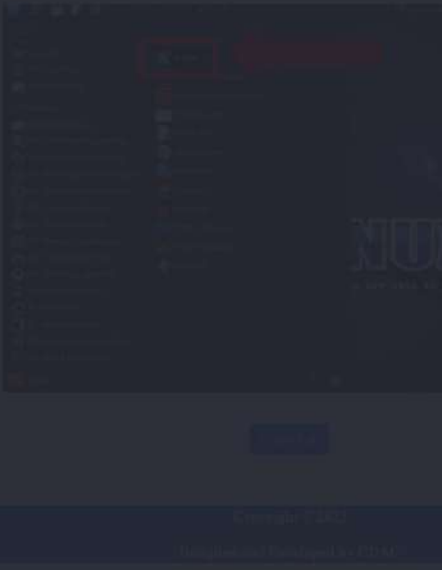


```
root@kali: /home/kiyotaka/Downloads
root@kali)-[/home/kiyotaka/Downloads]
# amass enum -d hackersploit.com 80,443,8080,8443
hackersploit.com (FQDN) --> ns_record --> nsg1.namebrightdns.com (FQDN)
hackersploit.com (FQDN) --> ns_record --> nsg2.namebrightdns.com (FQDN)

The enumeration has finished

root@kali)-[/home/kiyotaka/Downloads]
[ ]
```



Copyright © 2022
Unauthorized Use Prohibited by EULA

```
(root@kali)-[/home/kiyotaka/Downloads]
# amass enum -d hackersploit.com,google.com -active
hackersploit.com (FQDN) --> ns_record --> nsg1.namebrightdns.com (FQDN)
hackersploit.com (FQDN) --> ns_record --> nsg2.namebrightdns.com (FQDN)
google.com (FQDN) --> ns_record --> ns2.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns4.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns1.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns3.google.com (FQDN)
account.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
local.google.com (FQDN) --> cname_record --> maps.l.google.com (FQDN)
alerts.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
android.clients.google.com (FQDN) --> cname_record --> android.l.google.com (FQDN)
support.google.com (FQDN) --> a_record --> 142.250.185.142 (IPAddress)
support.google.com (FQDN) --> aaaa_record --> 2607:f8b0:4006:824::200e (IPAddress)
datafusion-api.cloud.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
dataproc-staging.cloud.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
chrome.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
ping.feedburner.google.com (FQDN) --> cname_record --> www4.l.google.com (FQDN)
baseline.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
142.250.160.0/19 (Netblock) --> contains --> 142.250.185.142 (IPAddress)
15169 (ASN) --> managed_by --> GOOGLE - Google LLC (RIR)Organization)
15169 (ASN) --> announces --> 142.250.160.0/19 (Netblock)
www.adwords.google.com (FQDN) --> cname_record --> adwords.google.com (FQDN)
groups.google.com (FQDN) --> cname_record --> wide-groups.l.google.com (FQDN)
google.com (FQDN) --> a_record --> 142.250.207.174 (IPAddress)
google.com (FQDN) --> aaaa_record --> 2404:6800:4009:806::200e (IPAddress)
productforums.google.com (FQDN) --> cname_record --> groups.l.google.com (FQDN)
mobile.google.com (FQDN) --> cname_record --> mobile.l.google.com (FQDN)
adsense.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
google.com (FQDN) --> mx_record --> smtp.google.com (FQDN)
lookerstudio.asia-southeast1.cloud.google.com (FQDN) --> a_record --> 142.251.40.238 (IPAddress)
lookerstudio.asia-southeast1.cloud.google.com (FQDN) --> aaaa_record --> 2a00:1450:4001:81c::200e (IPAddress)
spreadsheets.google.com (FQDN) --> cname_record --> spreadsheets.l.google.com (FQDN)
aboutme.google.com (FQDN) --> cname_record --> plus.l.google.com (FQDN)
composer-dev.cloud.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
datasetsearch.research.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
```

```
(root@kali)-[/home/kiyotaka/Downloads]
# amass enum -brute -d google.com -demo
google.com (FQDN) --> ns_record --> ns2.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns4.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns1.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns3.google.com (FQDN)
alerts.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
support.google.com (FQDN) --> a_record --> 142.250.4.102 (IPAddress)
support.google.com (FQDN) --> a_record --> 142.250.4.113 (IPAddress)
support.google.com (FQDN) --> a_record --> 142.250.4.100 (IPAddress)
support.google.com (FQDN) --> a_record --> 142.250.4.138 (IPAddress)
support.google.com (FQDN) --> a_record --> 142.250.4.101 (IPAddress)
datafusion-api.cloud.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
productforums.google.com (FQDN) --> cname_record --> groups.l.google.com (FQDN)
aboutme.google.com (FQDN) --> cname_record --> plus.l.google.com (FQDN)
composer-dev.cloud.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
