

Ciber Seguridad Básico. Reto 1.

Recolección de información tecnológica, como direcciones IPs en la red, información de la organización en internet, e información de vulnerabilidades de los sistemas.

- Detectar direcciones IP de equipos.

```
Simbolo del sistema

C:\Users\edura>ipconfig

Configuración IP de Windows

Adaptador de Ethernet vEthernet (Modificador pre):

    Su fijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::c405:ccda:f4c4:1fb6%10
    Dirección IPv4. . . . . : 172.30.127.177
    Máscara de subred. . . . . : 255.255.255.240
    Puerta de enlace predeterminada. . . . . :

Adaptador de Ethernet Ethernet:

    Su fijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::8da4:82f8:cb8a:96a4%4
    Dirección IPv4. . . . . : 192.168.0.8
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.0.1

Adaptador de túnel Teredo Tunneling Pseudo-Interface:

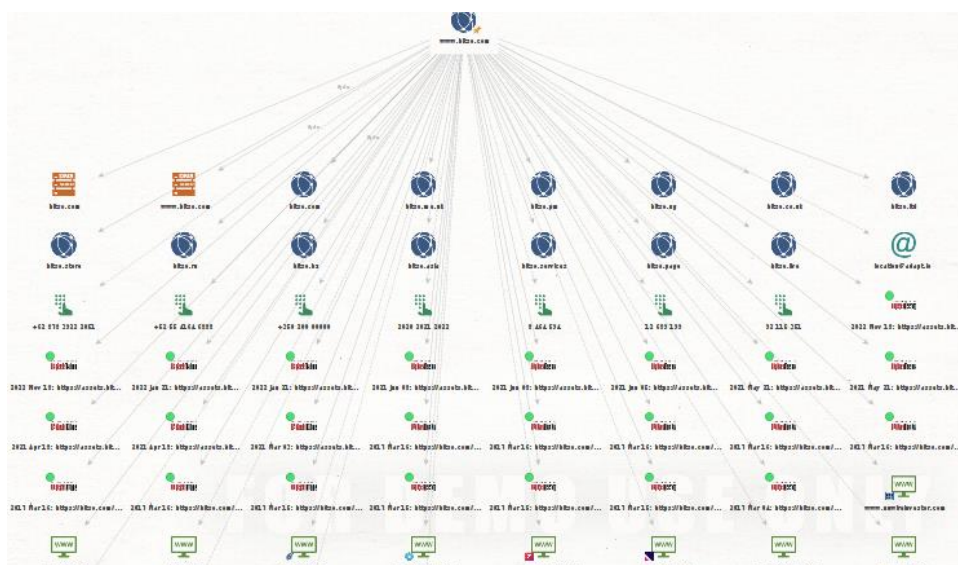
    Su fijo DNS específico para la conexión. . . :
    Dirección IPv6. . . . . : 2001:0:9d38:6abd:2897:1696:3f57:fff7
    Vínculo: dirección IPv6 local. . . : fe80::2897:1696:3f57:fff7%5
    Puerta de enlace predeterminada. . . . . :

kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.163.128  netmask 255.255.255.0  broadcast 192.168.163.255
    inet6 fe80::56d8:9104:240d:6799  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:a3:de:4e  txqueuelen 1000  (Ethernet)
    RX packets 11  bytes 1598 (1.6 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 31  bytes 4112 (4.0 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
```

- Recopilar información de sitios web.

```
(kali㉿kali)-[~]
$ whatweb www.bitso.com
http://www.bitso.com [301 Moved Permanently] Cookies[__cf_bm], Country[UNITED STATES][US], HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[162.159.130.10], RedirectLocation[https://bitso.com], UncommonHeaders[x-content-type-options,c f-ray]
https://bitso.com [200 OK] Cookies[__cf_bm], Country[UNITED STATES][US], HTML 5, HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[162.159.133.10], Open-Graph-Protocol[website], PoweredBy[crypto], Script[application/json], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Bitso: more than a crypto exchange, it's a complete solution], UncommonHeaders[x-nextjs-cache,x-envoy-upstream-service-time,cf-cache-status,x-content-type-options,c f-ray], X-Powered-By[Next.js]
```



- Identificar el tipo de sitio web.

```
(kali@kali)-[~]
$ nmap www.bitso.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-14 14:13 EDT
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 57.35% done; ETC: 14:13 (0:00:13 remaining)
Nmap scan report for www.bitso.com (162.159.133.10)
Host is up (0.11s latency).
Other addresses for www.bitso.com (not scanned): 162.159.130.10 2606:4700:7::a29f:820a
a29f:820a 2606:4700:7::a29f:850a
Not shown: 994 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 64.31 seconds

(kali@kali)-[~]
$ nikto -h www.bitso.com
- Nikto v2.5.0

+ Multiple IPs found: 162.159.133.10, 162.159.130.10, 2606:4700:7::a29f:850a,
2606:4700:7::a29f:820a
+ Target IP: 162.159.133.10
+ Target Hostname: www.bitso.com
+ Target Port: 80
+ Start Time: 2023-05-14 14:18:14 (GMT-4)

+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ Root page / redirects to: https://bitso.com
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 8074 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2023-05-14 14:52:15 (GMT-4) (2041 seconds)

+ 1 host(s) tested
```

Isis Mora práctica.