

## Contents

What is sublist3r ? .....	2
What is Amass ? .....	4
What is Htprobe ? .....	6
Wayback Machine .....	11
What is Nikto ? .....	13
Scan Using HTTPS: .....	15
What is nslookup ? .....	16
What is WhatWeb .....	19
What is Netcraft ? .....	21
What the Whois Lookup Tool Does ? .....	24
What is Domain Information Groper (DIG) Tool ? .....	26
What is Nmap (Network Mapper) ? .....	29
What is Dmitry (Deepmagic Information Gathering Tool) ? .....	35
What is Uniscan ? .....	49
What is Sqlmap ? .....	51
What is Xsser ? .....	53
Wpscan : .....	55

## 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  - outdated information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 Httpprobe ?

- 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)-[~]
└─$ go version
go version go1.23.4 linux/amd64

(kali㉿kali)-[~]
└─$ pwd
/home/kali

(kali㉿kali)-[~]
└─$ go install github.com/tomnomnom/httpprobe@latest
go: downloading github.com/tomnomnom/httpprobe v0.1.2

(kali㉿kali)-[~]
└─$ echo $(go env GOPATH)/bin
/home/kali/go/bin

(kali㉿kali)-[~]
└─$ export PATH=$PATH:/home/kali/go/bin

(kali㉿kali)-[~]
└─$ httpprobe -h
Usage of httpprobe:
  -c int
            set the concurrency level (default 20)
  -p value
            add additional probe (proto:port)
  -s      skip the default probes (http:80 and https:443)
  -t int
            timeout (milliseconds) (default 10000)
  -v      output errors to stderr
```

```
(kali㉿kali)-[~]
└─$ sudo apt install httpprobe
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  imagemagick-6-common  libfmt9                  libmagickcore-6.q16-7t64  libsuperlu6
  libbfiol               libmagickcore-6.q16-7-extra libmagickwand-6.q16-7t64
Use 'sudo apt autoremove' to remove them.

Installing:
  httpprobe

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 httpprobe amd64 0.2-0kali1 [1,597 kB]
Fetched 1,597 kB in 1s (1,341 kB/s)
Selecting previously unselected package httpprobe.
(Reading database ... 424909 files and directories currently installed.)
Preparing to unpack .../httpprobe_0.2-0kali1_amd64.deb ...
Unpacking httpprobe (0.2-0kali1) ...
Setting up httpprobe (0.2-0kali1) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
```

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

