

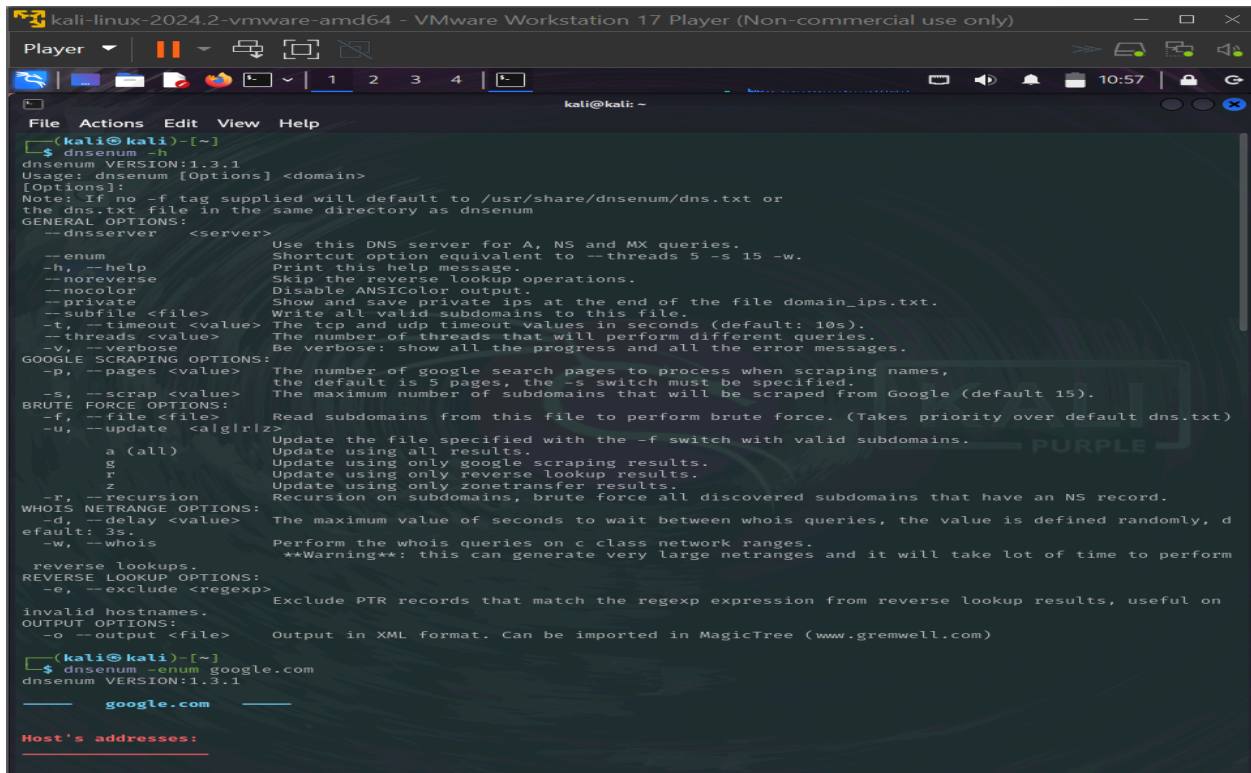
# GATHERING DNS INFO WITH DNSENUM

Tools: KALI LINUX

Site: GOOGLE.COM

**dnsenum** is a DNS enumeration tool widely used for information gathering and penetration testing. It is written in Perl and is commonly included in security distributions like Kali Linux. Its primary purpose is to extract valuable information about a domain, such as subdomains, host records, and more.

Input from kali:

