**Test de intrusión en la definición de vulnerabilidades y comandos en ciberseguridad**



Daniel Escaño Hernández CET Ciberseguridad

# 

# **1. Índice:**

[**1. Índice:**](#_4jq84lualx9d) **1**

[**2. Practica 1-2**](#_ofiic1av8ddq) **2**

[**2.1 Estudio del dominio y uso de comandos**](#_5d38uxjyswtl) **2**

[**2.2 Automatización mediante script, dnsrecon y ripe**](#_ht82r52mfzux) **7**

[**2.3 DNSEC**](#_ok2j9zegkqdo) **11**

[**2.4 Identificación de activos**](#_8y5yjlvzzz0t) **12**

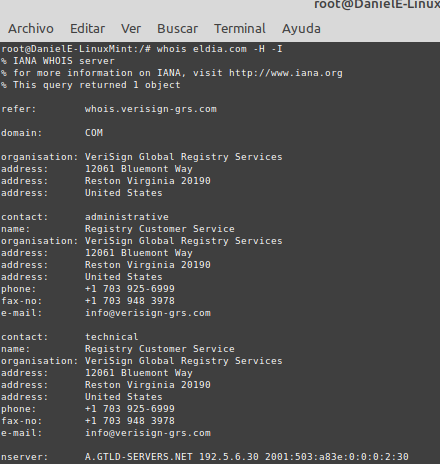
[**2.5 Identificación de subdominios, searchdns.netcraft y dnsdumpster**](#_rlimak9ln6qr) **14**

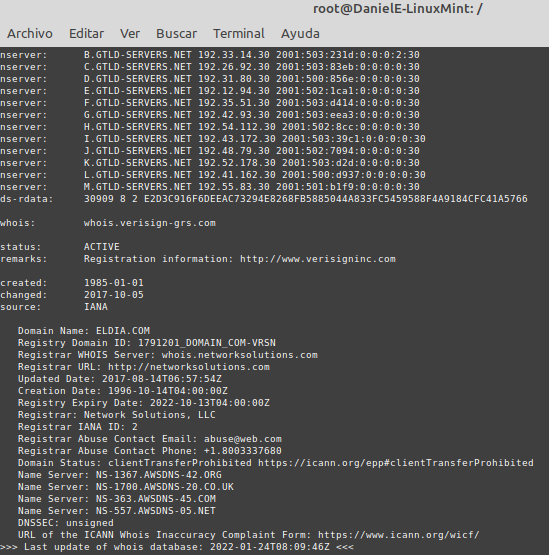
[**2.6 Automatización y escaneo mediante spiderfoot**](#_tjkscs96zdqb) **17**

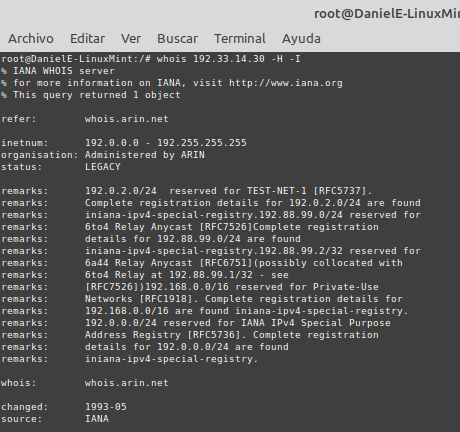
# **2. Practica 1-2**

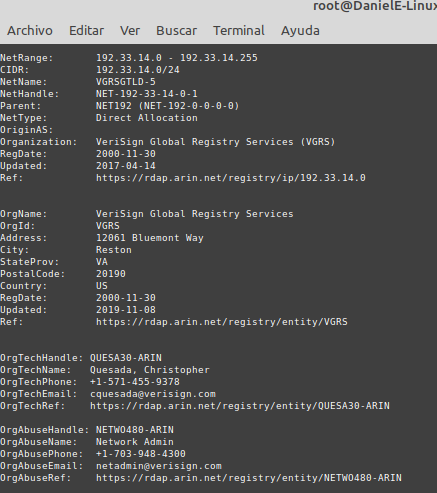
### **2.1 Estudio del dominio y uso de comandos**

Para este estudio utilizaremos varios comandos para realizar consultas sobre dominios integrados en linux entre ellos whois, w, who, dig, etc..