```
(kali㉿kali)-[~]
$ amass enum -d mercadolivre.com -o mercado.txt

mercadolivre.com (FQDN) → ns_record → ns-1708.awsdns-21.co.uk (FQDN)
mercadolivre.com (FQDN) → ns_record → ns-984.awsdns-59.net (FQDN)
mercadolivre.com (FQDN) → ns_record → ns-1451.awsdns-53.org (FQDN)
mercadolivre.com (FQDN) → ns_record → ns-368.awsdns-46.com (FQDN)
content.mercadolivre.com (FQDN) → cname_record → h-mercadolibre.online-metrix.net (FQDN)
developers-forum.mercadolivre.com (FQDN) → cname_record → melidevelopers.invisionzone.com (FQDN)
apps.mercadolivre.com (FQDN) → cname_record → list.mercadolivre.com (FQDN)
test-vendedores.mercadolivre.com (FQDN) → cname_record → dbjfce6tekir0.cloudfront.net (FQDN)
chattest.mercadolivre.com (FQDN) → cname_record → d2g9ak52q0ogkf.cloudfront.net (FQDN)
mobile.mercadolivre.com (FQDN) → cname_record → d2g9ak52q0ogkf.cloudfront.net (FQDN)
prodeng.mercadolivre.com (FQDN) → cname_record → prodeng-prod-public-alb-tmp-1129379816.us-east-1.elb.amazonaws.com (FQDN)
sellers.mercadolivre.com (FQDN) → cname_record → d2g9ak52q0ogkf.cloudfront.net (FQDN)
envios.mercadolivre.com (FQDN) → a_record → 143.204.98.4 (IPAddress)
ml-challenge.mercadolivre.com (FQDN) → cname_record → d2g9ak52q0ogkf.cloudfront.net (FQDN)
universidadvirtual.mercadolivre.com (FQDN) → cname_record → domssl.mercadolivre.com (FQDN)
webhooks.mercadolivre.com (FQDN) → cname_record → d2g9ak52q0ogkf.cloudfront.net (FQDN)
www.mercadolivre.com (FQDN) → cname_record → a35f64fcceb718ad27.awsglobalaccelerator.com (FQDN)
ads-preview.mercadolivre.com (FQDN) → cname_record → d2g9ak52q0ogkf.cloudfront.net (FQDN)
facturacion.mercadolivre.com (FQDN) → cname_record → d2g9ak52q0ogkf.cloudfront.net (FQDN)
hydratest.mercadolivre.com (FQDN) → cname_record → d2g9ak52q0ogkf.cloudfront.net (FQDN)
fraud-monitor.mercadolivre.com (FQDN) → cname_record → domssl.mercadolivre.com.ar (FQDN)
career.mercadolivre.com (FQDN) → cname_record → dbjfce6tekir0.cloudfront.net (FQDN)
gaia.mercadolivre.com (FQDN) → cname_record → d2g9ak52q0ogkf.cloudfront.net (FQDN)
tienda.mercadolivre.com (FQDN) → cname_record → domssl.mercadolivre.com.ar (FQDN)
fraudinkiru.mercadolivre.com (FQDN) → cname_record → domssl.mercadolivre.com.ar (FQDN)
publicar-test.mercadolivre.com (FQDN) → cname_record → domssl.mercadolivre.com.ar (FQDN)
m.mercadolivre.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

```
(kali㉿kali)-[~]
└─$ sublist3r -d mercadolibre.com -o mercadosub.txt

File System
└─mercadolibre.com
  └─www.mercadolibre.com
    └─a.mercadolibre.com
      └─alejandria-int.mercadolibre.com
        └─andes.mercadolibre.com
          └─andes-landings.mercadolibre.com
            └─api.mercadolibre.com
              └─www.api.mercadolibre.com
                └─api-cbt.mercadolibre.com
                  └─refpayments.baloto.mercadolibre.com
                    └─test.baloto.mercadolibre.com
                      └─bc-jpm-beta-ssl.mercadolibre.com
                        └─bc-jpm-beta-sslv2.mercadolibre.com
                          └─bc-jpm-beta-transfer.mercadolibre.com
                            └─bc-jpm-beta-update.mercadolibre.com
                              └─bc-jpm-prod-ssl.mercadolibre.com
                                └─bc-jpm-prod-transfer.mercadolibre.com
                                  └─bc-jpm-prod-update.mercadolibre.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for mercadolibre.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.12/multiprocessing/process.py", line 314, in _bootstrap
    self.run()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
                   ^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
    token = self.get_csrftoken(resp)
           ^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
           ^^^
IndexError: list index out of range
[!] Error: Virustotal probably now is blocking our requests
[-] Saving results to file: mercadosub.txt
[-] Total Unique Subdomains Found: 88
www.mercadolibre.com
a.mercadolibre.com
alejandria-int.mercadolibre.com
andes.mercadolibre.com
andes-landings.mercadolibre.com
api.mercadolibre.com
www.api.mercadolibre.com
api-cbt.mercadolibre.com
refpayments.baloto.mercadolibre.com
test.baloto.mercadolibre.com
bc-jpm-beta-ssl.mercadolibre.com
bc-jpm-beta-sslv2.mercadolibre.com
bc-jpm-beta-transfer.mercadolibre.com
bc-jpm-beta-update.mercadolibre.com
bc-jpm-prod-ssl.mercadolibre.com
bc-jpm-prod-transfer.mercadolibre.com
bc-jpm-prod-update.mercadolibre.com
```

Use output of sublist3r as the input of httpprobe

```
(kali㉿kali)-[~]
$ cat mercadosub.txt | httpprobe > mercado_live_subdomains.txt
File System
(kali㉿kali)-[~]
$ ls
active_subdomains.txt  Downloads      IDS          mercadosub.txt  natas12.jpg  Public       Sublist3r
Desktop                go             1123265592  mercado.txt    Pictures    sshkey.private  Templates
Documents               google_subdomains.txt  mercado_live_subdomains.txt  Music      private.key  student     Videos
(kali㉿kali)-[~]
$ cat mercado_live_subdomains.txt
http://api.mercadolibre.com
https://api.mercadolibre.com
http://andes-landings.mercadolibre.com
http://www.mercadolibre.com
http://andes.mercadolibre.com
http://encuestas.mercadolibre.com
http://global-selling.mercadolibre.com
http://ideas.mercadolibre.com
https://global-selling.mercadolibre.com
http://data.mercadolibre.com
http://developers-forum.mercadolibre.com
https://andes-landings.mercadolibre.com
http://Fooddeliverywebapp.mercadolibre.com
https://www.mercadolibre.com
https://data.mercadolibre.com
https://andes.mercadolibre.com
http://cbt.mercadolibre.com
http://jobs.mercadolibre.com
https://cbt.mercadolibre.com
https://investor.mercadolibre.com
http://investor.mercadolibre.com
https://jobs.mercadolibre.com
https://ideas.mercadolibre.com
https://Fooddeliverywebapp.mercadolibre.com
https://encuestas.mercadolibre.com
http://Learninghub-int.mercadolibre.com
http://Learninghub-studio-int.mercadolibre.com
http://manualdeestilo.mercadolibre.com
https://learninghub-int.mercadolibre.com
http://learning.mercadolibre.com
http://ucs.orion-prd.mercadolibre.com
http://lstage.mercadolibre.com
https://learning.mercadolibre.com
https://learninghub-studio-int.mercadolibre.com
https://lstage.mercadolibre.com
http://prodeng.mercadolibre.com
https://manualdeestilo.mercadolibre.com
http://test.mercadolibre.com
https://test.mercadolibre.com
https://op-scim.mercadolibre.com
http://survey.mercadolibre.com
https://ucs.orion-prd.mercadolibre.com
http://universidad.mercadolibre.com
```

