Amass

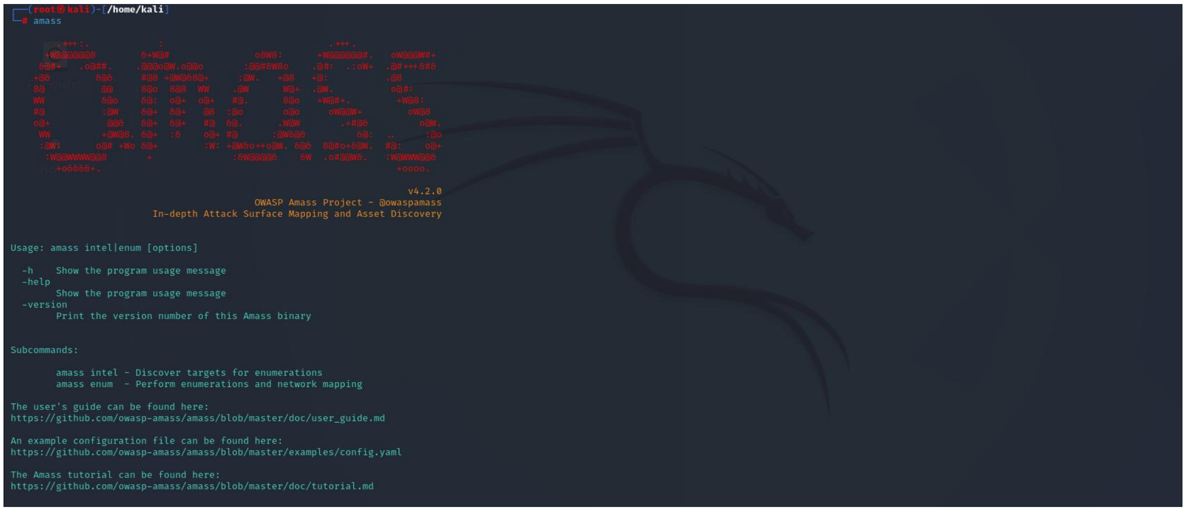
Amass is an open-source tool used for subdomain enumeration and network mapping. It's primarily employed in cybersecurity for reconnaissance purposes to gather information about a target domain's infrastructure. By enumerating subdomains, Amass helps security professionals identify potential entry points for attackers, vulnerabilities, and misconfigurations within a network.

Amass offers both passive and active reconnaissance techniques, utilizing sources like DNS, web scraping, and WHOIS information to collect data. It can be used to discover subdomains that might be overlooked, aiding in vulnerability assessments, penetration testing, and threat intelligence gathering.

Developed in Go, Amass is efficient and regularly updated to incorporate new features and improve performance. Its flexibility and command-line interface make it a popular choice among security professionals for reconnaissance tasks.

