

Ejercicio : Reconocimiento Pasivo


Dnsdumpster

A Records (subdomains from dataset)					
Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
analytics.totalplay.com.mx	54.146.73.14 ec2-54-146-73-14.compute-1.amazonaws.com	ASN:14618 54.144.0.0/14	AMAZON-AES United States	https: unknown server cn: .us-east-1.es.amazonaws.com	1
avisopago.totalplay.com.mx	15.197.143.162 a883c12563287485a.awsglob.alacelerator.com	ASN:16509 15.197.128.0/20	AMAZON-02 United States	https: nginx/1.20.0 title: Error-404 cn: .totalplay.com.mx o: Total Play Telecomunicaciones, S.A.P.I. de C.V. tech: Amazon CloudFront Amazon Web Services Nginx:1.20.0	3
www.avisopago.totalplay.com.mx	3.33.149.179 a883c12563287485a.awsglob.alacelerator.com	ASN:16509 3.33.144.0/20	AMAZON-02 United States	https: nginx/1.20.0 title: Error-404 cn: .totalplay.com.mx o: Total Play Telecomunicaciones, S.A.P.I. de C.V. tech: Nginx:1.20.0 Amazon CloudFront Amazon Web Services	
click.campaign.totalplay.com.mx	13.111.229.168 click.campaign.totalplay.com.mx	ASN:14340 13.111.0.0/16	SALESFORCE United States	http: unknown server title: 403 - Forbidden: Access is denied. https: unknown server title: 403 - Forbidden: Access is denied. cn: click.campaign.totalplay.com.mx o: Salesforce, Inc.	2
view.campaign.totalplay.com.mx	13.111.231.176 view.campaign.totalplay.com.mx	ASN:14340 13.111.0.0/16	SALESFORCE United States	http: unknown server title: Error tech: Microsoft Visual Studio https: unknown server title: Object moved	2

Start Test!


>> Free users are limited to 50 results for a single domain. Get 12 months [Plus Access](#) - on Sale Now.

System Locations




Hosting / Networks

TOTAL PLAY TELECOM	68
AMAZON-02	2
SALESFORCE	2
IRONPORT-SYSTEMS	2
AMAZON-AES	1



Services / Banners



nPerf/2.2.7 2022-10-14	68
nginx/1.20.0	2
Apache/2.4.37 (CentOS Stream)	2
Apache/2.4.62 (Rocky Linux)	1

Showing 50 records out of a total of 55 found.

A Records (subdomains from dataset)					
Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP



Utilities

Domain Dossier

Domain Check

Email Dossier

Browser Mirror

Ping

Traceroute

Nslookup / Dig

18.160.124.38

18.160.124.46

18.160.124.122

Domain Whois record

Queried whois.mx with "totalplay.com.mx"...

Domain Name:totalplay.com.mx

Created On:2010-02-08

Expiration Date:2026-02-07

Last Updated On:2025-01-22

Registrar:AKKY ONLINE SOLUTIONS, S.A. DE C.V.

URL:http://www.akky.mx

Whois TCP URI:whois.akky.mx

Whois Web URL:http://www.akky.mx/herramientas/whois.jsf

Registrant:

Name:Oswaldo Cortes Palacios

City:Mexico

State:Distrito Federal

Country:Mexico

Administrative Contact:

Name:Administrador Pagos Dominios GS

City:D.F.

State:Distrito Federal

Country:Mexico

Technical Contact:

Name:Administrador Pagos Dominios GS

City:D.F.

