CHEAT SHEET
RECONOCIMIENTO DNS

NOTA: el dominio que usaremos es example.com

1. Obtener información básica de un dominio

```
$ whois example.com
```

2. Obtener TLDs de un dominio

Objetivo: obtener nuevos dominios de primer nivel (example.es, example.us, …) y sus ips

```
$ dnsrecon -t tld -d example
```

3. Buscar más información en RIRs

Objetivo: obtener *netnames*, *inetnum* (rangos de IPs), ASNs, e indirectamente, nombres de personas y datos de contacto, ubicaciones, ...

Alternativa1: usar web del RIR. Ej. www.ripe.net

Alternativa 2: usar *whois*

De una IP obtengo netname e inetnum al que pertenece:

```
$ whois -h whois.ripe.net IP
```

Puedo consultar los rangos de IPs de un *netname*:

```
$ whois [NETNAME] -h whois.ripe.net | grep inetnum
```

4. Obtener nombres de dominio a partir de rangos de IP

De una ip:

```
$ host -t ptr [IP]
```

De un rango:

```
$ dnsrecon -r IP_INICIAL-IP_FINAL -t rvl -d example
```

5. Obtener info de servidores de correo:

Obtener los servidores de correo:

```
$ host -t mx example.com
```

Ver IPs de cada servidor (es normal tener varias con el mismo nombre de dominio: balanceo, redundancia, …):

```
$ host mx.example.com
```

Investigar cada IP obtenida con whois, para ver si pertenecen a la empresa investigada o no:

```
$ whois ip_servidor_detectado
```

6. Obtener info de servidores de nombres:

Obtener servidores de nombres:

```
$ host -t ns example.com
```

Se procede igual que con los de correo

7. Obtener subdominios de un dominio

Objetivo: descubrir nuevos nombres de hosts y subdominios:

```
$ dnsenum example.com
$ fierce --domain example.com
$ dnsrecon -d example.com -D wordlist
```

8. Obtener subdominios con certificados digitales

Objetivo: La herramienta ct-exposer consulta los certificados digitales emitidos para un dominio para descubrir subdominios:

```
$ ct-exposer -d example.com
```

9. Transferencia de zona

```
$ dnsrecon -a -d example.com
$ dig example.com axfr
```

10. Herramientas online

Robtex: https://www.robtex.com

Netcraft: https://searchdns.netcraft.com

Dnsdumpster: https://dnsdumpster.com/

Domain Tools: www.domaintools.com

Virus Total: www.virustotal.com

11. Herramientas automatizadas

sublist3r: https://github.com/aboul3la/Sublist3r

```
$ sublist3r -d example.com
```

SpiderFoot:

Arrancar servidor local:

```
$ spiderfoot -l 127.0.0.1:5009
```

Acceder con navegador a http://127.0.0.1:5009