

## Lab 28 — Gathering DNS information with dnsenum

### ✓ Objective

→ Learn how to gather DNS information on a target using the `dnsenum` tool.

### ✓ Why? (Purpose)

→ DNS enumeration helps attackers and defenders collect valuable data about a target:

- Usernames
- Computer names
- IP addresses
- Subdomains
- Mail servers
- Name servers
- Possible domain takeovers  
→ In other words, it maps out the attack surface.

### ✓ Lab Environment

→ Kali Linux (can be run on a Virtual Machine)

---

## What is dnsenum?

- **dnsenum** is a program (a script) you run in Kali Linux.
- Its job is to find out information about a website or domain, like:
  - Its servers (computers that run the site)
  - The IP addresses of these servers
  - Email servers

- Subdomains (for example, [login.google.com](https://login.google.com), [mail.google.com](https://mail.google.com))
- Basically, anything connected to the domain's DNS records

Think of it like a **detective** who tries to find out everything about a website's infrastructure.

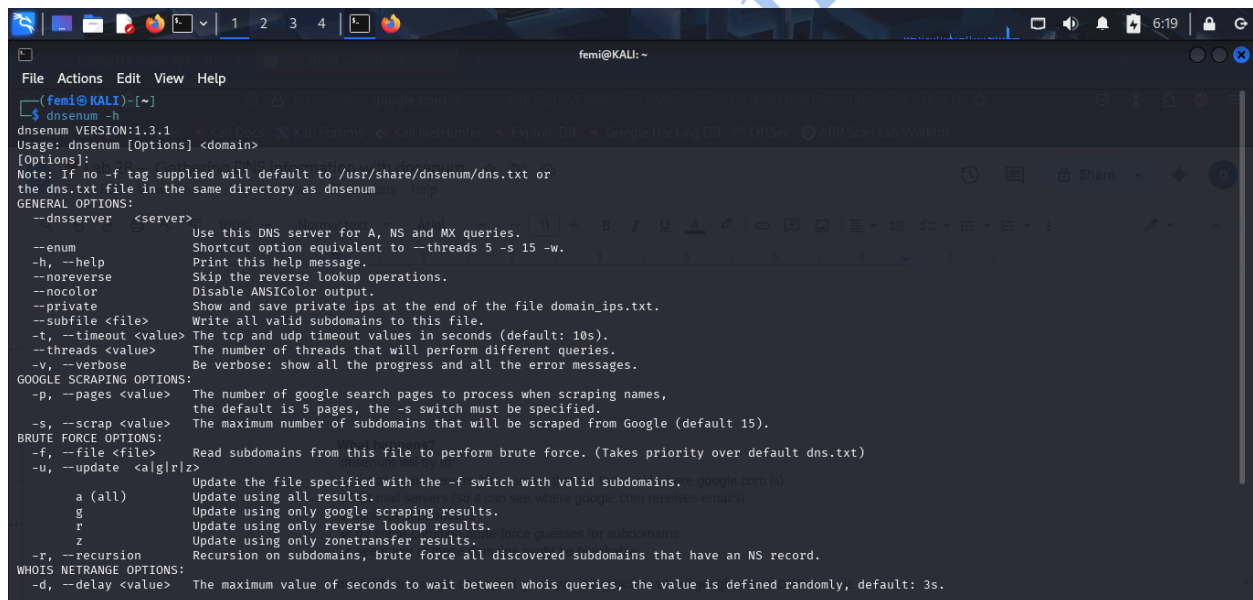
---

## Step-by-Step, Explained from Scratch

### Task 1 — First check if the tool works

In Kali, open your terminal and type:

`dnsenum -h`



```
femi@KALI: ~  
File Actions Edit View Help  
(femi@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 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 <alg|rz> 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, default: 3s.
```

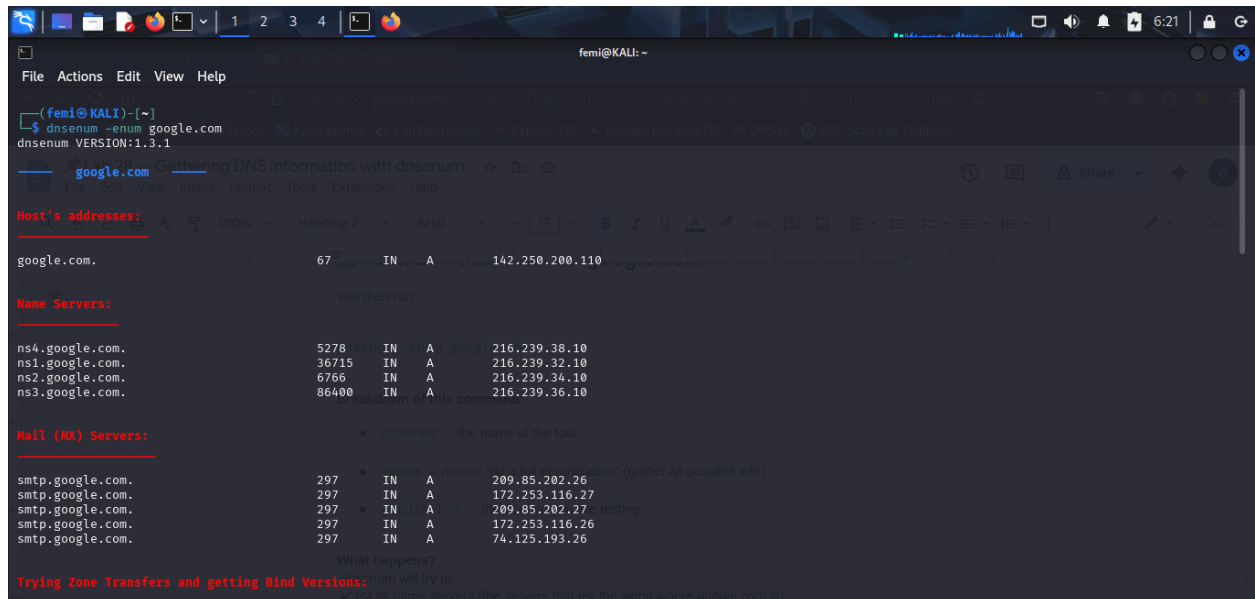
This just shows you the **help** screen of dnsenum, explaining the options you can use. Nothing scary — it's like asking the tool: “What can you do?”

