

## MÓDULO: VULNERABILIDADES WEB COMUNES

Actividad de aprendizaje:

Tipo de Ejercicio: individual - revisión en grupo

Para esta actividad el aprendiz deberá:

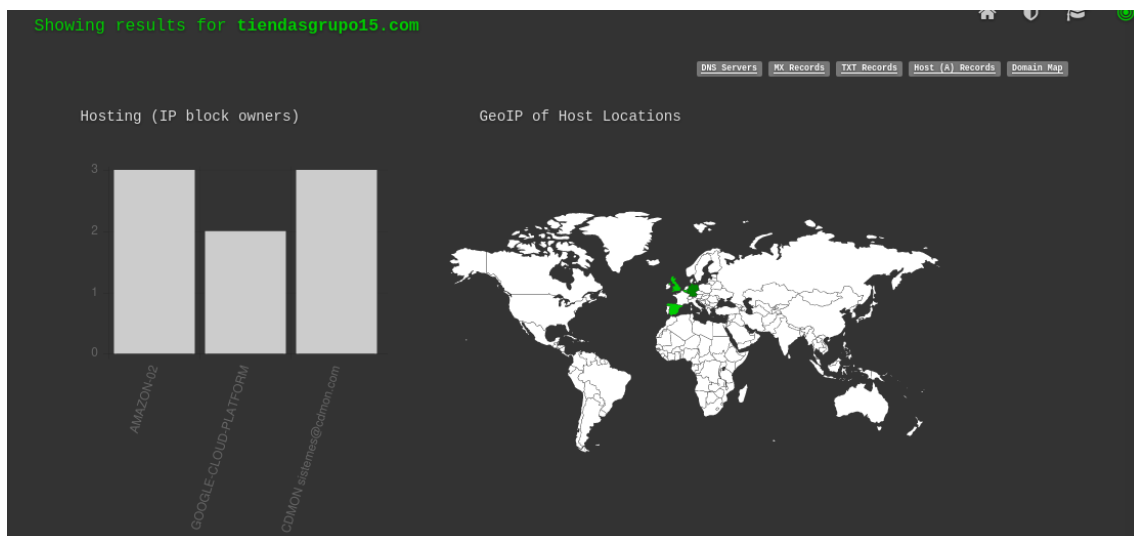
Investigar sobre las herramientas de enumeración web disponibles, realizar la instalación de las mismas en la máquina de ataque y realizar una prueba de funcionamiento de cada una.

Ejemplo de alguna de estas herramientas:

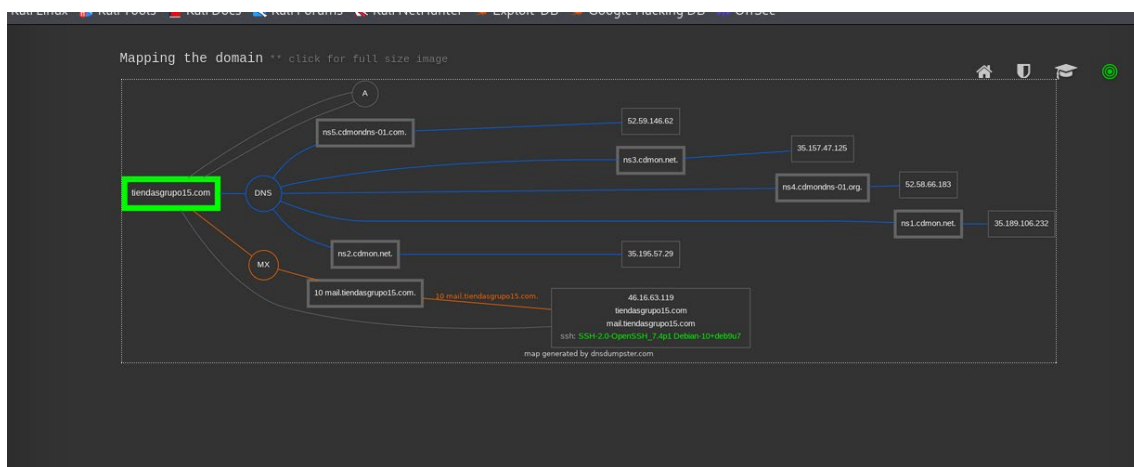
### - DNSDumpster

Esta herramienta se encuentra alojada en el dominio <https://dnsdumpster.com/>

DNSdumpster.com es una herramienta de búsqueda de dominios gratis que puede descubrir hosts relacionados con el dominio.