## Wayback Machine

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

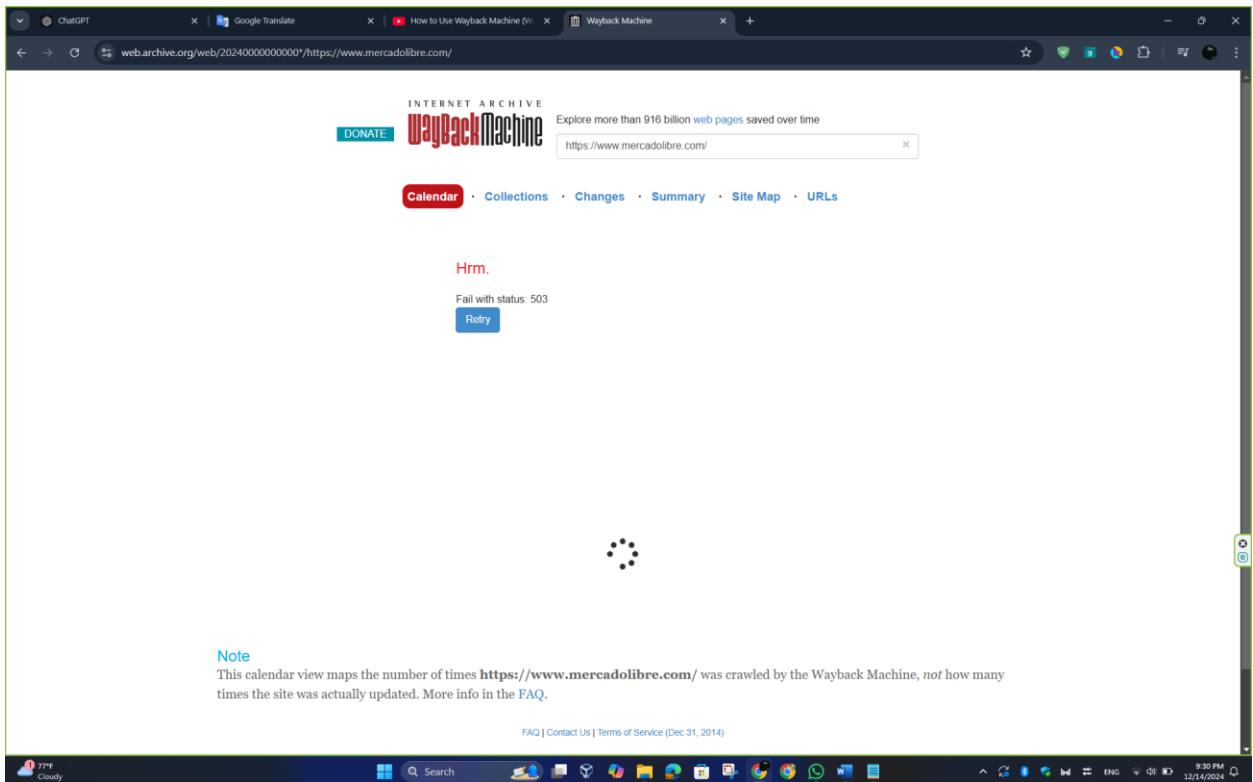
- archives websites by taking snapshots (HTML, text, media).
- Stores snapshots for public access to view historical versions of web pages.
- **Digital Forensics**
  - Investigate website changes or defacements over time
  - Recover deleted content
- Analyze past phishing websites and attacker tactics.
- 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.



## 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`

```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo apt install perl libwww-perl git -y

[sudo] password for kali:
perl is already the newest version (5.40.0-8).
libwww-perl is already the newest version (6.77-1).
libwww-perl set to manually installed.
git is already the newest version (1:2.45.2-1).
Summary:Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 12
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 12
Space needed: 23.6 kB / 59.1 GB available
```

### 2. Clone the Nikto repository:

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

```
└─(kali㉿kali)-[~]
$ git clone https://github.com/sullo/nikto.git
  % Total    Received = Total  Delta  Speed     Time    Time  Current
   0     0     0     0    0     0      0 --:--:--  --:--:--    0
  25    25    25    0     0     0      0  0:00:00  0:00:00    0
  50    50    50    0     0     0      0  0:00:00  0:00:00    0
  75    75    75    0     0     0      0  0:00:00  0:00:00    0
 100    100   100   25     0     0      0  0:00:00  0:00:00    0
Fetched 11.0 kB in 1s (14.2 kB/s)
Cloning into 'nikto' ...
remote: Enumerating objects: 7467, done.
remote: Counting objects: 100% (487/487), done.
remote: Compressing objects: 100% (222/222), done.
remote: Total 7467 (delta 400), reused 271 (delta 265), pack-reused 6980 (from 3)
Receiving objects: 100% (7467/7467), 4.65 MiB | 3.89 MiB/s, done.
Resolving deltas: 100% (5412/5412), done.
```