---

## ✓ Task 1 — Full scan on google.com

You then run:

`dnsenum -enum google.com`



```
femi@KALI: ~  
$ dnsenum -enum google.com  
dnsenum VERSION:1.3.1  
Gathering DNS information with dnsenum  
Host's addresses:  
google.com. 67 IN A 142.250.200.110  
Name Servers:  
ns4.google.com. 5278 IN A 216.239.38.10  
ns1.google.com. 36715 IN A 216.239.32.10  
ns2.google.com. 6766 IN A 216.239.34.10  
ns3.google.com. 86400 IN A 216.239.36.10  
Mail (MX) Servers:  
smtp.google.com. 297 IN A 209.85.202.26  
smtp.google.com. 297 IN A 172.253.116.27  
smtp.google.com. 297 IN A 209.85.202.27  
smtp.google.com. 297 IN A 172.253.116.26  
smtp.google.com. 297 IN A 74.125.193.26  
Trying Zone Transfers and getting Bind Versions:  
perhaps Google is blocking our queries.  
Check manually.  
Brute forcing with /usr/share/dnsenum/dns.txt:  
about.google.com. 300 IN CNAME www3.l.google.com.  
www3.l.google.com. 286 IN A 142.250.200.142  
accounts.google.com. 65 IN A 172.253.116.84  
admin.google.com. 300 IN A 142.250.201.78  
ads.google.com. 259 IN A 216.58.223.238  
america.google.com. 300 IN CNAME www3.l.google.com.  
www3.l.google.com. 283 IN A 142.250.200.142  
apps.google.com. 300 IN CNAME www3.l.google.com.  
www3.l.google.com. 282 IN A 142.250.200.142  
ap.google.com. 300 IN CNAME www2.l.google.com.  
www2.l.google.com. 99 IN A 142.250.200.68  
archive.google.com. 300 IN A 172.217.168.174  
asia.google.com. 300 IN A 216.58.223.228  
blog.google.com. 300 IN CNAME www.blogger.com.  
www.blogger.com. 220 IN CNAME blogger.l.google.com.  
blogger.l.google.com. 54 IN A 216.58.223.233  
channel.google.com. 300 IN A 216.58.223.238  
d.google.com. 300 IN CNAME www3.l.google.com.  
www3.l.google.com. 275 IN A 142.250.200.142  
dns.google.com. 561 IN A 8.8.4.4  
dns.google.com. 561 IN A 8.8.8.8  
directory.google.com. 300 IN CNAME www3.l.google.com.  
www3.l.google.com. 274 IN A 142.250.200.142
```

Breakdown of this command:

- `dnsenum` → the name of the tool

- `-enum` → means “do a full enumeration” (gather *all* possible info)
- `google.com` → the domain you are testing

## What happens?

dnsenum will try to:

- ✓ list all name servers (the servers that tell the world where google.com is)
- ✓ list mail servers (so it can see where google.com receives emails)
- ✓ look for subdomains
- ✓ try some common brute-force guesses for subdomains
- ✓ see if any of these domains might be hijackable

**In short:** one single command gives you a *big picture* about google.com’s DNS records.

## ✓ Task 2 — Using a custom wordlist

If you want to **brute-force** for subdomains beyond the default ones, you can use a wordlist (a text file containing possible subdomain names).

For example:

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

```
femi@KALI: ~
$ dnsenum -f list.txt -r google.com
dnsenum VERSION:1.3.1

google.com
Gathering DNS information with dnsenum

Host's addresses:
google.com. 181 IN A 142.250.184.14

Name Servers:
ns1.google.com. 41723 IN A 216.239.32.10
ns2.google.com. 10533 IN A 216.239.34.10
ns3.google.com. 86400 IN A 216.239.36.10
ns4.google.com. 64495 IN A 216.239.38.10

Mail (MX) Servers:
smtp.google.com. 297 IN A 209.85.203.27
smtp.google.com. 297 IN A 209.85.202.27
smtp.google.com. 297 IN A 209.85.202.26
smtp.google.com. 297 IN A 74.125.193.26
smtp.google.com. 297 IN A 209.85.203.26

Trying Zone Transfers and getting Bind Versions:

```

## Breakdown:

- `-f list.txt` → tells dnsenum to use your own file of subdomain guesses
- `-r` → means it will recursively try them
- `google.com` → still your target

Femi lana