

Lab: Information Gathering using AMASS Tool

a. Basic Command to enum target

amass enum -d testphp.vulnweb.com

```
File Actions Edit View Help

(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 testphp.vulnweb.com 443, 8080

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

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 testphp.vulnweb.com, google.com -active

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

- 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 google.com -demo

```
(root@cdac)-[~]
# amass enum -brute -src -d google.com -demo
[CertSpotter]    da-mtv-5.xx.xxx.xxxxxx.xxx
[DNS]            _ldaps.xxxx.xxxxxx.xxx
[HackerTarget]   216-239-45-33.xxxxxx.xxx
[DNS]            ldap.xxxxxx.xxx
[Crtsh]          prom-test.xxxxxxx.xxxxxx.xxx
[Reverse DNS]    mail-vk1-f186.xxxxxx.xxx
[Reverse DNS]    mail-ua1-f59.xxxxxx.xxx
[CertSpotter]    console.xx.xxxxxx.xxxxxx.xxx
[Reverse DNS]    mail-wr1-f21.xxxxxx.xxx
[Reverse DNS]    mail-ua1-f98.xxxxxx.xxx
[Reverse DNS]    mail-qk1-f143.xxxxxx.xxx
[Reverse DNS]    mail-qk1-f217.xxxxxx.xxx
[AlienVault]     alt13620212015.xxx.xxxxxx.xxx
[Reverse DNS]    mail-wr1-f87.xxxxxx.xxx
[Reverse DNS]    mail-lf1-x147.xxxxxx.xxx
[Reverse DNS]    mail-wr1-f10.xxxxxx.xxx
[Reverse DNS]    mail-wr1-f125.xxxxxx.xxx
[Reverse DNS]    mail-wr1-f122.xxxxxx.xxx
[Reverse DNS]    mail-qk1-f235.xxxxxx.xxx
[Reverse DNS]    mail-wr1-f62.xxxxxx.xxx
[HackerTarget]   alt300.xxxxxx.xxxxxx.xxx
[Reverse DNS]    mail-vk1-f136.xxxxxx.xxx
[Reverse DNS]    mail-wr1-f126.xxxxxx.xxx
[Reverse DNS]    mail-vk1-f189.xxxxxx.xxx
[Reverse DNS]    mail-qk1-f156.xxxxxx.xxx
[AlienVault]     mail-vs1-f70.xxxxxx.xxx
[Reverse DNS]    mail-qk1-f164.xxxxxx.xxx
[Reverse DNS]    mail-lf1-x15d.xxxxxx.xxx
[Reverse DNS]    mail-ua1-f97.xxxxxx.xxx

OWASP Amass v3.21.2                                     https://github.com/OWASP/Amass
s
-
-
45 names discovered - cert: 5, dns: 33, api: 7
-
ASN: xxxxx - xxxxxx - xxxxxx xxx
    xx.xxx.xx.x/24      1      Subdomain Name(s)
    xx.xxx.xxx.x/24     1      Subdomain Name(s)
    xxx.xxx.xx.x/20     4      Subdomain Name(s)
    xxx.xxx.x.x/15      7      Subdomain Name(s)
    xxx.xxx.xxx.x/24     6      Subdomain Name(s)
    xxxxxxxxxxxxxxxx/48  1      Subdomain Name(s)
    xxxxxxxxxxxxxxxx/48  5      Subdomain Name(s)
    xxx.xxx.xxx.x/24     1      Subdomain Name(s)
    xxx.xxx.xx.x/24      1      Subdomain Name(s)
    xxxxxxxxxxxxxxxx/48  2      Subdomain Name(s)
    xxx.xx.xxx.x/17      27     Subdomain Name(s)
    xxxxxxxxxxxxxxxx/48  1      Subdomain Name(s)
    xx.xxx.x.x/20        1      Subdomain Name(s)
    xx.xxx.xxx.x/19      1      Subdomain Name(s)
    xxxxxxxxxxxx/32      7      Subdomain Name(s)

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

e. To do Passive Scanning

amass enum -passive -d google.com -src

```
[Crtsh] staging-d.blogger.corp.google.com
[Crtsh] cache2.c.video.google.com
[Crtsh] cache5.c.docs.google.com
[Crtsh] orkut-impersonation.corp.google.com
[Crtsh] orkut-vctask0.corp.google.com
[Crtsh] cache3.c.video.google.com
[Crtsh] prom.corp.google.com
[Crtsh] cache2.c.docs.google.com
[Crtsh] cache6.c.play.google.com
[Crtsh] sites-googlegroups-qa02.corp.google.com
[Crtsh] prom-test.corp.google.com
[Crtsh] orkut-yqvrify.corp.google.com
[Crtsh] sites-googlegroups-qa06.corp.google.com
[Crtsh] staging-gaia.blogger.corp.google.com
[Crtsh] blogger.corp.google.com
[Crtsh] auth.corp.google.com
[Crtsh] orkut-yqtask0.corp.google.com
[Yahoo] duo.google.com
[Yahoo] remotedesktop.google.com
[Yahoo] pixel.google.com
[Google] developers.home.google.com

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

f. Identify domains by using -whois option

amass intel -d google.com -whois

