Contents

What is sublist3r ?

- identify subdomains of a target domain.

Information gathering

- also called reconnaissance
- collects details about a target.
- 2types
  - Active Reconnaissance
  - Passive Reconnaissance

1. Active Reconnaissance

- sends packets directly to the target to determine which ports are open.
- directly interacting with the target system or network to gather information.
- traces in logs or alerts.
- provides detailed and up-to-date information
  - Identifying specific services running on open ports and their versions(nmap, netcat)
  - determine the operating system of the target(nmap)
  - Actively querying a DNS for information about domain names, IP addresses.(nslookup)

2. Passive Reconnaissance

- without directly interacting with the target system
- does not trigger alarms, making it less likely to be detected.
- outdated information
  - Gathering information from publicly available documents
  - Scanning social media platforms
  - provide a list of SSL certificates issued for a domain

Active Reconnaissance is useful when you need real-time and detailed data but should be used with caution, especially if you need to avoid detection.

Passive Reconnaissance is ideal when you want to remain undetected and gather initial information without interacting directly with the target.

Sublist3r is **passive** because it collects publicly available information from third-party services, leaving no direct trace or interaction with the target domain.

Run Sublist3r from the command line

Command : **python sublist3r.py -d example.com -o subdomains.txt**

- **-d:** Specify the domain to search.
- **-o:** Save the output to a file.
- **-b:** Use brute-forcing for additional results.
- **-v:** Enable verbose output to see the progress in real time

What is Amass ?

- open-source cybersecurity tool for mapping and identifying assets and subdomains of domain or organization.

What it does ?

- identifies subdomains related to a domain
- gathers DNS records like IP addresses, CNAMEs
- Finds and maps out network infrastructure, such as IP ranges and Autonomous System Numbers (ASNs).
- Passive and Active Recon:
  Passive: Collects data from third-party sources without interacting with the target.
  Active: Performs direct probing to discover more assets.
- Generates a complete picture of an organization's external-facing assets.

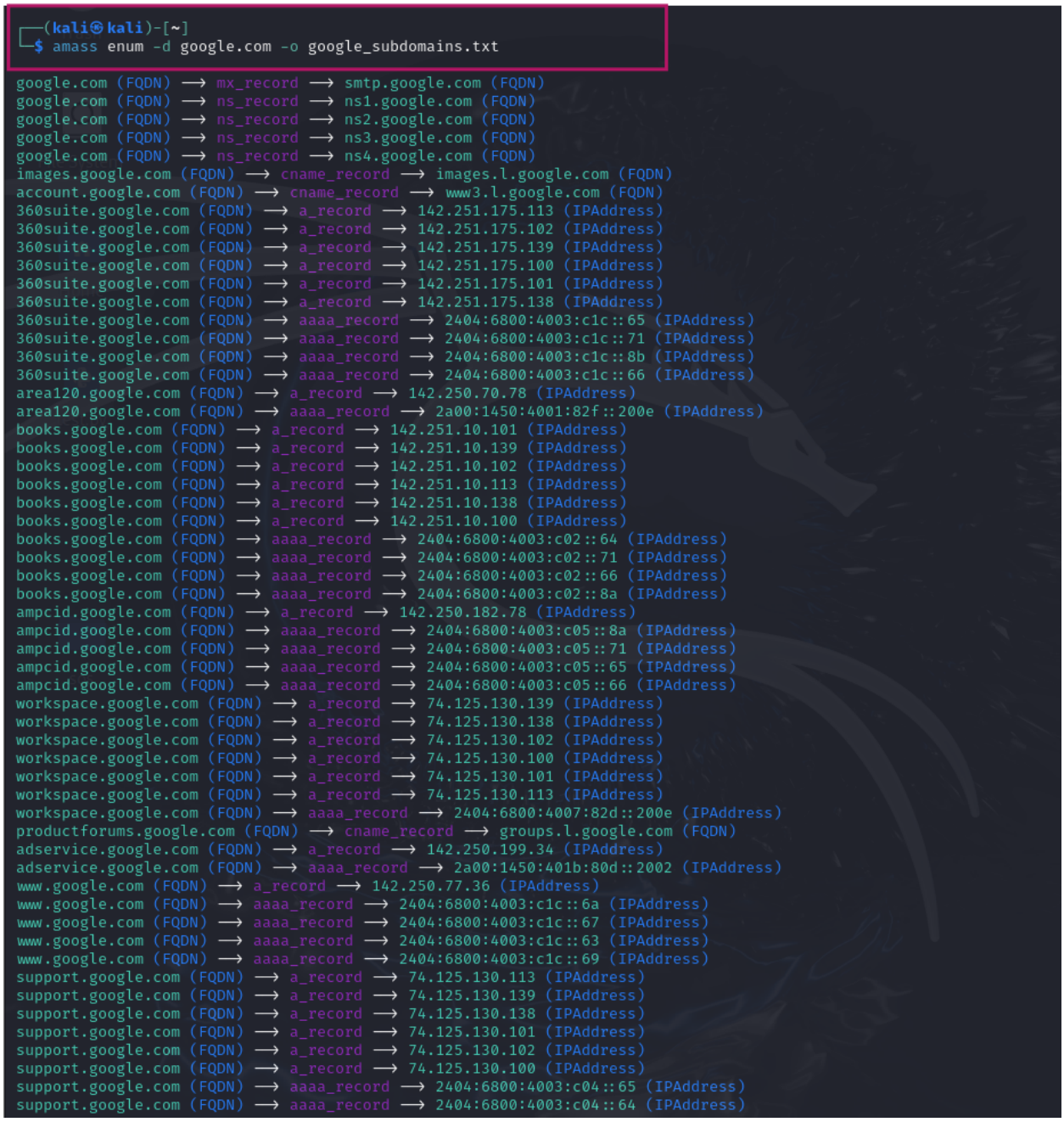
How to use Amass ?

amass enum -d example.com

example :

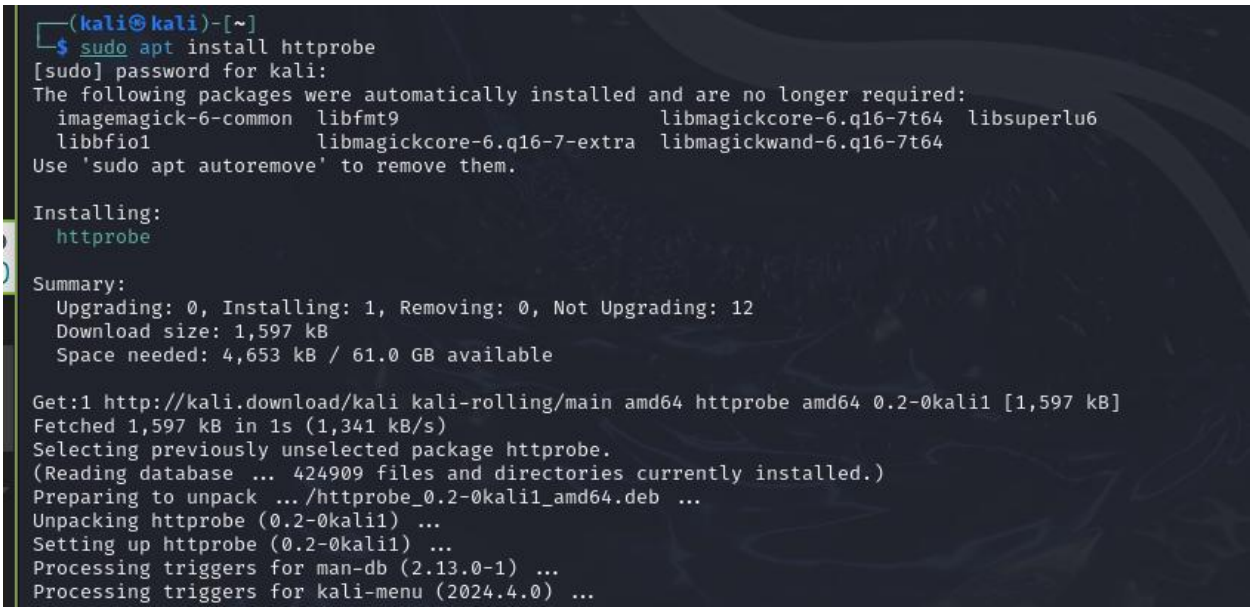
amass enum -d google.com -o google_subdomains.txt -src

- **amass**: The tool being used for reconnaissance and subdomain enumeration.
- **enum**: The enumeration mode, which is the default for Amass.
- **-d google.com**: Specifies the target domain for which subdomains will be enumerated.
- **-o output.txt :** to save the output to a file.


┌──(kali㉿kali)-[~]
└─$ amass enum -d google.com -o google_subdomains.txt
google.com (FQDN) --> mx_record --> smtp.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns1.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns2.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns3.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns4.google.com (FQDN)
images.google.com (FQDN) --> cname_record --> images.l.google.com (FQDN)
account.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
360suite.google.com (FQDN) --> a_record --> 142.251.175.113 (IPAddress)
360suite.google.com (FQDN) --> a_record --> 142.251.175.102 (IPAddress)
360suite.google.com (FQDN) --> a_record --> 142.251.175.139 (IPAddress)
360suite.google.com (FQDN) --> a_record --> 142.251.175.100 (IPAddress)
360suite.google.com (FQDN) --> a_record --> 142.251.175.101 (IPAddress)
360suite.google.com (FQDN) --> a_record --> 142.251.175.138 (IPAddress)
360suite.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c1c::65 (IPAddress)
360suite.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c1c::71 (IPAddress)
360suite.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c1c::8b (IPAddress)
360suite.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c1c::66 (IPAddress)
area120.google.com (FQDN) --> a_record --> 142.250.70.78 (IPAddress)
area120.google.com (FQDN) --> aaaa_record --> 2a00:1450:4001:82f::200e (IPAddress)
books.google.com (FQDN) --> a_record --> 142.251.10.101 (IPAddress)
books.google.com (FQDN) --> a_record --> 142.251.10.139 (IPAddress)
books.google.com (FQDN) --> a_record --> 142.251.10.102 (IPAddress)
books.google.com (FQDN) --> a_record --> 142.251.10.113 (IPAddress)
books.google.com (FQDN) --> a_record --> 142.251.10.138 (IPAddress)
books.google.com (FQDN) --> a_record --> 142.251.10.100 (IPAddress)
books.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c02::64 (IPAddress)
books.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c02::71 (IPAddress)
books.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c02::66 (IPAddress)
books.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c02::8a (IPAddress)
ampcid.google.com (FQDN) --> a_record --> 142.250.182.78 (IPAddress)
ampcid.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c05::8a (IPAddress)
ampcid.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c05::71 (IPAddress)
ampcid.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c05::65 (IPAddress)
ampcid.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c05::66 (IPAddress)
workspace.google.com (FQDN) --> a_record --> 74.125.130.139 (IPAddress)
workspace.google.com (FQDN) --> a_record --> 74.125.130.138 (IPAddress)
workspace.google.com (FQDN) --> a_record --> 74.125.130.102 (IPAddress)
workspace.google.com (FQDN) --> a_record --> 74.125.130.100 (IPAddress)
workspace.google.com (FQDN) --> a_record --> 74.125.130.101 (IPAddress)
workspace.google.com (FQDN) --> a_record --> 74.125.130.113 (IPAddress)
workspace.google.com (FQDN) --> aaaa_record --> 2404:6800:4007:82d::200e (IPAddress)
productforums.google.com (FQDN) --> cname_record --> groups.l.google.com (FQDN)
adservice.google.com (FQDN) --> a_record --> 142.250.199.34 (IPAddress)
adservice.google.com (FQDN) --> aaaa_record --> 2a00:1450:401b:80d::2002 (IPAddress)
www.google.com (FQDN) --> a_record --> 142.250.77.36 (IPAddress)
www.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c1c::6a (IPAddress)
www.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c1c::67 (IPAddress)
www.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c1c::63 (IPAddress)
www.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c1c::69 (IPAddress)
support.google.com (FQDN) --> a_record --> 74.125.130.113 (IPAddress)
support.google.com (FQDN) --> a_record --> 74.125.130.139 (IPAddress)
support.google.com (FQDN) --> a_record --> 74.125.130.138 (IPAddress)
support.google.com (FQDN) --> a_record --> 74.125.130.101 (IPAddress)
support.google.com (FQDN) --> a_record --> 74.125.130.102 (IPAddress)
support.google.com (FQDN) --> a_record --> 74.125.130.100 (IPAddress)
support.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c04::65 (IPAddress)
support.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c04::64 (IPAddress)

What is Httprobe ?

- Identify live web servers among a list of domains or IP addresses.
- by sending HTTP/HTTPS requests to each domain and checking if the server responds.


┌──(kali㉿kali)-[~]
└─$ sudo apt install httprobe
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
imagemagick-6-common libfmt9 libmagickcore-6.q16-7t64 libsuperlu6
libbfio1 libmagickcore-6.q16-7-extra libmagickwand-6.q16-7t64
Use 'sudo apt autoremove' to remove them.
Installing:
httprobe
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 12
Download size: 1,597 kB
Space needed: 4,653 kB / 61.0 GB available
Get:1 http://kali.download/kali kali-rolling/main amd64 httprobe amd64 0.2-0kali1 [1,597 kB]
Fetched 1,597 kB in 1s (1,341 kB/s)
Selecting previously unselected package httprobe.
(Reading database ... 424909 files and directories currently installed.)
Preparing to unpack .../httprobe_0.2-0kali1_amd64.deb ...
Unpacking httprobe (0.2-0kali1) ...
Setting up httprobe (0.2-0kali1) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...

