

- Detectar direcciones IP de equipos

Ifconfig:

```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.134.129 netmask 255.255.255.0 broadcast 192.168.134.255
    inet6 fe80::1fee:42bd:636:204f prefixlen 64 scopeid 0<link>
    ether 00:0c:29:11:91:4d txqueuelen 1000 (Ethernet)
    RX packets 2 bytes 684 (684.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 41 bytes 5249 (5.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[/home/kali]
└─# ss
```

ip A:

```
(root@kali)-[/home/kali]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:11:91:4d brd ff:ff:ff:ff:ff:ff
    inet 192.168.134.129/24 brd 192.168.134.255 scope global dynamic noprefixroute eth0
        valid_lft 1429sec preferred_lft 1429sec
    inet6 fe80::1fee:42bd:636:204f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[/home/kali]
└─# ss
```

nmap

```
(root@kali)-[/home/kali]
# nmap 192.168.134.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-10 16:20 EDT
Nmap scan report for 192.168.134.129 (192.168.134.129)
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.134.129 (192.168.134.129) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

```
(root@kali)-[/home/kali]
# nmap -sC 192.168.134.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-10 16:20 EDT
Nmap scan report for 192.168.134.129 (192.168.134.129)
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.134.129 (192.168.134.129) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds

(root@kali)-[/home/kali]
# nmap -sV 192.168.134.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-10 16:21 EDT
Nmap scan report for 192.168.134.129 (192.168.134.129)
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.134.129 (192.168.134.129) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds

(root@kali)-[/home/kali]
# nmap -A -v 192.168.134.129
Nmap version 7.93 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-3.0.7 libssh2-1.10.0 libz-1.2.11 libpcrc-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

## • Recopilar información de sitios web

whatweb:

```
(root@kali)-[/home/kali]
# whatweb https://udg.mx
https://udg.mx [200 OK] Content-Language[es], Cookies[SSESSc1b40e4449efa7f26edc92037c99d13b], Country[MEXICO][MX], Drupal, HTML5, HTTP
Server[nginx/1.12.2], HttpOnly[SSESSc1b40e4449efa7f26edc92037c99d13b], IP[148.202.34.157], JQuery[1.7], MetaGenerator[Drupal 7 (http://
/drupal.org)], PHP[5.4.16], Script[text/javascript], Title[Inicio | Universidad de Guadalajara], UncommonHeaders[x-drupal-cache,x-cont
ent-type-options,permissions-policy,x-generator,link], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/5.4.16], nginx[1.12.2]
```

## • Identificar el tipo de sitio web

whatweb -v

(al ejecutarlo en mi propia máquina me marca error, por lo que lo copié ejemplo del curso)

```
(kali@kali)-[~]
$ whatweb jalisco.gob.mx
http://jalisco.gob.mx [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[awselb/2.0], IP[3.208.83.203], RedirectLocation[https://jalisco.gob.mx:443/], Title[301 Moved Permanently]
https://jalisco.gob.mx/ [200 OK] Apache[2.4.18], Bootstrap, Content-Language[es], Country[UNITED STATES][US], Drupal, Frame, HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[3.208.83.203], JQuery[1.10.1,1.10.2], Lightbox, MetaGenerator[Drupal 7 (http://drupal.org)], Modernizr, Script[text/javascript], Title[Bienvenido | Gobierno del Estado de Jalisco], UncommonHeaders[x-drupal-cache,x-generator,link], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge]
```

```
(kali@kali)-[~]
$ whatweb -v sideclara.sesaj.org
WhatWeb report for http://sideclara.sesaj.org
Status : 301 Moved Permanently
Title : 301 Moved Permanently
IP : 52.1.205.13
Country : UNITED STATES, US

Summary : HTTPServer[awselb/2.0], RedirectLocation[https://sideclara.sesaj.org:443/]
```

Detected Plugins:

[ HTTPServer ]

HTTP server header string. This plugin also attempts to identify the operating system from the server header.