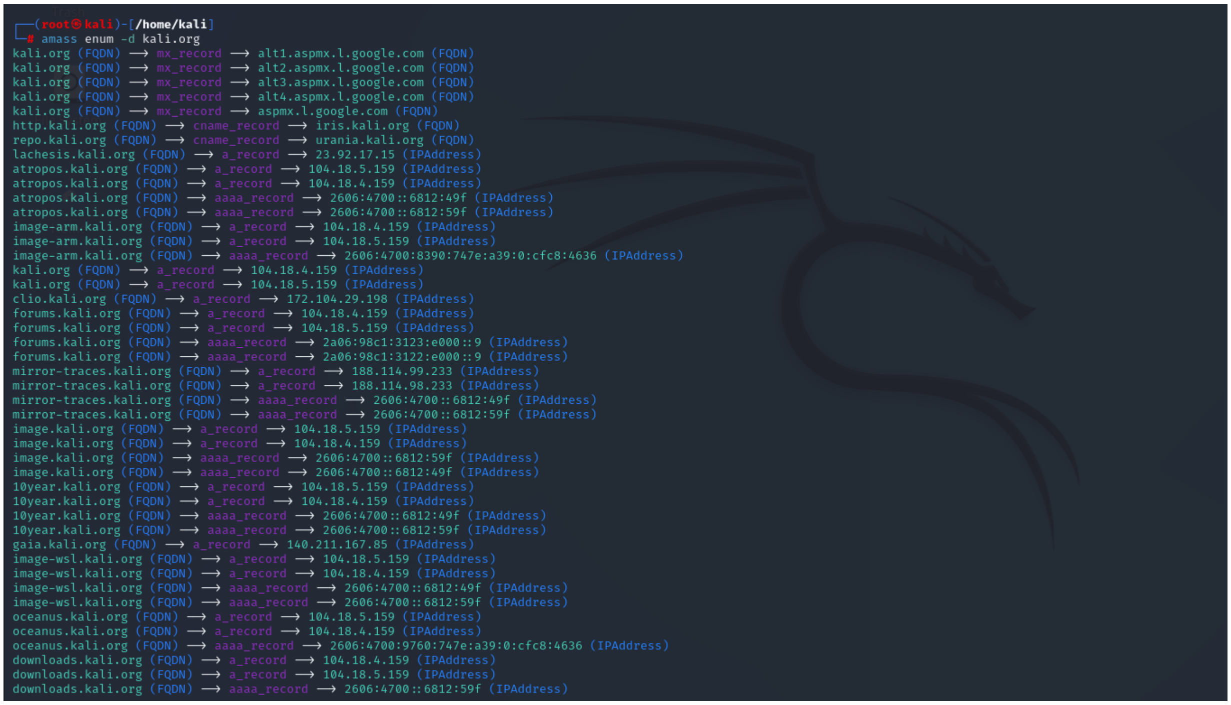
Steps to Enumerate Subdomains:-

1. In latest Linux Distribution Amass Tool is pre install and we can run it simply just typing amass inside the terminal.



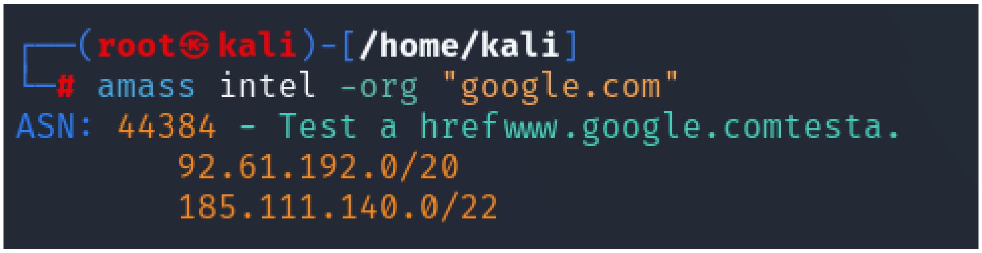
```
┌──(root㉿kali)-[/home/kali]
└─# amass

                                                                              v4.2.0
                                                   OWASP Amass Project - @owaspamass
                                      In-depth Attack Surface Mapping and Asset Discovery


Usage: amass intel|enum [options]

  -h    Show the program usage message
  -help
        Show the program usage message
  -version
        Print the version number of this Amass binary


Subcommands:

        amass intel - Discover targets for enumerations
        amass enum  - Perform enumerations and network mapping

The user's guide can be found here:
https://github.com/owasp-amass/amass/blob/master/doc/user_guide.md

An example configuration file can be found here:
https://github.com/owasp-amass/amass/blob/master/examples/config.yaml

The Amass tutorial can be found here:
https://github.com/owasp-amass/amass/blob/master/doc/tutorial.md
```