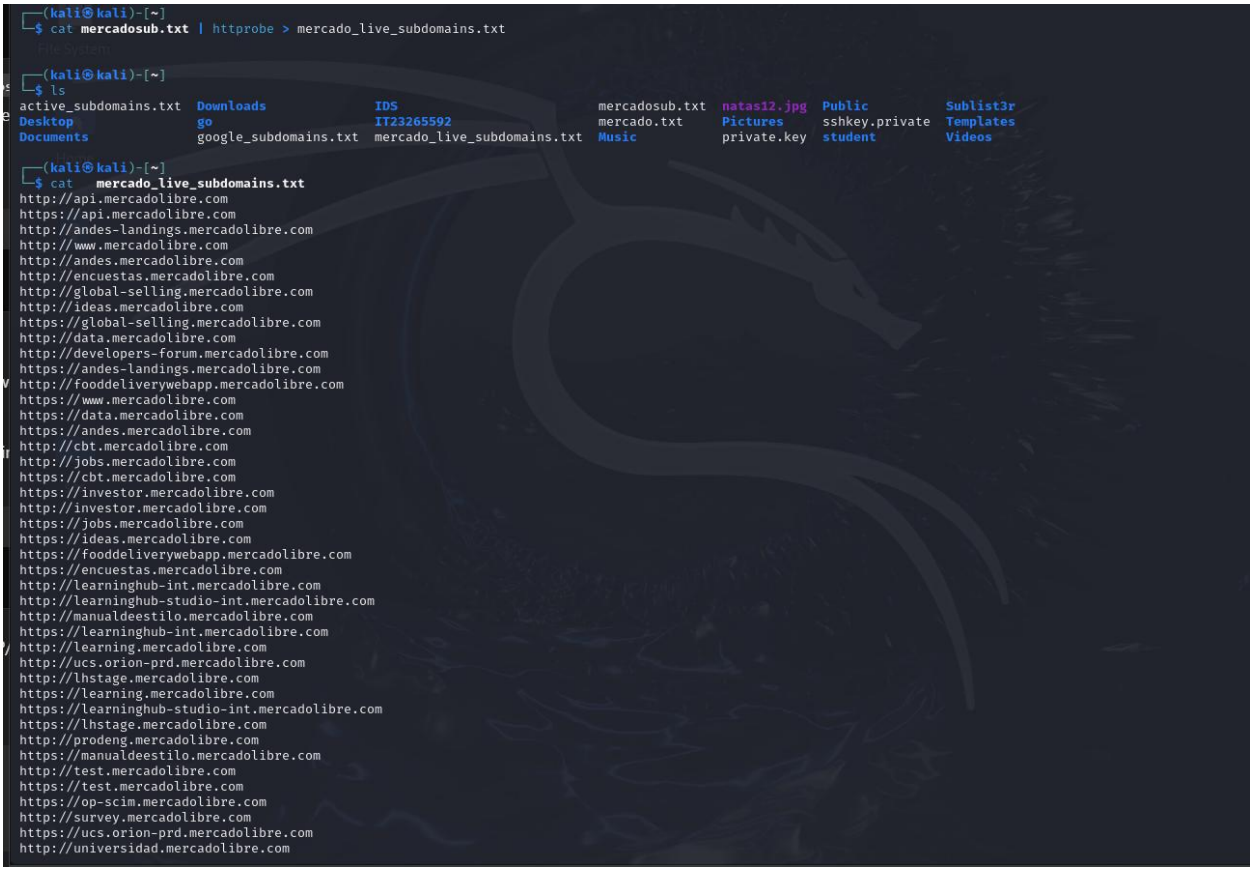
Command : **amass enum -d mercadolibre.com -o mercado.txt**

```
┌──(kali㉿kali)-[~]
└─$ amass enum -d mercadolibre.com -o mercado.txt

mercadolibre.com (FQDN) --> ns_record --> ns-1708.awsdns-21.co.uk (FQDN)
mercadolibre.com (FQDN) --> ns_record --> ns-984.awsdns-59.net (FQDN)
mercadolibre.com (FQDN) --> ns_record --> ns-1451.awsdns-53.org (FQDN)
mercadolibre.com (FQDN) --> ns_record --> ns-368.awsdns-46.com (FQDN)
content.mercadolibre.com (FQDN) --> cname_record --> h-mercadolibre.online-metrix.net (FQDN)
developers-forum.mercadolibre.com (FQDN) --> cname_record --> melidevelopers.invisionzone.com (FQDN)
apps.mercadolibre.com (FQDN) --> cname_record --> list.mercadolibre.com (FQDN)
test-vendedores.mercadolibre.com (FQDN) --> cname_record --> dbjfce6tekir0.cloudfront.net (FQDN)
chattest.mercadolibre.com (FQDN) --> cname_record --> d2g9ak52q0ogkf.cloudfront.net (FQDN)
mobile.mercadolibre.com (FQDN) --> cname_record --> d2g9ak52q0ogkf.cloudfront.net (FQDN)
prodeng.mercadolibre.com (FQDN) --> cname_record --> prodeng-prod-public-alb-tmp-1129379816.us-east-1.elb.ama
com (FQDN)
sellers.mercadolibre.com (FQDN) --> cname_record --> d2g9ak52q0ogkf.cloudfront.net (FQDN)
envios.mercadolibre.com (FQDN) --> a_record --> 143.204.98.4 (IPAddress)
ml-challenge.mercadolibre.com (FQDN) --> cname_record --> d2g9ak52q0ogkf.cloudfront.net (FQDN)
universidadvirtual.mercadolibre.com (FQDN) --> cname_record --> domssl.mercadolibre.com (FQDN)
webhooks.mercadolibre.com (FQDN) --> cname_record --> d2g9ak52q0ogkf.cloudfront.net (FQDN)
www.mercadolibre.com (FQDN) --> cname_record --> a35f64fceb718ad27.awsglobalaccelerator.com (FQDN)
ads-preview.mercadolibre.com (FQDN) --> cname_record --> d2g9ak52q0ogkf.cloudfront.net (FQDN)
facturacion.mercadolibre.com (FQDN) --> cname_record --> d2g9ak52q0ogkf.cloudfront.net (FQDN)
hydratest.mercadolibre.com (FQDN) --> cname_record --> d2g9ak52q0ogkf.cloudfront.net (FQDN)
fraud-monitor.mercadolibre.com (FQDN) --> cname_record --> domssl.mercadolibre.com.ar (FQDN)
career.mercadolibre.com (FQDN) --> cname_record --> dbjfce6tekir0.cloudfront.net (FQDN)
gaia.mercadolibre.com (FQDN) --> cname_record --> d2g9ak52q0ogkf.cloudfront.net (FQDN)
tienda.mercadolibre.com (FQDN) --> cname_record --> domssl.mercadolibre.com.ar (FQDN)
fraudinkiru.mercadolibre.com (FQDN) --> cname_record --> domssl.mercadolibre.com.ar (FQDN)
publicar-test.mercadolibre.com (FQDN) --> cname_record --> domssl.mercadolibre.com.ar (FQDN)
m.mercadolibre.com (FQDN) --> cname_record --> d2g9ak52q0ogkf.cloudfront.net (FQDN)
produsa-hap-webs-pub-pd-tf-e30a6a2d54a768bf.elb.us-east-1.amazonaws.com (FQDN) --> a_record --> 52.204.118.147 (IPAddress)
produsa-hap-webs-pub-pd-tf-e30a6a2d54a768bf.elb.us-east-1.amazonaws.com (FQDN) --> a_record --> 34.226.21.195 (IPAddress)
34.224.0.0/12 (Netblock) --> contains --> 34.226.21.195 (IPAddress)
52.192.0.0/12 (Netblock) --> contains --> 52.204.118.147 (IPAddress)
16509 (ASN) --> announces --> 52.192.0.0/12 (Netblock)
ns-775.awsdns-32.net (FQDN) --> a_record --> 205.251.195.7 (IPAddress)
ns-775.awsdns-32.net (FQDN) --> aaaa_record --> 2600:9000:5303:700::1 (IPAddress)
2600:9000:5300::/45 (Netblock) --> contains --> 2600:9000:5303:700::1 (IPAddress)
^C

The enumeration has finished
```

How it works

Get subdomain by using sublist3r

Use output of sublist3r as the input of httprobe



Wayback Machine

Link : https://web.archive.org/

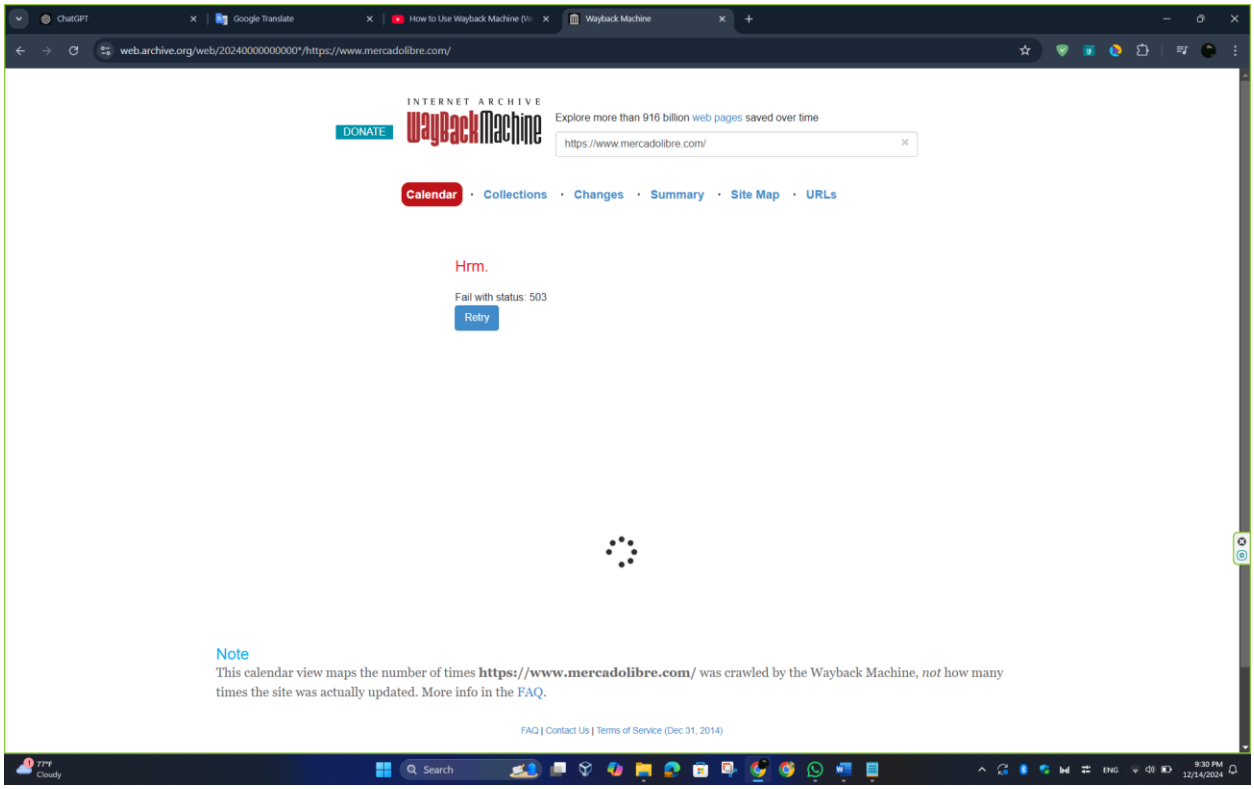
- archives websites by taking snapshots (HTML, text, media).
- Stores snapshots for public access to view historical versions of web pages.
- **Digital Forensics**
    - Investigate website changes or defacements over time
    - Recover deleted content
- Analyze past phishing websites and attacker tactics.
- Track malicious domains' historical infrastructure
- Compare historical configurations to detect overlooked vulnerabilities.
- Rebuild lost content using archived versions.
- Detect fake or impersonating websites and analyze their activity.

Limitation

- all sites or dates archived
- Delayed updates (no real-time snapshots).
- Limited depth (dynamic or protected content not archived).

Common Use Cases:

- **Check Deleted Content**: Find pages or content that have been removed.
- **Analyze Changes**: Compare website updates or changes over time.
- **Gather Evidence**: Capture archived content for legal or security investigations.
- **Research Historical Data**: Understand how websites or online campaigns looked in the past.


ChatGPT
Google Translate
How to Use Wayback Machine (W
Wayback Machine
web.archive.org/web/20240000000000*/https://www.mercadolibre.com/
INTERNET ARCHIVE
DONATE
WaybackMachine
Explore more than 916 billion web pages saved over time
https://www.mercadolibre.com/
Calendar · Collections · Changes · Summary · Site Map · URLs
Hrm.
Fail with status: 503
Retry
Note
This calendar view maps the number of times https://www.mercadolibre.com/ was crawled by the Wayback Machine, not how many times the site was actually updated. More info in the FAQ.
FAQ | Contact Us | Terms of Service (Dec 31, 2014)
77°F
Cloudy
Search
ENG
9:30 PM
12/14/2024

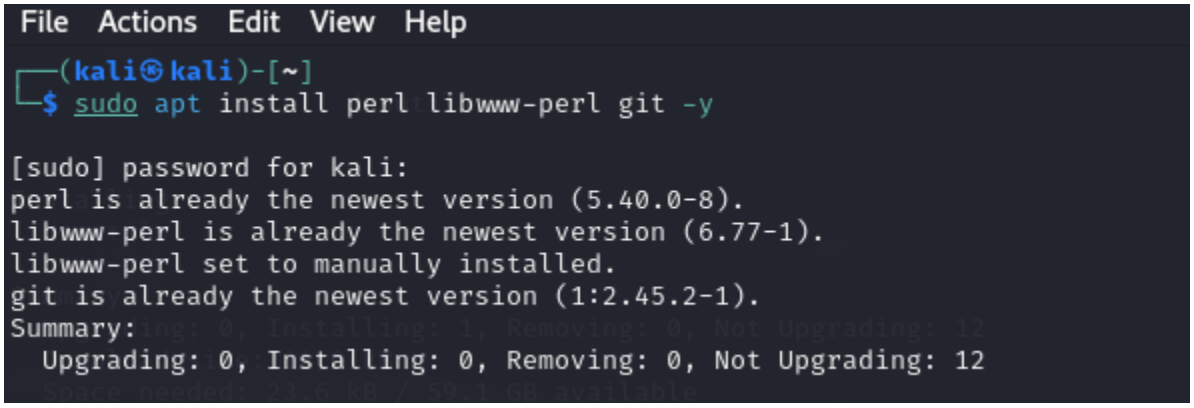
What is Nikto ?

- web server scanner
- identify vulnerabilities and misconfigurations in web servers.
- Detects outdated software versions, insecure headers, or improperly configured SSL/TLS
- Enumeration of Server Information: (server types, installed modules, about directories, files, or potential entry points)
- Identifies insecure default configurations
- Scans for common issues (XSS, SQL injection, and potential authentication bypasses.)
- Conducts quick, automated scans of targets, saving time during reconnaissance.