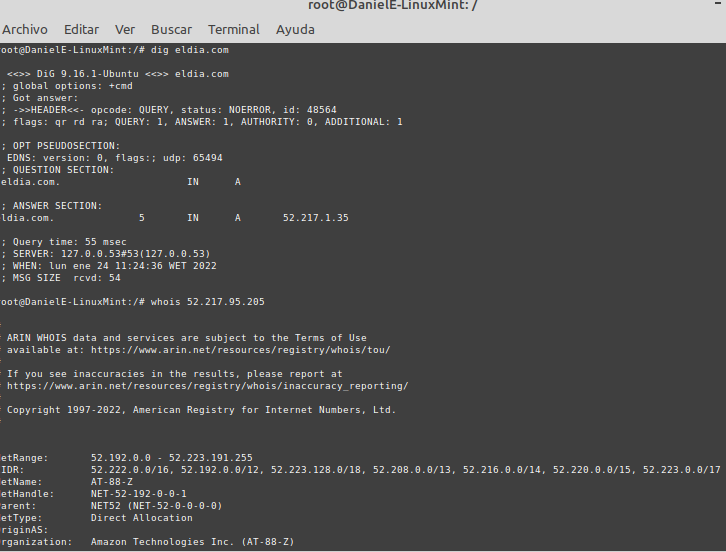


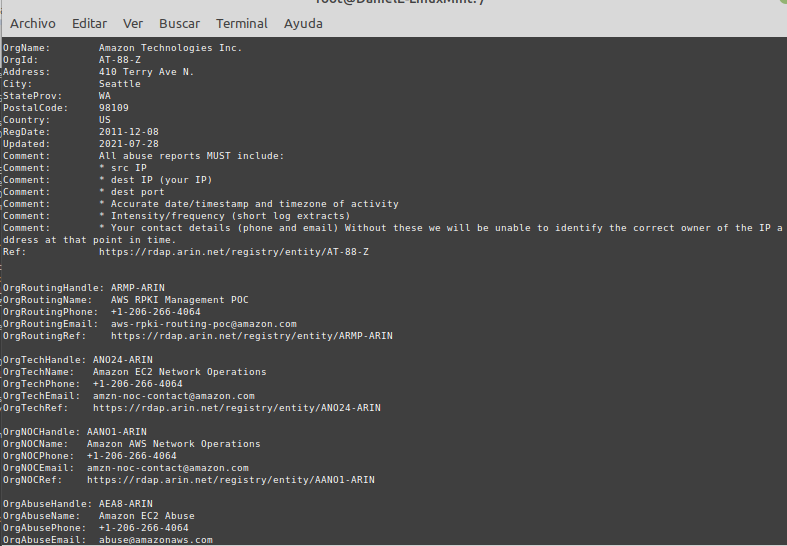


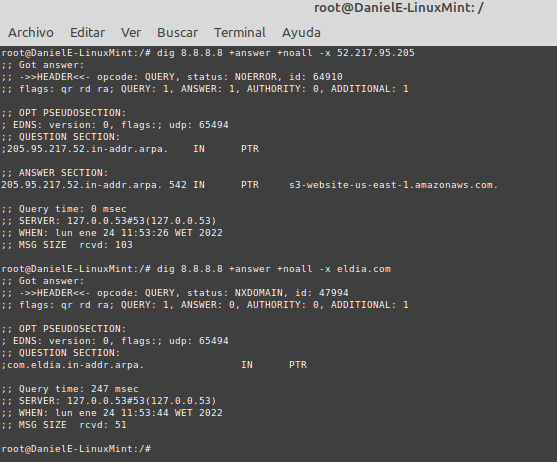




Lanzamos un DIG normal al dominio anterior y otro utilizando parámetros. Realizamos un whois al registro A previamente encontrado, que nos muestra:

