Dnsenum

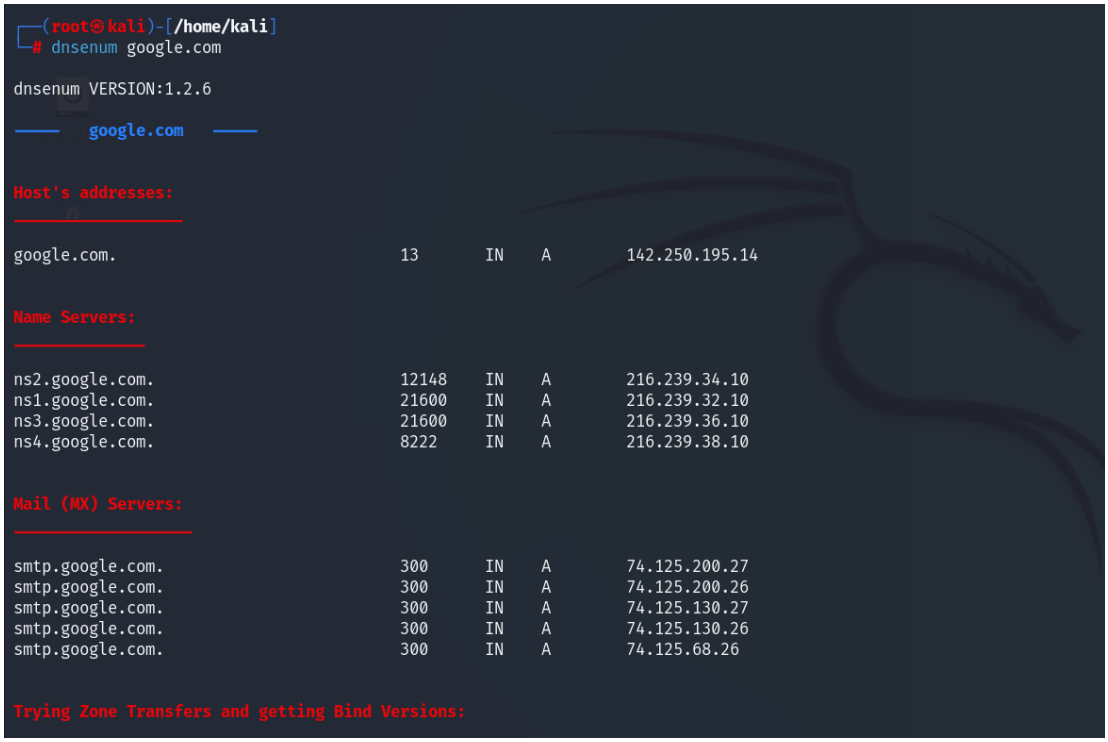
DNSenum is a DNS enumeration tool that helps in discovering DNS information about a target domain. It is useful for penetration testers and security researchers to gather information such as subdomains, domain information, and more.

Usecase: - In penetration testing, the first phase is often reconnaissance, where the goal is to gather as much information as possible about the target. DNSenum helps by providing detailed DNS information, which can reveal:

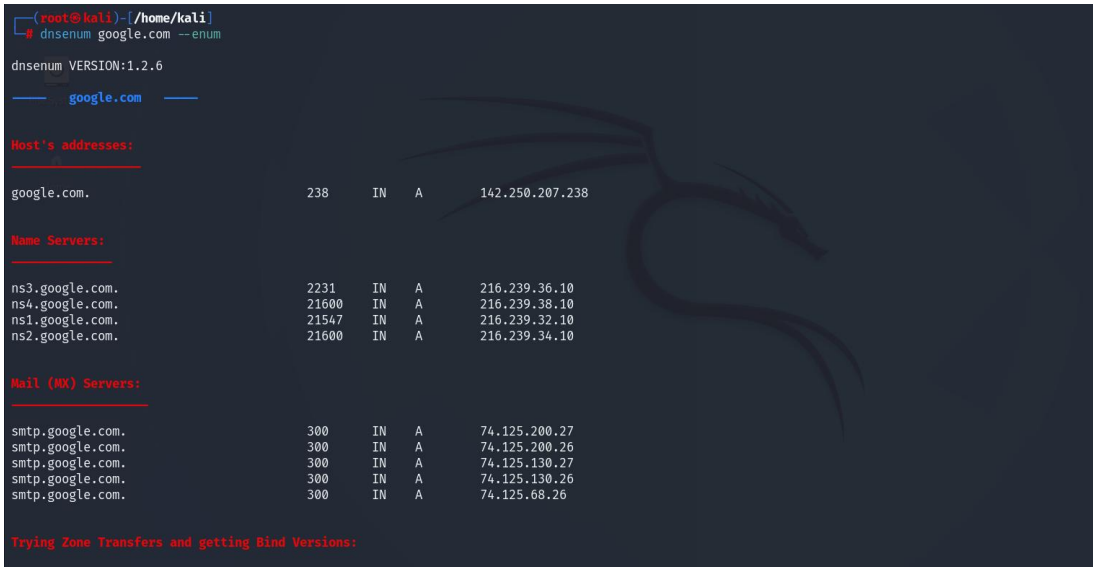
- Subdomains and hidden services
- Mail servers and their configurations
- Potential attack vectors through DNS misconfigurations or weak records
- Infrastructure details through WHOIS information