1. Installing Nikto

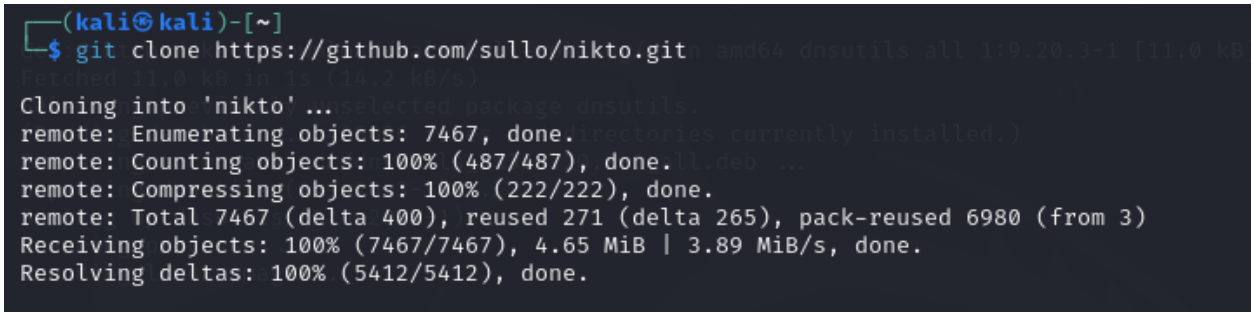
Nikto is a Perl-based tool, so you need to have Perl installed first.

Command : **sudo apt install perl libwww-perl git -y**



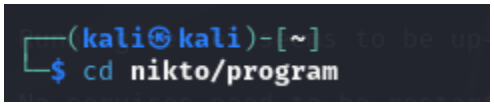
2. Clone the Nikto repository:

Command : **git clone** https://github.com/sullo/nikto.git



3. Navigate to the Nikto directory:

Command : **cd nikto/program**



4. Run Nikto:

Command : **perl nikto.pl**

Scan Using HTTPS:

Command : **perl nikto.pl -h https://example.com**

Specify a Port:

Command : **perl nikto.pl -h http://example.com -p 8080**

Verbose Mode: (Runs the scan with detailed output.)

Command : **perl nikto.pl -h http://example.com -v**

Output Results to a File:

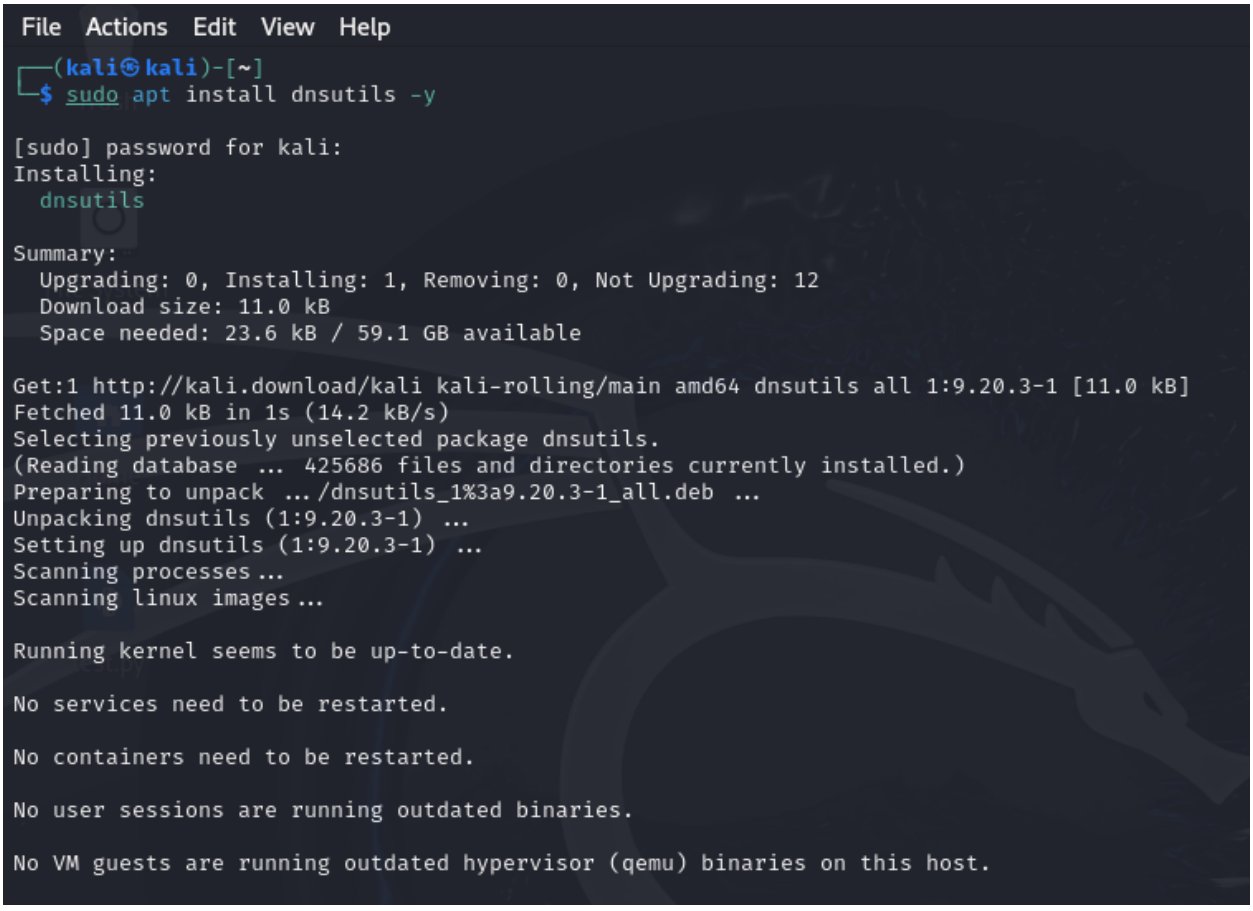
Command : **perl nikto.pl -h http://example.com -o results.txt**

What is nslookup ?

- Use **nslookup** to map the target's DNS infrastructure, find subdomains, and locate potential targets
- command-line tool for querying Domain Name System (DNS) records
- Identifies IP addresses associated with a domain.
- Reveals subdomains, often overlooked but might contain vulnerable applications.
- Information Gathering (identify third-party services used by the target, which could be potential points of attack.)
- Discover Misconfigurations (Identifies outdated DNS records or unused subdomains)
- Finds open DNS resolvers that can be exploited in DNS amplification attacks.
- Confirms DNS changes after exploitation, like DNS poisoning or cache manipulation.
- Displays the configured default DNS server

How to install

Command : **sudo apt install dnsutils -y**



Run nslookup
Command : **nslookup**

Check whether is it running ?
Command : **nslookup** example.com

Explanation of Output

1. **Server: 192.168.1.1**
   - This is the DNS server your system is using for queries (likely your router or a local DNS resolver).
2. **Address: 192.168.1.1#53**
   - The #53 indicates the port number being used for DNS (port 53 is standard for DNS traffic).
3. **Non-authoritative answer:**
   - This means the DNS server used is not the authoritative server for facebook.com. It provided the information from its cache or queried an authoritative server on your behalf.
4. **Name: facebook.com**
   - The domain name you queried.
5. **Address: 57.144.144.1**
   - One of the IPv4 addresses for facebook.com.
6. **Address: 2a03:2880:f10c:381:face:b00c:0:25de**
   - The IPv6 address for facebook.com.

- Use **nslookup** to map the target's DNS infrastructure, find subdomains, and locate potential targets (e.g., staging environments).
- Use **Nikto** to scan those targets for vulnerabilities or misconfigurations to identify exploitable vectors.

What is WhatWeb

- Identifies technologies used by a website (e.g., web servers, content management systems, analytics tools, and more).
- Used for CMS detection

- The output might include information such as:
  - Web server software (e.g., Apache, Nginx)
  - Content Management System (CMS) (e.g., WordPress, Magento)
  - JavaScript frameworks (e.g., React, Angular)
  - Analytics tools (e.g., Google Analytics)
  - SSL/TLS certificate information

Install WhatWeb:

Command : **sudo apt install whatweb**

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install whatweb
[sudo] password for kali:
whatweb is already the newest version (0.5.5-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 12
```

Run WhatWeb:

Command : whatweb example.com

