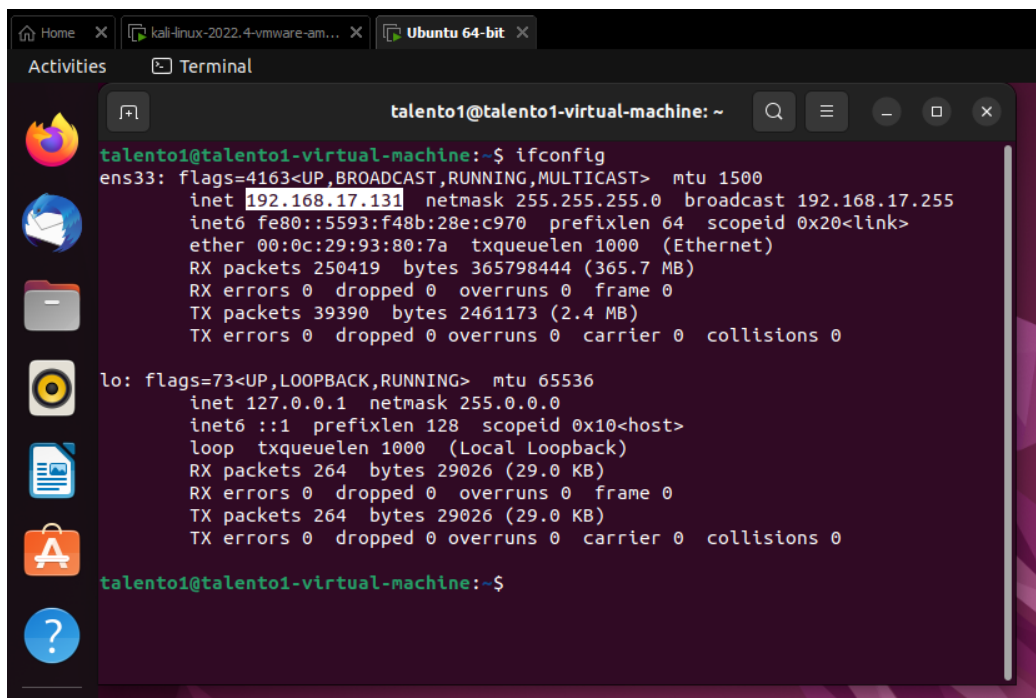


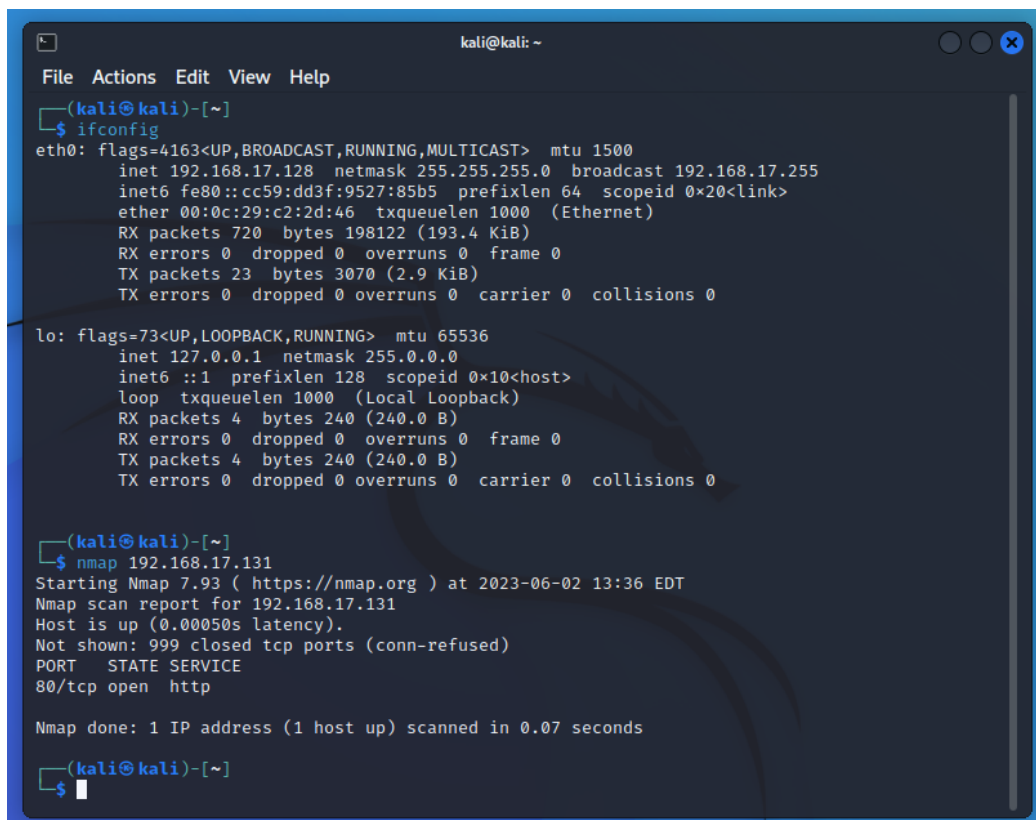
- Detectar direcciones IP de equipos



```
talento1@talento1-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.17.131 netmask 255.255.255.0 broadcast 192.168.17.255
    inet6 fe80::5593:f48b:28e:c970 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:93:80:7a txqueuelen 1000 (Ethernet)
    RX packets 250419 bytes 365798444 (365.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 39390 bytes 2461173 (2.4 MB)
    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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 264 bytes 29026 (29.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 264 bytes 29026 (29.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

talento1@talento1-virtual-machine:~$
```



```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.17.128 netmask 255.255.255.0 broadcast 192.168.17.255
    inet6 fe80::cc59:dd3f:9527:85b5 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c2:2d:46 txqueuelen 1000 (Ethernet)
    RX packets 720 bytes 198122 (193.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23 bytes 3070 (2.9 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 0x10<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:~$ nmap 192.168.17.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 13:36 EDT
Nmap scan report for 192.168.17.131
Host is up (0.00050s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

kali@kali:~$
```