dataproc-image-staging.cloud.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
sb.google.com (FQDN) --> cname_record --> sb.l.google.com (FQDN)
support.google.com (FQDN) --> aaaa_record --> 2607:f8b0:4006:824::200e (IPAddress)
support.google.com (FQDN) --> a_record --> 142.250.4.139 (IPAddress)
spreadsheets.l.google.com (FQDN) --> a_record --> 142.250.184.238 (IPAddress)
spreadsheets.l.google.com (FQDN) --> aaaa_record --> 2a00:1450:4001:831::200e (IPAddress)
tensorboard-staging.cloud.google.com (FQDN) --> a_record --> 142.251.222.110 (IPAddress)
tensorboard-staging.cloud.google.com (FQDN) --> aaaa_record --> 2404:6800:4007:804::200e (IPAddress)
gmail.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
gemini.google.com (FQDN) --> a_record --> 142.250.65.174 (IPAddress)
gemini.google.com (FQDN) --> aaaa_record --> 2404:6800:4002:804::200e (IPAddress)
education.google.com (FQDN) --> a_record --> 172.217.70.113 (IPAddress)
education.google.com (FQDN) --> a_record --> 172.217.70.102 (IPAddress)
education.google.com (FQDN) --> a_record --> 172.217.70.101 (IPAddress)
education.google.com (FQDN) --> a_record --> 172.217.70.138 (IPAddress)
education.google.com (FQDN) --> a_record --> 172.217.70.139 (IPAddress)
education.google.com (FQDN) --> a_record --> 172.217.70.100 (IPAddress)
education.google.com (FQDN) --> aaaa_record --> 2607:f8b0:4006:80b::200e (IPAddress)
shop.google.com (FQDN) --> a_record --> 74.125.68.92 (IPAddress)
shop.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c03::5c (IPAddress)
```

```
Apps Places Jul 10 02:46 2% 35% ↑ 10 KB ↓ 13 KB root@kali: /home/kiyotaka/Downloads

root@kali)-[/home/kiyotaka/Downloads]
# amass enum -passive -d google.com
google.com (FQDN) --> ns_record --> ns2.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns4.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns1.google.com (FQDN)
google.com (FQDN) --> ns_record --> ns3.google.com (FQDN)
google.com (FQDN) --> mx_record --> smtp.google.com (FQDN)
alerts.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
adsense.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
aboutme.google.com (FQDN) --> cname_record --> plus.l.google.com (FQDN)
browsersync.google.com (FQDN) --> cname_record --> browsersync.l.google.com (FQDN)
alt42.aspmx.google.com (FQDN) --> a_record --> 192.178.164.26 (IPAddress)
alt42.aspmx.google.com (FQDN) --> aaaa_record --> 2607:f8b0:4023:2009::1b (IPAddress)
sb.google.com (FQDN) --> cname_record --> sb.l.google.com (FQDN)
gmail.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
videos.google.com (FQDN) --> cname_record --> video.google.com (FQDN)
blog.google.com (FQDN) --> cname_record --> www.blogger.com (FQDN)
catalog.google.com (FQDN) --> cname_record --> books.google.com (FQDN)
books.google.com (FQDN) --> a_record --> 142.251.42.78 (IPAddress)
books.google.com (FQDN) --> aaaa_record --> 2404:6800:4009:831::200e (IPAddress)
w.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
about.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
sprint.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
142.251.32.0/19 (Netblock) --> contains --> 142.251.42.78 (IPAddress)
192.178.0.0/15 (Netblock) --> contains --> 192.178.164.26 (IPAddress)
15169 (ASN) --> managed_by --> GOOGLE - Google LLC (RIROrganization)
15169 (ASN) --> announces --> 142.251.32.0/19 (Netblock)
15169 (ASN) --> announces --> 192.178.0.0/15 (Netblock)
baseline.google.com (FQDN) --> cname_record --> www3.l.google.com (FQDN)
adwords.google.com (FQDN) --> a_record --> 142.250.4.113 (IPAddress)
adwords.google.com (FQDN) --> a_record --> 142.250.4.139 (IPAddress)
adwords.google.com (FQDN) --> a_record --> 142.250.4.100 (IPAddress)
adwords.google.com (FQDN) --> a_record --> 142.250.4.138 (IPAddress)
adwords.google.com (FQDN) --> a_record --> 142.250.4.102 (IPAddress)
adwords.google.com (FQDN) --> a_record --> 142.250.4.101 (IPAddress)
adwords.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c05::65 (IPAddress)
```