A screenshot of a Kali Linux terminal window titled "kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)". The terminal shows the command "dnsenum -h" being executed, which displays the help text for the tool. The help text includes the version (1.3.1), usage instructions, and a list of options categorized into General, Google Scraping, Brute Force, and Reverse Lookups. At the bottom, the command "dnsenum -enum google.com" is entered, and the output "Host's addresses:" is visible.

```
kali@kali:~$ dnsenum -h
dnsenum VERSION:1.3.1
Usage: dnsenum [Options] <domain>
[Options]:
Note: If no -f tag supplied will default to /usr/share/dnsenum/dns.txt or
the dns.txt file in the same directory as dnsenum
GENERAL OPTIONS:
--dnsserver <server>    Use this DNS server for A, NS and MX queries.
--enum                  Shortcut option equivalent to --threads 5 -s 15 -w.
-h, --help              Print this help message.
--noreverse             Skip the reverse lookup operations.
--nocolor               Disable ANSIColor output.
--private <file>        Show and save private ips at the end of the file domain_ips.txt.
--subfile <file>         Write all valid subdomains to this file.
-t, --timeout <value>   The tcp and udp timeout values in seconds (default: 10s).
--threads <value>        The number of threads that will perform different queries.
-v, --verbose           Be verbose: show all the progress and all the error messages.
GOOGLE SCRAPING OPTIONS:
-p, --pages <value>     The number of google search pages to process when scraping names,
                        the default is 5 pages, the -s switch must be specified.
-s, --scrap <value>     The maximum number of subdomains that will be scraped from Google (default 15).
BRUTE FORCE OPTIONS:
-f, --file <file>       Read subdomains from this file to perform brute force. (Takes priority over default dns.txt)
-u, --update <algrlz>   Update the file specified with the -f switch with valid subdomains.
                        a (all)      Update using all results.
                        g             Update using only google scraping results.
                        r             Update using only reverse lookup results.
                        z             Update using only zonetransfer results.
-r, --recursion          Recursion on subdomains, brute force all discovered subdomains that have an NS record.
WHOIS NETRANGE OPTIONS:
-d, --delay <value>     The maximum value of seconds to wait between whois queries, the value is defined randomly, d
                        efault: 3s.
-w, --whois              Perform the whois queries on c class network ranges.
                        **Warning**: this can generate very large netranges and it will take lot of time to perform
reverse lookups.
REVERSE LOOKUP OPTIONS:
-e, --exclude <regex>   Exclude PTR records that match the regex expression from reverse lookup results, useful on
invalid hostnames.
OUTPUT OPTIONS:
-o, --output <file>     Output in XML format. Can be imported in MagicTree (www.gremwell.com)

(kali@kali)~$ dnsenum -enum google.com
dnsenum VERSION:1.3.1

google.com

Host's addresses:
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
kali@kali: ~

google.com.                250      IN      A       142.250.200.206

Name Servers:
ns2.google.com.            345431   IN      A       216.239.34.10
ns4.google.com.            297926   IN      A       216.239.38.10
ns1.google.com.            345431   IN      A       216.239.32.10
ns3.google.com.            325269   IN      A       216.239.36.10

Mail (MX) Servers:
smtp.google.com.           215      IN      A       173.194.69.27
smtp.google.com.           215      IN      A       173.194.79.26
smtp.google.com.           215      IN      A       173.194.79.27
smtp.google.com.           215      IN      A       108.177.96.27

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for google.com on ns3.google.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for google.com on ns4.google.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for google.com on ns1.google.com ...
AXFR record query failed: corrupt packet
Trying Zone Transfer for google.com on ns2.google.com ...
AXFR record query failed: corrupt packet

Scraping google.com subdomains from Google:

___ Google search page: 1 ___
support
___ Google search page: 2 ___
support
___ Google search page: 3 ___
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
kali@kali: ~

___ Google search page: 3 ___
support
___ Google search page: 4 ___
support
___ Google search page: 5 ___
support

Google Results:
support.google.com.        66       IN      A       216.58.223.238

Brute forcing with /usr/share/dnsenum/dns.txt:
about.google.com.         300      IN      CNAME   www3.l.google.com.
www3.l.google.com.        216      IN      A       142.251.37.206
accounts.google.com.      222      IN      A       74.125.128.84
admin.google.com.         273      IN      A       172.217.19.142
ads.google.com.           208      IN      A       142.251.37.238
ap.google.com.            300      IN      CNAME   www2.l.google.com.
www2.l.google.com.        274      IN      A       142.251.37.36
apps.google.com.          300      IN      CNAME   www3.l.google.com.
www3.l.google.com.        208      IN      A       142.251.37.206
archive.google.com.       300      IN      A       172.217.171.238
asia.google.com.          300      IN      A       216.58.223.228
america.google.com.       295      IN      CNAME   www3.l.google.com.
www3.l.google.com.        205      IN      A       142.251.37.206
blog.google.com.          300      IN      CNAME   www.blogger.com.
www.blogger.com.          224      IN      CNAME   blogger.l.google.com.
blogger.l.google.com.     33       IN      A       172.217.171.233
channel.google.com.       300      IN      A       142.250.203.238
d.google.com.             300      IN      CNAME   www3.l.google.com.
www3.l.google.com.        184      IN      A       142.251.37.206
directory.google.com.     300      IN      CNAME   www3.l.google.com.
www3.l.google.com.        182      IN      A       142.251.37.206
dns.google.com.           756      IN      A       8.8.8.8
dns.google.com.           756      IN      A       8.8.4.4
elections.google.com.     300      IN      A       172.217.21.14
environment.google.com.   300      IN      A       142.250.200.238
europe.google.com.        295      IN      A       216.58.223.196
finance.google.com.       300      IN      CNAME   www3.l.google.com.
www3.l.google.com.        156      IN      A       142.251.37.206
health.google.com.        300      IN      A       142.250.201.14
issuetracker.google.com.  300      IN      A       142.250.200.238
jobs.google.com.          300      IN      CNAME   www3.l.google.com.
www3.l.google.com.        135      IN      A       142.251.37.206
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player 1 2 3 4

kali@kali: ~
File Actions Edit View Help
└─$ dnsenum -f list.txt -r google.com
dnsenum VERSION:1.3.1

┌─── google.com ───┐

Host's addresses:
┌──────────┴──────────┐
google.com.          201      IN      A       142.250.200.206

Name Servers:
┌──────────┴──────────┐
ns2.google.com.      345570  IN      A       216.239.34.10
ns4.google.com.      297574  IN      A       216.239.38.10
ns1.google.com.      345569  IN      A       216.239.32.10
ns3.google.com.      324917  IN      A       216.239.36.10

Mail (MX) Servers:
┌──────────┴──────────┐
smtp.google.com.     231     IN      A       142.251.18.27
smtp.google.com.     231     IN      A       142.251.18.26
smtp.google.com.     231     IN      A       142.250.153.26
smtp.google.com.     231     IN      A       142.250.153.27
smtp.google.com.     231     IN      A       142.250.145.27

Trying Zone Transfers and getting Bind Versions:
┌──────────┴──────────┐
Trying Zone Transfer for google.com on ns3.google.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for google.com on ns1.google.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for google.com on ns4.google.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for google.com on ns2.google.com ...
AXFR record query failed: corrupt packet

Brute forcing with list.txt:
┌──────────┴──────────┐
Error: make sure that the file list.txt exists and has a size greater than zero.

(kali@kali)-[~]
└─$
```

