Installation

```
$ snap install amass
amass v3.12.3 from Jeff Foley (caffix) installed
```

Configuration

```
# Should results only be collected passively and
# without DNS resolution? Not recommended.
#mode = passive

# Would you like to use active techniques that
# communicate directly with the discovered assets,
# such as pulling TLS certificates from discovered IP
# addresses and attempting DNS zone transfers?
mode = active

# The directory that stores the Cayley graph database
# and other output files
# The default for Linux systems is:
# $HOME/.config/amass
output_directory = /home/$USER/amass

# DNS resolvers used globally by the amass package.
[resolvers]
monitor_resolver_rate = true
```

resolver = 1.1.1.1 ; Cloudflare

resolver = 8.8.8.8 ; Google

resolver = 1.0.0.1 ; Cloudflare Secondary

resolver = 8.8.4.4 ; Google Secondary

[scope]

The network infrastructure settings expand scope, not
restrict the scope.

Single IP address or range (e.g. a.b.c.10-245)

address = 192.168.1.1

cidr = 192.168.1.0/24

asn = 26808

port = 80

port = 443

port = 8080

Root domain names used in the enumeration. The

findings are limited by the root domain names # provided.

[scope.domains]

domain=securedigitallife.com

domain=securityweekly.com

domain=securityweekly.net

domain=psw.io

domain=hacknaked.tv

```
# The graph database discovered DNS names, associated #
network infrastructure, results from data sources, #
etc.

# This information is then used in future enumerations
# and analysis of the discoveries.

[graphdbs]

local_database = true ; Set this to false to disable
use of the local database.


# Settings related to DNS name brute forcing.

[bruteforce]

enabled = true

recursive = true

# Number of discoveries made in a subdomain before #
performing recursive brute forcing: Default is 1.

minimum_for_recursive = 1

wordlist_file = /home/$USER/wordlists/sub5000.txt


# Multiple lists can be used.

#wordlist_file = /usr/share/wordlists/all.txt

#wordlist_file = /usr/share/wordlists/all.txt


# Would you like to permute resolved names?

[alterations]

enabled = false
```

```
[data_sources]
# When set, this time-to-live is the minimum value
applied to all data source caching.
minimum_ttl = 1440 ; One day

# https://otx.alienvault.com (Free)
[data_sources.AlienVault]
[data_sources.AlienVault.Credentials]
apikey = <key>

# https://app.binaryedge.com (Free)
[data_sources.BinaryEdge]
ttl = 10080
[data_sources.BinaryEdge.Credentials]
apikey = <key>

# https://censys.io (Free)
[data_sources.Censys]
ttl = 10080
[data_sources.Censys.Credentials]
apikey = <key>
secret = <secret>

# https://cloudflare.com (Free)
[data_sources.Cloudflare]
[data_sources.Cloudflare.Credentials]
```

```
apikey = <key>

# https://passivetotal.com (Free)
[data_sources.PassiveTotal]
ttl = 10080
[data_sources.PassiveTotal.Credentials]
username = <email>
apikey = <key>

# https://securitytrails.com (Free)
[data_sources.SecurityTrails]
ttl = 1440
[data_sources.SecurityTrails.Credentials]
apikey = <key>

# https://shodan.io (Free)
[data_sources.Shodan]
ttl = 10080
[data_sources.Shodan.Credentials]
apikey = <key>

# https://urlscan.io (Free)
# URLScan can be used without an API key, but the key # allows new submissions to be made
[data_sources.URLScan]
[data_sources.URLScan.Credentials]
```

apikey = <key>

https://virustotal.com (Free)

[data_sources.VirusTotal]

ttl = 10080

[data_sources.VirusTotal.Credentials]

apikey = <key>

Commands

Don’t do this, put your targets in the config file!

amass enum -config ~/.config/amass/config.ini -src -ip -o myoutput.txt -d "$(< domains.txt)

Do this instead:

amass enum -config ~/.config/amass/config.ini -src -ip -o myoutput.txt

Results

```
[BufferOver]      test.securityweekly.com 35.196.248.27
[VirusTotal]      bolivar.securityweekly.net
104.130.139.158,2001:4800:7818:103:be76:4eff:fe05:904
[Riddler]         email.securityweekly.com 172.217.12.147
[PassiveTotal]    resources.infosecworldusa.com 205.162.44.70
[BufferOver]      hubbyapi.psw.io 50.116.23.207
```

[VirusTotal] archives.securityweekly.net 35.196.248.27

[BufferOver] hsmail.cyberleadersunite.com 199.60.103.30

[Riddler] archive.securityweekly.com 35.196.248.27

[Brute Forcing] wiki.psw.io 69.164.202.59

[SecurityTrails] www.securityweekly.net 35.196.248.27

[BufferOver] webhooks.cyberriskalliance.com 2606:4700:3034::6815:4932,104.21.73.50,172.67.140.153,2606:4700:3035::ac43:8c99