En este ejercicio pudimos detectar que el IP de la maquina de Ubuntu esta abierto en el puerto 80 usando nmap desde Kali

• Recopilar información de sitios web

```
kali@kali: ~  
File Actions Edit View Help  
  
* Scan reddit.com slashdot.org with verbose plugin descriptions.  
./whatweb -v reddit.com slashdot.org  
  
* An aggressive scan of wired.com detects the exact version of WordPress.  
./whatweb -a 3 www.wired.com  
  
* Scan the local network quickly and suppress errors.  
whatweb --no-errors 192.168.0.0/24  
  
* Scan the local network for https websites.  
whatweb --no-errors --url-prefix https:// 192.168.0.0/24  
  
* Scan for crossdomain policies in the Alexa Top 1000.  
./whatweb -i plugin-development/alexa-top-100.txt \  
--url-suffix /crossdomain.xml -p crossdomain_xml  
  
(kali@kali)-[~]  
└─$ whatweb totalplay.com  
http://totalplay.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[108.138.159.42], RedirectLocation[https://totalplay.com/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 aa88f5ac0a69879d3546c78099e47b86.cloudfront.net (CloudFront)]  
https://totalplay.com/ [200 OK] Bootstrap, Country[UNITED STATES][US], Email[close_24px@4x.svg,close_24px@4xWhite.png,colaboracion.justicia@totalplay.com.mx], Frame, Google-Analytics[Universal][UA-7618852-5], HTML5, HTTPServer[AmazonS3], IP[108.138.159.25], JQuery[3.5.1], Script[text/javascript], Strict-Transport-Security[max-age=63072000; includeSubdomains; preload], Title[Provedores de Internet | Somos Totalplay: Tu Compañía de Internet], UncommonHeaders[x-amz-server-side-encryption,x-amz-version-id,x-content-type-options,x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 f0c5f04b5aed6cb215ba05a03ff69770.cloudfront.net (CloudFront)], X-Frame-Options[DENY], X-UA-Compatible[ie=edge], X-XSS-Protection[1; mode=block]  
  
(kali@kali)-[~]  
└─$
```

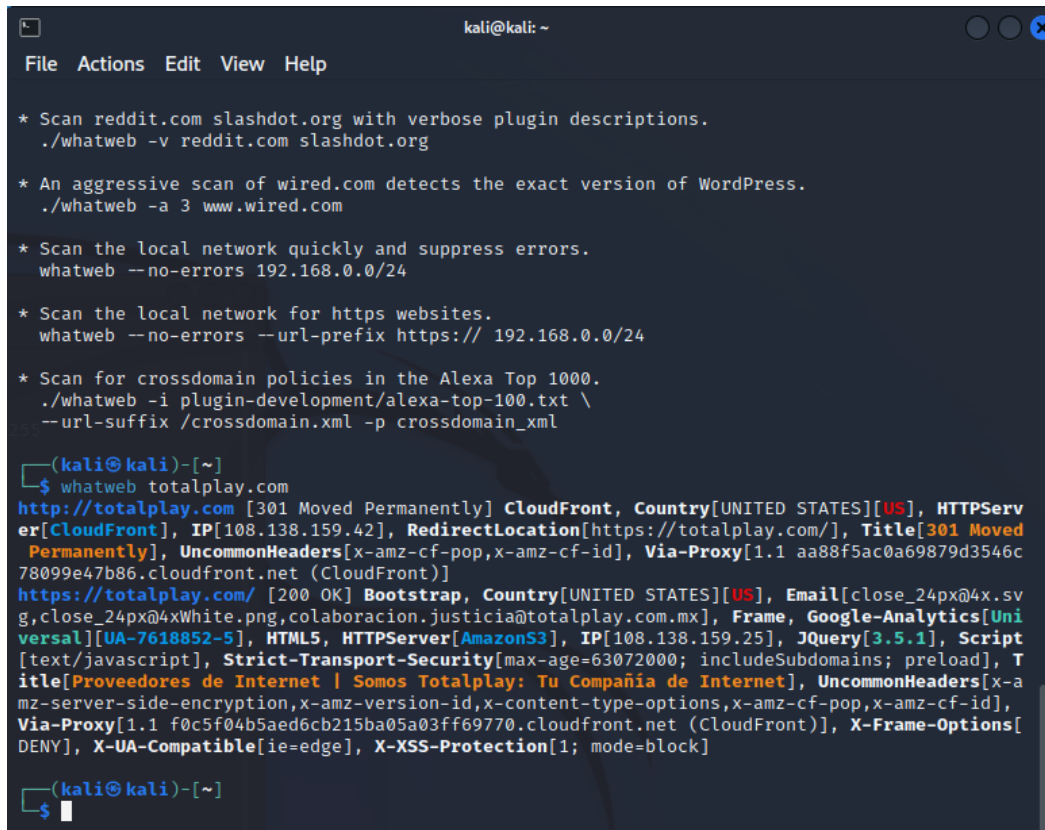
Usando el comando de Whatweb pudimos buscar información del sitio de Total Play el cual nos arroja diferentes datos como que esta en estados unidos, su ip, que usa html5, etc.