State:Distrito Federal

Country:Mexico

Billing Contact:

Name:Administrador Pagos Dominios GS

Utilities

Domain Dossier

Domain Check

Email Dossier

Browser Mirror

Ping

Traceroute

Nslookup / Dig

OrgHandle: AAR01-ARIN

OrgName: Amazon AWS Network Operations

OrgPhone: +1-206-555-0000

OrgEmail: amzn-nsd-contact@amazon.com

OrgRef: https://rdap.arin.net/registry/entity/AAR01-ARIN

OrgRoutingHandle: ARNP-ARIN

OrgRoutingName: AWS RPT Management POC

OrgRoutingPhone: +1-206-555-0000

OrgRoutingEmail: aws-rpt-management-poc@amazon.com

OrgRoutingRef: https://rdap.arin.net/registry/entity/ARNP-ARIN

DNS records

name	class	type	data	time to live
totalplay.com.mx	IN	NS	ns5.totalplay.com.mx	3600s (01:00)
totalplay.com.mx	IN	NS	ns4.totalplay.com.mx	3600s (01:00)
totalplay.com.mx	IN	NS	ns3.totalplay.com.mx	3600s (01:00)
totalplay.com.mx	IN	TXT	v=spf1 ip4:200.38.115.23 ip4:200.38.115.24 ip4:200.38.122.54 ip4:200.38.122.55 ip4:200.38.100.47 ip4:200.38.100.48 ip4:200.38.115.110 ip4:200.38.115.111 ip4:200.38.122.65 include:spf.protection.outlook.com -all	3600s (01:00)
totalplay.com.mx	IN	TXT	google-site-verification=sCabNGDHym1grun6XEaZebJPACvO2IFBBJdvPABM	3600s (01:00)
totalplay.com.mx	IN	TXT	MS=ms21879637	3600s (01:00)
totalplay.com.mx	IN	TXT	_k5095yew7wlp6b6jldg2ym5fw	3600s (01:00)
totalplay.com.mx	IN	TXT	3a1038298575b75bb1d4648ac69241d1cc84f21be155e955ba3dea6dd183102	3600s (01:00)
totalplay.com.mx	IN	TXT	google-site-verification=puq7NGgID3NPeMLu93F2dm4MtzayVC26S70z3Qzlw	3600s (01:00)
totalplay.com.mx	IN	TXT	3492sqjh3mc1ykb79bjc41hmdz3sp	3600s (01:00)
totalplay.com.mx	IN	TXT	trustcor-ca-m555XvC7EX8nUDKJL94dLorPJLaG6CJ1htuVGAIQHNRd5EbJEO5ERZ30mIpKGQPSyQAWIGF559K3mFGdvtasBvFP5CXIX0r11u4e5DCp5YtHP4GfIAM8B8Bfq/C01D9uLB7JN85s+qvT	3600s (01:00)
totalplay.com.mx	IN	TXT	ZOOM_verify_DKN4DDAQgOp4gp4am05JQ	3600s (01:00)
totalplay.com.mx	IN	TXT	dropbox-domain-verification=9458kc392o0h	3600s (01:00)
totalplay.com.mx	IN	TXT	discoidomainverification=a76b629b849195107147dc60a283ce7b4dcfb308e246aa7ee6e416b75d5c	3600s (01:00)
totalplay.com.mx	IN	TXT	hVRIEfaY4AG09kullqit+OH2DCLDHd8pB9Mvvlqm4oaO7eXau34tGh475aYzR7zjpsLGCTEB17s8NoDwmvg==	3600s (01:00)
totalplay.com.mx	IN	TXT	MS=D4478FB308FD312E2ACCAF730C1E9987D3EBC667	3600s (01:00)
totalplay.com.mx	IN	MX	preference: 10 exchange: mx1.hs751-2.lghmx.com	3600s (01:00)

Shodan

The screenshot displays the Shodan search engine interface. At the top, there's a search bar with the IP address 18.160.124.57 entered. Below the search bar, the results are categorized into 'General Information' and 'Web Technologies'.

General Information:

- Hostnames: server-18-160-124-57-prod1.cloudfront.net
- Domains: cloudfront.net
- Cloud Provider: Amazon
- Cloud Region: GLOBAL
- Cloud Service: CLOUDFRONT
- Country: Mexico
- City: Santiago de Querétaro
- Organization: Amazon.com, Inc.
- ISP: Amazon.com, Inc.
- ASN: AS1609

Web Technologies:

- CDN: Amazon CloudFront
- SSL: Amazon Web Services

On the right side, there's a section for 'Open Ports' showing results for port 80/TCP. The results indicate that the request could not be satisfied, likely due to a timeout or a connection error.