2. Here we have used -d flag to specify our target domain.



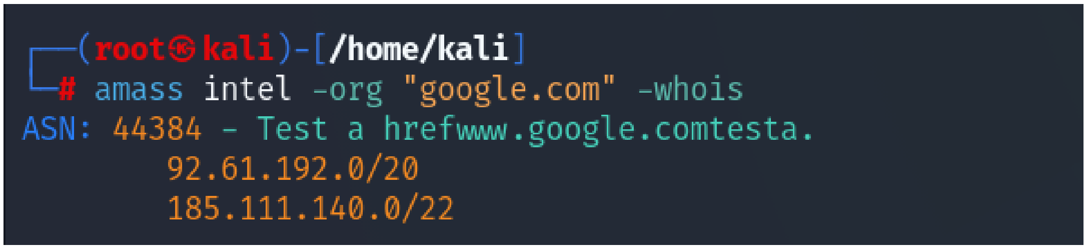
```
┌──(root㉿kali)-[/home/kali]
└─# amass enum -d kali.org
kali.org (FQDN) ⟶ mx_record ⟶ alt1.aspmx.l.google.com (FQDN)
kali.org (FQDN) ⟶ mx_record ⟶ alt2.aspmx.l.google.com (FQDN)
kali.org (FQDN) ⟶ mx_record ⟶ alt3.aspmx.l.google.com (FQDN)
kali.org (FQDN) ⟶ mx_record ⟶ alt4.aspmx.l.google.com (FQDN)
kali.org (FQDN) ⟶ mx_record ⟶ aspmx.l.google.com (FQDN)
http.kali.org (FQDN) ⟶ cname_record ⟶ iris.kali.org (FQDN)
repo.kali.org (FQDN) ⟶ cname_record ⟶ urania.kali.org (FQDN)
lachesis.kali.org (FQDN) ⟶ a_record ⟶ 23.92.17.15 (IPAddress)
atropos.kali.org (FQDN) ⟶ a_record ⟶ 104.18.5.159 (IPAddress)
atropos.kali.org (FQDN) ⟶ a_record ⟶ 104.18.4.159 (IPAddress)
atropos.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:49f (IPAddress)
atropos.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:59f (IPAddress)
image-arm.kali.org (FQDN) ⟶ a_record ⟶ 104.18.4.159 (IPAddress)
image-arm.kali.org (FQDN) ⟶ a_record ⟶ 104.18.5.159 (IPAddress)
image-arm.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700:8390:747e:a39:0:cfc8:4636 (IPAddress)
kali.org (FQDN) ⟶ a_record ⟶ 104.18.4.159 (IPAddress)
kali.org (FQDN) ⟶ a_record ⟶ 104.18.5.159 (IPAddress)
clio.kali.org (FQDN) ⟶ a_record ⟶ 172.104.29.198 (IPAddress)
forums.kali.org (FQDN) ⟶ a_record ⟶ 104.18.4.159 (IPAddress)
forums.kali.org (FQDN) ⟶ a_record ⟶ 104.18.5.159 (IPAddress)
forums.kali.org (FQDN) ⟶ aaaa_record ⟶ 2a06:98c1:3123:e000::9 (IPAddress)
forums.kali.org (FQDN) ⟶ aaaa_record ⟶ 2a06:98c1:3122:e000::9 (IPAddress)
mirror-traces.kali.org (FQDN) ⟶ a_record ⟶ 188.114.99.233 (IPAddress)
mirror-traces.kali.org (FQDN) ⟶ a_record ⟶ 188.114.98.233 (IPAddress)
mirror-traces.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:49f (IPAddress)
mirror-traces.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:59f (IPAddress)
image.kali.org (FQDN) ⟶ a_record ⟶ 104.18.5.159 (IPAddress)
image.kali.org (FQDN) ⟶ a_record ⟶ 104.18.4.159 (IPAddress)
image.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:59f (IPAddress)
image.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:49f (IPAddress)
10year.kali.org (FQDN) ⟶ a_record ⟶ 104.18.5.159 (IPAddress)
10year.kali.org (FQDN) ⟶ a_record ⟶ 104.18.4.159 (IPAddress)
10year.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:49f (IPAddress)
10year.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:59f (IPAddress)
gaia.kali.org (FQDN) ⟶ a_record ⟶ 140.211.167.85 (IPAddress)
image-wsl.kali.org (FQDN) ⟶ a_record ⟶ 104.18.5.159 (IPAddress)
image-wsl.kali.org (FQDN) ⟶ a_record ⟶ 104.18.4.159 (IPAddress)
image-wsl.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:49f (IPAddress)
image-wsl.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:59f (IPAddress)
oceanus.kali.org (FQDN) ⟶ a_record ⟶ 104.18.5.159 (IPAddress)
oceanus.kali.org (FQDN) ⟶ a_record ⟶ 104.18.4.159 (IPAddress)
oceanus.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700:9760:747e:a39:0:cfc8:4636 (IPAddress)
downloads.kali.org (FQDN) ⟶ a_record ⟶ 104.18.4.159 (IPAddress)
downloads.kali.org (FQDN) ⟶ a_record ⟶ 104.18.5.159 (IPAddress)
downloads.kali.org (FQDN) ⟶ aaaa_record ⟶ 2606:4700::6812:59f (IPAddress)
```