**3. Navigate to the Nikto directory:**

Command : **cd nikto/program**

```
(kali㉿kali)-[~]s to be up
└─$ cd nikto/program
```

**4. Run Nikto:**

Command : **perl nikto.pl**

```
(kali㉿kali)-[~/nikto/program]...
└─$ perl nikto.pl -l (192.168.3.1) ...
Scanning processes...
- Nikto v2.5.0 images ...
```

## Scan Using HTTPS:

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

```
(kali㉿kali)-[~/nikto/program]
$ perl nikto.pl -h https://www.mercadolibre.com/
- Nikto v2.5.0
+ Multiple IPs found: 15.197.170.90, 3.33.182.45
+ Target IP: 15.197.170.90
+ Target Hostname: www.mercadolibre.com
+ Target Port: 443
+ SSL Info: Subject: /CN=*.mercadolibre.com
Ciphers: ECDHE-RSA-AES128-GCM-SHA256
Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M03
+ Start Time: 2024-12-17 04:34:48 (GMT-5)
+ Server: Tengine
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-d2id' found, with contents: 99ddaa10f-4d7b-4b9d-9c7c-76cfaaeefdd08.
+ /: Uncommon header 'x-amz-server-side-encryption' found, with contents: AES256.
+ /: Uncommon header 'x-amz-replication-status' found, with contents: COMPLETED.
+ /: Uncommon header 'x-amz-id-2' found, with contents: SrYI1pN46uVj0S8qiAl+rMzvAx+DjPH8806IBtt6mNxrv7LxerfeqjiaH/eEnfy6GgoCz6VkaY-.
+ /: Uncommon header 'x-request-id' found, with contents: 99ddaa10f-4d7b-4b9d-9c7c-76cfaaeefdd08.
+ /: Uncommon header 'x-amz-request-id' found, with contents: B8MM8T0VZ253CX5.
+ /: Uncommon header 'x-request-device-id' found, with contents: 99ddaa10f-4d7b-4b9d-9c7c-76cfaaeefdd08.
+ /: Cookie _d2id created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Server banner changed from 'Tengine' to 'awselb/2.0'.
+ /7oG0UpqJ.log: 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/
+ /7oG0UpqJ.ashx: Uncommon header 'x-amz-error-message' found, with contents: The specified key does not exist.
+ /7oG0UpqJ.ashx: Uncommon header 'x-amz-error-detail-key' found, with contents: data2/homes/7oG0UpqJ.ashx.
+ /7oG0UpqJ.ashx: Uncommon header 'x-amz-error-code' found, with contents: NoSuchKey.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Uncommon header 'x-envoy-upstream-service-time' found, with contents: root_com.
+ /robots.txt: Uncommon header 'x-robots-file' found, with contents: root_com.
+ /robots.txt: contains 11 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Server is using a wildcard certificate: *.mercadolibre.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
```

## 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**

```

File Actions Edit View Help
[(kali㉿kali)-[~]]$ sudo apt install dnsutils -y

[sudo] password for kali:
Installing:
  dnsutils

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 12
  Download size: 11.0 kB
  Space needed: 23.6 kB / 59.1 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 dnsutils all 1:9.20.3-1 [11.0 kB]
Fetched 11.0 kB in 1s (14.2 kB/s)
Selecting previously unselected package dnsutils.
(Reading database ... 425686 files and directories currently installed.)
Preparing to unpack .../dnsutils_1%3a9.20.3-1_all.deb ...
Unpacking dnsutils (1:9.20.3-1) ...
Setting up dnsutils (1:9.20.3-1) ...
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

```

Run nslookup

Command : **nslookup**

Check whether is it running ?

Command : **nslookup example.com**

```
(kali㉿kali)-[~]
$ nslookup facebook.com

Server:      192.168.1.1
Address:      192.168.1.1#53

Non-authoritative answer:
Name:  facebook.com
Address: 57.144.144.1
Name:  facebook.com
Address: 2a03:2880:f10c:381:face:b00c:0:25de
```

### **Explanation of Output**

1. **Server: 192.168.1.1**
  - o 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**
  - o The #53 indicates the port number being used for DNS (port 53 is standard for DNS traffic).
3. **Non-authoritative answer:**
  - o 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**
  - o The domain name you queried.
5. **Address: 57.144.144.1**
  - o One of the IPv4 addresses for facebook.com.
6. **Address: 2a03:2880:f10c:381:face:b00c:0:25de**
  - o The IPv6 address for facebook.com.

```
(kali㉿kali)-[~]
└─$ nslookup https://www.mercadolibre.com/

Server:      192.168.1.1
Address:     192.168.1.1#53

** server can't find https://www.mercadolibre.com/: NXDOMAIN

(kali㉿kali)-[~]
└─$ nslookup https://www.mercadolibre.com

Server:      192.168.1.1
Address:     192.168.1.1#53

** server can't find https://www.mercadolibre.com: NXDOMAIN
```