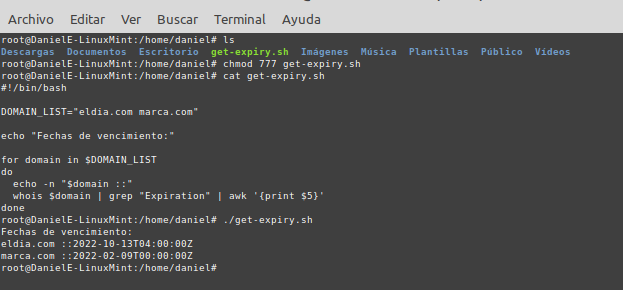




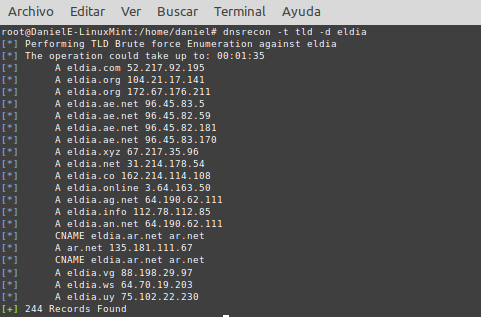


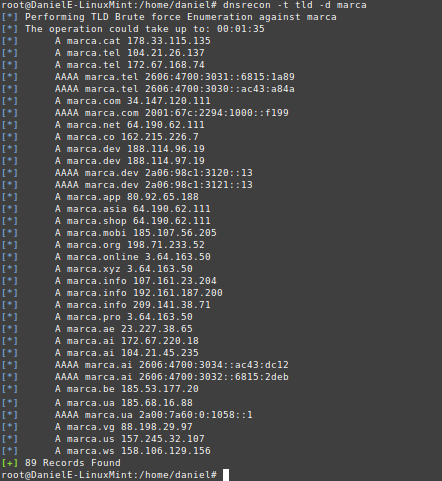
### **2.2 Automatización mediante script, dnsrecon y ripe**

Crearemos un script para obtener las fechas de vencimiento de diferentes dominios, resultando así al ejecutarlo:

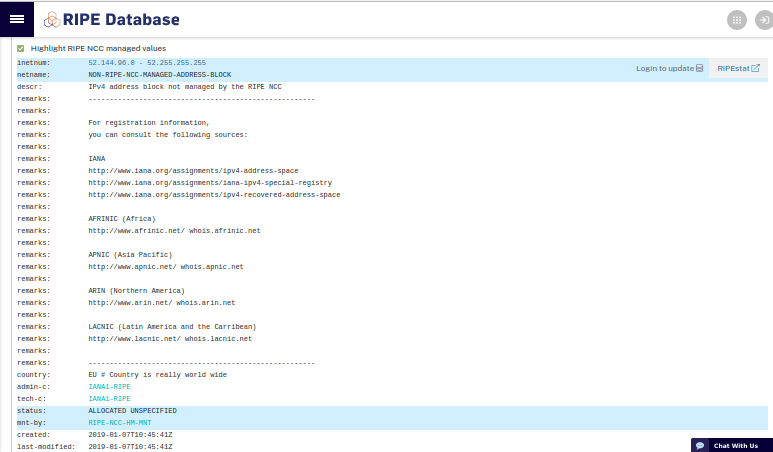


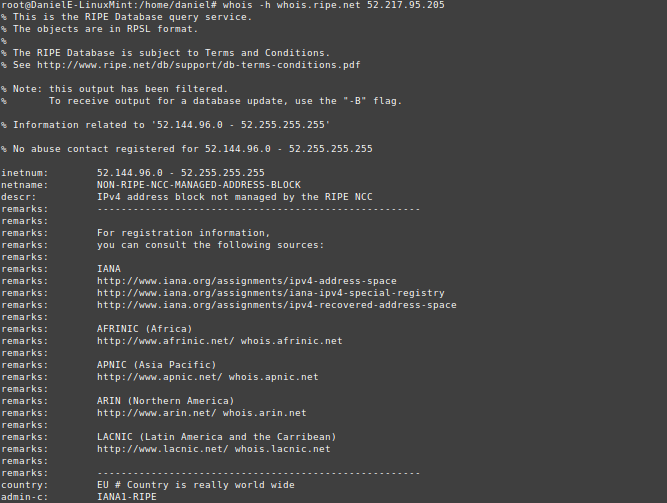
Utilizamos dnsrecon para mostrar las distintas IPs de todos los dominios que coincidan.



