

Information Gathering using AMASS Tool

Amass is an open source network mapping and attack surface discovery tool that uses information gathering and other techniques such as active reconnaissance and external asset discovery to scrap all the available data. In order to accomplish this, it uses its own internal machinery and it also integrates smoothly with different external services to increase its results, efficiency and power.

This tool maintains a strong focus on DNS, HTTP and SSL/TLS data discovering and scrapping.

It also uses different web archiving engines to scrape the bottom of the internet's forgotten data deposits.

FEATURES OF AMASS

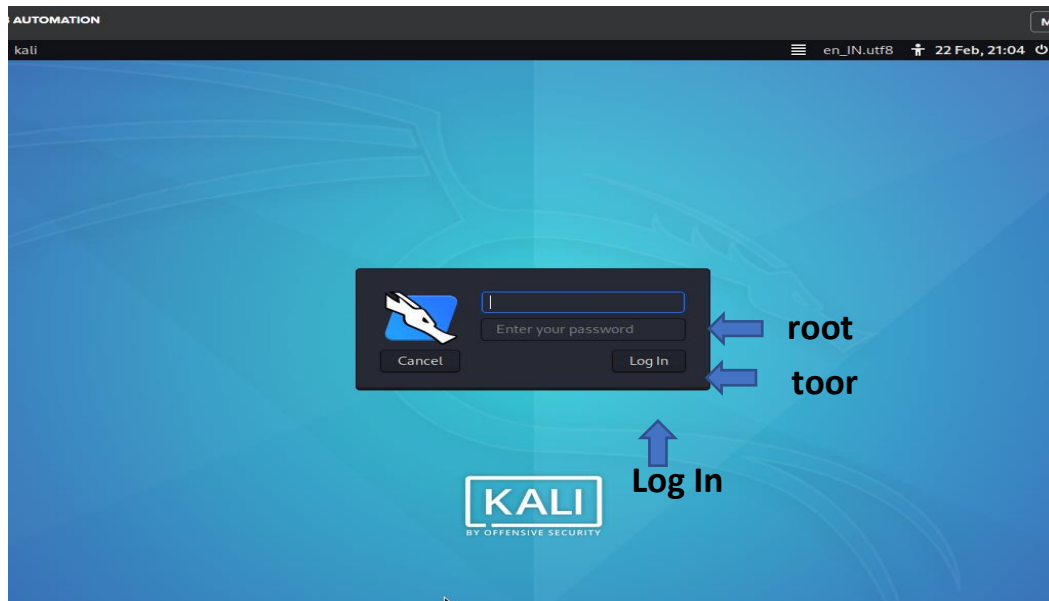
- Discover targets for enumerations.
- Perform enumerations and network mapping.
- Track differences between enumerations.
- Resolve DNS names at high performance.

In this exercise, we will scan subdomains using Amass Tool.

Guided Exercise

Step to Perform this Exercise

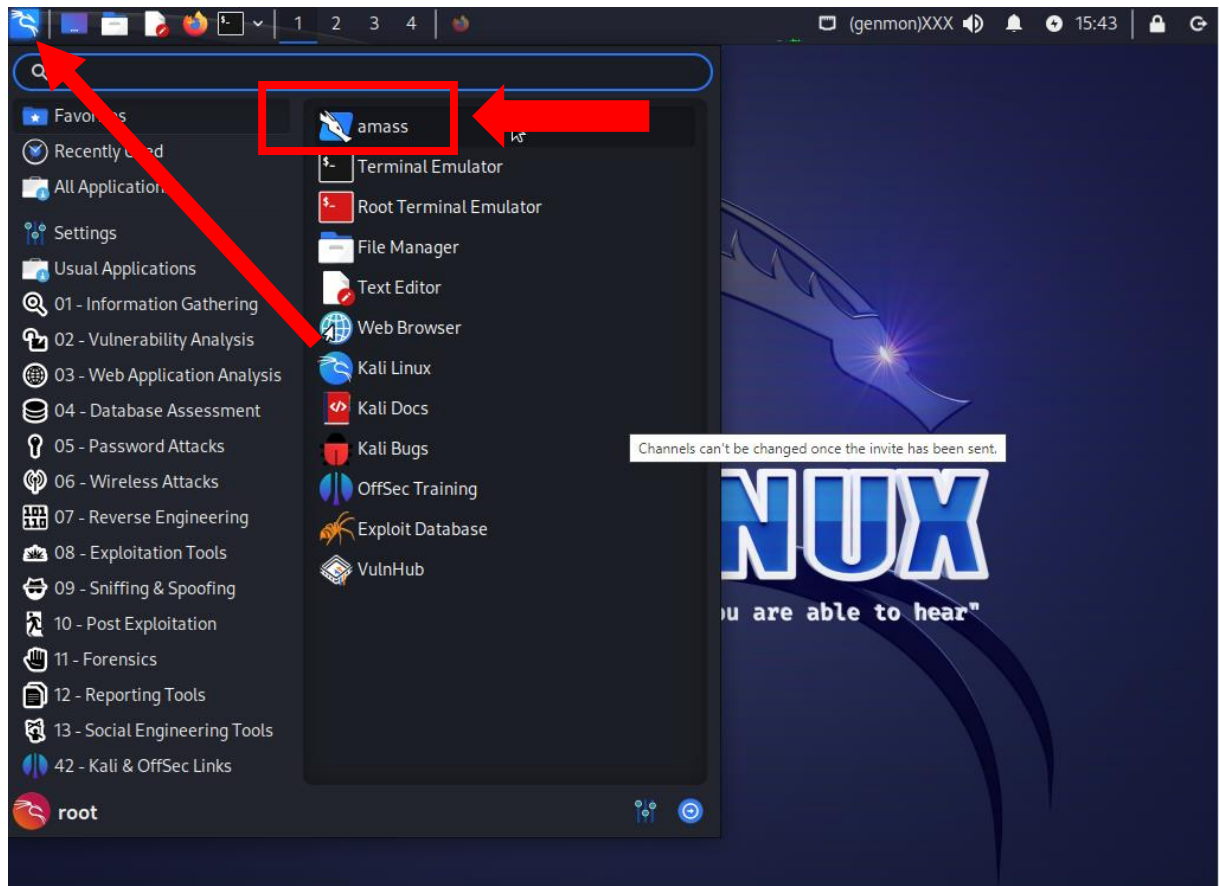
1. Connect to the kali Linux machine, created by you, using the RDP protocol. Kali Linux machine is being used as Attacker's machine.
2. When prompted for the username and password, enter **root** as username and **toor** as password. The root is the administrator user of the machine.



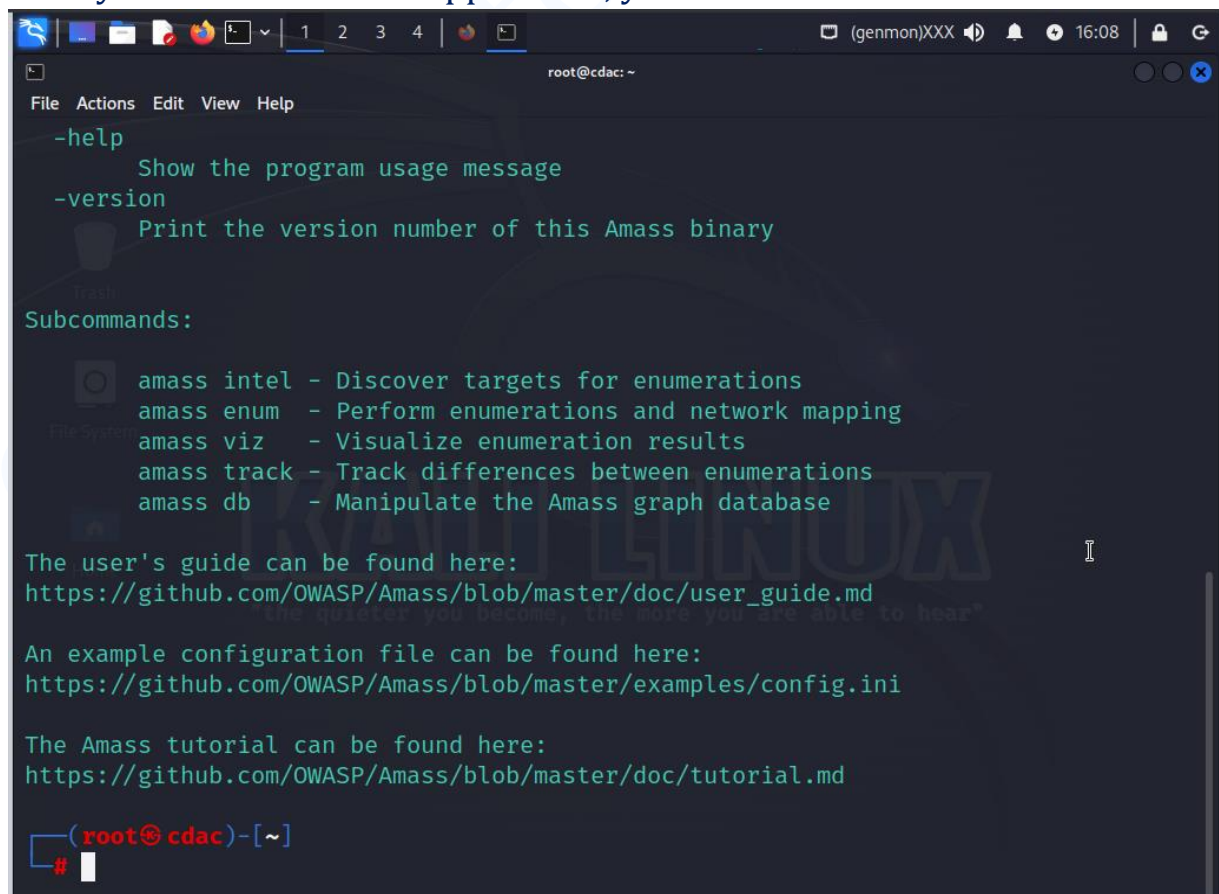
Once you successfully login in, you will see a screen like this.



3. Now, click on the application tab. Here you can see **AMASS** Application, click on Application "**amass**" to start.



Once you will click on the Application, you will see a screen like this

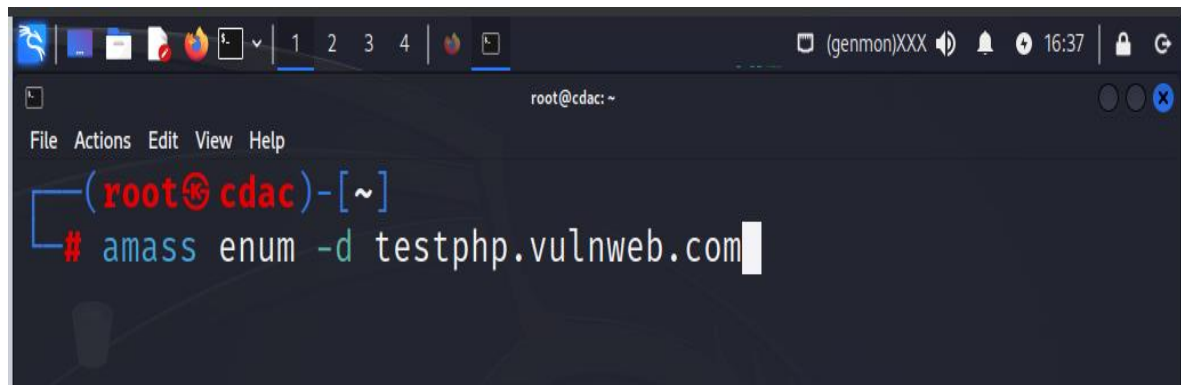


Top Example Usage of Amass

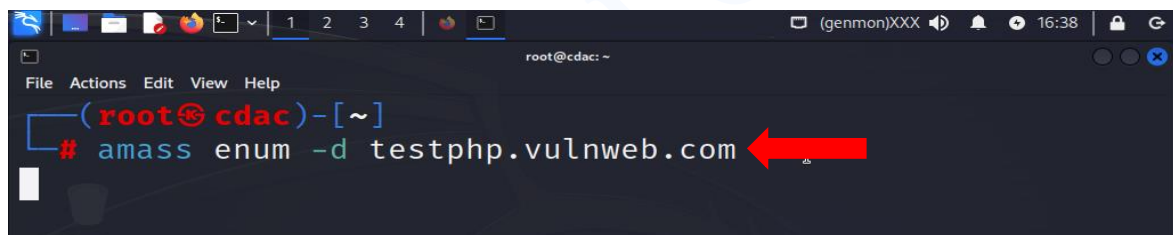
a) Basic Command to enum target

amass enum -d <URL>

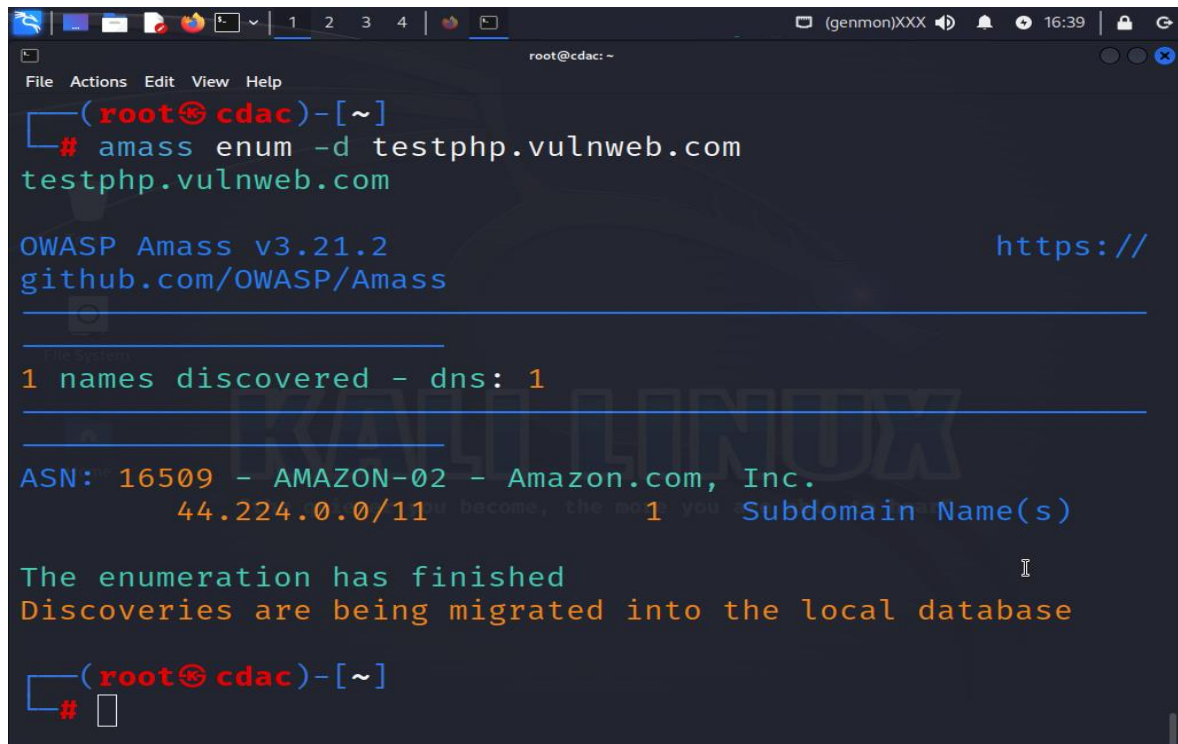
Enter the domain name which you want to search for, here we are searching for **testphp.vulnweb.com**

A terminal window titled 'root@cdac: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(root@cdac)-[~]'. The command '# amass enum -d testphp.vulnweb.com' is entered and the cursor is at the end of the line. The terminal has a dark background with syntax highlighting: red for the prompt, blue for the command, and green for the domain. The window title bar shows '(genmon)XXX' and the time '16:37'.

Press enter and scanning process will start

A terminal window titled 'root@cdac: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(root@cdac)-[~]'. The command '# amass enum -d testphp.vulnweb.com' is entered. A red arrow points to the end of the command line. The terminal has a dark background with syntax highlighting: red for the prompt, blue for the command, and green for the domain. The window title bar shows '(genmon)XXX' and the time '16:38'.

Here's the Output

A terminal window titled 'root@cdac: ~' showing the execution of the 'amass enum' command. The command is '# amass enum -d testphp.vulnweb.com'. The output includes the OWASP Amass version (v3.21.2), the GitHub repository link (github.com/OWASP/Amass), a separator line, and the results: '1 names discovered - dns: 1'. Below this, it shows 'ASN: 16509 - AMAZON-02 - Amazon.com, Inc.' and '44.224.0.0/11' with a '1' in the 'Subdomain Name(s)' column. The terminal concludes with 'The enumeration has finished' and 'Discoveries are being migrated into the local database'.

```
(root@cdac)-[~]
# amass enum -d testphp.vulnweb.com
testphp.vulnweb.com

OWASP Amass v3.21.2 https://
github.com/OWASP/Amass

1 names discovered - dns: 1

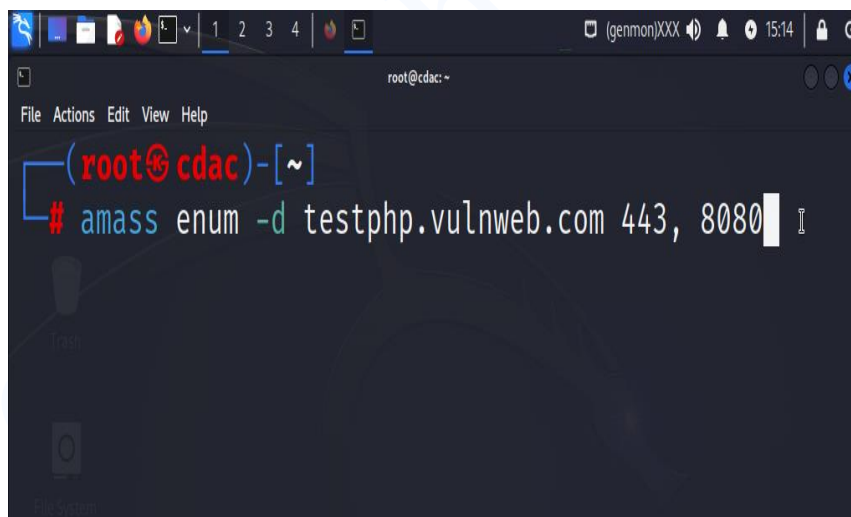
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
44.224.0.0/11 1 Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database

(root@cdac)-[~]
#
```

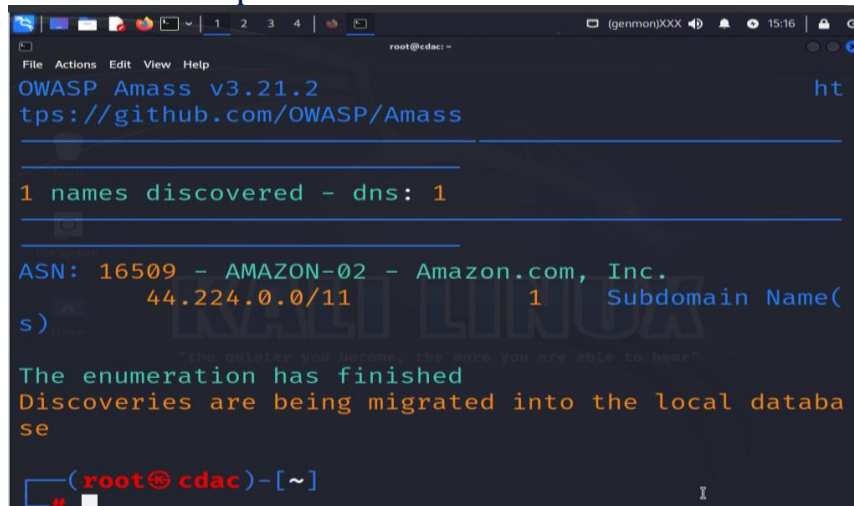
b) Mention Ports for the Scan

amass enum -d <URL> -p 443,8080

A terminal window titled 'root@cdac: ~' showing the command '# amass enum -d testphp.vulnweb.com 443, 8080' being entered. The cursor is at the end of the command.

```
(root@cdac)-[~]
# amass enum -d testphp.vulnweb.com 443, 8080
```

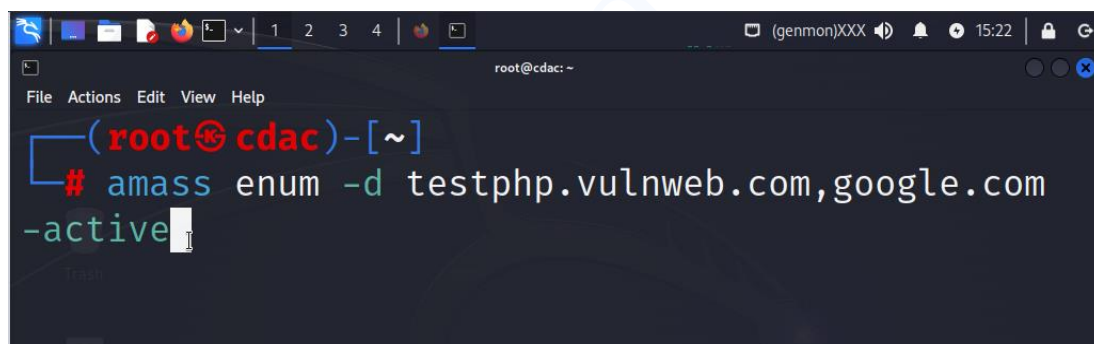
Here's the Output



```
root@cdac: ~  
OWASP Amass v3.21.2  
tps://github.com/OWASP/Amass  
  
1 names discovered - dns: 1  
  
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.  
44.224.0.0/11 1 Subdomain Name(s)  
The enumeration has finished  
Discoveries are being migrated into the local database  
  
(root@cdac)-[~]
```

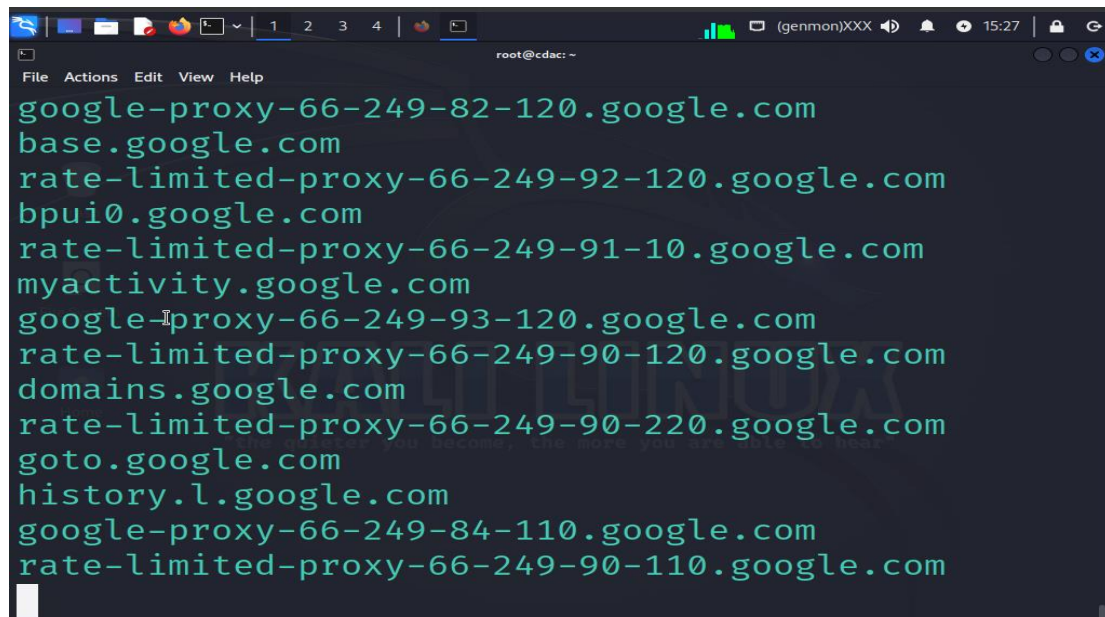
- c) Combining different options to get more refined results.
-d options enable users to enter multiple URLs and -active options use active recon methods.

amass enum -d <URL1>,<URL2> -active



```
root@cdac: ~  
(root@cdac)-[~]  
# amass enum -d testphp.vulnweb.com,google.com  
-active
```

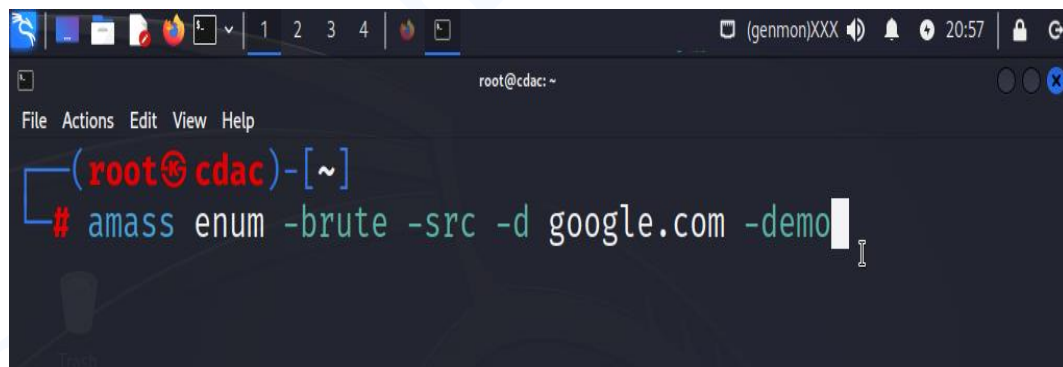

Here's the Output



```
root@cdac: ~  
google-proxy-66-249-82-120.google.com  
base.google.com  
rate-limited-proxy-66-249-92-120.google.com  
bpui0.google.com  
rate-limited-proxy-66-249-91-10.google.com  
myactivity.google.com  
google-proxy-66-249-93-120.google.com  
rate-limited-proxy-66-249-90-120.google.com  
domains.google.com  
rate-limited-proxy-66-249-90-220.google.com  
goto.google.com  
history.l.google.com  
google-proxy-66-249-84-110.google.com  
rate-limited-proxy-66-249-90-110.google.com
```

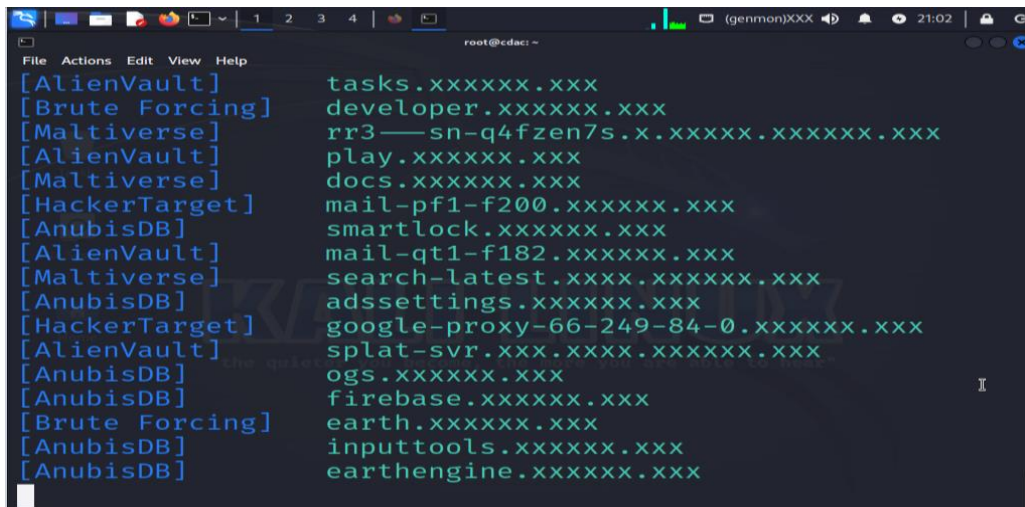
- d) Perform brute force by using - brute option for subdomain enumeration. -src option display data sources for the discovered names and -demo option display results in a presentable manner

amass enum -brute -src -d <URL> -demo



```
root@cdac: ~  
(root@cdac)-[~]  
# amass enum -brute -src -d google.com -demo
```

Here's the Output



```
root@cdac: ~  
File Actions Edit View Help  
[AlienVault] tasks.xxxxxx.xxx  
[Brute Forcing] developer.xxxxxx.xxx  
[Maltiverse] rr3—sn-q4fzen7s.x.xxxxxx.xxxxxx.xxx  
[AlienVault] play.xxxxxx.xxx  
[Maltiverse] docs.xxxxxx.xxx  
[HackerTarget] mail-pf1-f200.xxxxxx.xxx  
[AnubisDB] smartlock.xxxxxx.xxx  
[AlienVault] mail-qt1-f182.xxxxxx.xxx  
[Maltiverse] search-latest.xxxx.xxxxxx.xxx  
[AnubisDB] adssettings.xxxxxx.xxx  
[HackerTarget] google-proxy-66-249-84-0.xxxxxx.xxx  
[AlienVault] splat-svr.xxx.xxxx.xxxxxx.xxx  
[AnubisDB] ogs.xxxxxx.xxx  
[AnubisDB] firebase.xxxxxx.xxx  
[Brute Forcing] earth.xxxxxx.xxx  
[AnubisDB] inputtools.xxxxxx.xxx  
[AnubisDB] earthengine.xxxxxx.xxx
```

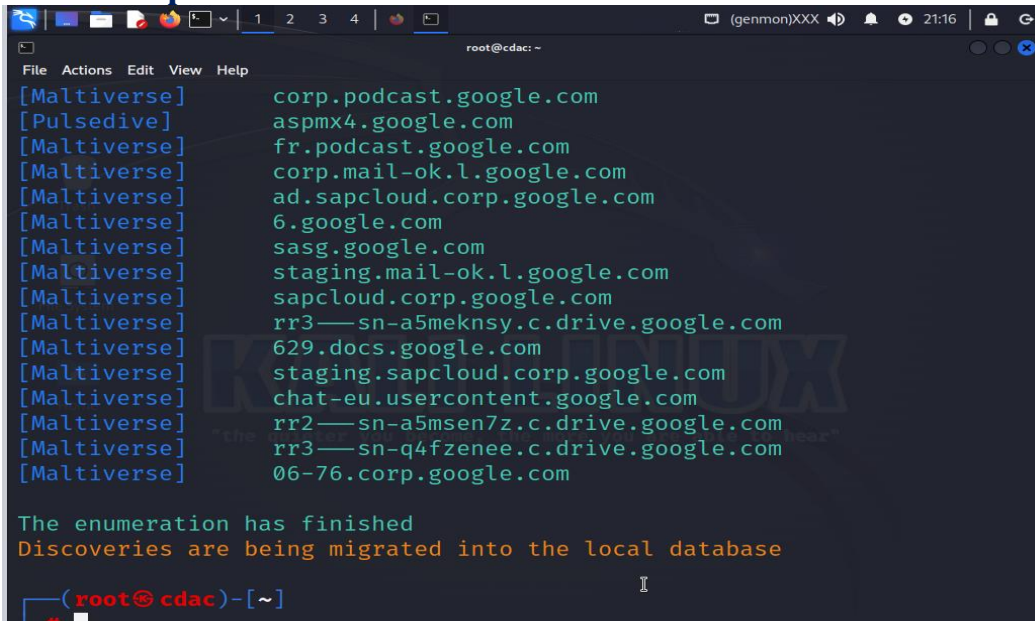
e) To do Passive Scanning

amass enum -passive -d <URL> -src



```
root@cdac: ~  
File Actions Edit View Help  
(root@cdac)~  
# amass enum -passive -d google.com -src
```

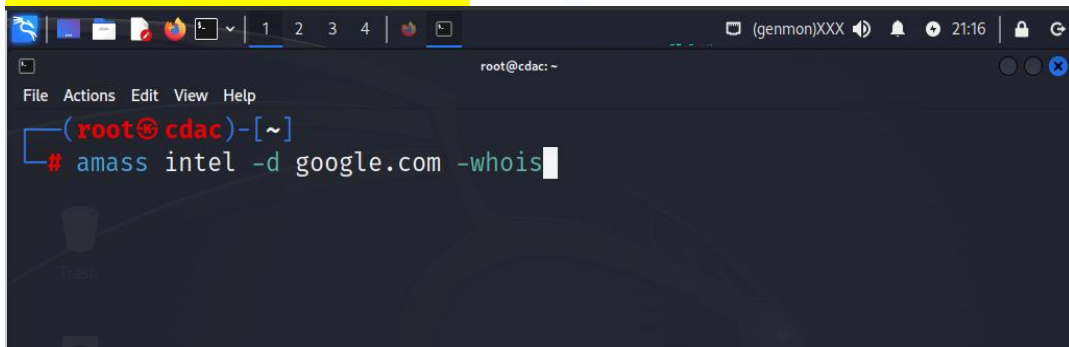

Here's the Output



```
root@cdac: ~  
[Maltiverse] corp.podcast.google.com  
[Pulsedive] aspmx4.google.com  
[Maltiverse] fr.podcast.google.com  
[Maltiverse] corp.mail-ok.l.google.com  
[Maltiverse] ad.sapcloud.corp.google.com  
[Maltiverse] 6.google.com  
[Maltiverse] sasg.google.com  
[Maltiverse] staging.mail-ok.l.google.com  
[Maltiverse] sapcloud.corp.google.com  
[Maltiverse] rr3—sn-a5meknsy.c.drive.google.com  
[Maltiverse] 629.docs.google.com  
[Maltiverse] staging.sapcloud.corp.google.com  
[Maltiverse] chat-eu.usercontent.google.com  
[Maltiverse] rr2—sn-a5msen7z.c.drive.google.com  
[Maltiverse] rr3—sn-q4fzenee.c.drive.google.com  
[Maltiverse] 06-76.corp.google.com  
  
The enumeration has finished  
Discoveries are being migrated into the local database  
  
(root@cdac)-[~]
```

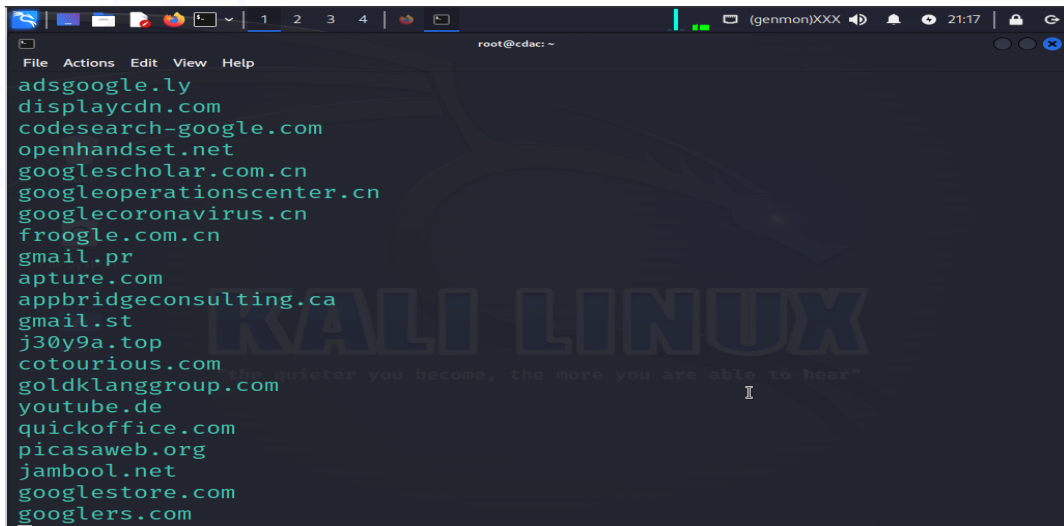
f) Identify domains by using -whois option

amass intel -d <url> -whois



```
root@cdac: ~  
(root@cdac)-[~]  
# amass intel -d google.com -whois
```

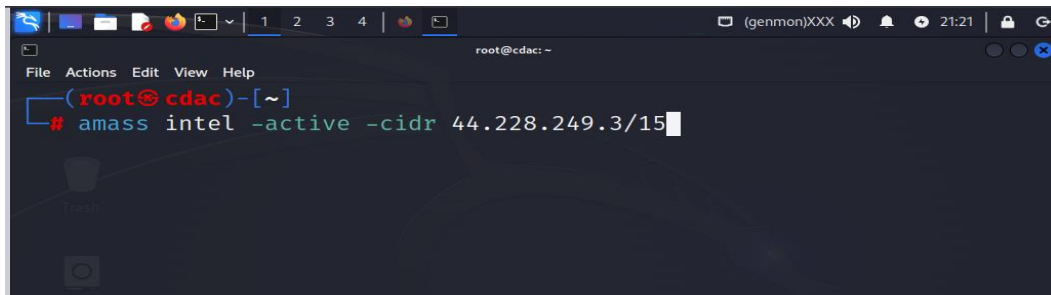
Here's the Output



```
root@cdac: ~  
adsgoogle.ly  
displaycdn.com  
codesearch-google.com  
openhandset.net  
googlescholar.com.cn  
googleoperationscenter.cn  
googlecoronavirus.cn  
froogle.com.cn  
gmail.pr  
apture.com  
appbridgeconsulting.ca  
gmail.st  
j30y9a.top  
cotourious.com  
goldklanggroup.com  
youtube.de  
quickoffice.com  
picasaweb.org  
jambool.net  
googlestore.com  
googlers.com
```

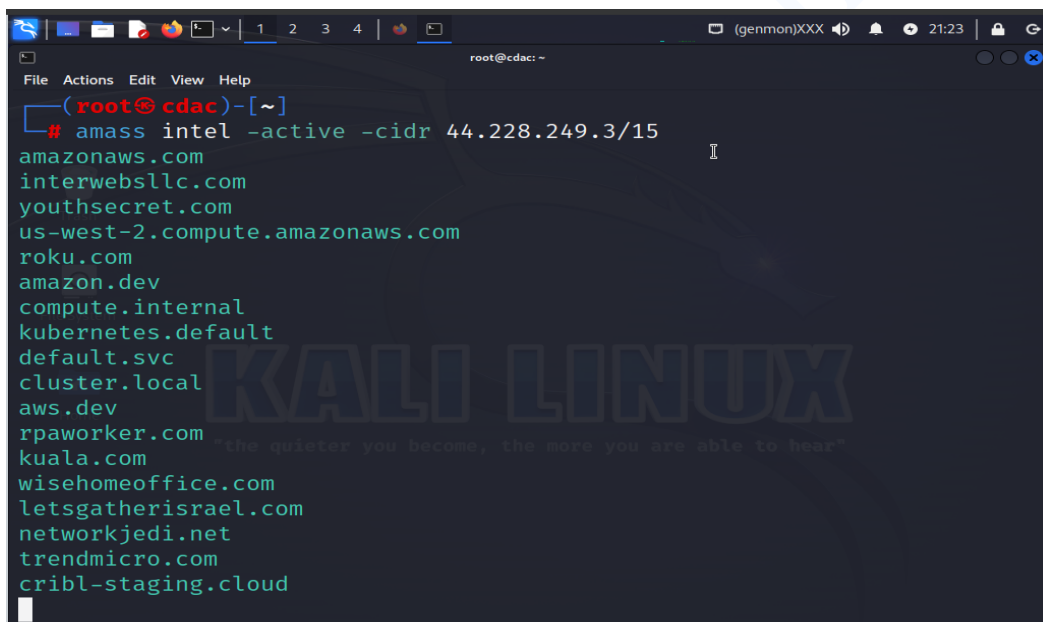
g) Enable active recon method

amass intel -active -cidr 123.134.0.0/15



```
root@cdac: ~  
# amass intel -active -cidr 44.228.249.3/15
```

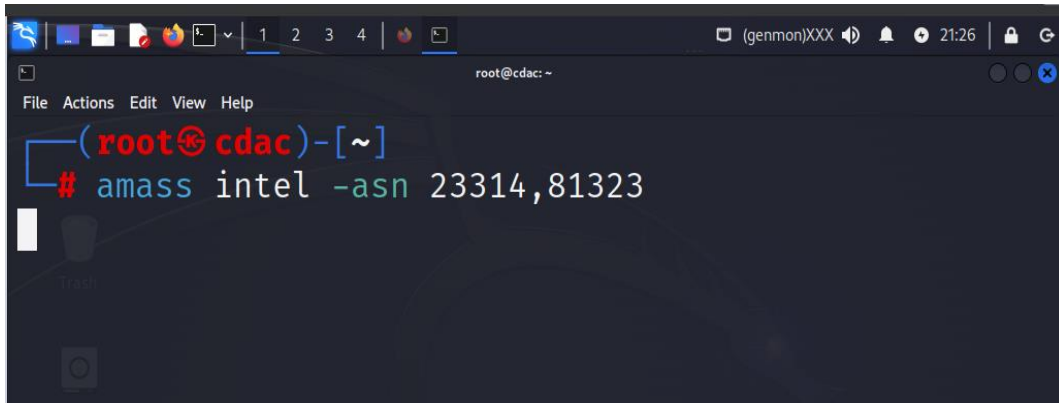
Here's the Output



```
root@cdac: ~  
# amass intel -active -cidr 44.228.249.3/15  
amazonaws.com  
interwebsllc.com  
youthsecret.com  
us-west-2.compute.amazonaws.com  
roku.com  
amazon.dev  
compute.internal  
kubernetes.default  
default.svc  
cluster.local  
aws.dev  
rpaworker.com  
kuala.com  
wisehomeoffice.com  
letsgatherisrael.com  
networkjedi.net  
trendmicro.com  
cribl-staging.cloud
```

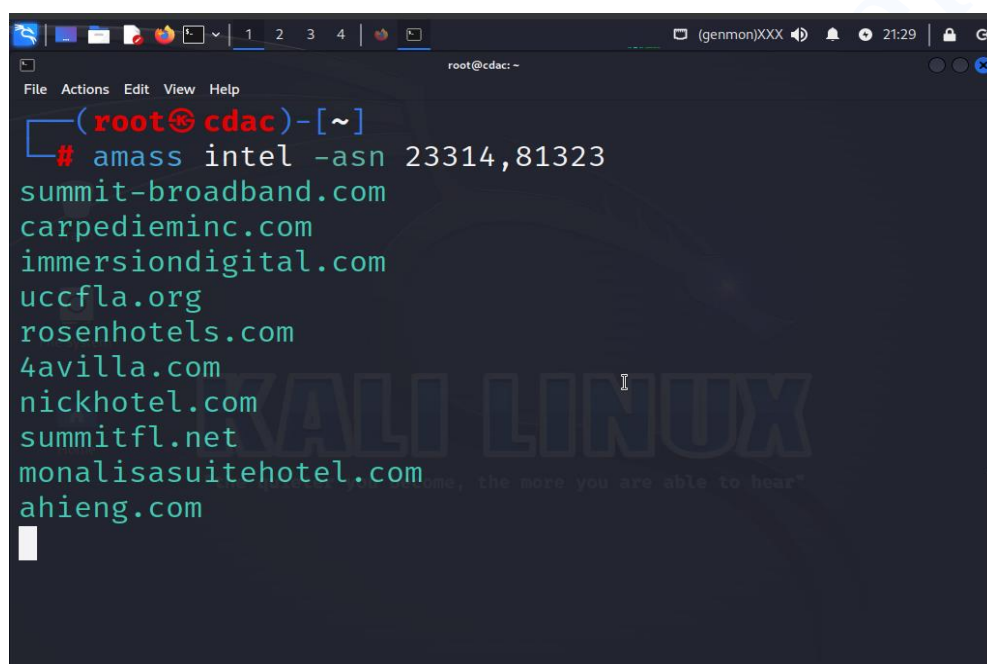
h) Search Based on ASN

amass intel -asn 23314,81323



```
root@cdac: ~  
# amass intel -asn 23314,81323
```

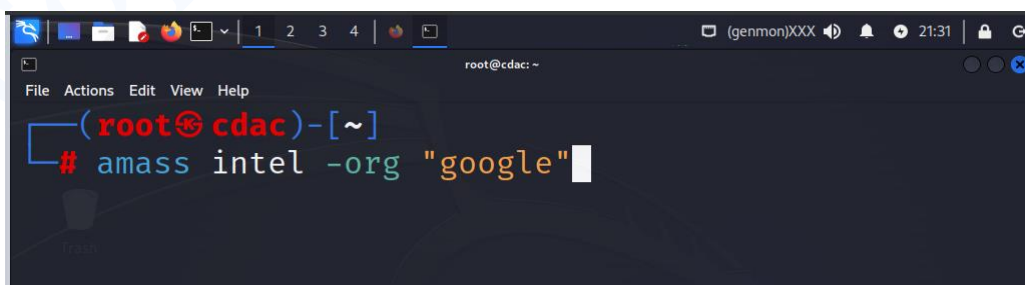
Here's the Output



```
root@cdac: ~  
# amass intel -asn 23314,81323  
summit-broadband.com  
carpedieminc.com  
immersiondigital.com  
uccfla.org  
rosenhoteles.com  
4avilla.com  
nickhotel.com  
summitfl.net  
monalisasuitehotel.com  
ahieng.com
```

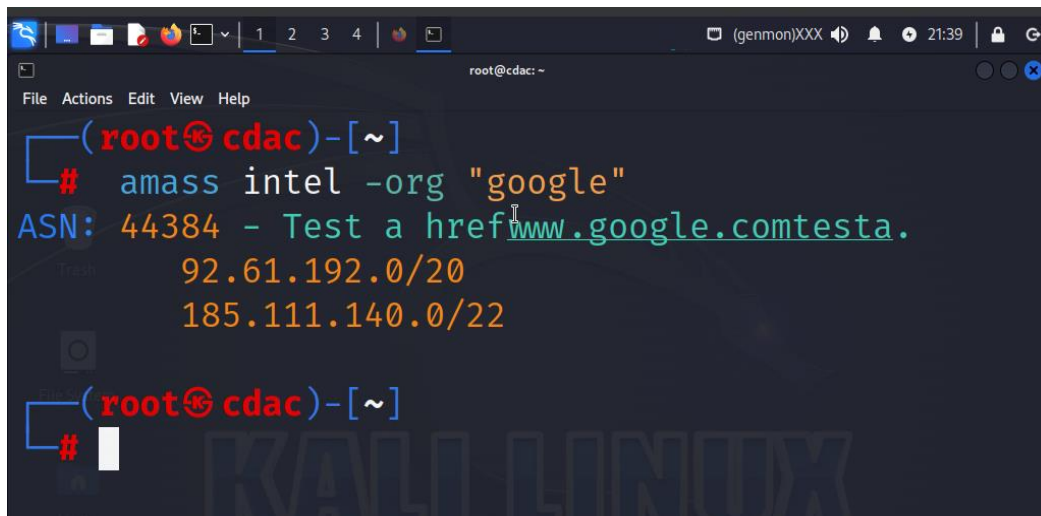
i) Search string based on AS description information

amass intel -org "google"



```
root@cdac: ~  
# amass intel -org "google"
```

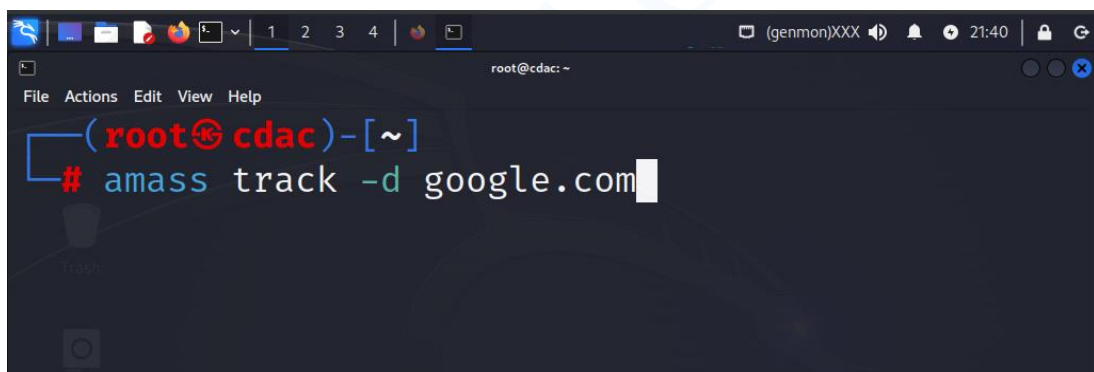
Here's the Output



```
root@cdac: ~  
# amass intel -org "google"  
ASN: 44384 - Test a hrefwww.google.comtesta.  
92.61.192.0/20  
185.111.140.0/22  
  
root@cdac: ~  
#
```

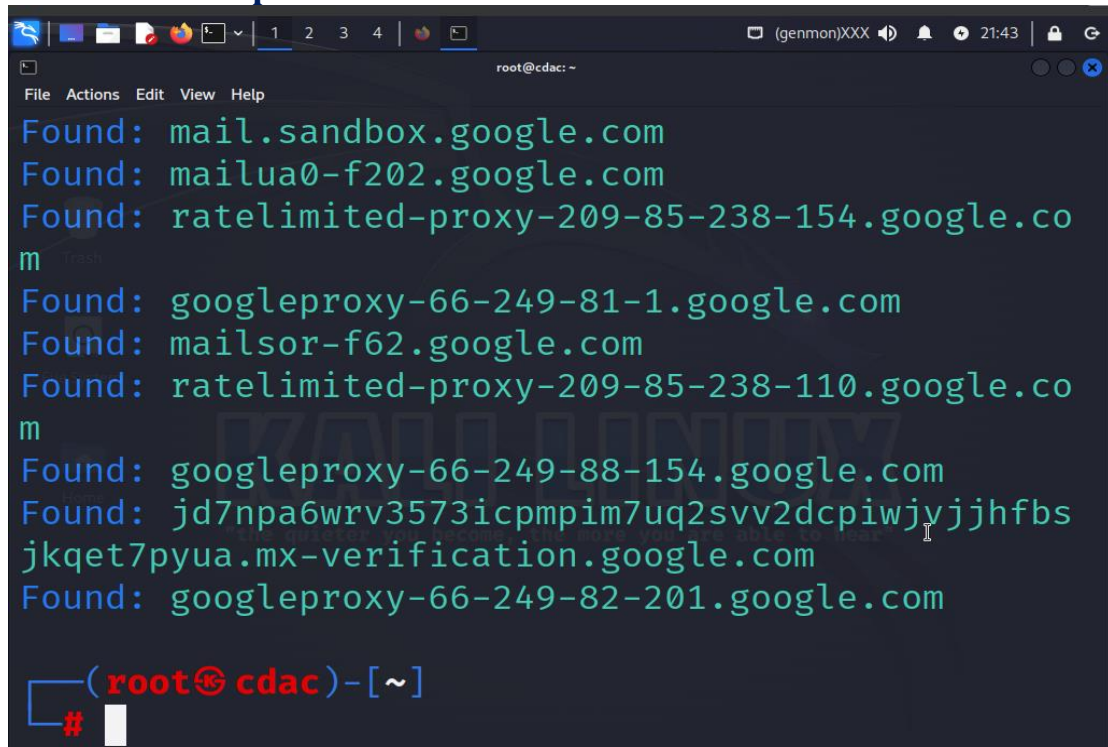
j) Basic command using track option

amass track -d example.com



```
root@cdac: ~  
# amass track -d google.com
```

Here's the Output



```
Found: mail.sandbox.google.com
Found: mailua0-f202.google.com
Found: ratelimited-proxy-209-85-238-154.google.com
Found: googleproxy-66-249-81-1.google.com
Found: mailsor-f62.google.com
Found: ratelimited-proxy-209-85-238-110.google.com
Found: googleproxy-66-249-88-154.google.com
Found: jd7npa6wrv3573icpmpim7uq2svv2dcpiwjyjhhfbs
      jkqet7pyua.mx-verification.google.com
Found: googleproxy-66-249-82-201.google.com

(root@cdac) - [~]
```

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.