```
whatweb -v www.mercadolibre.com    # For verbose output
whatweb -a 3 www.mercadolibre.com  # For aggressive scanning
```

- Command : Command : whatweb mercadolibre.com

1. Redirect Information:

- **URL**: http://www.mercadolibre.com
- **Status Code**: 301 Moved Permanently — The website is redirecting to a secure version (HTTPS).
- **Country**: United States (US)
- **HTTP Server**: awselb/2.0 — Indicates the use of an AWS Elastic Load Balancer.
- **IP Address**: 3.33.182.45
- **Redirect Location**: https://www.mercadolibre.com:443/ — The website is being redirected to the HTTPS version.
- **Title**: 301 Moved Permanently

2. Secure Connection Information:

- **URL**: https://www.mercadolibre.com/
- **Status Code**: 200 OK — The secure HTTPS connection is active and working.
- **Cookies**: _d2id
- **Country**: United States (US)
- **HTML5**: The page uses HTML5.
- **HTTP Server**: Tengine — A web server that is commonly associated with websites hosted on Alibaba Cloud.
- **IP Address**: 3.33.182.45
- **Strict-Transport-Security**: max-age=604800; includeSubDomains; — The website is enforcing HTTPS for the next 7 days, including its subdomains.
- **Title**: Mercado Libre - Envíos Gratis en el día
- **Uncommon Headers**: These are additional headers indicating AWS and security-related information:
    - x-amz-id-2, x-amz-request-id, x-amz-replication-status, x-amz-server-side-encryption
    - x-request-id, x-request-device-id, x-d2id, x-content-type-options, referrer-policy
- **X-XSS-Protection**: 1; mode=block — Cross-site scripting protection is enabled.

Key Takeaways:

- The website is using **AWS Elastic Load Balancer** and **Tengine** server.
- **Strict-Transport-Security (HSTS)** is enabled, ensuring the site only connects over HTTPS.

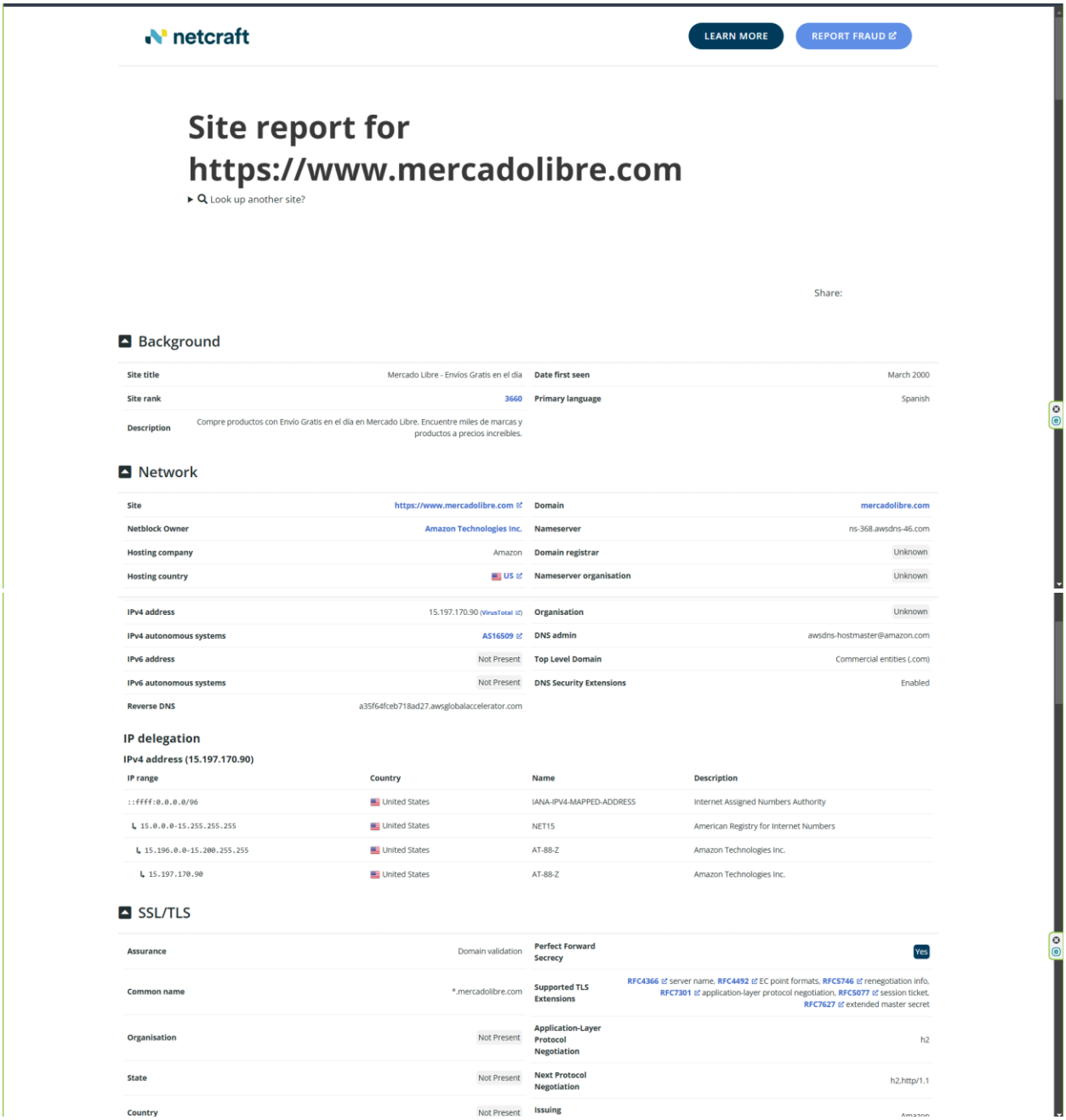
- Security headers like X-XSS-Protection and x-content-type-options are in place, enhancing security against cross-site scripting (XSS) and content type sniffing.

What is Netcraft ?

- Provides web server and website information, such as hosting details, SSL certificates, and historical data about a website.

  Website : https://www.netcraft.com/

- Do information gathering
- Can identify outdated technologies or poorly configured servers



netcraft

LEARN MORE REPORT FRAUD

Site report for https://www.mercadolibre.com

▸ Look up another site?

Share:

Background

Site title	Mercado Libre - Envíos Gratis en el día	**Date first seen**	March 2000
Site rank	3660	**Primary language**	Spanish
Description	Compre productos con Envío Gratis en el día en Mercado Libre. Encuentre miles de marcas y productos a precios increíbles.		

Network

Site	https://www.mercadolibre.com	**Domain**	mercadolibre.com
Netblock Owner	Amazon Technologies Inc.	**Nameserver**	ns-368.awsdns-46.com
Hosting company	Amazon	**Domain registrar**	Unknown
Hosting country	US	**Nameserver organisation**	Unknown
IPv4 address	15.197.170.90 (VirusTotal)	**Organisation**	Unknown
IPv4 autonomous systems	AS16509	**DNS admin**	awsdns-hostmaster@amazon.com
IPv6 address	Not Present	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	Not Present	**DNS Security Extensions**	Enabled
Reverse DNS	a35f64fceb718ad27.awsglobalaccelerator.com		

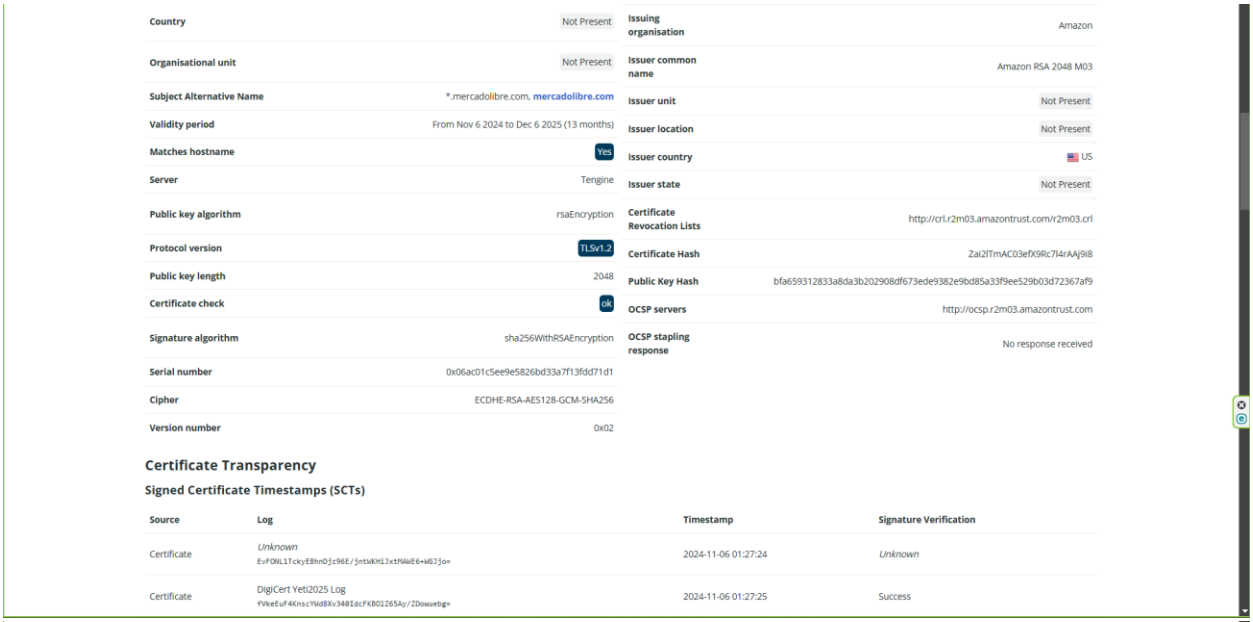
IP delegation

IPv4 address (15.197.170.90)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 15.0.0.0-15.255.255.255	United States	NET15	American Registry for Internet Numbers
↳ 15.196.0.0-15.200.255.255	United States	AT-88-Z	Amazon Technologies Inc.
↳ 15.197.170.90	United States	AT-88-Z	Amazon Technologies Inc.

SSL/TLS

Assurance	Domain validation	**Perfect Forward Secrecy**	Yes
Common name	*.mercadolibre.com	**Supported TLS Extensions**	RFC4366 server name, RFC4492 EC point formats, RFC5746 renegotiation info, RFC7301 application-layer protocol negotiation, RFC5077 session ticket, RFC7627 extended master secret
Organisation	Not Present	**Application-Layer Protocol Negotiation**	h2
State	Not Present	**Next Protocol Negotiation**	h2,http/1.1
Country	Not Present	**Issuing**	



Country	Not Present	**Issuing organisation**	Amazon
Organisational unit	Not Present	**Issuer common name**	Amazon RSA 2048 M03
Subject Alternative Name	*.mercadolibre.com, **mercadolibre.com**	**Issuer unit**	Not Present
Validity period	From Nov 6 2024 to Dec 6 2025 (13 months)	**Issuer location**	Not Present
Matches hostname	Yes	**Issuer country**	US
Server	Tengine	**Issuer state**	Not Present
Public key algorithm	rsaEncryption	**Certificate Revocation Lists**	http://crl.r2m03.amazontrust.com/r2m03.crl
Protocol version	TLSv1.2	**Certificate Hash**	Zai2ITmAC03efX9Rc7l4rAAj9I8
Public key length	2048	**Public Key Hash**	bfa659312833a8da3b202908df673ede9382e9bd85a33f9ee529b03d72367af9
Certificate check	ok	**OCSP servers**	http://ocsp.r2m03.amazontrust.com
Signature algorithm	sha256WithRSAEncryption	**OCSP stapling response**	No response received
Serial number	0x06ac01c5ee9e5826bd33a7f13fdd71d1		
Cipher	ECDHE-RSA-AES128-GCM-SHA256		
Version number	0x02		

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	*Unknown* EvFONL1TckyEBhnDjz96E/jntWKHiJxtHAWE6+WGJjo=	2024-11-06 01:27:24	*Unknown*
Certificate	DigiCert Yeti2025 Log fVkeEuF4KnscYWd8Xv340IdcFKBOlZ65Ay/ZDowuebg=	2024-11-06 01:27:25	Success
Certificate	DigiCert Nessie2025 Log 5tIxY0B3jMEQQQbXcbnOwdJA9paEhvu6hzId/R43jlA=	2024-11-06 01:27:25	Success

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. More information about Heartbleed detection.

SSL Certificate Chain

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of **rules**. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see **open-spf.org**.

Warning: It appears that this host does not have an SPF record. There may be an SPF record on mercadolibre.com: Check the **site report**.

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any **mail-enabled subdomains**. It is recommended to add an SPF record to any subdomain with an MX record.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see **dmarc.org**.

This host does not have a DMARC record. There may be a DMARC record on the site report for mercadolibre.com: Check the **site report**.

What the Whois Lookup Tool Does ?

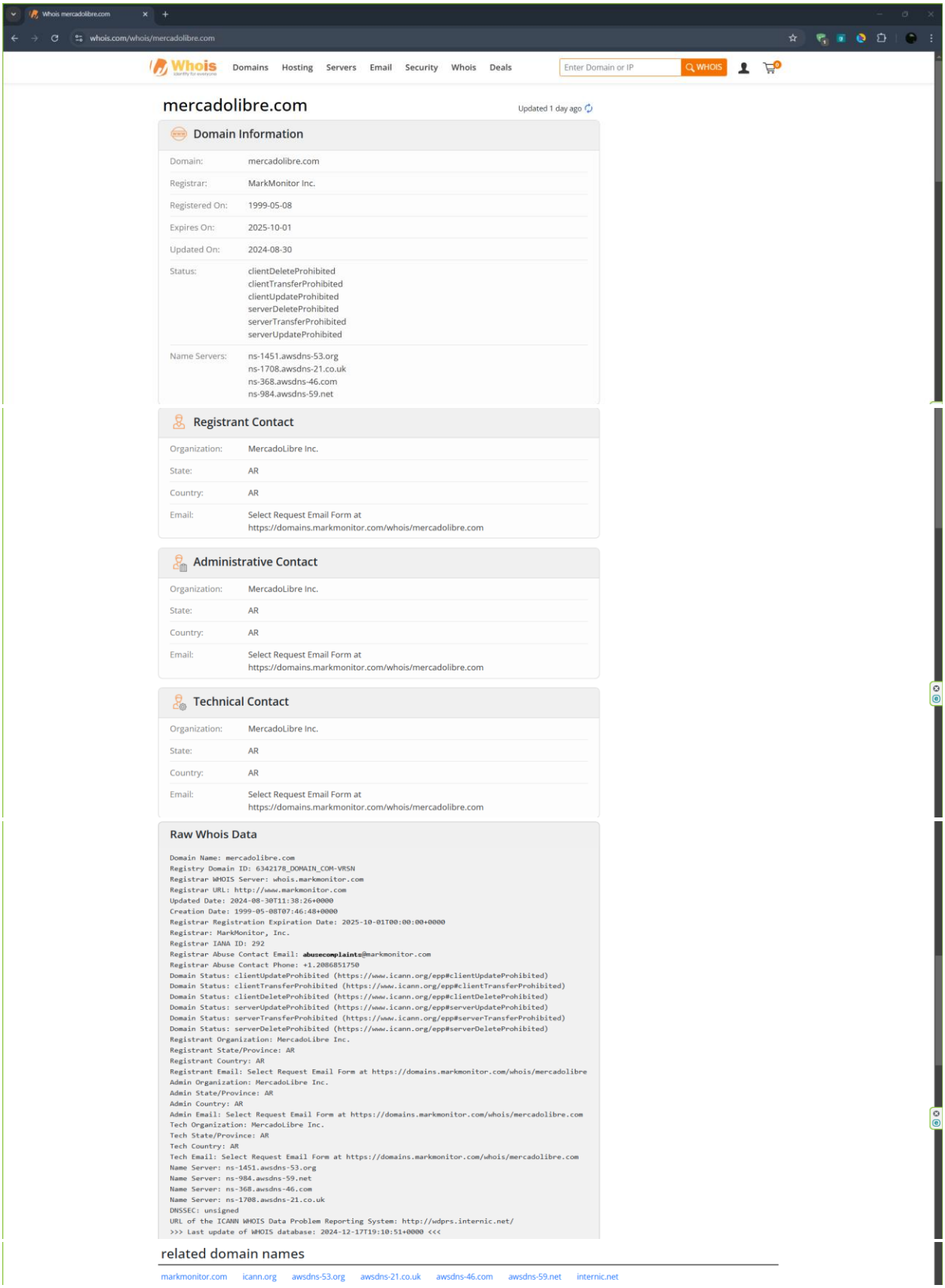
Link : https://www.whois.com/whois/

- Can get information such as
    - Registration details (name , date)
    - Administrative contacts (name , emails, managing domains)
    - Nameservers (DNS records)
    - Domain status (active , locked)

- Determine whether a specific domain is part of the target's owned infrastructure. This is important to avoid testing unauthorized systems.
- Monitor Expired domains from the same organization may be vulnerable.

By using this metadata like domain ownership or DNS records , we can identify

- Discover misconfigured servers and subdomains
- Identify test environments
- Can get more chance to uncover vulnerabilities by gaining context about an organization’s infrastructure.


Whois mercadolibre.com
whois.com/whois/mercadolibre.com
Whois
Domains
Hosting
Servers
Email
Security
Whois
Deals
Enter Domain or IP
WHOIS
mercadolibre.com
Updated 1 day ago
Domain Information
Domain: mercadolibre.com
Registrar: MarkMonitor Inc.
Registered On: 1999-05-08
Expires On: 2025-10-01
Updated On: 2024-08-30
Status: clientDeleteProhibited
clientTransferProhibited
clientUpdateProhibited
serverDeleteProhibited
serverTransferProhibited
serverUpdateProhibited
Name Servers: ns-1451.awsdns-53.org
ns-1708.awsdns-21.co.uk
ns-368.awsdns-46.com
ns-984.awsdns-59.net
Registrant Contact
Organization: MercadoLibre Inc.
State: AR
Country: AR
Email: Select Request Email Form at
https://domains.markmonitor.com/whois/mercadolibre.com
Administrative Contact
Organization: MercadoLibre Inc.
State: AR
Country: AR
Email: Select Request Email Form at
https://domains.markmonitor.com/whois/mercadolibre.com
Technical Contact
Organization: MercadoLibre Inc.
State: AR
Country: AR
Email: Select Request Email Form at
https://domains.markmonitor.com/whois/mercadolibre.com
Raw Whois Data
Domain Name: mercadolibre.com
Registry Domain ID: 6342178_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-08-30T11:38:26+0000
Creation Date: 1999-05-08T07:46:48+0000
Registrar Registration Expiration Date: 2025-10-01T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: MercadoLibre Inc.
Registrant State/Province: AR
Registrant Country: AR
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/mercadolibre
Admin Organization: MercadoLibre Inc.
Admin State/Province: AR
Admin Country: AR
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/mercadolibre.com
Tech Organization: MercadoLibre Inc.
Tech State/Province: AR
Tech Country: AR
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/mercadolibre.com
Name Server: ns-1451.awsdns-53.org
Name Server: ns-984.awsdns-59.net
Name Server: ns-368.awsdns-46.com
Name Server: ns-1708.awsdns-21.co.uk
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-12-17T19:10:51+0000 <<<
related domain names
markmonitor.com
icann.org
awsdns-53.org
awsdns-21.co.uk
awsdns-46.com
awsdns-59.net
internic.net

What is Domain Information Groper (DIG) Tool ?

- A network administration command-line tool
- Querying DNS (Domain Name System) records
- Gathering detailed information about domains and IP addresses
- Identify subdomains
- Identify mail servers
- Performs reverse DNS lookups
- identify services that are running on the domain,(VoIp, chat servers which could be vulnerable)
- evaluates whether an organisation's email infrastructure is properly configured to prevent spoofing or phishing attack by checking TXT records
- exploiting misconfigurations

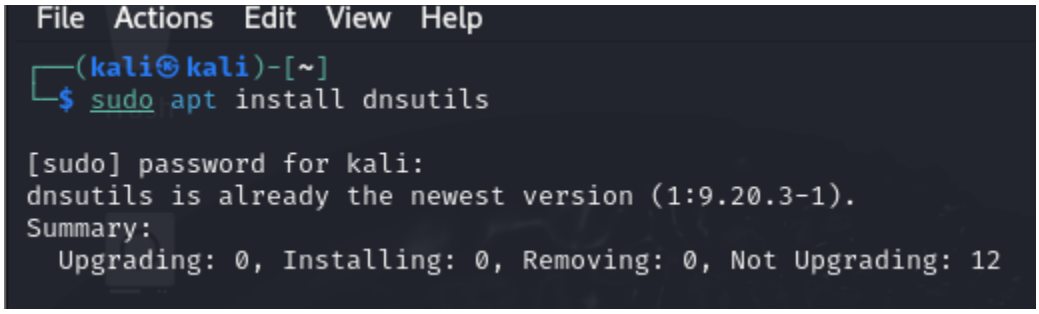
Main types of DNS records that can be retrieved using DIG:

Summary of Common DNS Record Types:

Record Type	Purpose	Example Query
A	IPv4 Address	dig example.com A
AAAA	IPv6 Address	dig example.com AAAA
MX	Mail Servers	dig example.com MX
NS	Name Servers	dig example.com NS
CNAME	Canonical Name (alias)	dig example.com CNAME
TXT	Text Records (SPF, DKIM, etc.)	dig example.com TXT
SOA	Start of Authority (DNS info)	dig example.com SOA
PTR	Reverse DNS (IP to domain)	dig -x 192.168.1.1
SRV	Service Records (e.g., SIP, XMPP)	dig _sip._tcp.example.com SRV

How to install

Command : **sudo apt install dnsutils**



Run dig

Command : **dig example.com**