```
(root@cdac)-[~]
# amass intel -d google.com -whois
google.ca
googlescholar.com
google.com.lv
googlecovid-19.com.cn
froogle.com
coturious.com
google-maps.fr
google.hk
financegoogle.fr
googleai.fr
developerdays.net
google.com.co
gkecnapps.cn
gugel.ca
google-patent-search.net
googletransparent.net
revolv.com
googletrends.com.cn
omnisio.com
youtubeonsale.com
admob.com.fr
googlebusiness.cn
googltalk.com
time-me.com
thinkwithgoogle.cn
googlepay.ms
googlelaiba.cn
googgle.com
gstatic.cn
indianagetonline.com
youtube.in
googlemashupeditor.ca
blogger.ca
openhands.net
domaintest.financial
mygmailrewards.com
waze.com
googlephoto.ca
```

g. Enable active recon method

amass intel -active -cidr 172.31.0.0/15

```
(root@cdac)~#  
# amass intel -active -cidr 172.31.0.0/15  
  
(root@cdac)~#
```

h. Search Based on ASN

amass intel -asn 23314,81323

```
(root@cdac)~#  
# amass intel -asn 23314,81323  
summit-broadband.com  
huge-dns.com  
naplesgarden.org  
brainchild.com  
ecsort.com  
beautifulmusic.cc  
btgfla.com  
floridaysorlando.com  
noblehousehotels.com  
boycehouse.com  
globalhrresearch.com  
visit.keznews.com  
obtssolutions.net  
provinsure.com  
centurylink.net  
rosenhotels.com  
collins-dupont.com  
mtg-fl.com  
cmgflorida.com  
horizonbusinessservices.com  
kooserver.kooline.com
```

i. Search string based on AS description information

amass intel -org "google"

```
(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 google.com


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

```
Between 08/10 16:46:52 2024 UTC → 08/10 20:48:30 2024 UTC  
and    08/10 21:51:58 2024 UTC → 08/10 21:52:29 2024 UTC
```

```
Found: googleproxy-66-249-81-31.google.com  
Found: rate-limited-proxy-108-177-72-220.google.com  
Found: mailot0-f193.google.com  
Found: mailvk0-f100.google.com  
Found: googleproxy-66-102-8-3.google.com  
Found: googleproxy-66-249-93-40.google.com  
Found: ratelimited-proxy-66-249-92-32.google.com  
Found: mailyb0-f204.google.com  
Found: googleproxy-66-249-81-252.google.com  
Found: cache8.c.play.google.com  
Found: googleproxy-66-249-81-212.google.com  
Found: googleproxy-66-102-9-13.google.com  
Found: mailpf0-f252.google.com  
Found: googleproxy-66-249-84-171.google.com  
Found: mailpf0-f153.google.com  
Found: mailyb0-f190.google.com  
Found: googleproxy-66-249-80-34.google.com  
Found: mailoi0-f32.google.com  
Found: mailio0-f243.google.com
```

```
Found: notebooklm.google.com  
Found: mailvk0-f11.google.com  
Found: ratelimited-proxy-66-249-87-180.google.com  
Found: ratelimited-proxy-66-249-87-14.google.com  
Found: mailpl0-f24.google.com  
Found: youtube-ui.l.google.com  
Found: people-pa.clients6.google.com  
Found: googleproxy-64-233-172-150.google.com  
Found: ratelimited-proxy-66-249-90-193.google.com  
Found: tools.l.google.com  
Found: google-proxy-66-249-93-110.google.com  
Found: ratelimited-proxy-66-249-87-83.google.com  
Found: mail-qal.sandbox.google.com  
Found: snap-storage-cdn.l.google.com  
Found: mailqk0-f183.google.com  
Found: googleproxy-66-249-93-4.google.com  
Found: mail.flexpack.google.com  
Found: googleproxy-66-249-81-74.google.com  
Found: feelinsonice.appspot.l.google.com  
Found: googleproxy-66-249-83-142.google.com  
Found: mailwm0-f13.google.com  
Found: staging-c.blogger.corp.google.com  
Found: googleproxy-66-249-82-200.google.com  
Found: mailpf0-f164.google.com  
Found: l.google.com  
Found: ratelimited-proxy-209-85-238-213.google.com  
Found: sites-googlegroups-qa08.corp.google.com  
Found: googleproxy-66-249-88-33.google.com  
Found: maillyw0-f224.google.com  
Found: vp.video.l.google.com  
Removed: _caldav._tcp.google.com  
Removed: _caldavs._tcp.google.com  
Removed: _ldaps._tcp.google.com 2001:4860:4802:32::3a,216.239.32.58  
Removed: _ldap._tcp.google.com 216.239.32.58,2001:4860:4802:32::3a  
Removed: _carddavs._tcp.google.com 142.251.39.14,2a00:1450:4005:802::200e
```