Examples: -

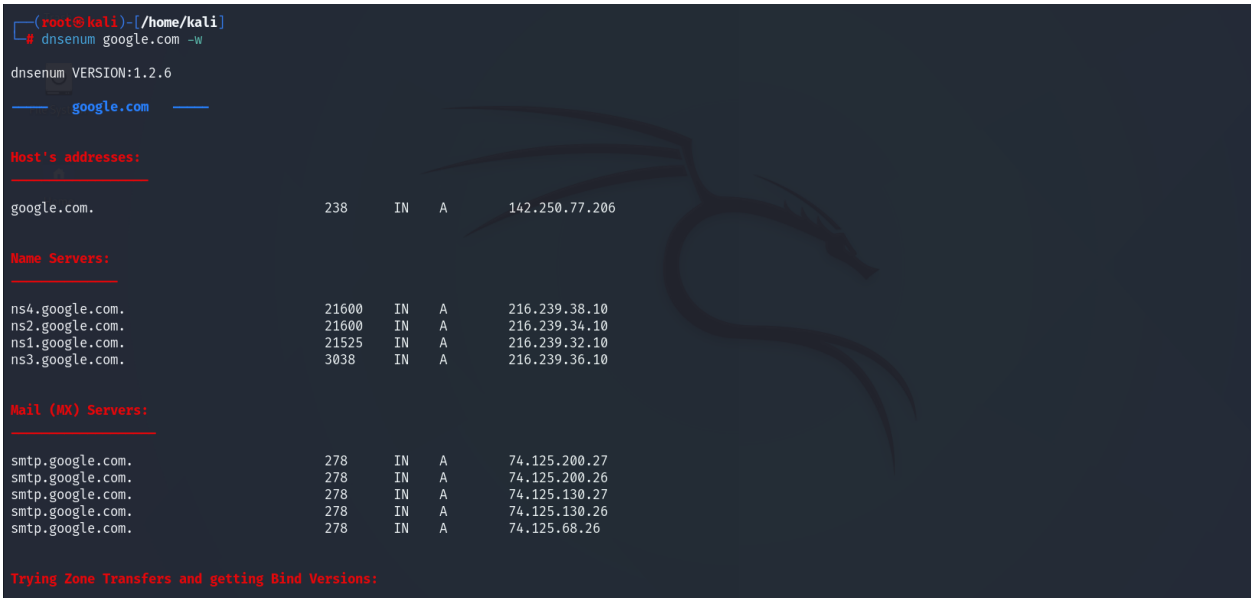
1. To perform a basic enumeration of a domain