```
┌──(kali㉿kali)-[~]
└─$ dig www.mercadolibre.com

; <<>> DiG 9.20.3-1-Debian <<>> www.mercadolibre.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57158
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1ac9288983d8b1520100000067643bbac0830250032fad71 (good)
;; QUESTION SECTION:
;www.mercadolibre.com.          IN      A

;; ANSWER SECTION:
www.mercadolibre.com.   300     IN      CNAME   a35f64fceb718ad27.awsglobalaccelerator.com.
a35f64fceb718ad27.awsglobalaccelerator.com. 300 IN A 15.197.170.90
a35f64fceb718ad27.awsglobalaccelerator.com. 300 IN A 3.33.182.45

;; Query time: 388 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Thu Dec 19 10:28:58 EST 2024
;; MSG SIZE  rcvd: 165
```

- **CNAME Records**
  - Pointing to a35f64fceb718ad27.awsglobalaccelerator.com
  - It means website is using **AWS Global Accelerator**

- **A Records**:
  - **15.197.170.90 , 3.33.182.45**
  - These are the actual IP addresses that clients will use to connect to www.mercadolibre.com

- Query took **388 milliseconds** to complete.
- Query was resolved using the DNS server at **192.168.1.1**.

What is Nmap (Network Mapper) ?

- For reconnaissance and scanning
- Nmap is used to discover hosts, services, and potential vulnerabilities on a target network.
- Use targeted scans to avoid being noisy (e.g., focus on specific IPs or ranges).
- Combine Nmap with other tools like Burp Suite or Nikto for deeper analysis.

To install nmap

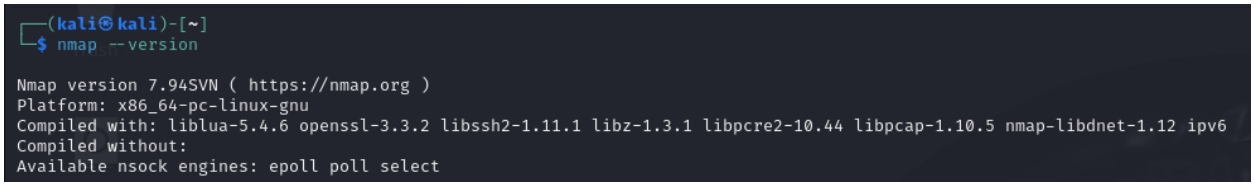
Command :

sudo apt install nmap -y

Nmap version :

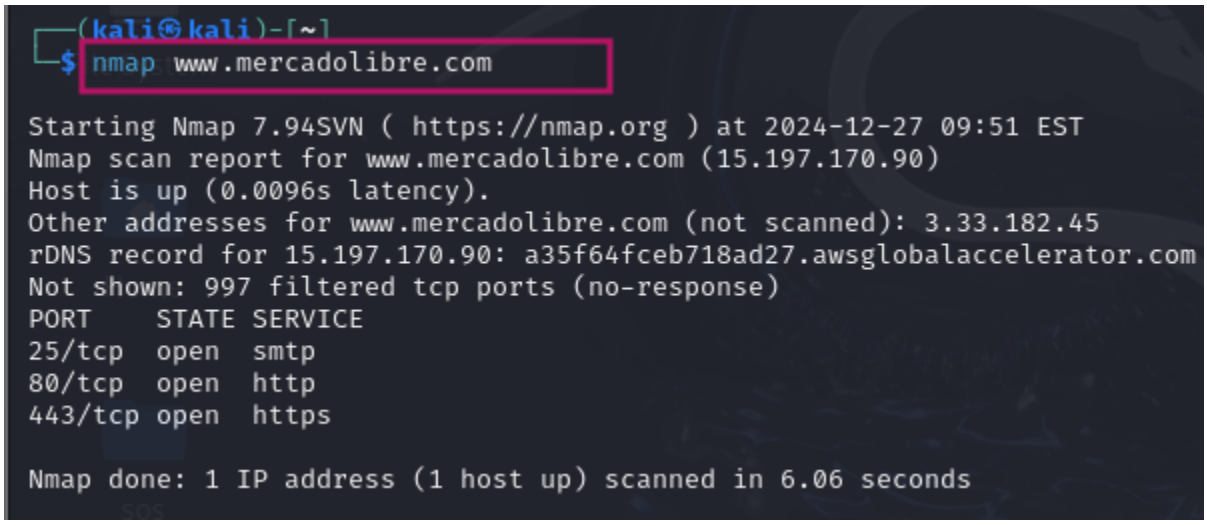
Command :

nmap --version



Basic command :

nmap <target>

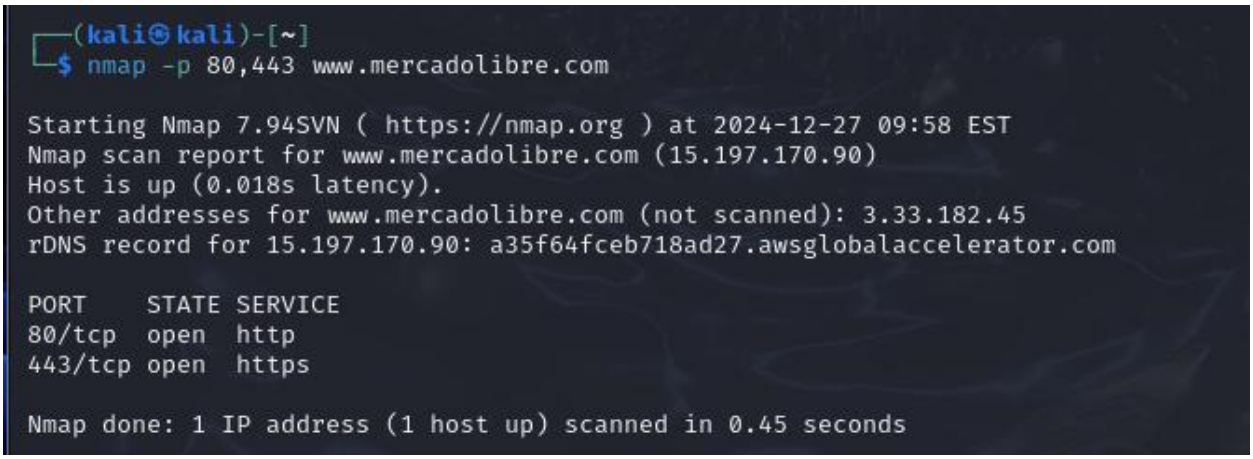


- Port Scanning

  Identify open ports on the target:

Command :

nmap -p- <target> # Scans all 65535 ports



- Service and Version Detection

  Detect services running on open ports and their versions:

Command :

nmap -sV <target>

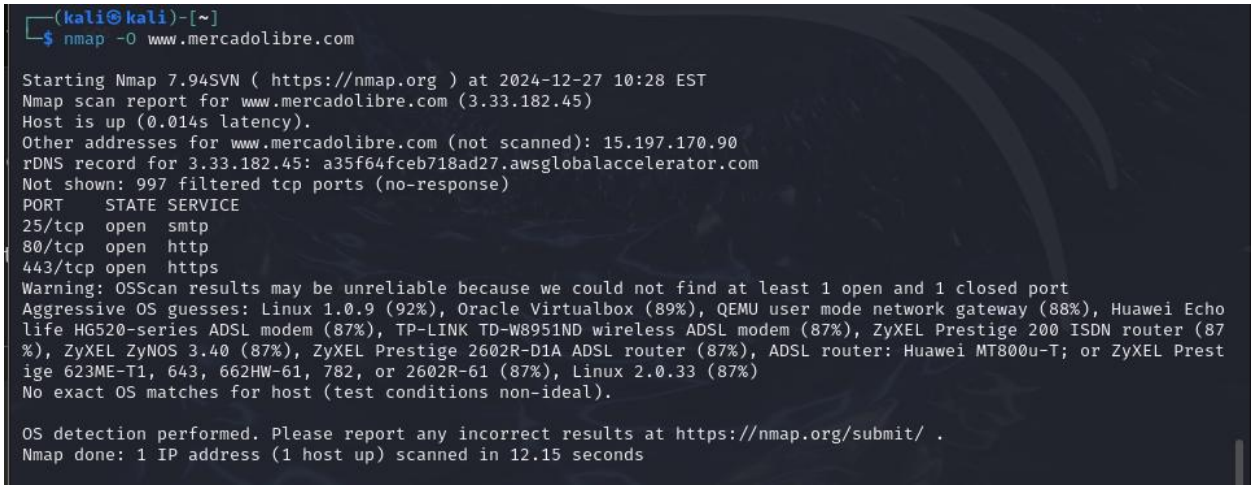
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV www.mercadolibre.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-27 09:53 EST
Nmap scan report for www.mercadolibre.com (15.197.170.90)
Host is up (0.0097s latency).
Other addresses for www.mercadolibre.com (not scanned): 3.33.182.45
rDNS record for 15.197.170.90: a35f64fceb718ad27.awsglobalaccelerator.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
25/tcp  open  smtp?
80/tcp  open  http     awselb/2.0
443/tcp open  ssl/http Tengine httpd
2 services unrecognized despite returning data. If you know the service/vers
rints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port25-TCP:V=7.94SVN%I=7%D=12/27%Time=676EBF7A%P=x86_64-pc-linux-gnu%r(
SF:Hello,2A,"552\x20Invalid\x20domain\x20name\x20in\x20EHLO\x20command\.\r
SF:\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94SVN%I=7%D=12/27%Time=676EBF7C%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,182,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nServer:\x20
SF:awselb/2\.0\r\nDate:\x20Fri,\x2027\x20Dec\x202024\x2014:53:31\x20GMT\r\
SF:nContent-Type:\x20text/html\r\nContent-Length:\x20134\r\nConnection:\x2
SF:0close\r\nLocation:\x20https://frontend-row-traffic-laye-80c90e-1347733
SF:461\.us-east-1\.elb\.amazonaws\.com:443/\r\n\r\n<html>\r\n<head><title>
SF:301\x20Moved\x20Permanently</title></head>\r\n<body>\r\n<center><h1>301
SF:\x20Moved\x20Permanently</h1></center>\r\n</body>\r\n</html>\r\n")%r(HT
SF:TPOptions,182,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nServer:\x20a
SF:wselb/2\.0\r\nDate:\x20Fri,\x2027\x20Dec\x202024\x2014:53:33\x20GMT\r\n
SF:Content-Type:\x20text/html\r\nContent-Length:\x20134\r\nConnection:\x20
SF:close\r\nLocation:\x20https://frontend-row-traffic-laye-80c90e-13477334
SF:61\.us-east-1\.elb\.amazonaws\.com:443/\r\n\r\n<html>\r\n<head><title>3
SF:01\x20Moved\x20Permanently</title></head>\r\n<body>\r\n<center><h1>301\
SF:x20Moved\x20Permanently</h1></center>\r\n</body>\r\n</html>\r\n")%r(RTS
SF:PRequest,7A,"<html>\r\n<head><title>400\x20Bad\x20Request</title></head
SF:>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n</bod
SF:y>\r\n</html>\r\n")%r(X11Probe,110,"HTTP/1\.1\x20400\x20Bad\x20Request\
SF:r\nServer:\x20awselb/2\.0\r\nDate:\x20Fri,\x2027\x20Dec\x202024\x2014:5
SF:3:34\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20122\r\n
SF:Connection:\x20close\r\n\r\n<html>\r\n<head><title>400\x20Bad\x20Reques
SF:t</title></head>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></c
SF:enter>\r\n</body>\r\n</html>\r\n")%r(FourOhFourRequest,10A,"HTTP/1\.1\x
SF:20403\x20Forbidden\r\nServer:\x20awselb/2\.0\r\nDate:\x20Fri,\x2027\x20
SF:Dec\x202024\x2014:53:35\x20GMT\r\nContent-Type:\x20text/html\r\nContent
SF:-Length:\x20118\r\nConnection:\x20close\r\n\r\n<html>\r\n<head><title>4
SF:03\x20Forbidden</title></head>\r\n<body>\r\n<center><h1>403\x20Forbidde
SF:n</h1></center>\r\n</body>\r\n</html>\r\n")%r(RPCCheck,110,"HTTP/1\.1\x
SF:20400\x20Bad\x20Request\r\nServer:\x20awselb/2\.0\r\nDate:\x20Fri,\x202
SF:7\x20Dec\x202024\x2014:53:42\x20GMT\r\nContent-Type:\x20text/html\r\nCo
SF:ntent-Length:\x20122\r\nConnection:\x20close\r\n\r\n<html>\r\n<head><ti
SF:tle>400\x20Bad\x20Request</title></head>\r\n<body>\r\n<center><h1>400\x
SF:20Bad\x20Request</h1></center>\r\n</body>\r\n</html>\r\n");

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 48.87 seconds
```

- Operating System Detection

  Guess the operating system of the target:

Command

nmap -O <target>

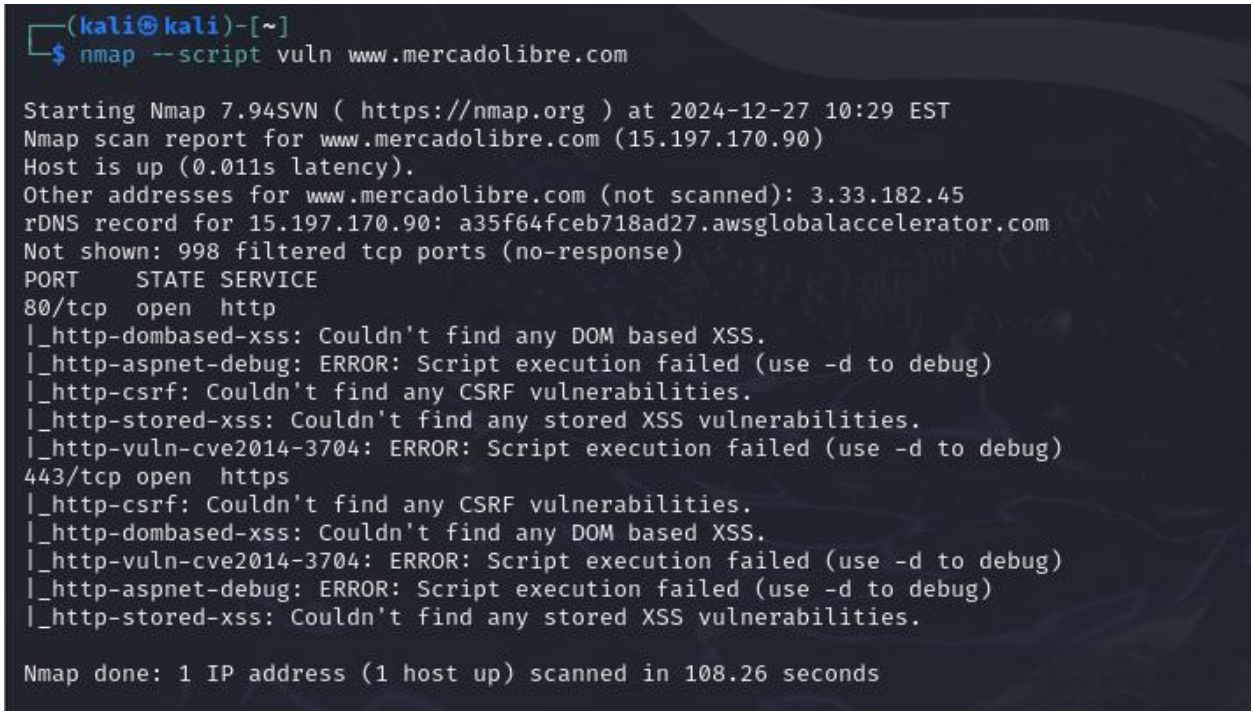


- Script Scanning

  Use NSE (Nmap Scripting Engine) for vulnerability detection:

Command

nmap --script vuln <target>



- Aggressive Scan

  Combines multiple scans (OS, version, and script scans):

Command :

nmap -A <target>

```
|_  http/1.1
| ssl-cert: Subject: commonName=*.mercadolibre.com
| Subject Alternative Name: DNS:*.mercadolibre.com, DNS:mercadolibre.com
| Not valid before: 2024-11-06T00:00:00
|_Not valid after:  2025-12-06T23:59:59
|_http-title: Site doesn't have a title (text/html).
1 service unrecognized despite returning data. If you know the service/version, please submit the followi
ng fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.94SVN%I=7%D=12/27%Time=676EBFED%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,182,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nServer:\x20
SF:awselb/2\.0\r\nDate:\x20Fri,\x2027\x20Dec\x202024\x2014:55:25\x20GMT\r\
SF:nContent-Type:\x20text/html\r\nContent-Length:\x20134\r\nConnection:\x2
SF:0close\r\nLocation:\x20https://frontend-row-traffic-laye-80c90e-1347733
SF:461\.us-east-1\.elb\.amazonaws\.com:443/\r\n\r\n<html>\r\n<head><title>
SF:301\x20Moved\x20Permanently</title></head>\r\n<body>\r\n<center><h1>301
SF:\x20Moved\x20Permanently</h1></center>\r\n</body>\r\n</html>\r\n")%r(HT
SF:TPOptions,182,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nServer:\x20a
SF:wselb/2\.0\r\nDate:\x20Fri,\x2027\x20Dec\x202024\x2014:55:27\x20GMT\r\n
SF:Content-Type:\x20text/html\r\nContent-Length:\x20134\r\nConnection:\x20
SF:close\r\nLocation:\x20https://frontend-row-traffic-laye-80c90e-13477334
SF:61\.us-east-1\.elb\.amazonaws\.com:443/\r\n\r\n<html>\r\n<head><title>3
SF:01\x20Moved\x20Permanently</title></head>\r\n<body>\r\n<center><h1>301\
SF:x20Moved\x20Permanently</h1></center>\r\n</body>\r\n</html>\r\n")%r(RTS
SF:PRequest,7A,"<html>\r\n<head><title>400\x20Bad\x20Request</title></head
SF:>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n</bod
SF:y>\r\n</html>\r\n")%r(X11Probe,110,"HTTP/1\.1\x20400\x20Bad\x20Request\
SF:r\nServer:\x20awselb/2\.0\r\nDate:\x20Fri,\x2027\x20Dec\x202024\x2014:5
SF:5:28\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20122\r\n
SF:Connection:\x20close\r\n\r\n<html>\r\n<head><title>400\x20Bad\x20Reques
SF:t</title></head>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></c
SF:enter>\r\n</body>\r\n</html>\r\n")%r(FourOhFourRequest,10A,"HTTP/1\.1\x
SF:20403\x20Forbidden\r\nServer:\x20awselb/2\.0\r\nDate:\x20Fri,\x2027\x20
SF:Dec\x202024\x2014:55:28\x20GMT\r\nContent-Type:\x20text/html\r\nContent
SF:-Length:\x20118\r\nConnection:\x20close\r\n\r\n<html>\r\n<head><title>4
SF:03\x20Forbidden</title></head>\r\n<body>\r\n<center><h1>403\x20Forbidde
SF:n</h1></center>\r\n</body>\r\n</html>\r\n")%r(RPCCheck,110,"HTTP/1\.1\x
SF:20400\x20Bad\x20Request\r\nServer:\x20awselb/2\.0\r\nDate:\x20Fri,\x202
SF:7\x20Dec\x202024\x2014:55:35\x20GMT\r\nContent-Type:\x20text/html\r\nCo
SF:ntent-Length:\x20122\r\nConnection:\x20close\r\n\r\n<html>\r\n<head><ti
SF:tle>400\x20Bad\x20Request</title></head>\r\n<body>\r\n<center><h1>400\x
SF:20Bad\x20Request</h1></center>\r\n</body>\r\n</html>\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BaySta
ck 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   2.32 ms 10.0.2.2
2   2.50 ms a35f64fceb718ad27.awsglobalaccelerator.com (3.33.182.45)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.96 seconds
```

What is Dmitry (Deepmagic Information Gathering Tool) ?

- Dmitry specializes in passive reconnaissance to gather information about the target.

Basic Usage
Command :
dmitry <options> <target>

```
┌──(kali㉿kali)-[~]
└─$ dmitry www.mercadolibre.com

Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:3.33.182.45
HostName:www.mercadolibre.com

Gathered Inet-whois information for 3.33.182.45
---------------------------------------------------


inetnum:        3.0.0.0 - 4.255.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------------
remarks:
remarks:        For registration information,
emarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
et
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ------------------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
-01-07T10:50:00Z
last-modified:  2019-01-07T10:50:00Z
source:         RIPE

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
```

```
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered
% This query was served by the RIPE Database Query Service version 1.114 (DE
XTER)



Gathered Inic-whois information for mercadolibre.com
---------------------------------
   Domain Name: MERCADOLIBRE.COM
   Registry Domain ID: 6342178_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-08-30T11:38:26Z
   Creation Date: 1999-05-08T07:46:48Z
   Registry Expiry Date: 2025-10-01T02:39:12Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
entDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTrans
ferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateP
rohibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteP
rohibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTrans
ferProhibited
hibited
   Name Server: NS-1451.AWSDNS-53.ORG
   Name Server: NS-1708.AWSDNS-21.CO.UK
   Name Server: NS-368.AWSDNS-46.COM
   Name Server: NS-984.AWSDNS-59.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/w
icf/
```

```
Gathered Netcraft information for www.mercadolibre.com
---------------------------------

Retrieving Netcraft.com information for www.mercadolibre.com
Netcraft.com Information gathered

Gathered Subdomain information for mercadolibre.com
---------------------------------
Searching Google.com:80 ...
HostName:www.mercadolibre.com
HostIP:15.197.170.90
HostName:global-selling.mercadolibre.com
HostIP:13.225.4.24
HostName:play.mercadolibre.com
HostIP:13.225.4.116
HostName:investor.mercadolibre.com
HostIP:104.18.6.86
HostName:survey.mercadolibre.com
HostIP:125.252.219.170
HostName:mobile.mercadolibre.com
HostIP:13.225.4.97
HostName:api.mercadolibre.com
HostIP:108.158.1.111
HostName:careers-meli.mercadolibre.com
HostIP:18.155.68.13
HostName:centrodepartners.mercadolibre.com
HostIP:13.225.4.97
HostName:pppi.mercadolibre.com
HostIP:18.155.68.13
HostName:hp.mercadolibre.com
HostIP:13.225.4.27
Searching Altavista.com:80 ...
Found 11 possible subdomain(s) for host mercadolibre.com, Searched 0 pages c
ontaining 0 results

Gathered E-Mail information for mercadolibre.com
---------------------------------
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host mercadolibre.com, Searched 0 pages containing 0 r
esults
```

```
Gathered TCP Port information for 3.33.182.45
---------------------------------

 Port           State

80/tcp          open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed


All scans completed, exiting
```

Common Options

- **Gather Subdomains**

  Command :

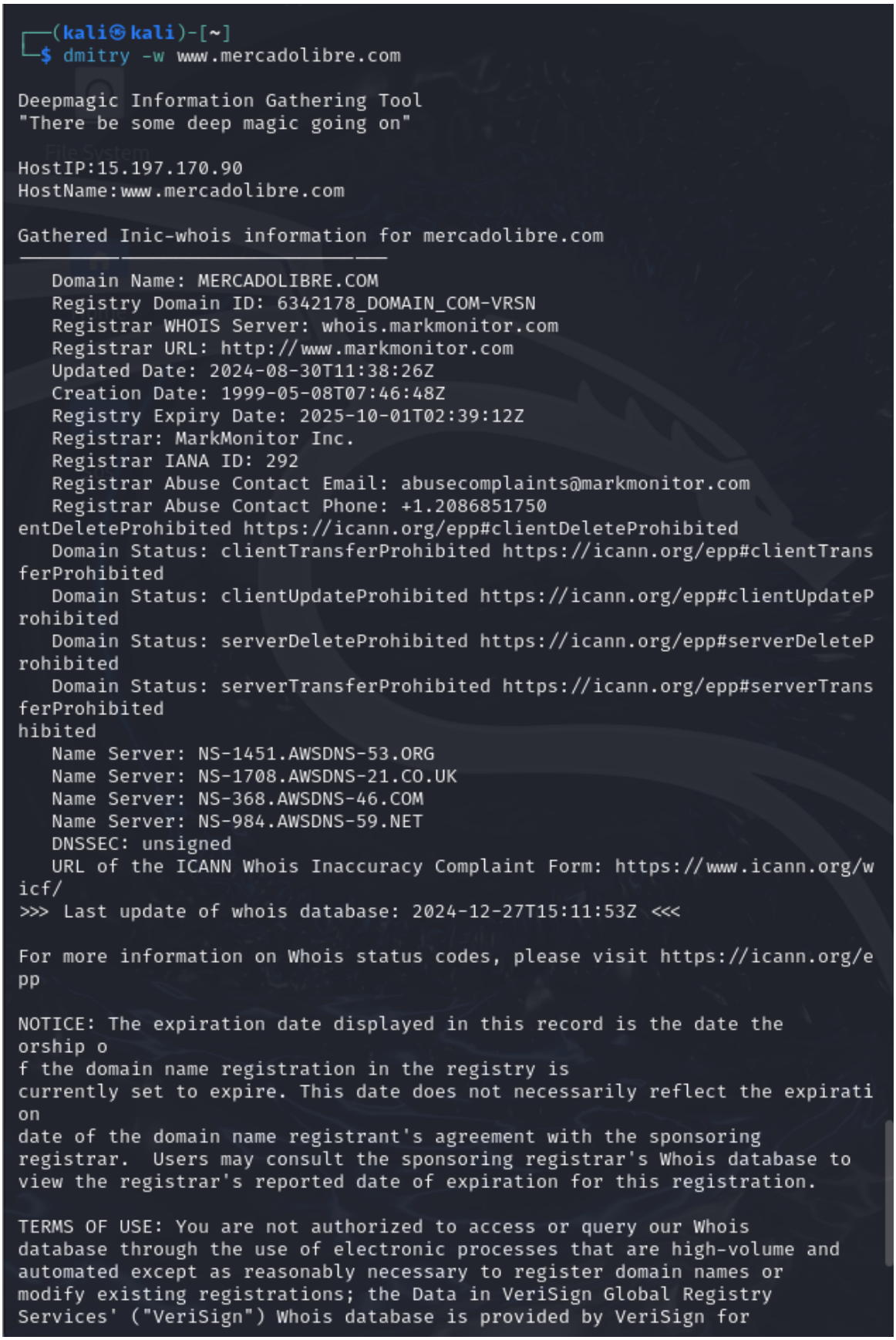
  dmitry -s <target>

```
┌──(kali㉿kali)-[~]
└─$ dmitry -s www.mercadolibre.com

Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:15.197.170.90
HostName:www.mercadolibre.com

Gathered Subdomain information for mercadolibre.com
---------------------------------------
Searching Google.com:80 ...
HostName:www.mercadolibre.com
HostIP:3.33.182.45
HostName:global-selling.mercadolibre.com
HostIP:13.225.4.24
HostName:play.mercadolibre.com
HostIP:13.225.4.27
HostName:investor.mercadolibre.com
HostIP:104.18.7.86
HostName:survey.mercadolibre.com
HostIP:125.252.219.170
HostName:mobile.mercadolibre.com
HostIP:13.225.4.27
HostName:api.mercadolibre.com
HostIP:108.139.64.109
HostName:careers-meli.mercadolibre.com
HostIP:18.155.68.13
HostName:centrodepartners.mercadolibre.com
HostIP:13.225.4.27
HostName:pppi.mercadolibre.com
HostIP:18.155.68.17
HostName:hp.mercadolibre.com
HostIP:13.225.4.97
Searching Altavista.com:80 ...
Found 11 possible subdomain(s) for host mercadolibre.com, Searched 0 pages c
ontaining 0 results

All scans completed, exiting
```