- 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 : whatweb mercadolibre.com

```
(kali㉿kali)-[~]
$ whatweb www.mercadolibre.com

http://www.mercadolibre.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[awselb/2.0], IP[3.33.182.45], RedirectLocation[https://www.mercadolibre.com:443/], Title[301 Moved Permanently]
https://www.mercadolibre.com/ [200 OK] Cookies[_d2id], Country[UNITED STATES][US], Email[flags@2x.png], HTML5, HTTPS Server[Tengine], IP[3.33.182.45], Script, Strict-Transport-Security[max-age=604800; includeSubDomains;], Tengine-Web-Server, Title[Mercado Libre - Envíos Gratis en el día], UncommonHeaders[x-amz-id-2,x-amz-request-id,x-amz-replicatio-n-status,x-amz-server-side-encryption,x-amz-version-id,x-request-id,x-request-device-id,x-d2id,x-content-type-options,referrer-policy], X-XSS-Protection[1; mode=block]

(kali㉿kali)-[~]
$
```

### 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: [Email](#) [Print](#) [Copy URL](#)

### 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	Domain	mercadolibre.com	
Netblock Owner	Amazon Technologies Inc.	ns-368.awsdns-46.com	
Hosting company	Amazon	Unknown	
Hosting country	US	Unknown	
IPv4 address	15.197.170.90 (View total 10)	Organization	
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	a35f64fcbe718ad27.awsglobalaccelerator.com		

### IP delegation

IPv4 address (15.197.170.90)	Country	Name	Description
1::ffff:0.0.0.0/96	United States	IANA-IPv4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
4. 15.0.0-15.255.255.255	United States	NET15	American Registry for Internet Numbers
4. 15.196.0-15.200.255.255	United States	AT-88-Z	Amazon Technologies Inc.
4. 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	Amazon

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	<input checked="" type="checkbox"/>	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	Zal2ITmAC03efx9Rc74rAAj9iB
Public key length	2048	Public Key Hash	bfa659312833a8da3b202908df673ede9382e9bd85a33f9ee529b03d72367af9
Certificate check	<input checked="" type="checkbox"/>	OCSP servers	http://ocsp.r2m03.amazontrust.com
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	No response received
Serial number	0x06ac01c5ee9e5826bd33a7f13fd71d1		
Cipher	ECDHE-RSA-AES128-GCM-SHA256		
Version number	0x02		

**Certificate Transparency**

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Unknown EVFOIL1ckyEBm0Djz96E/jntrWKh1xtfWaiE6+wGJjo=	2024-11-06 01:27:24	Unknown
Certificate	DigiCert Yeti2025 Log FVketuf4KnscYw0Bx3461dcFKB01265A//ZDowuebg=	2024-11-06 01:27:25	Success
Certificate	DigiCert Nsslie2025 Log 5t1xv083jH0Q000XcbnOvd349paHvu6hzId/843j1A=	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 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 <a href="https://domains.markmonitor.com/whois/mercadolibre.com">https://domains.markmonitor.com/whois/mercadolibre.com</a>

### Administrative Contact

Organization:	MercadoLibre Inc.
State:	AR
Country:	AR
Email:	Select Request Email Form at <a href="https://domains.markmonitor.com/whois/mercadolibre.com">https://domains.markmonitor.com/whois/mercadolibre.com</a>

### Technical Contact

Organization:	MercadoLibre Inc.
State:	AR
Country:	AR
Email:	Select Request Email Form at <a href="https://domains.markmonitor.com/whois/mercadolibre.com">https://domains.markmonitor.com/whois/mercadolibre.com</a>

### 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: +1.2086851798
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
Tech Organization: MercadoLibre Inc.
Tech State/Province: AR
Tech Country: AR
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/mercadolibre
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**

```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo apt install dnsutils

[sudo] password for kali:
dnsutils is already the newest version (1:9.20.3-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 12
```

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, ADDITION
AL: 1
      test.py
;; 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](http://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
```

```
(kali㉿kali)-[~]
$ nmap --version

Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.3.2 libssh2-1.11.1 libz-1.3.1 libpcre2-10.44 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Basic command :

```
nmap <target>
```

```
(kali㉿kali)-[~]
$ nmap www.mercadolibre.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-27 09:51 EST
Nmap scan report for www.mercadolibre.com (15.197.170.90)
Host is up (0.0096s latency).
Other addresses for www.mercadolibre.com (not scanned): 3.33.182.45
rDNS record for 15.197.170.90: a35f64fcceb718ad27.awsglobalaccelerator.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 6.06 seconds
```

- Port Scanning

Identify open ports on the target:

Command :

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

```
(kali㉿kali)-[~]
$ nmap -p 80,443 www.mercadolibre.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-27 09:58 EST
Nmap scan report for www.mercadolibre.com (15.197.170.90)
Host is up (0.018s latency).
Other addresses for www.mercadolibre.com (not scanned): 3.33.182.45
rDNS record for 15.197.170.90: a35f64fcceb718ad27.awsglobalaccelerator.com

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

- 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: a35f64fce718ad27.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\x20EHL0\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:HTTPRequest,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:\x20
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-1347734
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</body>\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><t
SF:title>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>**