2. You can use DNSenum to brute-force subdomains using a dictionary file. The tool comes with a default dictionary

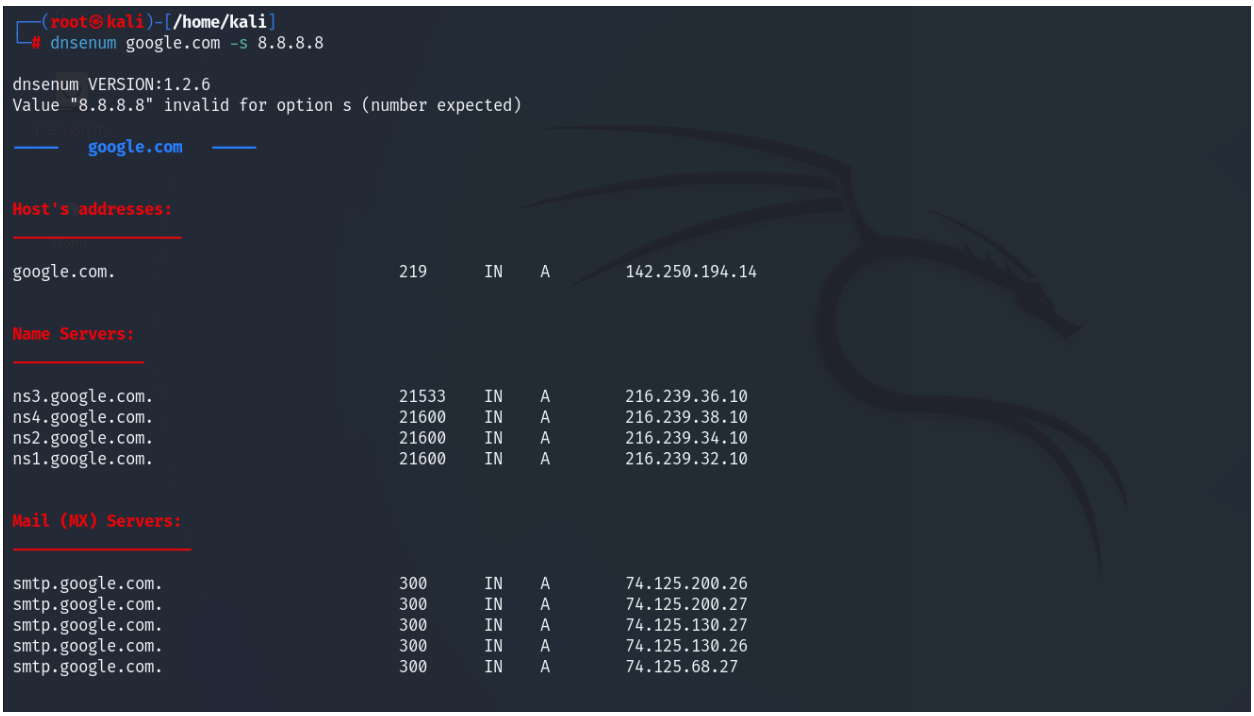


3. To retrieve WHOIS information about a domain, you can use the -w flag



```
┌──(root㉿kali)-[/home/kali]
└─# dnsenum google.com -w

dnsenum VERSION:1.2.6

-----   google.com   -----


Host's addresses:
__________________

google.com.                              238      IN    A        142.250.77.206


Name Servers:
______________

ns4.google.com.                          21600    IN    A        216.239.38.10
ns2.google.com.                          21600    IN    A        216.239.34.10
ns1.google.com.                          21525    IN    A        216.239.32.10
ns3.google.com.                          3038     IN    A        216.239.36.10


Mail (MX) Servers:
___________________

smtp.google.com.                         278      IN    A        74.125.200.27
smtp.google.com.                         278      IN    A        74.125.200.26
smtp.google.com.                         278      IN    A        74.125.130.27
smtp.google.com.                         278      IN    A        74.125.130.26
smtp.google.com.                         278      IN    A        74.125.68.26


Trying Zone Transfers and getting Bind Versions:
```

4. You can specify which DNS servers to use for the queries using the -s flag:



```
┌──(root㉿kali)-[/home/kali]
└─# dnsenum google.com -s 8.8.8.8

dnsenum VERSION:1.2.6
Value "8.8.8.8" invalid for option s (number expected)

-----   google.com   -----


Host's addresses:
__________________

google.com.                              219      IN    A        142.250.194.14


Name Servers:
______________

ns3.google.com.                          21533    IN    A        216.239.36.10
ns4.google.com.                          21600    IN    A        216.239.38.10
ns2.google.com.                          21600    IN    A        216.239.34.10
ns1.google.com.                          21600    IN    A        216.239.32.10


Mail (MX) Servers:
___________________

smtp.google.com.                         300      IN    A        74.125.200.26
smtp.google.com.                         300      IN    A        74.125.200.27
smtp.google.com.                         300      IN    A        74.125.130.27
smtp.google.com.                         300      IN    A        74.125.130.26
smtp.google.com.                         300      IN    A        74.125.68.27
```