Usando la misma dinámica pero agregando una v al final (whatweb -v) nos da la información en un formato mas ordenado:

```
kali@kali: ~  
File Actions Edit View Help  
  
└─$ whatweb -v totalplay.com  
WhatWeb report for http://totalplay.com  
Status : 301 Moved Permanently  
Title : 301 Moved Permanently  
IP : 108.138.159.25  
Country : UNITED STATES, US  
  
Summary : CloudFront, HTTPServer[CloudFront], RedirectLocation[https://totalplay.com/], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 0ff069aca3fe928478ab0a75540e3a58.cloudfront.net (CloudFront)]  
  
Detected Plugins:  
[ CloudFront ]  
CloudFront Server  
  
[ HTTPServer ]  
HTTP server header string. This plugin also attempts to identify the operating system from the server header.  
String : CloudFront (from server string)  
  
[ RedirectLocation ]  
HTTP Server string location. used with http-status 301 and 302  
String : https://totalplay.com/ (from location)  
  
[ 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  
String : x-amz-cf-pop,x-amz-cf-id (from headers)  
  
[ Via-Proxy ]  
This plugin extracts the proxy server details from the Via param of the HTTP header.  
String : 1.1 0ff069aca3fe928478ab0a75540e3a58.cloudfront.net (CloudFront)
```

• Identificar el tipo de sitio web

Usando el ejemplo anterior para Total Play podemos ver que se trata de un sitio web de tipo HTML5, marcado después de la línea donde pone “Versal” en color verde en la imagen.



```
kali@kali: ~  
File Actions Edit View Help  
  
* Scan reddit.com slashdot.org with verbose plugin descriptions.  
./whatweb -v reddit.com slashdot.org  
  
* An aggressive scan of wired.com detects the exact version of WordPress.  
./whatweb -a 3 www.wired.com  
  
* Scan the local network quickly and suppress errors.  
whatweb --no-errors 192.168.0.0/24  
  
* Scan the local network for https websites.  
whatweb --no-errors --url-prefix https:// 192.168.0.0/24  
  
* Scan for crossdomain policies in the Alexa Top 1000.  
./whatweb -i plugin-development/alexa-top-100.txt \  
--url-suffix /crossdomain.xml -p crossdomain.xml  
  
(kali@kali)-[~]  
$ whatweb totalplay.com  
http://totalplay.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[108.138.159.42], RedirectLocation[https://totalplay.com/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 aa88f5ac0a69879d3546c78099e47b86.cloudfront.net (CloudFront)]  
https://totalplay.com/ [200 OK] Bootstrap, Country[UNITED STATES][US], Email[close_24px@4x.svg,close_24px@4xWhite.png,colaboracion.justicia@totalplay.com.mx], Frame, Google-Analytics[Universal][UA-7618852-5], HTML5, HTTPServer[AmazonS3], IP[108.138.159.25], JQuery[3.5.1], Script[text/javascript], Strict-Transport-Security[max-age=63072000; includeSubdomains; preload], Title[Proveedores de Internet | Somos Totalplay: Tu Compañía de Internet], UncommonHeaders[x-amz-server-side-encryption,x-amz-version-id,x-content-type-options,x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 f0c5f04b5aed6cb215ba05a03ff69770.cloudfront.net (CloudFront)], X-Frame-Options[DENY], X-UA-Compatible[ie=edge], X-XSS-Protection[1; mode=block]  
  
(kali@kali)-[~]  
$
```

Así como este existen tipos como HTML, PHP y WebGL / WebAssembly