P0f

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo apt install p0f
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Installing:
p0f

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
Download size: 80.0 kB
Space needed: 223 kB / 63.6 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 p0f amd64 3.09b-4 [80.0 kB]
Fetched 80.0 kB in 2s (53.3 kB/s)
Selecting previously unselected package p0f.
(Reading database ... 413034 files and directories currently installed.)
Preparing to unpack .../archives/p0f_3.09b-4_amd64.deb ...
Unpacking p0f (3.09b-4) ...
Setting up p0f (3.09b-4) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...
```

```
(kali@kali)-[~]
└─$ sudo p0f i eth0
p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx>

[-] PROGRAM ABORT : Filter rule must be a single parameter (use quotes).
    Location : main(), p0f.c:1166
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::3410:1308:87e...	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for
2	17.504468508	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3	20.517572841	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
4	23.518485237	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
5	26.524424375	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
6	29.524619264	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
7	32.539845474	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
8	38.506811047	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
9	41.520907659	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
10	44.527552124	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
11	44.729484282	fe80::36d3:fa23:113...	ff02::2	ICMPv6	62	Router Solicitation
12	50.016159269	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
13	53.017679325	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
14	56.028671247	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
15	65.170738906	192.168.217.135	132.248.30.3	NTP	90	NTP Version 4, client
16	65.252969465	132.248.30.3	192.168.217.135	NTP	90	NTP Version 4, server
17	69.010282905	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.217.2? Tel

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface eth0
 Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: ff:ff:ff:ff:ff:ff
 Internet Protocol Version 6, Src: fe80::3410:1308:87e..., Dst: ff02::1:ff00:1
 Internet Control Message Protocol v6

0000 33 33 ff 00 00 01 00 50 56 c0 00 08 86 dd 60
 0010 00 00 00 20 3a ff fe 80 00 00 00 00 00 00 34
 0020 13 08 87 ed c0 0c ff 02 00 00 00 00 00 00 00
 0030 00 01 ff 00 00 01 87 00 96 70 00 00 00 00 fe
 0040 00 00 00 00 00 00 00 00 00 00 00 00 01 01
 0050 00 50 56 c0 00 08

File Actions Edit View Help

(kali@kali)-[~]
\$ sudo p0f -i eth0

— p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> —

[+] Closed 1 file descriptor.
 [+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
 [+] Intercepting traffic on interface 'eth0'.
 [+] Default packet filtering configured [+VLAN].
 [+] Entered main event loop.

6 29.524619264 192.168.217.1 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
 7 32.539845474 192.168.217.1 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
 8 38.506811047 192.168.217.1 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
 9 41.520907659 192.168.217.1 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
 10 44.527552124 192.168.217.1 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
 11 44.729484282 fe80::36d3:fa23:113... ff02::2 ICMPv6 62 Router Solicitation
 12 50.016159269 192.168.217.1 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
 13 53.017679325 192.168.217.1 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
 14 56.028671247 192.168.217.1 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
 15 65.170738906 192.168.217.135 132.248.30.3 NTP 90 NTP Version 4, client
 16 65.252969465 132.248.30.3 192.168.217.135 NTP 90 NTP Version 4, server
 17 69.010282905 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.217.2? Tel

.-[192.168.217.135/52028 → 23.39.228.19/443 (syn)]-
 client = 192.168.217.135/52028
 os = Linux 2.2.x-3.x
 dist = 0
 params = generic
 raw_sig = 4:64+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df,id+:0

.-[192.168.217.135/52028 → 23.39.228.19/443 (mtu)]-
 client = 192.168.217.135/52028
 link = Ethernet or modem
 raw_mtu = 1500