3. If you are looking for an organization using "google" in their name then use intel -org to get the output.



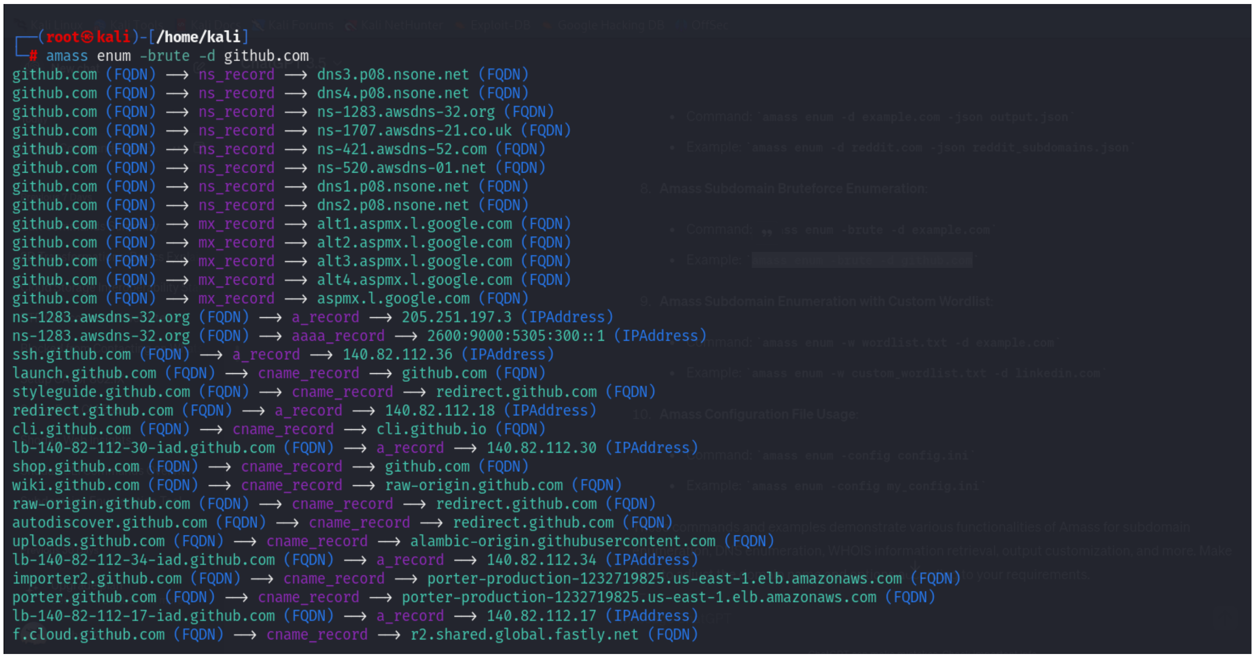
```
┌──(root㉿kali)-[/home/kali]
└─# amass intel -org "google.com"
ASN: 44384 - Test a hrefwww.google.comtesta.
        92.61.192.0/20
        185.111.140.0/22
```

4. We can use -whois to grab the details from the specified domain’s whois records, and then tries to find other domains with the similar whois records.



```
┌──(root㉿kali)-[/home/kali]
└─# amass intel -org "google.com" -whois
ASN: 44384 - Test a hrefwww.google.comtesta.
        92.61.192.0/20
        185.111.140.0/22
```