String : awselb/2.0 (from server string)

[ RedirectLocation ]

HTTP Server string location. used with http-status 301 and 302

String : https://sideclara.sesaj.org:443/ (from location)

HTTP Headers:

HTTP/1.1 301 Moved Permanently  
Server: awselb/2.0  
Date: Fri, 21 Apr 2023 02:01:11 GMT  
Content-Type: text/html  
Content-Length: 134  
Connection: close  
Location: https://sideclara.sesaj.org:443/

WhatWeb report for https://sideclara.sesaj.org/

Status : 200 OK  
Title : Bienvenido(a)  
IP : 52.1.205.13  
Country : UNITED STATES, US

Summary : Bootstrap[4.5.0], Cookies[csrftoken], Django, HTML5, HTTPServer[nginx/1.21.1], JQuery[3.5.1], nginx[1.21.1], Script[text/javascript], UncommonHeaders[x-content-type-options], X-Frame-Options[DENY]

Detected Plugins:

[ Bootstrap ]

Bootstrap is an open source toolkit for developing with HTML, CSS, and JS.



```
Version      : 4.5.0
Version      : 4.5.0
Website      : https://getbootstrap.com/
```

[ **Cookies** ]

Display the names of cookies in the HTTP headers. The values are not returned to save on space.

```
String       : csrfToken
```

[ **Django** ]

Django is a high-level Python Web framework that encourages rapid development and clean, pragmatic design.

```
Website      : https://www.djangoproject.com/
```

[ **HTML5** ]

HTML version 5, detected by the doctype declaration

[ **HTTPServer** ]

HTTP server header string. This plugin also attempts to identify the operating system from the server header.

```
String       : nginx/1.21.1 (from server string)
```

[ **JQuery** ]

A fast, concise, JavaScript that simplifies how to traverse HTML documents, handle events, perform animations, and add

```
String       : text/javascript
```

[ **UncommonHeaders** ]

Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version. Info about headers can be found at [www.http-stats.com](http://www.http-stats.com)

```
String       : x-content-type-options (from headers)
```

[ **X-Frame-Options** ]

This plugin retrieves the X-Frame-Options value from the HTTP header. - More Info:  
<http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx>

```
String       : DENY
```

[ **nginx** ]

Nginx (Engine-X) is a free, open-source, high-performance HTTP server and reverse proxy, as well as an IMAP/POP3 proxy server.

```
Version      : 1.21.1
Website      : http://nginx.net/
```

HTTP Headers:

```
HTTP/1.1 200 OK
Date: Fri, 21 Apr 2023 02:01:12 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 67592
Connection: close
```


```
Server: nginx/1.21.1
Vary: Authorization, Cookie
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Set-Cookie: csrftoken=7K7C9P2JaDNsRYP5MXJ6TauNJJodleComhcsrLsl3PGMkSkTEtDPhaDzUWJfmTG
H; expires=Fri, 19 Apr 2024 02:01:12 GMT; Max-Age=31449600; Path=/; SameSite=Lax
```

nslookup:

```
(root@kali)-[/home/kali]
# nslookup https://www.udg.mx/
Server:      192.168.134.2
Address:     192.168.134.2#53
```

crt.sh

https://crt.sh/?q=www.telmex.com

**crt.sh** Identity Search  [Group by Issuer](#)

Criteria Type: Identity Match: ILIKE Search: 'www.telmex.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	<a href="#">1122590423</a>	2019-01-18	2019-01-10	2020-03-10	telmex.com	www.telmex.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
	<a href="#">1098715338</a>	2019-01-10	2019-01-10	2020-03-10	telmex.com	www.telmex.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
	<a href="#">345025022</a>	2018-03-01	2018-02-23	2019-02-23	telmex.com	www.telmex.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
	<a href="#">339460292</a>	2018-02-23	2018-02-23	2019-02-23	telmex.com	www.telmex.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA