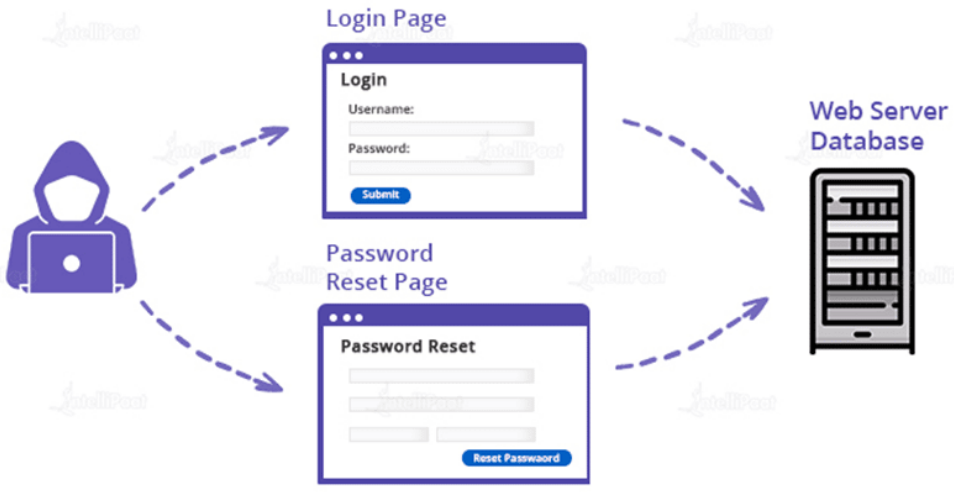
GATHERING DOMAIN INFORMATION USING DNS ENUMERATION TOOL

WHAT IS ENUMERATION

Enumeration is the process of obtaining information from a system, such as user identities, machine names, network resources, shares, and services. The attacker establishes an active connection to the system at this point and launches directed queries to learn more about the target. The information acquired is then utilized to pinpoint any weaknesses in system security that can be exploited during the system acquiring phase.

Enumeration is also called as Information Gathering Phase which is the first phase where hackers try to gather information and try to establish an active connection with the devices or systems. Attackers often evaluate attack vectors by using the output of the enumeration to exploit the system further. Additionally, malicious actors utilize penetration testing tools to gather data on network services and shares, IP routing tables, hostnames, DNS details, SNMP information, and users on database records.

To collect usernames, hostnames, IP addresses, passwords, configurations, and other information, enumeration is used. Hackers control the objective framework once a working connection has been established with the objective host. At that time, they steal personal information and data. Additionally, aggressors have occasionally been found to modify how the objective frameworks are set up. The information or data that the attacker will have access to depends on how the connection is set up to the host.



WHAT IS DNS ENUMERATION ?

Finding every DNS server and its accompanying entries for an organization is known as DNS enumeration. A map or an address book is analogous to DNS.

The process of translating an IP address (192.111.1.120) to the name www.example.com and back is actually similar to that of a distributed database.

Before launching an attack, DNS enumeration is performed to learn as much as possible about your target. DNS servers can provide details about prospective target systems, like usernames, machine names, and IP addresses. To find a lot of data, DNS enumeration is performed. Numerous sorts of data related to a domain are frequently stored in the DNS system.

TECHNIQUES USED FOR ENUMERATION

- User names can be extracted using email IDs
- Information can be retrieved using the default password
- Active Directory using brute force
- Using SNMP, extract user names.
- Windows user groups can be extracted
- Utilizing DNS Zone transfer, more data

ADVANTAGES OF ENUMERATION

- Enumeration is important because it methodically gathers information.
- This makes it possible for pentesters to fully inspect the system.
- In the enumeration stage of ethical hacking the pentesters gather data regarding the weak links.

DISADVANTAGES OF ENUMERATION

- They are typically simple to find and simple to take advantage of.
- They are hazardous because they frequently make it possible for attackers to fully control the software and steal the data.

In this Exercise, We will gather as much as possible about domain using DNSenum Tool.

DNSenum

Dnsenum is a multithreaded perl script to enumerate DNS information of a domain and to discover non-contiguous ip blocks. The main purpose of Dnsenum is to gather as much information as possible about a domain. The program currently performs the following operations:

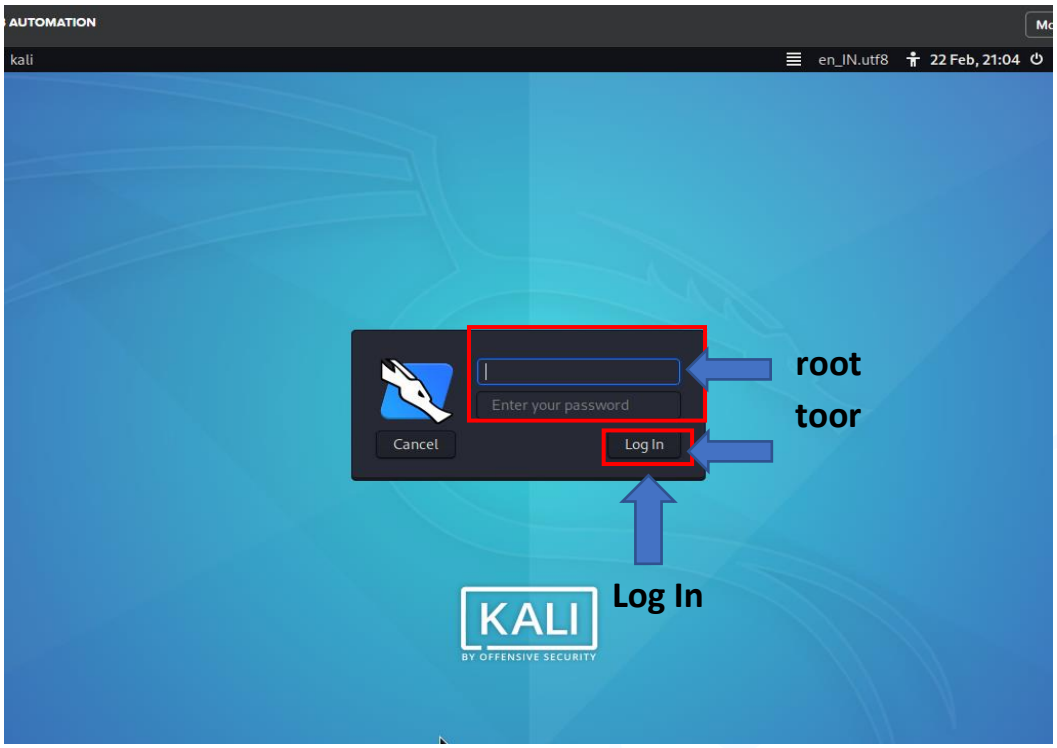
- Get the host's addresses (A record).
- Get the namservers (threaded).
- Get the MX record (threaded).
- Perform axfr queries on nameservers and get BIND versions(threaded).
- Get extra names and subdomains via google scraping (google query = "allinurl: -www site:domain").
- Brute force subdomains from file, can also perform recursion on subdomain that have NS records (all threaded).
- Calculate C class domain network ranges and perform whois queries on them (threaded).
- Perform reverse lookups on netranges (C class or/and whois netranges) (threaded).
- Write to domain_ips.txt file ip-blocks.

This program is useful for pen testers, ethical hackers and forensics experts. It can also be used for security tests.

Guided Exercise

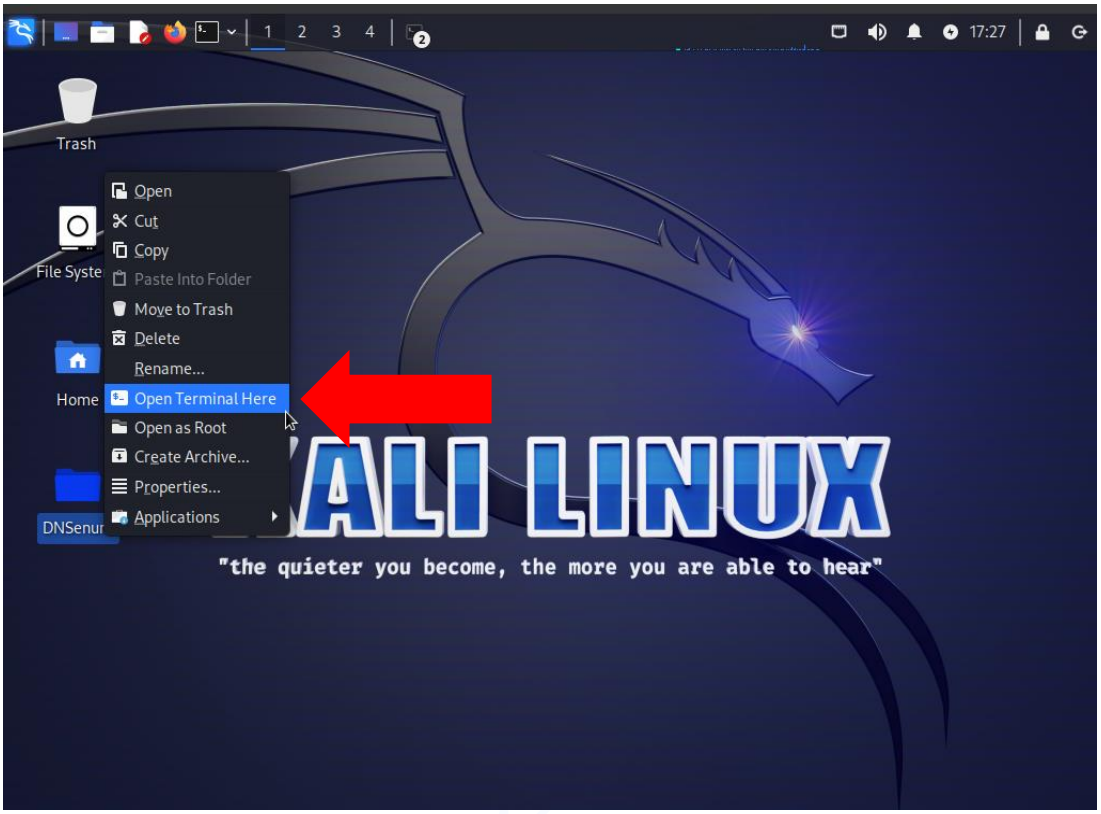
Step to Perform this Exercise

1. Connect to the kali Linux machine, created by you, using the RDP protocol. Kali Linux machine is being used as Attacker's machine.
2. When prompted for the username and password, enter **root** as username and **toor** as password. The root is the administrator user of the machine.

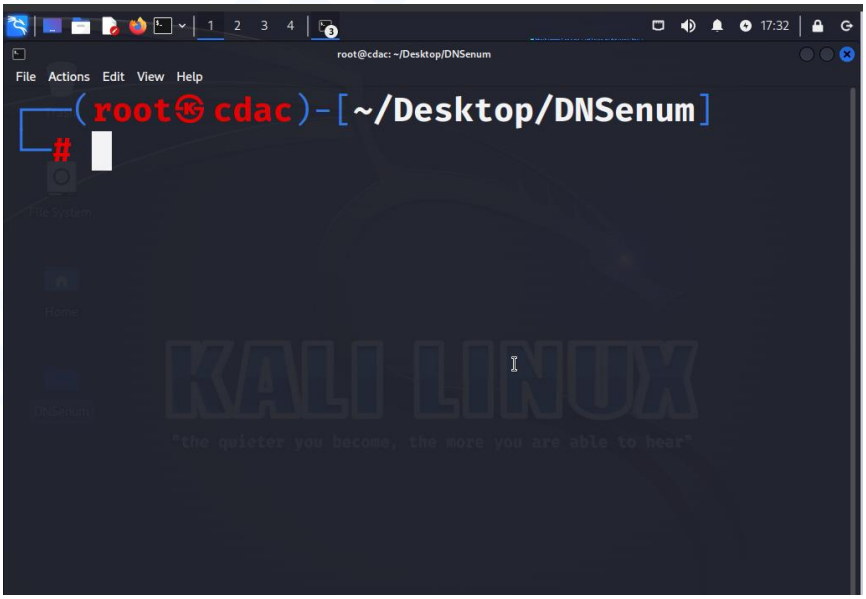


Once you successfully login in, you will see a screen like this. Here you can see one folder named as **DNSenum**, double click on the folder to open it

3. Now Right Click on the folder **DNSenum** and choose the option of **Open Terminal Here**

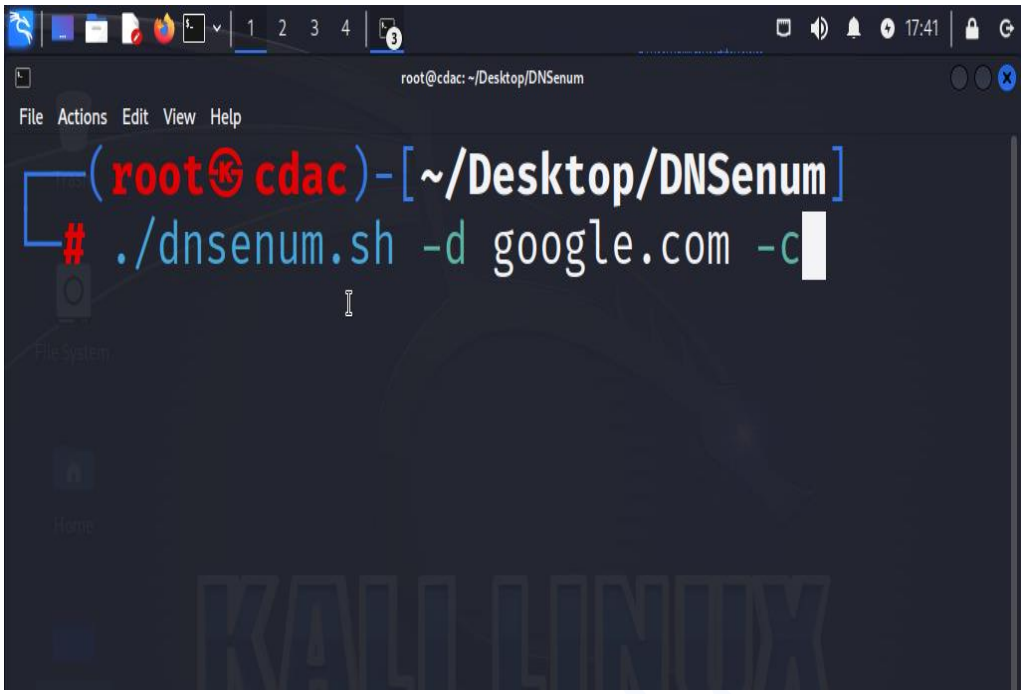


A Screen like this will Open.

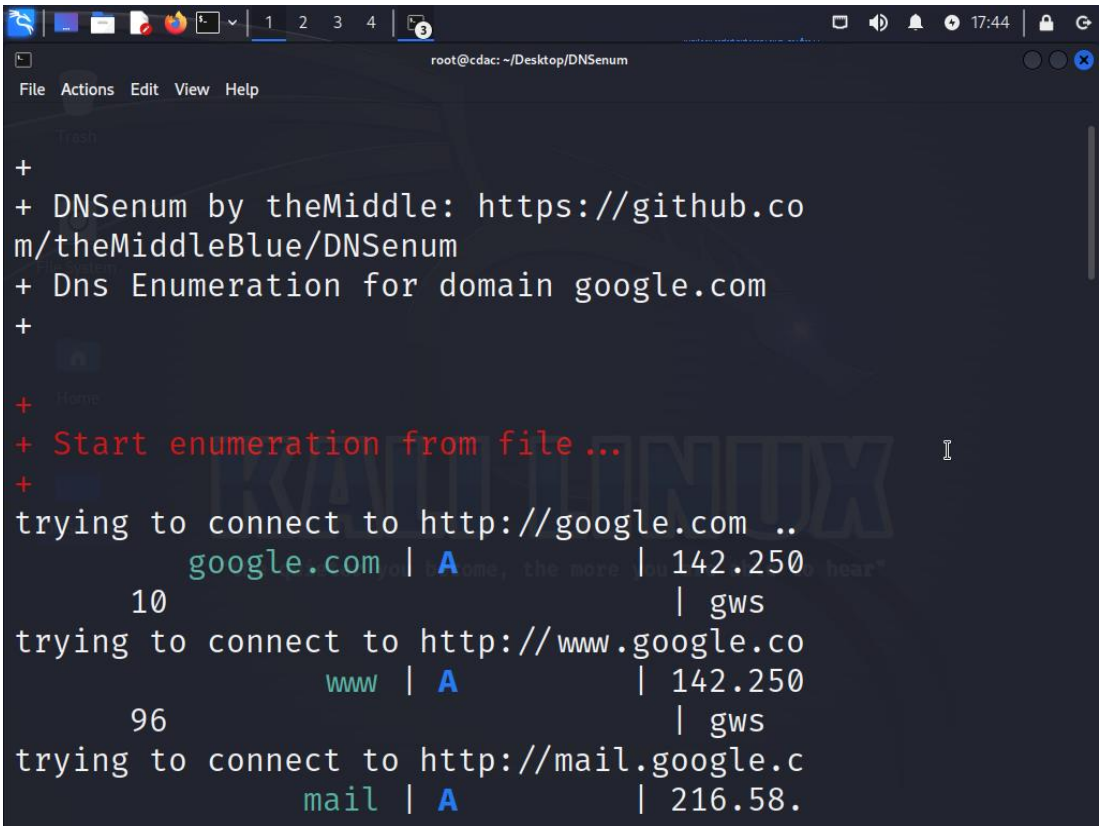


4. Now, Select a target to scan, Here we are using this command

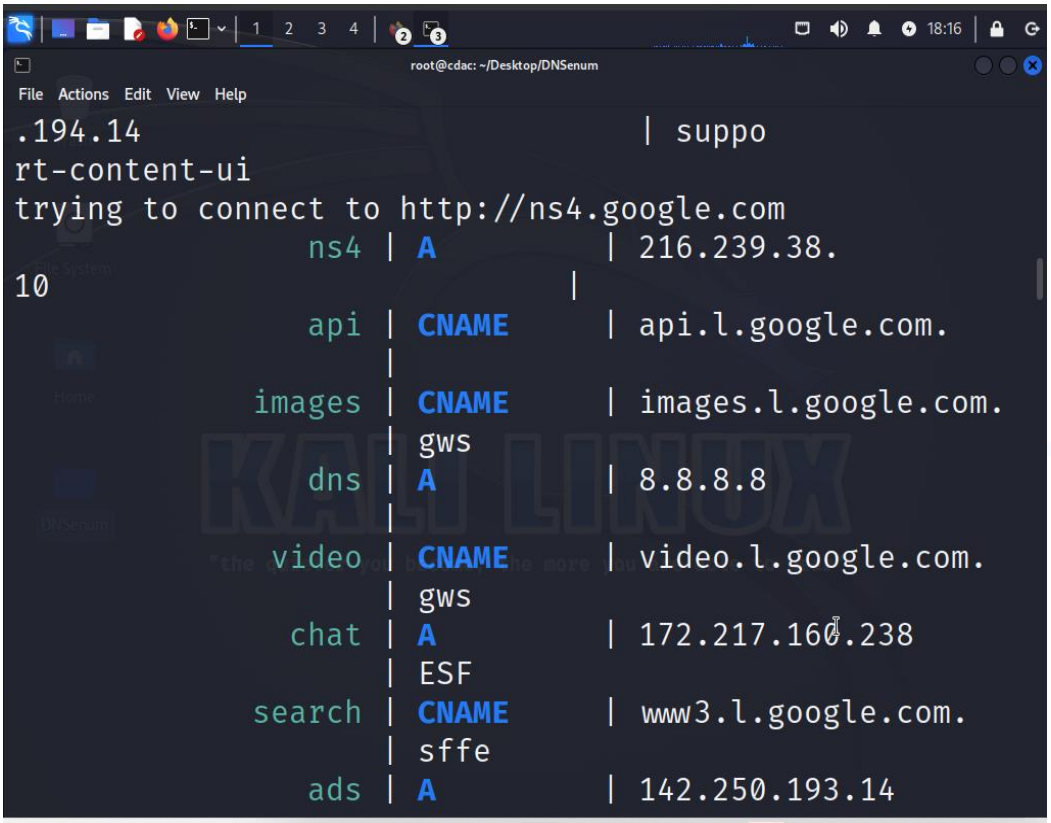
./dnsenum.sh -d google.com -c

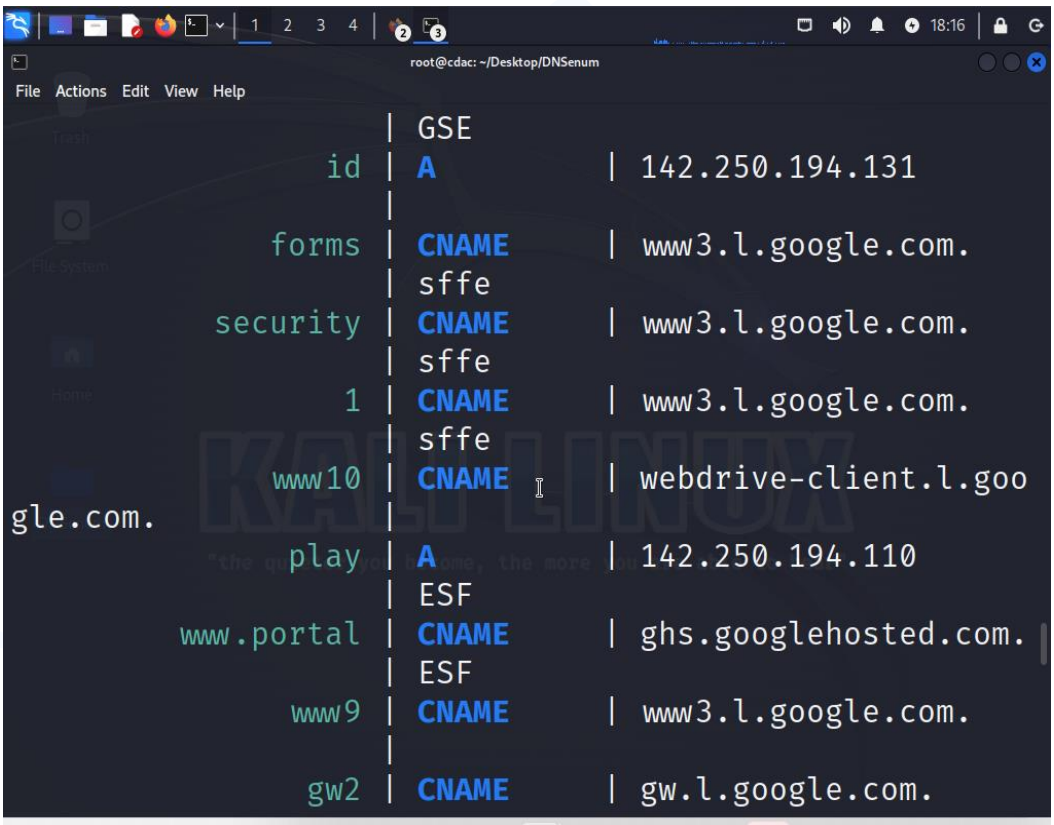


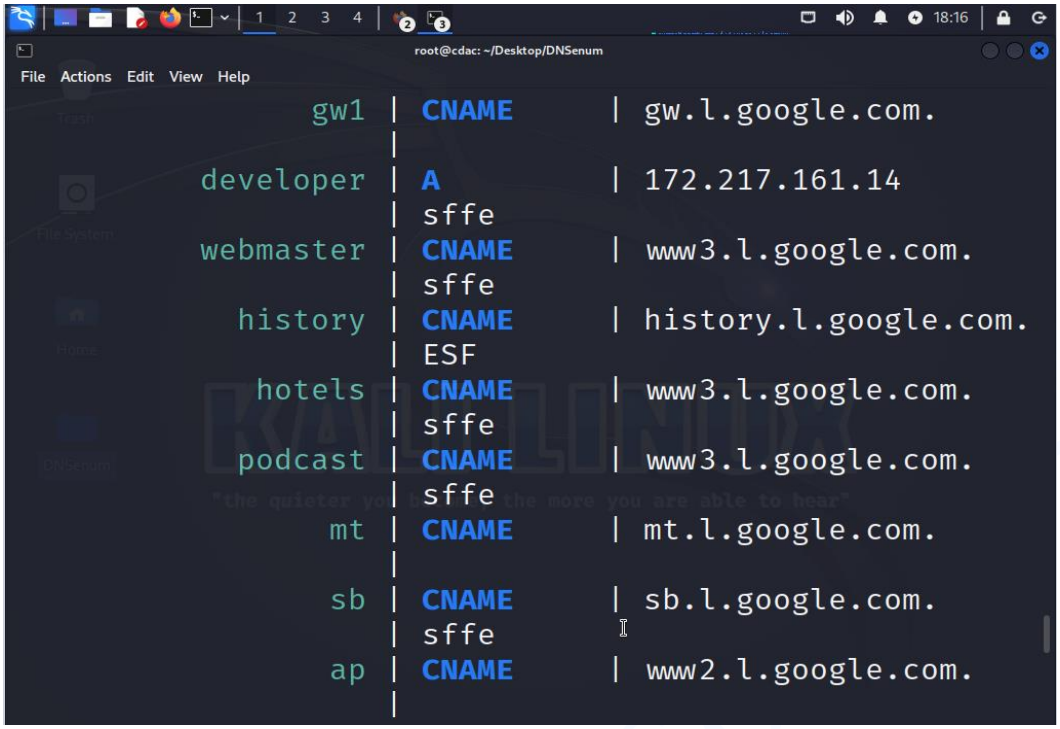
The enumeration process has started. Here you can see the output.

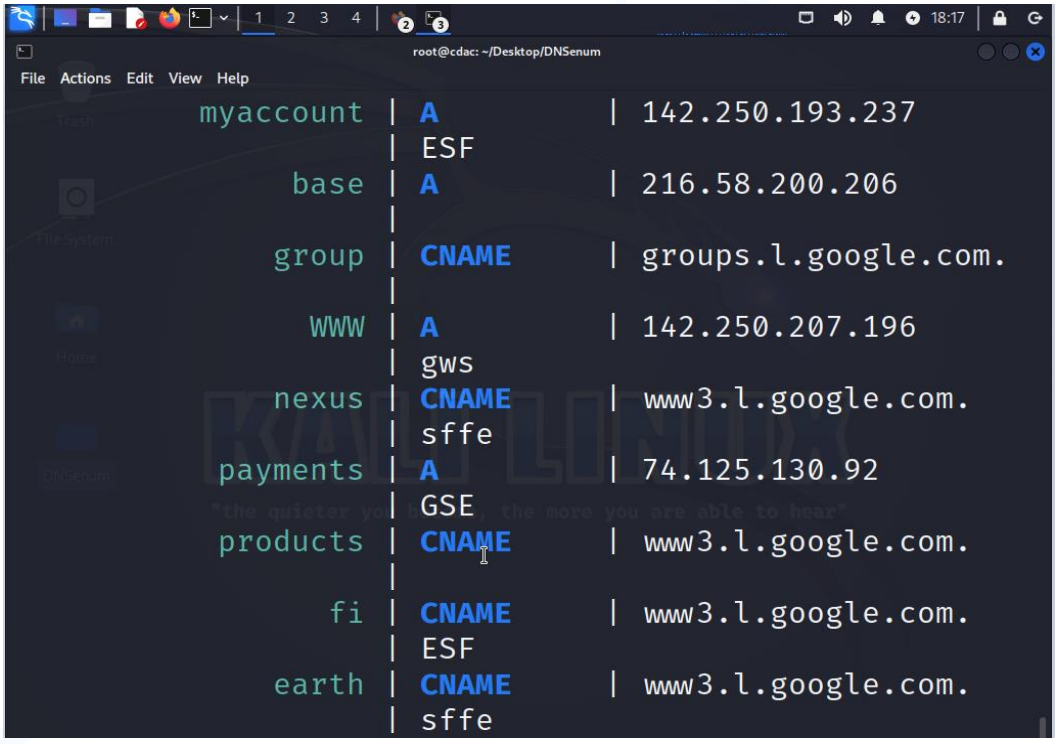


Here you are getting Host address, nameserver and MX reocrds, Subdomains information of **google.com** domian


root@cdac: ~/Desktop/DNSenum
File Actions Edit View Help
.194.14 | suppo
rt-content-ui
trying to connect to http://ns4.google.com
ns4 | A | 216.239.38.
10 |
api | CNAME | api.l.google.com.
|
images | CNAME | images.l.google.com.
| gws
dns | A | 8.8.8.8
|
video | CNAME | video.l.google.com.
| gws
chat | A | 172.217.160.238
| ESF
search | CNAME | www3.l.google.com.
| sffe
ads | A | 142.250.193.14


root@cdac: ~/Desktop/DNSenum
File Actions Edit View Help
| GSE
id | A | 142.250.194.131
|
forms | CNAME | www3.l.google.com.
| sffe
security | CNAME | www3.l.google.com.
| sffe
1 | CNAME | www3.l.google.com.
| sffe
www10 | CNAME | webdrive-client.l.goo
gle.com.
|
play | A | 142.250.194.110
| ESF
www.portal | CNAME | ghs.googlehosted.com.
| ESF
www9 | CNAME | www3.l.google.com.
|
gw2 | CNAME | gw.l.google.com.





Here are some of the best ways to protect your website from information leakage

- Make sure that everyone involved in producing the website is fully aware of what information is considered sensitive. Sometimes seemingly harmless information can be much more useful to an attacker than people realize. Highlighting these dangers can help make

sure that sensitive information is handled more securely in general by your organization.

- Audit any code for potential information disclosure as part of your QA or build processes.
- Use generic error messages as much as possible. Don't provide attackers with clues about application behaviour unnecessarily.
- Double-check that any debugging or diagnostic features are disabled in the production environment.
- Make sure you fully understand the configuration settings, and security implications, of any third-party technology that you implement. Take the time to investigate and disable any features and settings that you don't actually need.