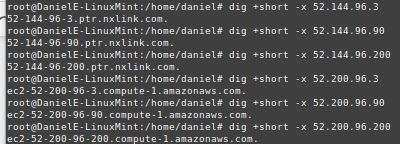


Realizamos dos búsquedas en el servicio de búsqueda de ripe, una por navegador y otra mediante el comando whois:



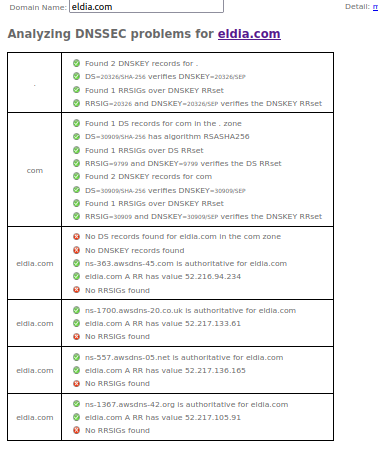


Realizamos una búsqueda inversa para conocer qué rangos de IPs están registrados para el inetnum encontrado.



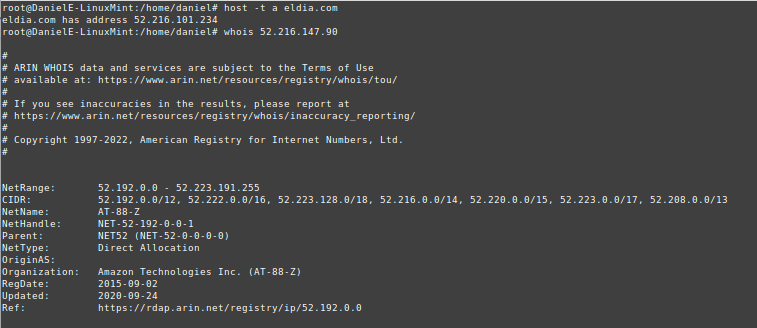
### **2.3 DNSEC**

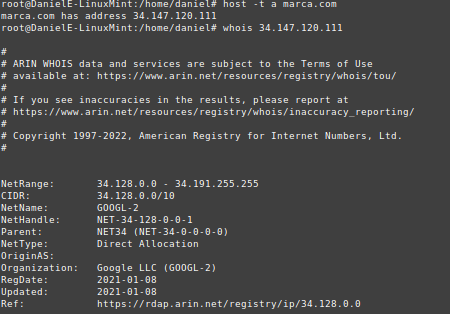
Vamos a utilizar el recurso DNSSEC-Analyzer para comprobar la seguridad y otros resultados obtenidos sobre el dominio elegido.



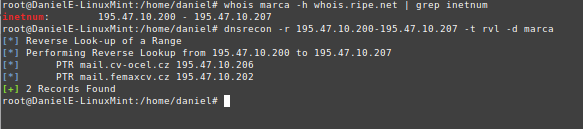
### **2.4 Identificación de activos**

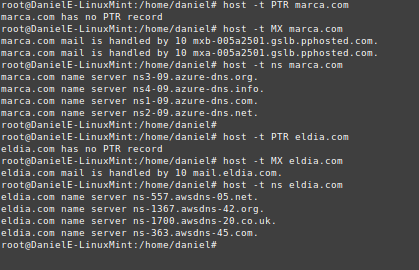
Realizamos una búsqueda con el comando host, con el resultado realizar un whois para obtener rango de direccionamiento y el netname. Vemos cómo podemos obtener mucha información sobre el dominio.