5. -brute is used to run a bruteforce subdomain enumeration.



```
┌──(root㉿kali)-[/home/kali]
└─# amass enum -brute -d github.com
github.com (FQDN) ⟶ ns_record ⟶ dns3.p08.nsone.net (FQDN)
github.com (FQDN) ⟶ ns_record ⟶ dns4.p08.nsone.net (FQDN)
github.com (FQDN) ⟶ ns_record ⟶ ns-1283.awsdns-32.org (FQDN)
github.com (FQDN) ⟶ ns_record ⟶ ns-1707.awsdns-21.co.uk (FQDN)
github.com (FQDN) ⟶ ns_record ⟶ ns-421.awsdns-52.com (FQDN)
github.com (FQDN) ⟶ ns_record ⟶ ns-520.awsdns-01.net (FQDN)
github.com (FQDN) ⟶ ns_record ⟶ dns1.p08.nsone.net (FQDN)
github.com (FQDN) ⟶ ns_record ⟶ dns2.p08.nsone.net (FQDN)
github.com (FQDN) ⟶ mx_record ⟶ alt1.aspmx.l.google.com (FQDN)
github.com (FQDN) ⟶ mx_record ⟶ alt2.aspmx.l.google.com (FQDN)
github.com (FQDN) ⟶ mx_record ⟶ alt3.aspmx.l.google.com (FQDN)
github.com (FQDN) ⟶ mx_record ⟶ alt4.aspmx.l.google.com (FQDN)
github.com (FQDN) ⟶ mx_record ⟶ aspmx.l.google.com (FQDN)
ns-1283.awsdns-32.org (FQDN) ⟶ a_record ⟶ 205.251.197.3 (IPAddress)
ns-1283.awsdns-32.org (FQDN) ⟶ aaaa_record ⟶ 2600:9000:5305:300::1 (IPAddress)
ssh.github.com (FQDN) ⟶ a_record ⟶ 140.82.112.36 (IPAddress)
launch.github.com (FQDN) ⟶ cname_record ⟶ github.com (FQDN)
styleguide.github.com (FQDN) ⟶ cname_record ⟶ redirect.github.com (FQDN)
redirect.github.com (FQDN) ⟶ a_record ⟶ 140.82.112.18 (IPAddress)
cli.github.com (FQDN) ⟶ cname_record ⟶ cli.github.io (FQDN)
lb-140-82-112-30-iad.github.com (FQDN) ⟶ a_record ⟶ 140.82.112.30 (IPAddress)
shop.github.com (FQDN) ⟶ cname_record ⟶ github.com (FQDN)
wiki.github.com (FQDN) ⟶ cname_record ⟶ raw-origin.github.com (FQDN)
raw-origin.github.com (FQDN) ⟶ cname_record ⟶ redirect.github.com (FQDN)
autodiscover.github.com (FQDN) ⟶ cname_record ⟶ redirect.github.com (FQDN)
uploads.github.com (FQDN) ⟶ cname_record ⟶ alambic-origin.githubusercontent.com (FQDN)
lb-140-82-112-34-iad.github.com (FQDN) ⟶ a_record ⟶ 140.82.112.34 (IPAddress)
importer2.github.com (FQDN) ⟶ cname_record ⟶ porter-production-1232719825.us-east-1.elb.amazonaws.com (FQDN)
porter.github.com (FQDN) ⟶ cname_record ⟶ porter-production-1232719825.us-east-1.elb.amazonaws.com (FQDN)
lb-140-82-112-17-iad.github.com (FQDN) ⟶ a_record ⟶ 140.82.112.17 (IPAddress)
f.cloud.github.com (FQDN) ⟶ cname_record ⟶ r2.shared.global.fastly.net (FQDN)
```

Few more examples of subdomains enumeration using amass:-

- amass intel -passive -d example.com
- amass intel -active -d example.com
- amass intel -ip -d example.com
- mass enum -d example.com -o output.txt
- amass enum -w wordlist.txt -d example.com