```
(kali㉿kali)-[~]
$ nmap -O www.mercadolibre.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-27 10:28 EST
Nmap scan report for www.mercadolibre.com (3.33.182.45)
Host is up (0.014s latency).
Other addresses for www.mercadolibre.com (not scanned): 15.197.170.90
rDNS record for 3.33.182.45: a35f64fce718ad27.awsglobalaccelerator.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 1.0.9 (92%), Oracle Virtualbox (89%), QEMU user mode network gateway (88%), Huawei Echo life HG520-series ADSL modem (87%), TP-LINK TD-W8951ND wireless ADSL modem (87%), ZyXEL Prestige 200 ISDN router (87%), ZyXEL ZyNOS 3.0 (87%), ZyXEL Prestige 2602R-D1A ADSL router (87%), ADSL router: Huawei MT800u-T; or ZyXEL Prestige 623ME-T1, 643, 662HW-61, 782, or 2602R-61 (87%), Linux 2.0.33 (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.15 seconds
```

- Script Scanning

Use NSE (Nmap Scripting Engine) for vulnerability detection:

Command

**nmap --script vuln <target>**

```
(kali㉿kali)-[~]
$ nmap --script vuln www.mercadolibre.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-27 10:29 EST
Nmap scan report for www.mercadolibre.com (15.197.170.90)
Host is up (0.011s latency).
Other addresses for www.mercadolibre.com (not scanned): 3.33.182.45
rDNS record for 15.197.170.90: a35f64fce718ad27.awsglobalaccelerator.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspx-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
443/tcp   open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspx-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

Nmap done: 1 IP address (1 host up) scanned in 108.26 seconds
```

- Aggressive Scan

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

Command :

**nmap -A <target>**

```
(kali㉿kali)-[~]
$ nmap -A www.mercadolibre.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-27 09:55 EST
Nmap scan report for www.mercadolibre.com (3.33.182.45)
Host is up (0.0081s latency).
Other addresses for www.mercadolibre.com (not scanned): 15.197.170.90
rDNS record for 3.33.182.45: a35f64fce718ad27.awsglobalaccelerator.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    awselb/2.0
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: awselb/2.0
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 403 Forbidden
|     Server: awselb/2.0
|     Date: Fri, 27 Dec 2024 14:55:28 GMT
|     Content-Type: text/html
|     Content-Length: 118
|     Connection: close
|     <html>
|     <head><title>403 Forbidden</title></head>
|     <body>
|     <center><h1>403 Forbidden</h1></center>
|     </body>
|     </html>
|   GetRequest:
|     HTTP/1.1 301 Moved Permanently
|     Server: awselb/2.0
|     Date: Fri, 27 Dec 2024 14:55:25 GMT
|     Content-Type: text/html
|     Content-Length: 134
|     Connection: close
|     Location: https://frontend-row-traffic-laye-80c90e-1347733461.us-east-1.elb.amazonaws.com:443/
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     </body>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 301 Moved Permanently
|     Server: awselb/2.0
|     Date: Fri, 27 Dec 2024 14:55:27 GMT
|     Content-Type: text/html
|     Content-Length: 134
|     Connection: close
|     Location: https://frontend-row-traffic-laye-80c90e-1347733461.us-east-1.elb.amazonaws.com:443/
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     </body>
|     </html>
|   RPCCheck:
|     HTTP/1.1 400 Bad Request
```

```

[-] 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 following 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:HTTPRequest,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(HTS
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><t
SF:title>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"\r);

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:bystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 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 a35f64fce718ad27.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,
                  you can consult the following sources:
emarks:
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 Caribbean)
remarks:          http://www.lacnic.net/ whois.lacnic.net
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 containing 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 results
```

```
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 containing 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 that 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 the 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>
```

```
(kali㉿kali)-[~]
$ dmitry -p www.mercadolibre.com

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

HostIP:3.33.182.45
HostName:www.mercadolibre.com

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
```

- **Search for Email Addresses**

Command :

```
dmitry -e <target>
```

```
(kali㉿kali)-[~]
$ dmitry -e www.mercadolibre.com

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

HostIP:15.197.170.90
HostName:www.mercadolibre.com

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 results

All scans completed, exiting
```

### **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
esrc:             IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks:          For registration information,
                  you can consult the following sources:
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 Caribbean)
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
```

```
:   Trasgo 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)  
System
```

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
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/epp>

**NOTICE:** The expiration date displayed in this record is the date the  
 ownership of the domain name registration in the registry is  
 currently set to expire. This date does not necessarily reflect the expiration  
 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 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 to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database 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 containing 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 results
```

