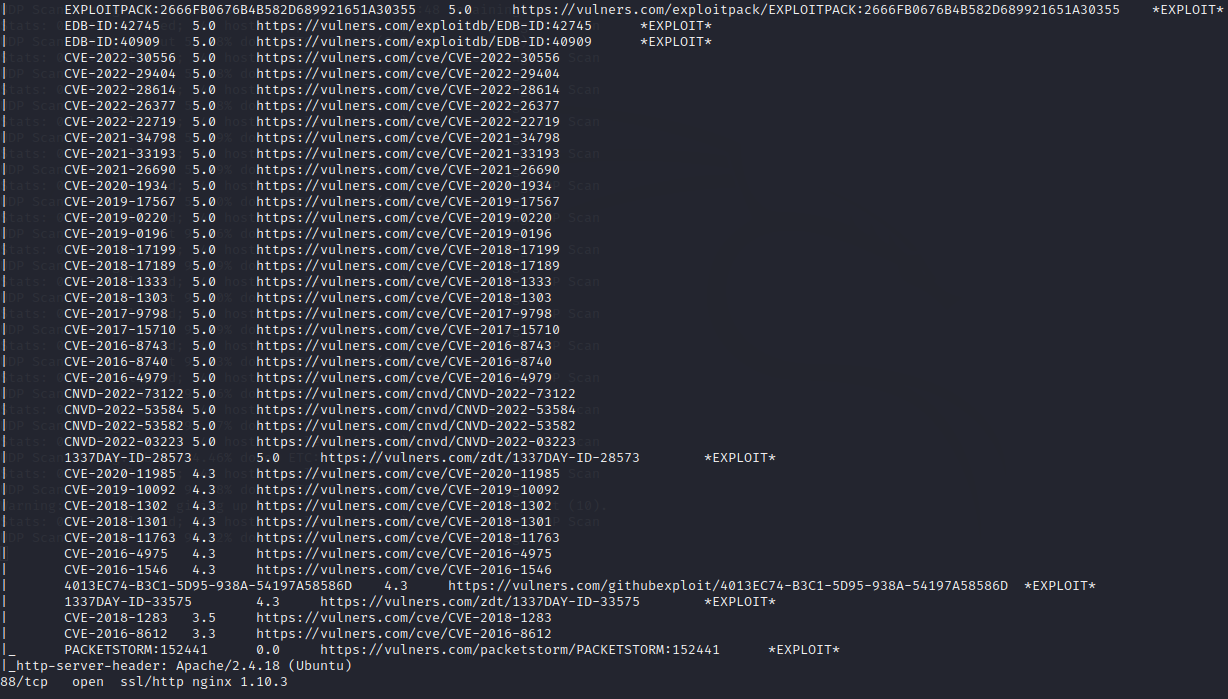
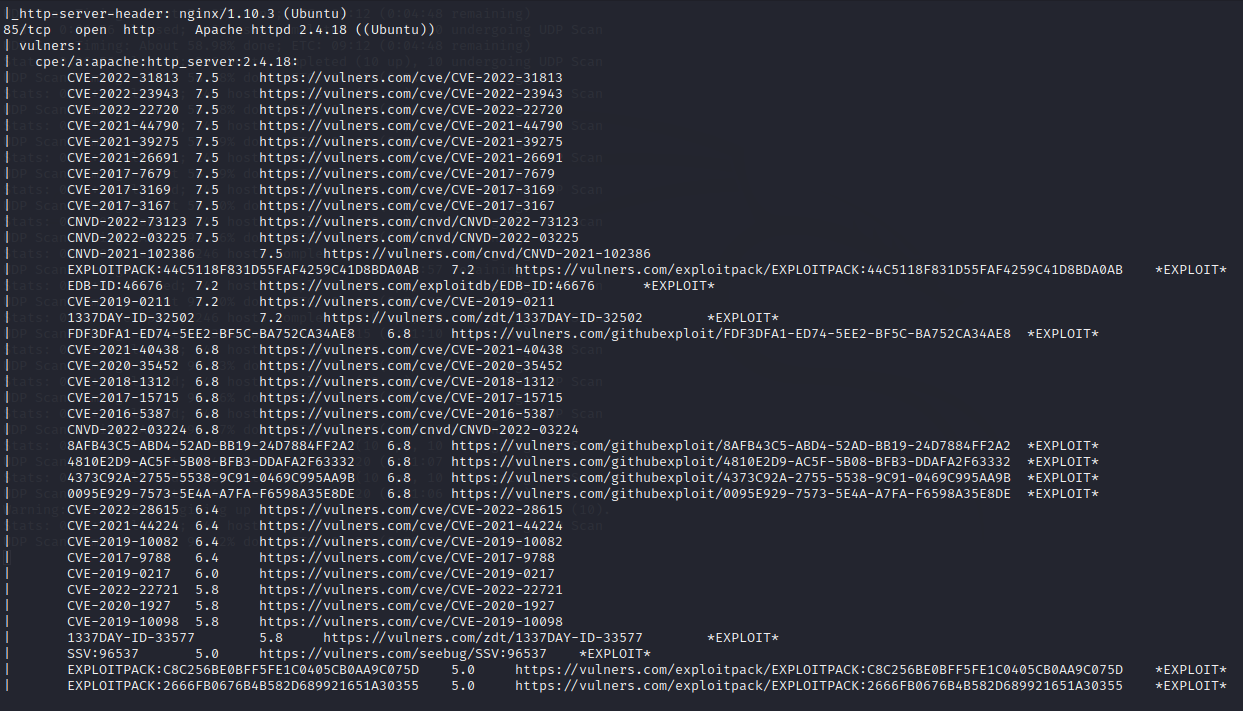
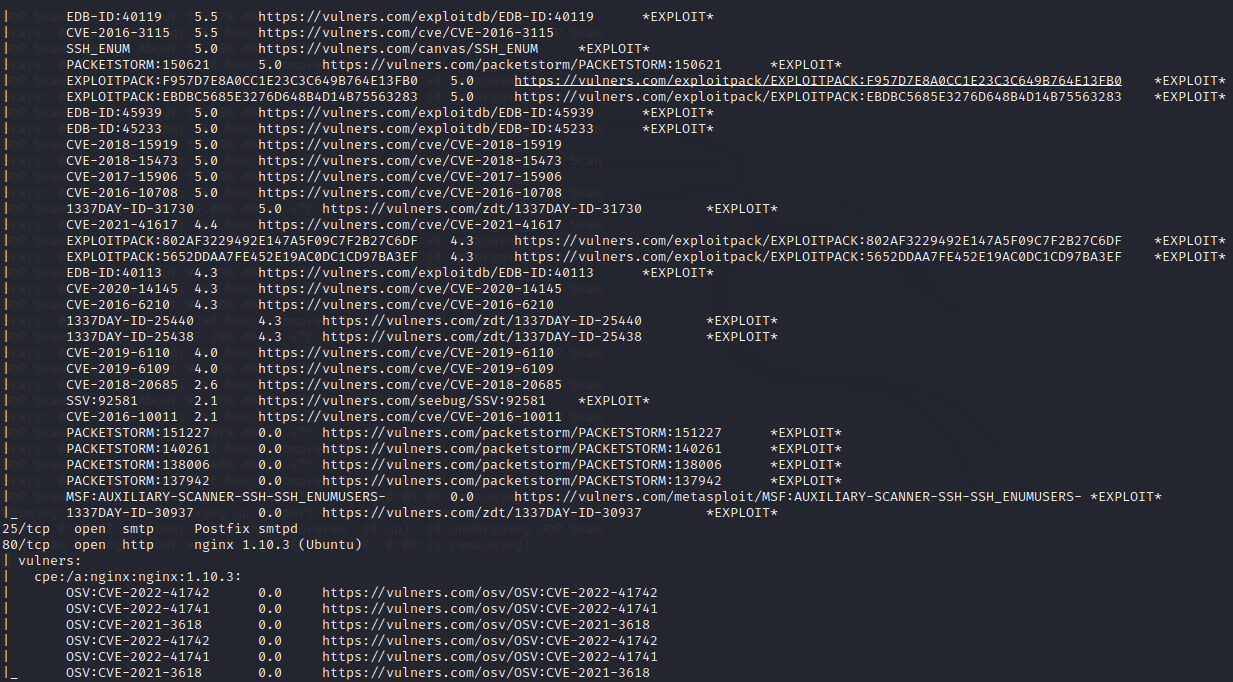
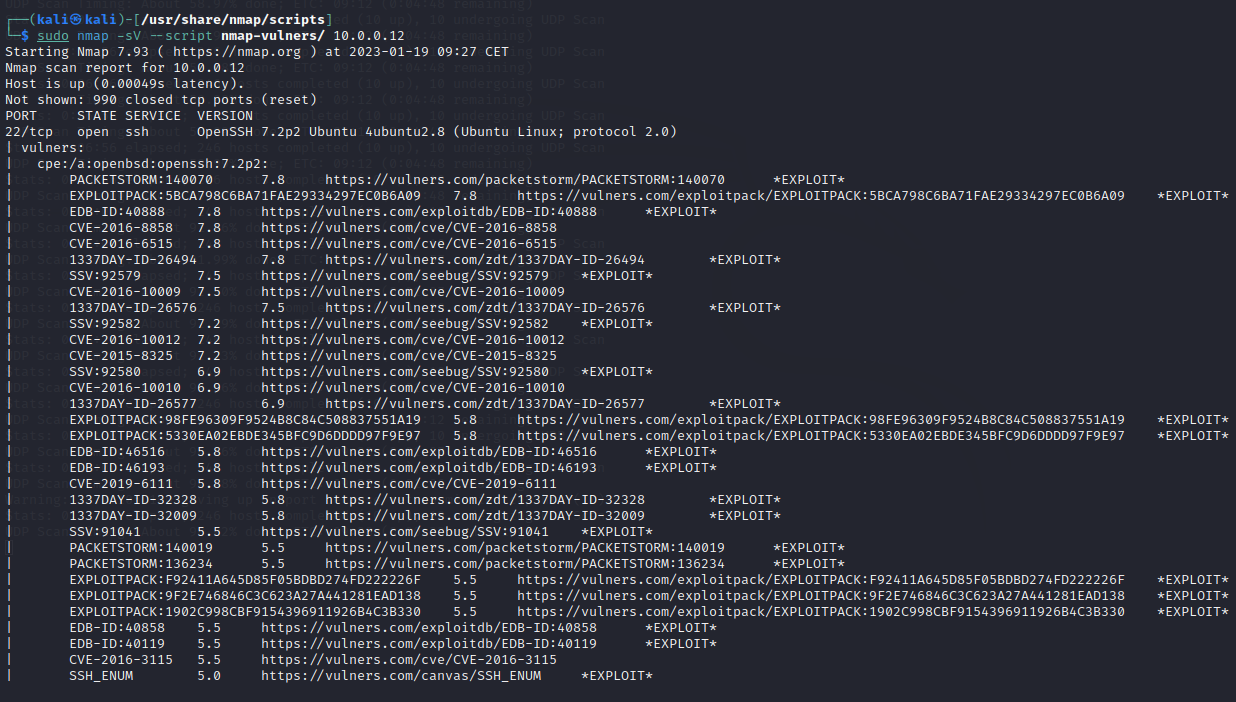
**Nmap scripts.**

**El primer paso es clonar el repositorio donde están los scripts, hay varios y cada uno tiene sus funciones pero yo he elegido este.**

****

**Ahora vamos a ver las posibles fallas de seguridad de los puertos abiertos en la 1.0.0.0.1**

****

**Ahora vamos a ver las posibles fallas de seguridad de los puertos abiertos en la 1.0.0.0.12. Podemos ver que hay unas cuantas.**

**Si tuviera un mayor conocimiento estoy seguro de que seria capaz de acceder y burlar la seguridad de la 10.0.0.12, posteriormente escalar privilegios y comprometer el equipo.**