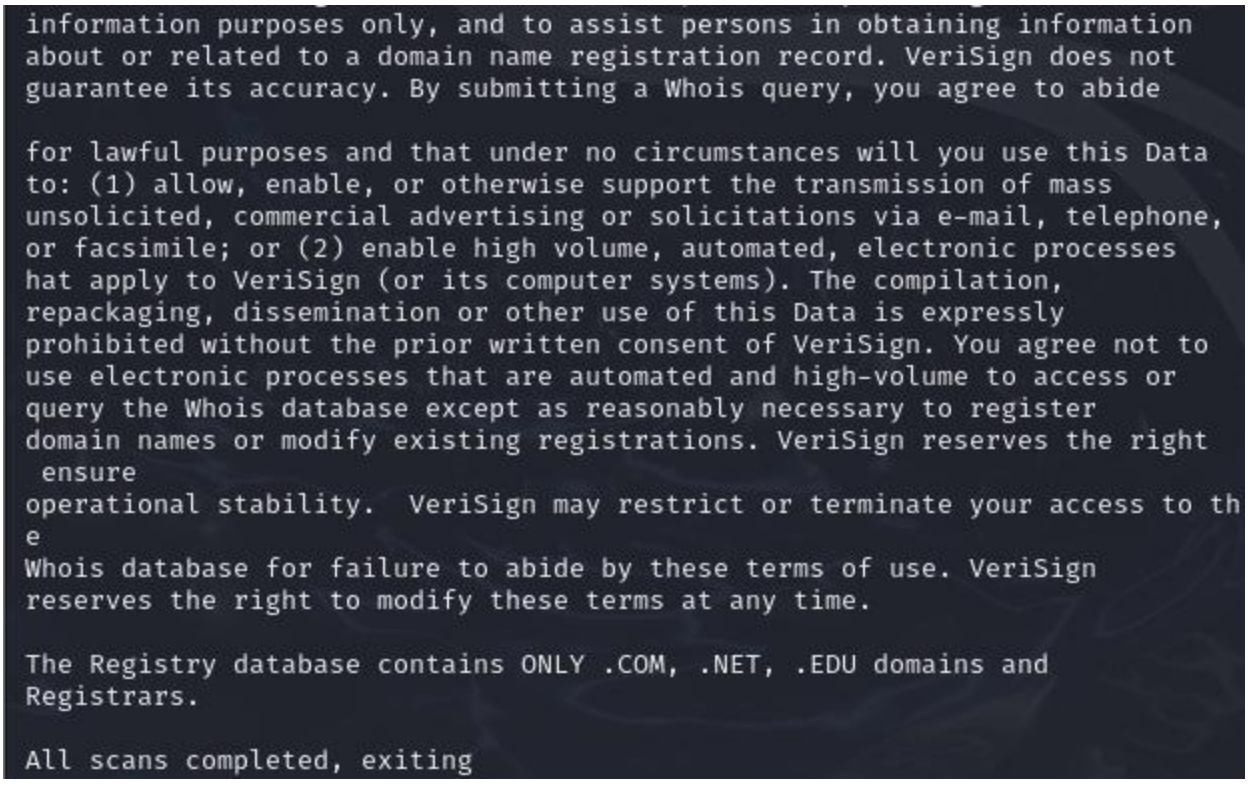
- **Perform Whois Lookup**

  Command :

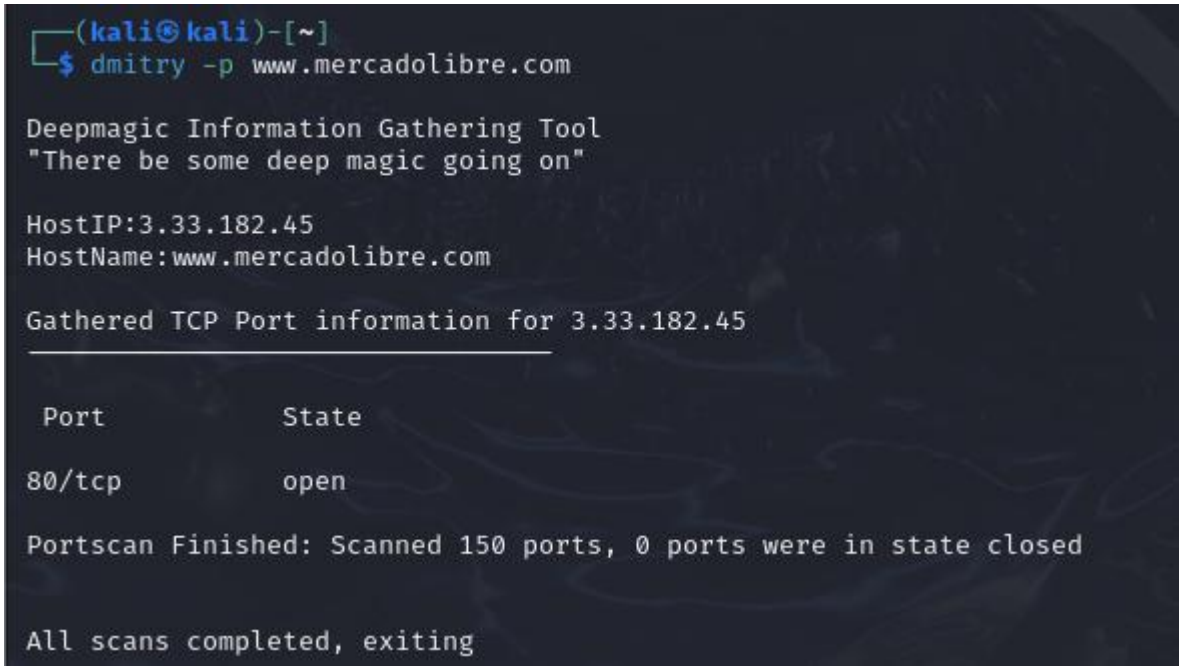
  dmitry -w <target>



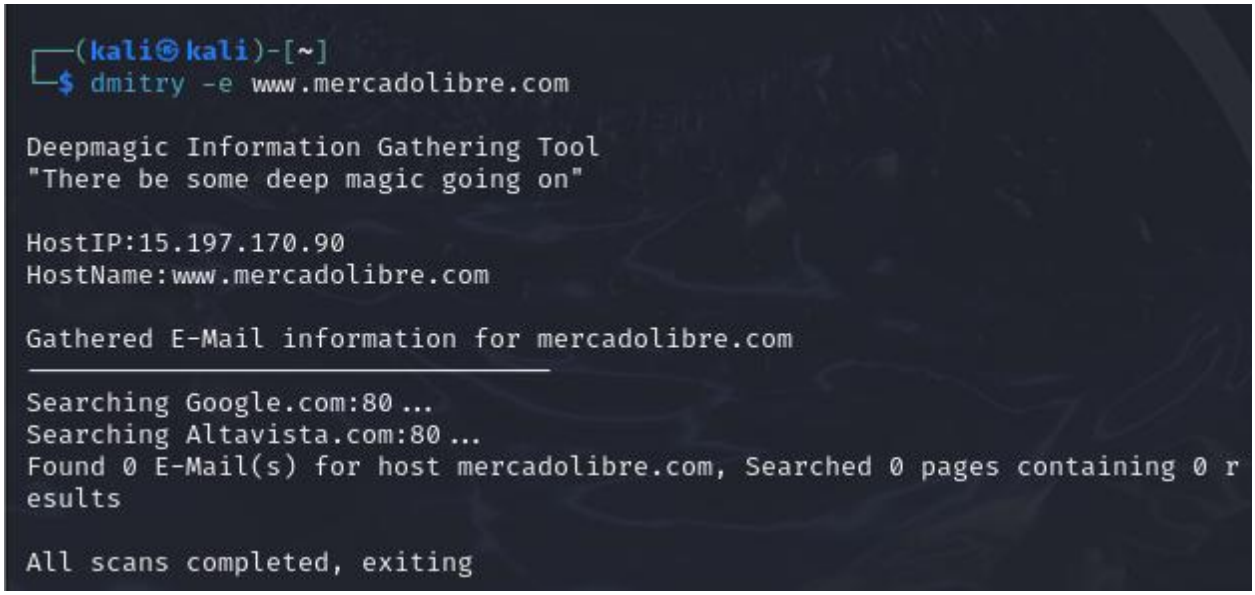
```
┌──(kali㉿kali)-[~]
└─$ dmitry -w www.mercadolibre.com

Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:15.197.170.90
HostName:www.mercadolibre.com

Gathered Inic-whois information for mercadolibre.com
---------------------------------------------------
   Domain Name: MERCADOLIBRE.COM
   Registry Domain ID: 6342178_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-08-30T11:38:26Z
   Creation Date: 1999-05-08T07:46:48Z
   Registry Expiry Date: 2025-10-01T02:39:12Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
entDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTrans
ferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateP
rohibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteP
rohibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTrans
ferProhibited
hibited
   Name Server: NS-1451.AWSDNS-53.ORG
   Name Server: NS-1708.AWSDNS-21.CO.UK
   Name Server: NS-368.AWSDNS-46.COM
   Name Server: NS-984.AWSDNS-59.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/w
icf/
>>> Last update of whois database: 2024-12-27T15:11:53Z <<<

For more information on Whois status codes, please visit https://icann.org/e
pp

NOTICE: The expiration date displayed in this record is the date the
orship o
f the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expirati
on
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
```


information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
hat apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
ensure
operational stability. VeriSign may restrict or terminate your access to th
e
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
All scans completed, exiting

- **Search for Open Ports**
  Command :
  dmitry -p <target>



- **Search for Email Addresses**
  Command :
  dmitry -e <target>



Combining Options

Use multiple options together to gather comprehensive information:

Command :

dmitry -winsep <target>

This includes:

- Whois lookup
- IP address lookup
- Subdomain search
- Email search
- Open ports scan


(kali㉿kali)-[~]
$ dmitry -winsep www.mercadolibre.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:3.33.182.45
HostName:www.mercadolibre.com
Gathered Inet-whois information for 3.33.182.45
inetnum: 3.0.0.0 - 4.255.255.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
escr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks:
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks:
remarks: LACNIC (Latin America and the Carribean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks:
ry: EU # Country is really world wide
admin-c: IANA1-RIPE
tech-c: IANA1-RIPE
status: ALLOCATED UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2019-01-07T10:50:00Z
last-modified: 2019-01-07T10:50:00Z
source: RIPE
role: Internet Assigned Numbers Authority
address: see http://www.iana.org.
admin-c: IANA1-RIPE
tech-c: IANA1-RIPE
nic-hdl: IANA1-RIPE
remarks: For more information on IANA services

```
:           go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114 (AB
ERDEEN)
```

```
Gathered Inic-whois information for mercadolibre.com
---------------------------------
   Domain Name: MERCADOLIBRE.COM
   Registry Domain ID: 6342178_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-08-30T11:38:26Z
   Creation Date: 1999-05-08T07:46:48Z
   Registry Expiry Date: 2025-10-01T02:39:12Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
entDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTrans
ferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateP
rohibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteP
rohibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTrans
ferProhibited
hibited
   Name Server: NS-1451.AWSDNS-53.ORG
   Name Server: NS-1708.AWSDNS-21.CO.UK
   Name Server: NS-368.AWSDNS-46.COM
   Name Server: NS-984.AWSDNS-59.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/w
icf/
>>> Last update of whois database: 2024-12-27T15:19:41Z <<<

For more information on Whois status codes, please visit https://icann.org/e
pp

NOTICE: The expiration date displayed in this record is the date the
orship o
f the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expirati
on
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide

for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
```

```
is expre
ssly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensu
re
operational stability.  VeriSign may restrict or terminate your access to th
e
ide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

Gathered Netcraft information for www.mercadolibre.com
-------------------------------------

Retrieving Netcraft.com information for www.mercadolibre.com
Netcraft.com Information gathered

Gathered Subdomain information for mercadolibre.com
-------------------------------------
Searching Google.com:80 ...
HostName:www.mercadolibre.com
HostIP:15.197.170.90
HostName:global-selling.mercadolibre.com
HostIP:13.225.4.116
HostName:play.mercadolibre.com
HostIP:13.225.4.116
HostName:investor.mercadolibre.com
HostIP:104.18.6.86
HostName:survey.mercadolibre.com
HostIP:23.57.78.82
HostName:mobile.mercadolibre.com
HostIP:13.225.4.24
HostName:careers-meli.mercadolibre.com
HostIP:18.155.68.92
HostName:centrodepartners.mercadolibre.com
HostIP:13.225.4.116
HostName:pppi.mercadolibre.com
HostIP:18.155.68.50
HostName:hp.mercadolibre.com
HostIP:13.225.4.116
HostName:developers.mercadolibre.com
HostIP:13.225.4.27
HostName:vendedores.mercadolibre.com
HostIP:13.225.4.27
Searching Altavista.com:80 ...
Found 12 possible subdomain(s) for host mercadolibre.com, Searched 0 pages c
ontaining 0 results
```

```
Gathered E-Mail information for mercadolibre.com
---------------------------------
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host mercadolibre.com, Searched 0 pages containing 0 r
esults
```

```
Gathered TCP Port information for 3.33.182.45
---------------------------------

 Port           State

80/tcp          open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed


All scans completed, exiting
```

What is Uniscan ?

- Uniscan is a vulnerability scanner designed for web applications.
- Identify common vulnerabilities like SQL injection, file inclusion, or directory traversal.
- Use the reports as a starting point and manually verify the findings.

Installation:

Command :

sudo apt-get install uniscan

Go to the Uniscan directory

Command :

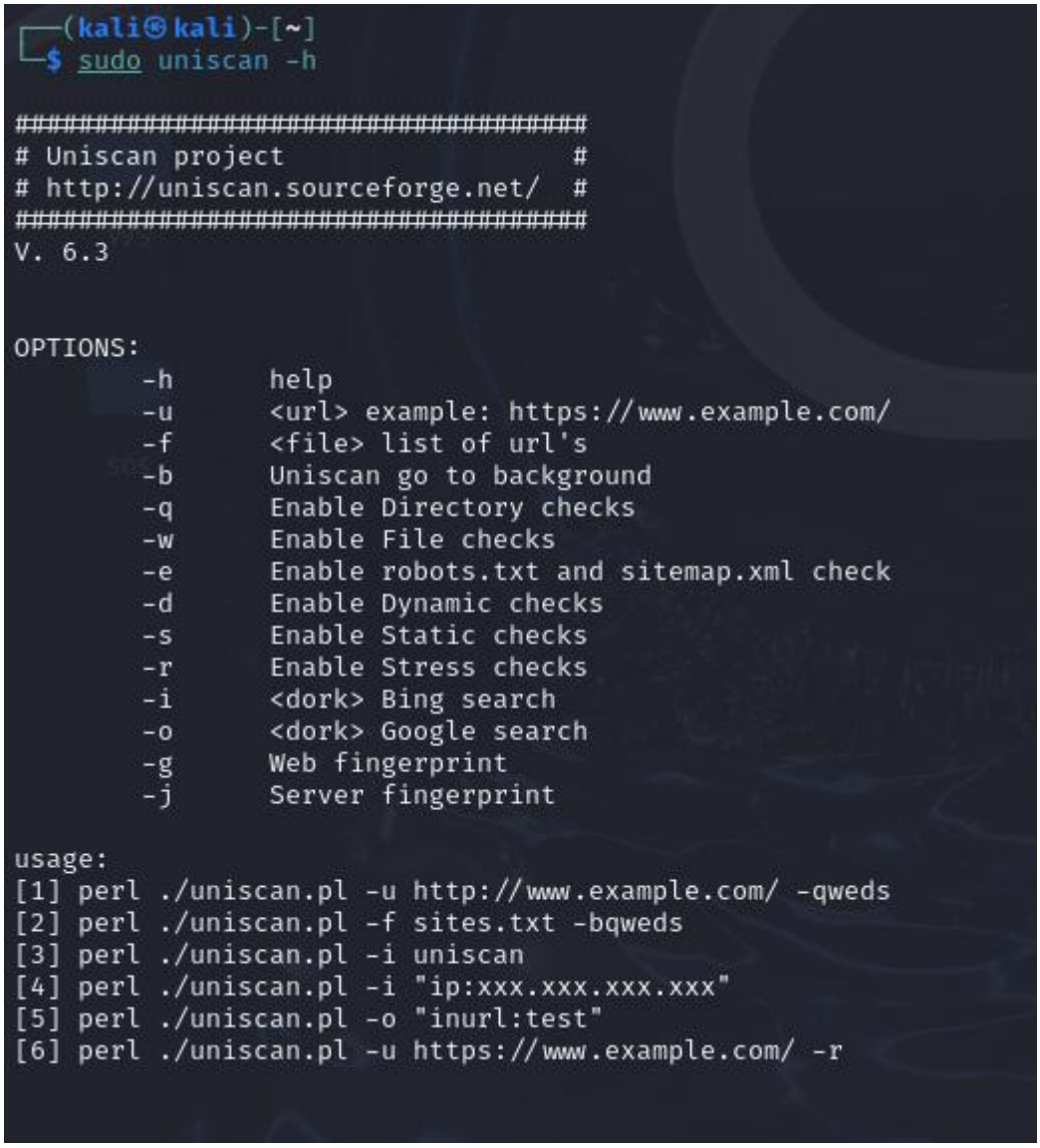
cd Uniscan

Usage:

- Basic Idea:

Command :

sudo uniscan -h



Advanced Options:

- -u : Specify the URL.
- -d : Enable dynamic checks (e.g., file inclusion).
- -e : Enable directory checks.