```
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
```



```
(kali㉿kali)-[~]
$ sudo apt-get install uniscan

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  golang-1.23 golang-1.23-doc golang-1.23-go golang-1.23-src openjdk-23-jre openjdk-23-jre-headless
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  uniscan
0 upgraded, 1 newly installed, 0 to remove and 1499 not upgraded.
Need to get 220 kB of archives.
After this operation, 1,257 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 uniscan all 6.3-0kali3 [220 kB]
Fetched 220 kB in 2s (113 kB/s)
Selecting previously unselected package uniscan.
(Reading database ... 442399 files and directories currently installed.)
Preparing to unpack .../uniscan_6.3-0kali3_all.deb ...
Unpacking uniscan (6.3-0kali3) ...
Setting up uniscan (6.3-0kali3) ...
Processing triggers for kali-menu (2024.4.0) ...
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
```

### Go to the Uniscan directory

Command :

```
cd Uniscan
```

### Usage:

- Basic Idea:

Command :

```
sudo uniscan -h
```

```
(kali㉿kali)-[~]
$ sudo uniscan -h

#####
# Uniscan project      #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

OPTIONS:
  -h      help
  -u      <url> example: https://www.example.com/
  -f      <file> list of url's
  -b      Uniscan go to background
  -q      Enable Directory checks
  -w      Enable File checks
  -e      Enable robots.txt and sitemap.xml check
  -d      Enable Dynamic checks
  -s      Enable Static checks
  -r      Enable Stress checks
  -i      <dork> Bing search
  -o      <dork> Google search
  -g      Web fingerprint
  -j      Server fingerprint

usage:
[1] perl ./uniscan.pl -u http://www.example.com/ -qweds
[2] perl ./uniscan.pl -f sites.txt -bqweds
[3] perl ./uniscan.pl -i uniscan
[4] perl ./uniscan.pl -i "ip:xxx.xxx.xxx.xxx"
[5] perl ./uniscan.pl -o "inurl:test"
[6] perl ./uniscan.pl -u https://www.example.com/ -r
```

#### 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
```

```
(kali㉿kali)-[~]
└─$ git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
cd sqlmap-dev
python sqlmap.py

Cloning into 'sqlmap-dev'...
remote: Enumerating objects: 733, done.
remote: Counting objects: 100% (733/733), done.
remote: Compressing objects: 100% (487/487), done.
remote: Total 733 (delta 249), reused 505 (delta 233), pack-reused 0 (from 0)
Receiving objects: 100% (733/733), 7.01 MiB | 4.74 MiB/s, done.
Resolving deltas: 100% (249/249), done.

  H
  |
  +-- [ ] {1.8.12.2#dev}
    +-- [ ] https://sqlmap.org

Usage: python sqlmap.py [options]

sqlmap.py: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list-tampers or --dependencies). Use -h for basic and -hh for advanced help
```

### Usage:

Basic SQL Injection Scan:

Command :

```
python sqlmap.py -u <URL>
```

```
(kali㉿kali)-[~/sqlmap-dev]
└─$ python sqlmap.py -u http://www.mercadolibre.com

  H
  |
  +-- [ ] {1.8.12.2#dev}
    +-- [ ] https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 08:47:49 /2024-12-31

[08:47:49] [INFO] testing connection to the target URL
[08:47:49] [CRITICAL] WAF/IPS identified as 'AWS WAF (Amazon)'
[08:47:49] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[08:47:49] [INFO] checking if the target is protected by some kind of WAF/IPS
[08:47:50] [INFO] testing if the target URL content is stable
[08:47:50] [INFO] target URL content is stable
[08:47:50] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--crawl=2'
[08:47:50] [WARNING] HTTP error codes detected during run: 403 (Forbidden) - 3 times

[*] ending @ 08:47:50 /2024-12-31/
```

#### Custom Parameters:

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

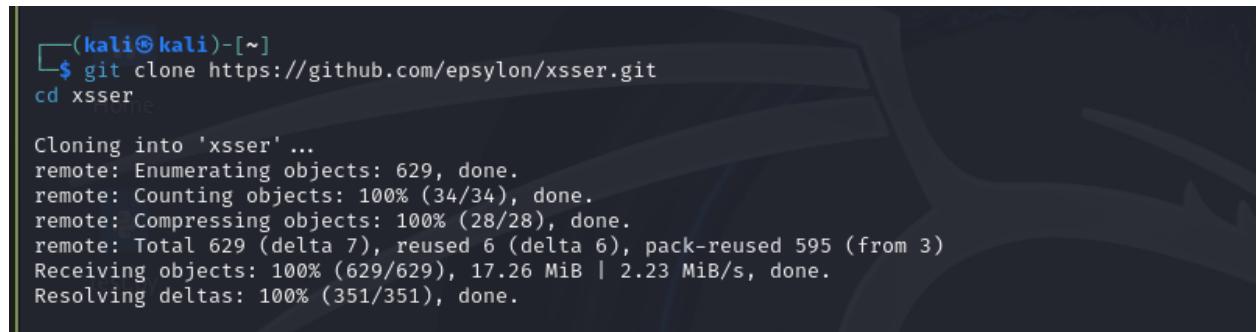
## What is Xsser ?