Here we would be using DNSENUM to gather information and test some of its uses. It comes pre installed in kali so we go on and check the help option with this command : `dnsenum -h`

## Comprehensive DNS Enumeration Using dnsenum

### Step 1: Performing a Comprehensive DNS Enumeration

To perform a comprehensive information-gathering scan on the domain `google.com`, use the following command:

```
dnsenum --enum google.com
```

This command will:

1. Gather information such as:
  - Host IP addresses
  - Name servers (NS)
  - Mail servers (MX)
  - Subdomains
2. Attempt **domain takeovers**, which could reveal misconfigurations or unclaimed DNS records.
3. Perform **automatic brute-forcing** of common subdomains, such as:
  - `admin.google.com`
  - `mail.google.com`
  - `webmail.google.com`

This provides insights into the target's DNS infrastructure and expands the attack surface.

### Step 2: Brute Force Search for Subdomains Using a Custom File

To perform a brute force search for subdomains with a custom list of keywords, follow these steps:

#### Create a Wordlist File

Create a file named `list.txt` and include subdomain keywords that you want to target. Example:

Copy code

mail

email

imap

pop3

smtp

webmail

admin

support

clients

secure

www

ftp

ldap

1.

## Run the Command

Use the following `dnsenum` command to perform the brute force search:

```
dnsenum -f list.txt -r google.com
```

2.

- `-f list.txt`: Specifies the custom wordlist file.
- `-r`: Enables reverse lookups on IP ranges discovered during the scan.

---

## Benefits of These Commands

- Reveals detailed DNS information, such as:
  - Subdomains
  - MX and NS records
- Identifies potential misconfigurations or vulnerabilities.

- Expands the attack surface by finding less obvious subdomains.
- Custom brute force allows you to focus on subdomains relevant to your objectives.

#### **Additional Tips**

- Use a comprehensive wordlist for brute-forcing to improve results. You can find or generate large wordlists with DNS-focused keywords.
- Combine this scan with other DNS tools for cross-validation of results.
- Only use these techniques on targets you have permission to assess to avoid legal or ethical issues.