[VirusTotal] resources.cyberriskalliance.com 205.162.44.69

[PassiveTotal] qa.securedigitallife.com 35.196.248.27

[Active Crawl] www.cyberleadersunite.com 199.60.103.226,199.60.103.30

[CertSpotter] streamer.psw.io 35.196.248.27

[VirusTotal] email.securityweekly.net 172.217.12.147

[VirusTotal] series.psw.io 3.130.164.237

[Riddler] docs.securityweekly.com 172.217.12.147

[Active Crawl] cdn.cyberleadersunite.com 172.67.73.48,104.26.1.138,104.26.0.138,2606:4700:20::681a:18a,2606:4700:20::681a:8a,2606:4700:20::ac43:4930

[Wayback] startup.securityweekly.com 35.196.248.27

[VirusTotal] events.infosecworldusa.com 205.162.44.64

[BufferOver] studio.psw.io 72.87.121.99

[BufferOver] chat.cyberleadersunite.com 104.26.0.138,172.67.73.48,104.26.1.138,2606:4700:20::681a:8a,2606:4700:20::681a:18a,2606:4700:20::ac43:4930

[BufferOver] pen.cyberleadersunite.com 172.67.73.48,104.26.0.138,104.26.1.138,2606:4700:20::681a:8a,2606:4700:20::681a:18a,2606:4700:20::ac43:4930

[BufferOver] staging.eventregistration.cyberriskalliance.com 64.227.31.61

[BufferOver] www.hacknaked.tv 35.196.248.27

[BufferOver] mail.cyberleadersunite.com 104.26.0.138,172.67.73.48,104.26.1.138,2606:4700:20::681a:8a,2606:4700:20::681a:18a,2606:4700:20::ac43:4930

[VirusTotal] cal.securityweekly.net 172.217.12.147

Tracking

```
amass track -d "$(<domains.txt)" -dir
/home/$USER/amass/ > track.txt
```

```
---------------------------------------------------------------------------
Between 03/15 12:20:59 2021 EDT -> 03/15 12:51:42 2021 EDT
and     03/18 09:01:20 2021 EDT -> 03/18 09:12:16 2021 EDT
---------------------------------------------------------------------------
Moved: docs.securityweekly.net
 from   172.217.7.19,2607:f8b0:4006:805::2013
 to     172.217.12.147
Moved: web.securityweekly.net
 from   172.217.7.19,2607:f8b0:4006:805::2013
 to     172.217.12.147
Moved: email.securityweekly.net
 from   172.217.7.19,2607:f8b0:4006:805::2013
 to     172.217.12.147
Removed: www.cybersecuritycollaboration.com
104.21.82.38,2606:4700:3037::ac43:98a9,2606:4700:3036::6815:5226,172.67.152.169
Removed: events.cybersecuritycollaboration.com 52.213.47.89,3.248.123.157
Removed: cybersecuritycollaboration.com
104.21.82.38,172.67.152.169,2606:4700:3036::6815:5226,2606:4700:3037::ac43:98a9
Removed: host.cybersecuritycollaboration.com
104.21.82.38,172.67.152.169,2606:4700:3037::ac43:98a9,2606:4700:3036::6815:5226
```

Putting it all together:

```
$ amass enum -config ~/.config/amass/config.ini -src -
ip -o results.txt
```

```
$ awk '{print $2}' results.txt | grep -v Crawl >
targets.txt
```

```
$ sudo nmap -p 80,443,8080 -sS -oX targets.xml -iL
targets.txt
```

```
$ git clone
https://github.com/FortyNorthSecurity/EyeWitness.git
```

```
$ cd EyeWitness/Python/setup
```

```
$ sudo ./setup.sh
```

```
$ cd ..
```

```
$ ./EyeWitness.py -x ~/asm/targets.xml --web -d
/home/$USER/asm/screens
```

https://startup.securityweekly.com
Resolved to: 35.196.248.27

Page Title: Business Security Weekly Archives - Security Weekly
Server: nginx
Date: Thu, 13 May 2021 17:45:54 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 129888
Connection: close
Vary: Accept-Encoding
Link: <https://securityweekly.com/wp-json/>; rel="https://api.w.org/"
X-Powered-By: WP Engine
X-Cacheable: SHORT
Cache-Control: max-age=600, must-revalidate
X-Cache: HIT: 4
X-Cache-Group: normal
Accept-Ranges: bytes
Response Code: 200

Source Code