- 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
```



```
(kali㉿kali)-[~]
└─$ git clone https://github.com/epsylon/xsser.git
cd xsser
Cloning into 'xsser' ...
remote: Enumerating objects: 629, done.
remote: Counting objects: 100% (34/34), done.
remote: Compressing objects: 100% (28/28), done.
remote: Total 629 (delta 7), reused 6 (delta 6), pack-reused 595 (from 3)
Receiving objects: 100% (629/629), 17.26 MiB | 2.23 MiB/s, done.
Resolving deltas: 100% (351/351), done.
```

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] [09.02]

[*] 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**

```
└──(kali㉿kali)-[~]
$ wpscan --version
/usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1477:in `rescue in block in activate_dependencies': Could not find 'struct' (>= 0.6) among 242 total gem(s) (Gem::MissingSpecError)
Checked in 'GEM_PATH=/home/kali/.local/share/gem/ruby/3.1.0:/var/lib/gems/3.1.0:/usr/local/lib/ruby/gems/3.1.0:/usr/lib/ruby/gems/3.1.0:/usr/share/rubygems-integration/3.1.0:/usr/share/rubygems-integration/all:/usr/lib/x86_64-linux-gnu/rubygems-integration/3.1.0' at: /usr/share/rubygems-integration/all/specifications/opt_parse_validator-1.10.1.gemspec, execute `gem env` for more information
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1474:in `block in activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1463:in `activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1445:in `activate'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1481:in `block in activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1463:in `activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1445:in `activate'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1481:in `block in activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1463:in `activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1445:in `activate'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1481:in `block in activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1463:in `activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1445:in `activate'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1481:in `block in activate_bin_path'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:284:in `synchronize'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:284:in `activate_bin_path'
    from /usr/bin/wpscan:25:in `main'
from /usr/bin/wpscan:25:in `<main>'

/usr/lib/ruby/vendor_ruby/rubygems/specification.rb:17:in `to_gems': Could not find 'struct' (>= 0.6) - did find: [struct-0.3.2] (Gem::MissingSpecVersionError)
Checked in 'GEM_PATH=/home/kali/.local/share/gem/ruby/3.1.0:/var/lib/gems/3.1.0:/usr/local/lib/ruby/gems/3.1.0:/usr/lib/ruby/gems/3.1.0:/usr/share/rubygems-integration/3.1.0:/usr/share/rubygems-integration/all:/usr/lib/x86_64-linux-gnu/rubygems-integration/3.1.0' , execute `gem env` for more information
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1475:in `block in activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1463:in `activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1445:in `activate'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1481:in `block in activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1463:in `activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1445:in `activate'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1481:in `block in activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1463:in `activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1445:in `activate'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1481:in `block in activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1463:in `activate_dependencies'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1445:in `activate'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:1481:in `block in activate_bin_path'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:284:in `synchronize'
    from /usr/lib/ruby/vendor_ruby/rubygems/specification.rb:284:in `activate_bin_path'
    from /usr/bin/wpscan:25:in `<main>'

└──(kali㉿kali)-[~]
```

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

#### How It Works:

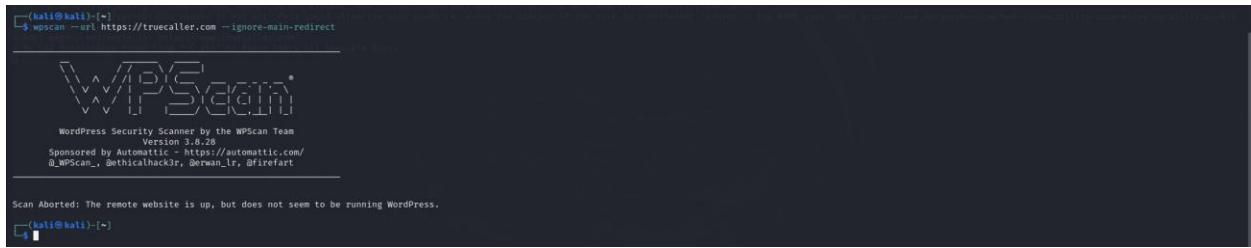
- **WPScan** is a tool specifically designed for scanning WordPress websites for vulnerabilities.
- By running **wpscan --url https://test.com**, you're asking WPScan to analyze the site and determine if it is powered by **WordPress**.
  - If the website is running **WordPress**, WPScan will try to identify 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



A terminal window showing the command \$ wpSCAN --url https://truecaller.com --ignore-main-redirect. The output includes the WPScan logo, version information (Version 3.8.28), and a message stating "Scan Aborted: The remote website is up, but does not seem to be running WordPress."

```
(kali㉿kali)-[~] $ wpSCAN --url https://truecaller.com --ignore-main-redirect
  _   _ 
 / \ / \
W P S C A N
  \ \ \ 
Wordpress Security Scanner by the WPScan Team
  Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Scan Aborted: The remote website is up, but does not seem to be running WordPress.
```

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