.-[192.168.217.135/43834 → 23.39.228.7/443 (syn)]-
 client = 192.168.217.135/43834
 os = Linux 2.2.x-3.x
 dist = 0
 params = generic
 raw_sig = 4:64+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df,id+:0

The harvester

```
whoisxml, zoomeye, venatus

(kali@kali)-[~]
$ theHarvester -d totalplay.com.mx -b bing

Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
*
*  theHarvester 4.8.0
*  Coded by Christian Martorella
*  Edge-Security Research
*  cmartorella@edge-security.com
*
*****

[*] Target: totalplay.com.mx

Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Searching 0 results.
[*] Searching Bing.
[*] No IPs found.
[*] No emails found.
[*] No people found.
[*] No hosts found.

(kali@kali)-[~]
$ theHarvester -d totalplay.com.mx -b duckduckgo

Read proxies.yaml from /etc/theHarvester/proxies.yaml
```

Capturing from eth0

No.	Time	Source	Destination	Protocol	Length	Info
620	332.002177689	VMware_c0:00:08	Broadcast	ARP	60	who has 192.168.217.2? Tell 192.168.217.1
621	332.849550406	0.0.0.0	239.255.255.255	RIP	100	RIP 11 (RIP Initiator Packet)
622	334.017259397	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
623	337.021229348	192.168.217.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
624	349.270802482	192.168.217.1	224.0.0.251	MDNS	393	Standard query response 0x0000 PTR G5._dosvc._tcp.local
625	349.271445741	fe80::3410:1308:87e...	ff02::fb	MDNS	413	Standard query response 0x0000 PTR G5._dosvc._tcp.local
626	349.271810617	192.168.217.1	224.0.0.251	MDNS	80	Standard query 0x0000 ANY G5._dosvc._tcp.local, "QM" que
627	349.272018305	fe80::3410:1308:87e...	ff02::fb	MDNS	100	Standard query 0x0000 ANY G5._dosvc._tcp.local, "QM" que
628	349.534621565	192.168.217.1	224.0.0.251	MDNS	80	Standard query 0x0000 ANY G5._dosvc._tcp.local, "QM" que
629	349.534628264	fe80::3410:1308:87e...	ff02::fb	MDNS	100	Standard query 0x0000 ANY G5._dosvc._tcp.local, "QM" que
630	349.797050536	192.168.217.1	224.0.0.251	MDNS	80	Standard query 0x0000 ANY G5._dosvc._tcp.local, "QM" que
631	349.797053336	fe80::3410:1308:87e...	ff02::fb	MDNS	100	Standard query 0x0000 ANY G5._dosvc._tcp.local, "QM" que
632	350.002788296	192.168.217.1	224.0.0.251	MDNS	445	Standard query response 0x0000 PTR, cache flush G5._dosvc
633	350.003188170	fe80::3410:1308:87e...	ff02::fb	MDNS	465	Standard query response 0x0000 PTR, cache flush G5._dosvc
634	350.003434555	192.168.217.1	224.0.0.251	MDNS	394	Standard query response 0x0000 SRV, cache flush 0 0 7680
635	350.003685139	fe80::3410:1308:87e...	ff02::fb	MDNS	414	Standard query response 0x0000 SRV, cache flush 0 0 7680
636	360.005738345	fe80::3410:1308:87e...	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for fe80::1 from 00:50:56:c0:00:08

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0

Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv6mcast

Internet Protocol Version 6, Src: fe80::3410:1308:87e:c00c, Dst: ff02::1

Internet Control Message Protocol v6

0000 33 33 ff 00 00 01 00 50 56 c0 00 08 86 dd 60 00 33 ... P V

0010 00 00 00 20 3a ff fe 80 00 00 00 00 00 00 34 10 : ...

0020 13 08 87 ed c0 0c ff 02 00 00 00 00 00 00 00 00 : ...

0030 00 01 ff 00 00 01 87 00 96 70 00 00 00 00 fe 80 : ...

0040 00 00 00 00 00 00 00 00 00 00 00 00 01 01 01 : ...

0050 00 50 56 c0 00 08 : ... PV ...