DNS Servers		
ns5.cdmondns-01.com. 🌐 🔄 🛡️ 🌱	52.59.146.62	AMAZON-02 Germany
ns3.cdmon.net. 🌐 🔄 🛡️ 🌱	35.157.47.125	AMAZON-02 Germany
ns4.cdmondns-01.org. 🌐 🔄 🛡️ 🌱	52.58.66.183	AMAZON-02 Germany
ns1.cdmon.net. 🌐 🔄 🛡️ 🌱	35.189.106.232	GOOGLE-CLOUD-PLATFORM United Kingdom
ns2.cdmon.net. 🌐 🔄 🛡️ 🌱	35.195.57.29	GOOGLE-CLOUD-PLATFORM Belgium
MX Records ** This is where email for the domain goes...		
10 mail.tiendasgrupo15.com. 🌐 🔄 🛡️ 🌱	46.16.63.119	CDMON sistemas@cdmon.com Spain
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations		
"v=spf1 include:_spf.srv.cat -all"		



Podemos ver el mapa del dominio, sus diferentes servidores DNS, Records, etc...

## - Netcraft

Dispone de varias herramientas para hacer escaneos web a un destinatario. En su página web, bajo el apartado resources se encuentran las Research Tools. En este ejemplo utilizaré la de sitereport.

Su funcionamiento es bastante parecido aunque un poco más completo que el de DNSDumpster.

**Description** PVP MMORPG online game with epic classes especially new class Pirate and Ninja, thousands of Quests and the global community of millions players!

**Primary language**

English

## Network

Site	<a href="http://conquer-warzone.com">http://conquer-warzone.com</a>	Domain	<a href="http://conquer-warzone.com">conquer-warzone.com</a>
Netblock Owner	<a href="#">Cloudflare, Inc.</a>	Nameserver	tia.ns.cloudflare.com
Hosting company	Cloudflare	Domain registrar	Unknown
Hosting country	<a href="#">US</a>	Nameserver organisation	whois.cloudflare.com
IPv4 address	104.21.62.49 ( <a href="#">VirusTotal</a> )	Organisation	Unknown
IPv4 autonomous systems	<a href="#">AS13335</a>	DNS admin	dns@cloudflare.com
IPv6 address	2606:4700:3034:0:0:ac43:dc41	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	<a href="#">AS13335</a>	DNS Security Extensions	Unknown
Reverse DNS	Unknown		

## IP delegation

IPv4 address (104.21.62.49)

Country	Name	Description
<a href="https://www.kali.org/docs/">https://www.kali.org/docs/</a>		

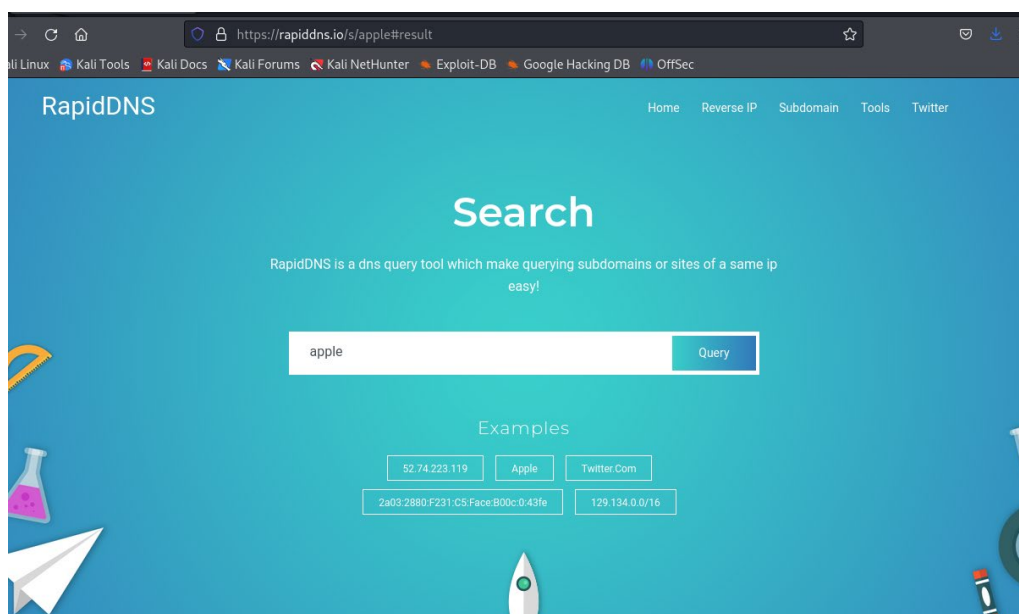
<https://sitereport.netcraft.com/?url=http://conquer-warzone.com>