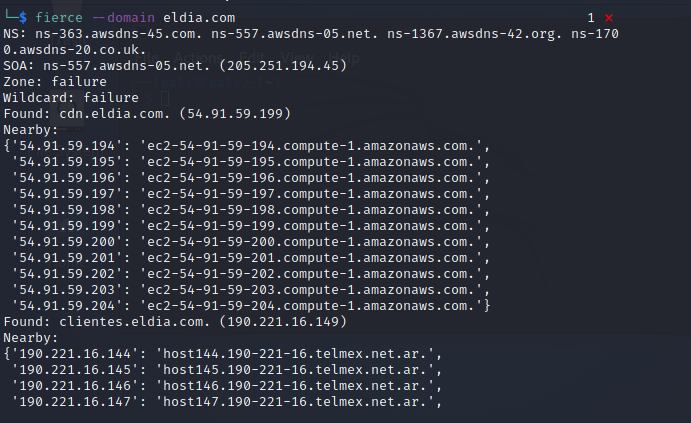




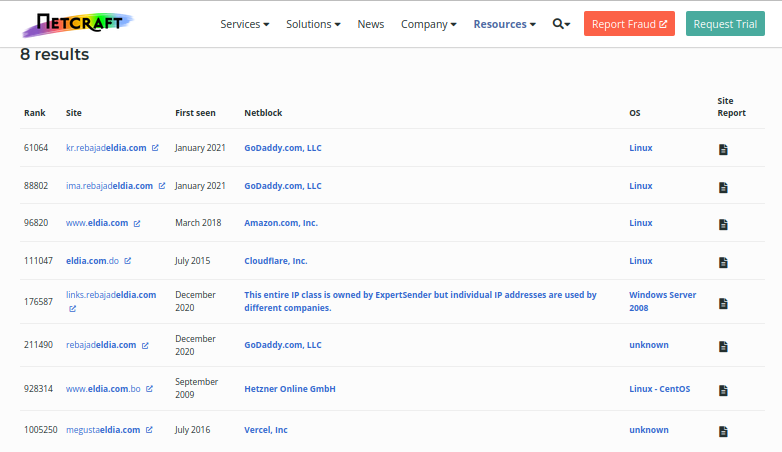


### **2.5 Identificación de subdominios, searchdns.netcraft y dnsdumpster**

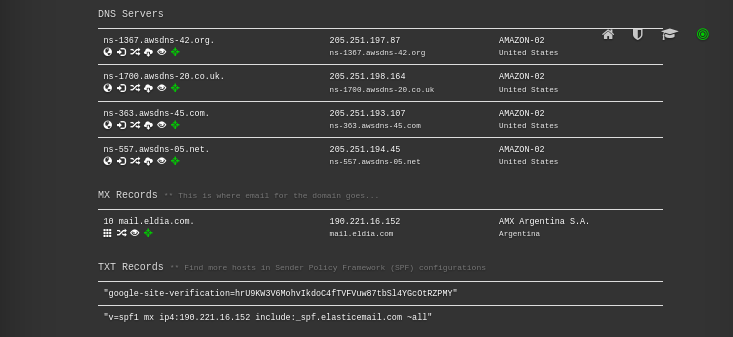
Realizamos una consulta sobre el dominio, con la herramienta fierce.

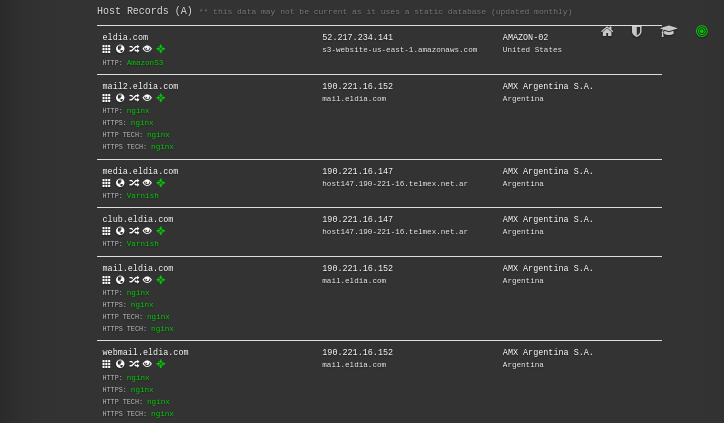


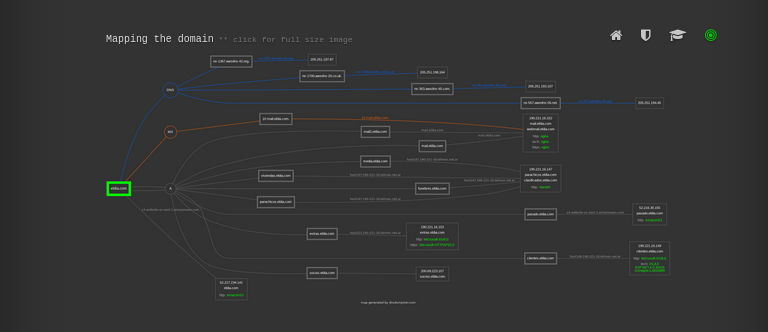
Utilizaremos las páginas web: searchdns.netcraft.com y dnsdumpster.com para obtener información útil sobre el dominio elegido.