What is Sqlmap ?

- Sqlmap automates the detection and exploitation of SQL injection flaws.
- Use on endpoints where parameters are passed, especially GET and POST requests.
- Check for blind SQL injection by adding flags

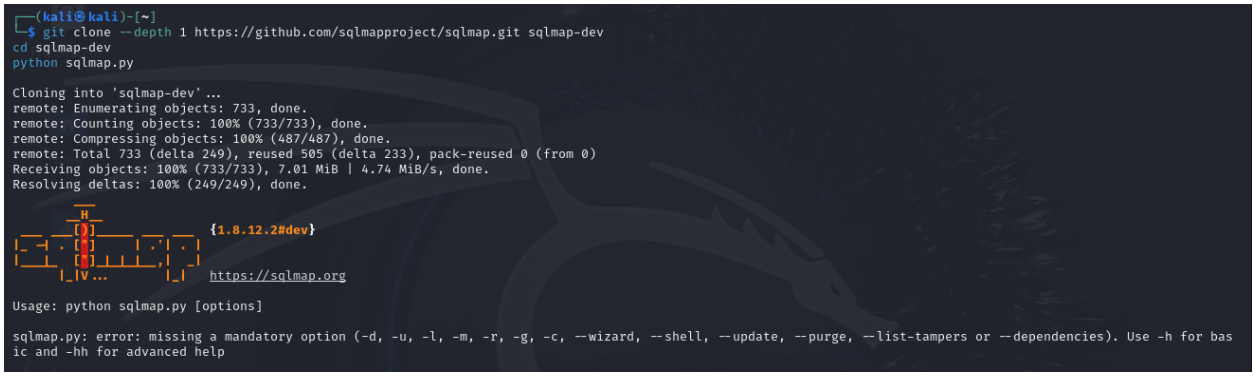
Installation:

Command :

git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev

cd sqlmap-dev

python sqlmap.py



Usage:

Basic SQL Injection Scan:

Command :

python sqlmap.py -u <URL>

Custom Parameters:

- *--dbs : Enumerate databases.*
- *-D : Specify the database.*
- *-T : Specify the table.*
- *--dump : Dump table contents.*

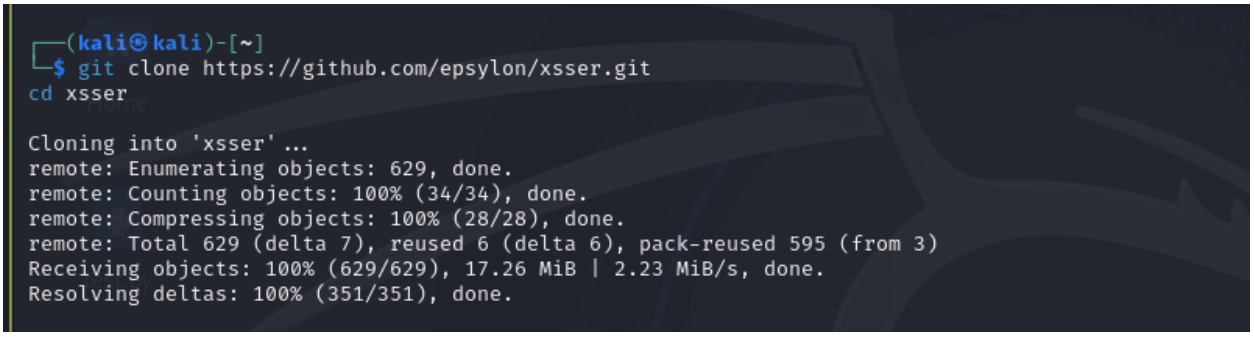
What is Xsser ?

- For detecting and exploiting cross-site scripting (XSS) vulnerabilities.
- Test user inputs, query parameters, and cookies.
- Pay attention to reflected and stored XSS vulnerabilities.

Installation:

Command :

git clone https://github.com/epsylon/xsser.git
cd xsser



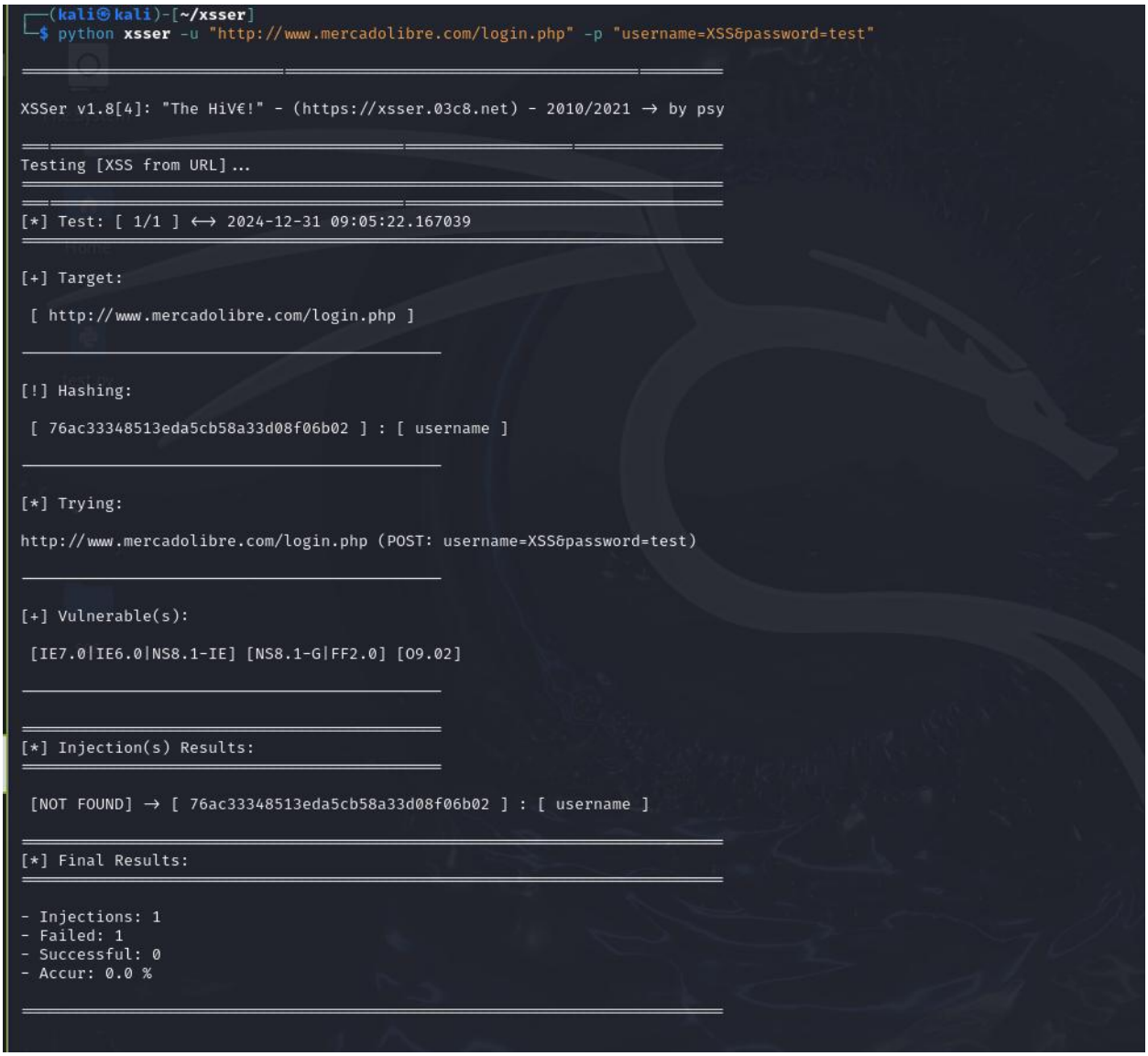
Usage:

Command :

python xsser -u <URL>

Advanced Options:

- --post : Test POST parameters.
- --cookie : Use cookies to simulate an authenticated user.
- --heuristic : Heuristically detect vulnerabilities.


(kali㉿kali)-[~/xsser]
$ python xsser -u "http://www.mercadolibre.com/login.php" -p "username=XSS&password=test"
XSSer v1.8[4]: "The HiV€!" - (https://xsser.03c8.net) - 2010/2021 → by psy
Testing [XSS from URL]...
[*] Test: [1/1] ↔ 2024-12-31 09:05:22.167039
[+] Target:
[http://www.mercadolibre.com/login.php]
[!] Hashing:
[76ac33348513eda5cb58a33d08f06b02] : [username]
[*] Trying:
http://www.mercadolibre.com/login.php (POST: username=XSS&password=test)
[+] Vulnerable(s):
[IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
[*] Injection(s) Results:
[NOT FOUND] → [76ac33348513eda5cb58a33d08f06b02] : [username]
[*] Final Results:
- Injections: 1
- Failed: 1
- Successful: 0
- Accur: 0.0 %

Wpscan :

1. Install WPScan via APT (Recommended)

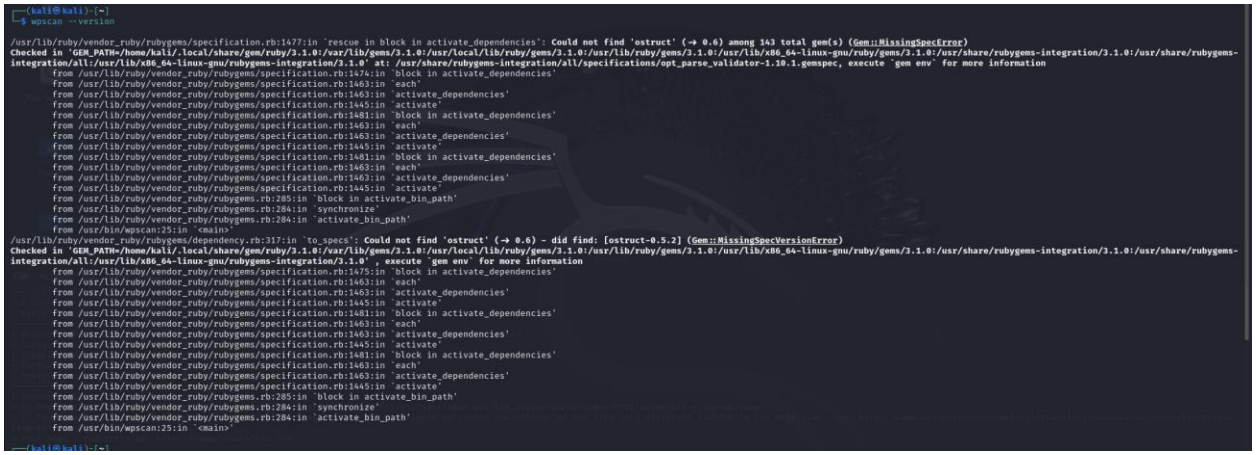
- WPScan is available in the **Kali Linux repositories**, so you can install it using:
- Command : **sudo apt update && sudo apt install wpscan -y**

3. Verify Installation

- After installation, confirm WPScan is installed by running:
- Command : **wpscan --version**

4. Update WPScan Database

- To keep the vulnerability database up to date:
- Command : **wpscan --update**



The command wpscan --url https://test.com is used to check if a given website (in this case, truecaller.com) is running **WordPress** as its content management system (CMS).

How It Works:

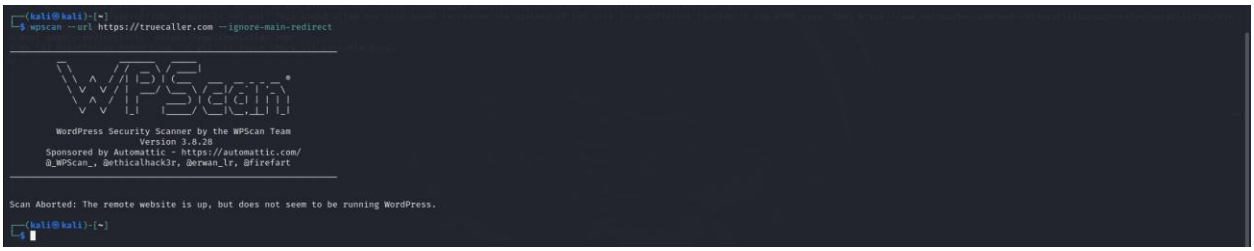
- **WPScan** is a tool specifically designed for scanning WordPress websites for vulnerabilities.
- By running wpscan --url https://test.com, you're asking WPScan to analyze the site and determine if it is powered by **WordPress**.
    - If the website **is running WordPress**, WPScan will try to identify any known vulnerabilities.
    - If the website **is not running WordPress**, WPScan will simply not find anything relevant, since it is designed specifically for WordPress sites.

Why Use This Command?

- This is useful to check if a site is based on WordPress before deciding to use WPScan for security assessments. Since **WPScan only works with WordPress websites**, it won't be useful on a non-WordPress website like **Truecaller**.

Scanning

- Identify vulnerabilities if use wordpress
- Command : wpscan --url https://www.quillbot.com



- Since this website not using webpress we cant use this wpsccan to identify vulnerabilities.