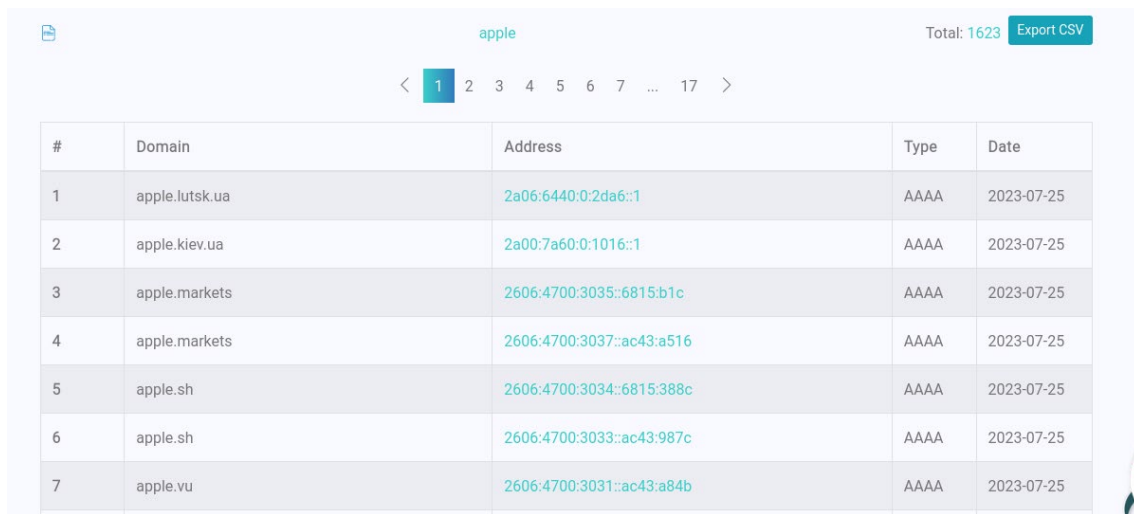
- IPv4info

No he encontrado información sobre esta herramienta.

- RapidDNS

RapidDNS es una herramienta de consulta de DNS que facilita la consulta de subdominios o sitios de una misma ip.





The screenshot shows the RapidDNS web interface. At the top, there is a search bar with the text 'apple' and a 'Total: 1623' indicator next to an 'Export CSV' button. Below the search bar is a pagination control showing a range from 1 to 17, with '1' highlighted. The main content is a table with 5 columns: '#', 'Domain', 'Address', 'Type', and 'Date'. The table contains 7 rows of data, all with a date of '2023-07-25' and type 'AAAA'. The domains listed are 'apple.lutsk.ua', 'apple.kiev.ua', 'apple.markets' (twice), 'apple.sh' (twice), and 'apple.vu'. The addresses are IPv6 format.

#	Domain	Address	Type	Date
1	apple.lutsk.ua	2a06:6440:0:2da6::1	AAAA	2023-07-25
2	apple.kiev.ua	2a00:7a60:0:1016::1	AAAA	2023-07-25
3	apple.markets	2606:4700:3035::6815:b1c	AAAA	2023-07-25
4	apple.markets	2606:4700:3037::ac43:a516	AAAA	2023-07-25
5	apple.sh	2606:4700:3034::6815:388c	AAAA	2023-07-25
6	apple.sh	2606:4700:3033::ac43:987c	AAAA	2023-07-25
7	apple.vu	2606:4700:3031::ac43:a84b	AAAA	2023-07-25

En esta ocasión RapidDNS nos permite exportar los resultados a un archivo .csv para poder observar los datos de una manera más legible.

Tan solo tenemos que poner el nombre o el dominio que queremos buscar en la barra y nos devuelve todos los dominios relacionados con esa query.