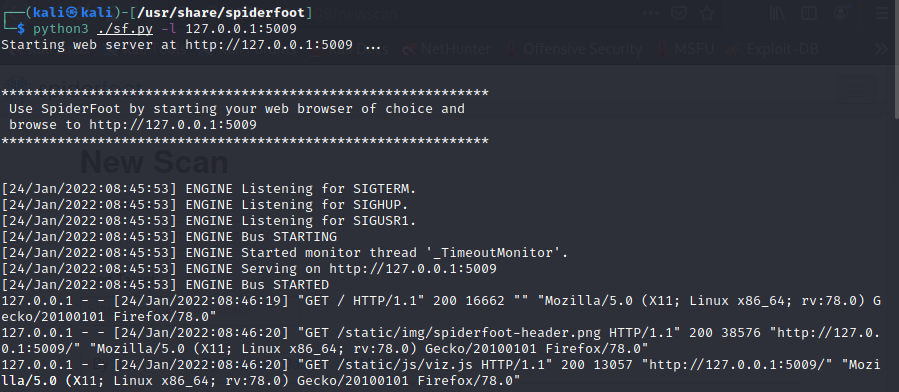




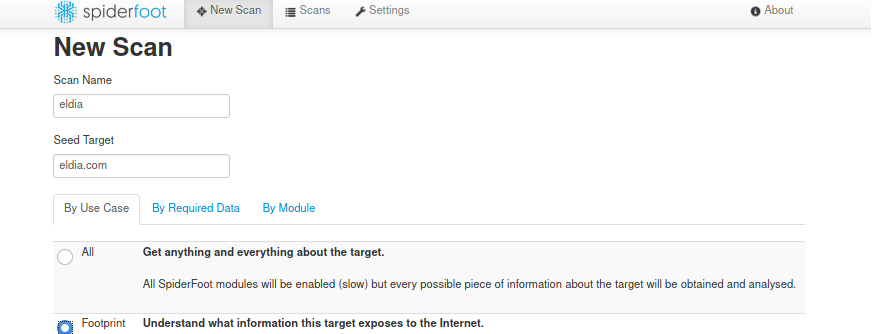


### **2.6 Automatización y escaneo mediante spiderfoot**

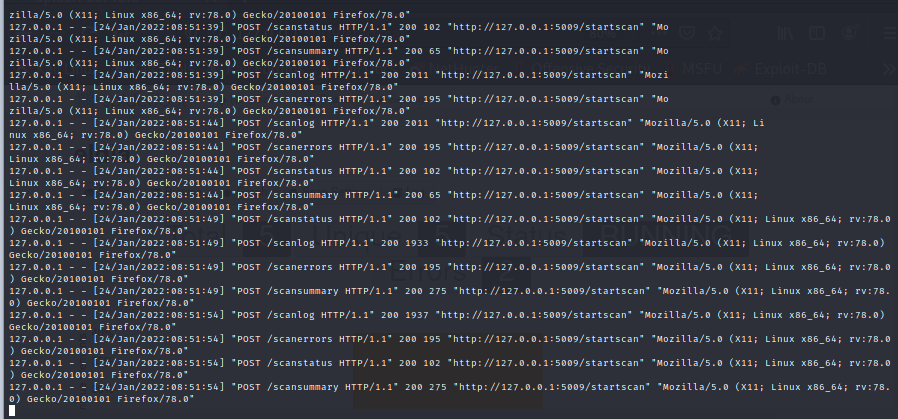
Ponemos en funcionamiento la herramienta spiderfoot.



Accedemos mediante el navegador, en la dirección: 127.0.0.1:5009 y realizamos un escaneo.



Observamos los procesos que se están ejecutando en la terminal



Comprobamos los resultados del escaneo:

