Build your own reconnaissance system with Osmedeus Next Generation

by Ai Ho (aka j3ssie)

whoami

- My name is Ai Ho (aka j3ssie)
- Hacker and developer combined
- ❤️ Open-source lover
- Author of several notable projects: Osmedeus, Jaeles and Metabigor
- Acknowledge by / Security hall of fame: Google, Apple, Microsoft, Yahoo, StackOverflow, DoD, Alibaba, Grab, Snapchat, Tencent, Django, Red Hat, FireEye, F-Secure, SAP, Hyatt, ATT, Mastercard and so on

Successfully hunt on

and many many more

Agenda

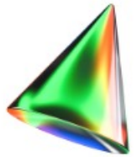
- Why?
- Archiecture
- Understand the Workflow
- Demo

Problem in reconnaissance ?

1. Too much repetitive manual work.
2. Too much time-consuming to build everything from scratch.
3. Too many tools available but each only does a few things.

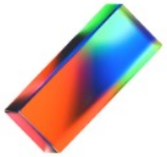
Main Osmedeus objectives

Significantly speed up your recon process



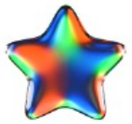
Efficiently to customize and optimize your recon process

Organize your scan results



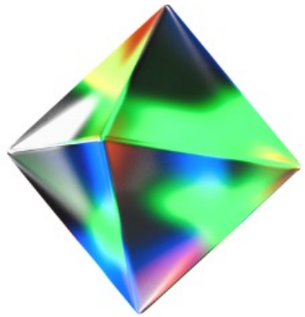
Easy to scale across large number of targets

Seamlessly integrate with new public and private tools



Easy to synchronize the results across many places

Architecture of Osmedeus

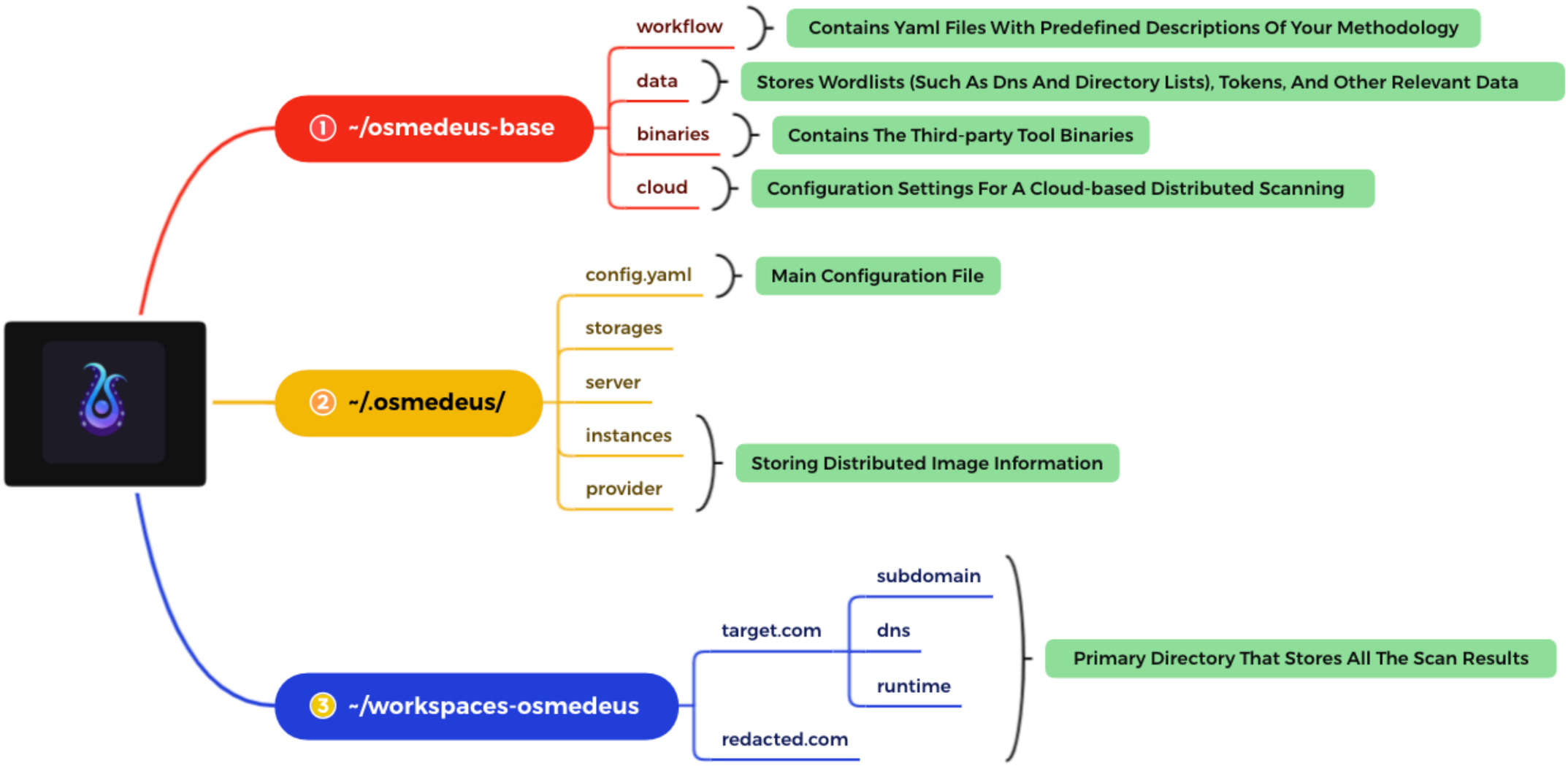


Core Engine

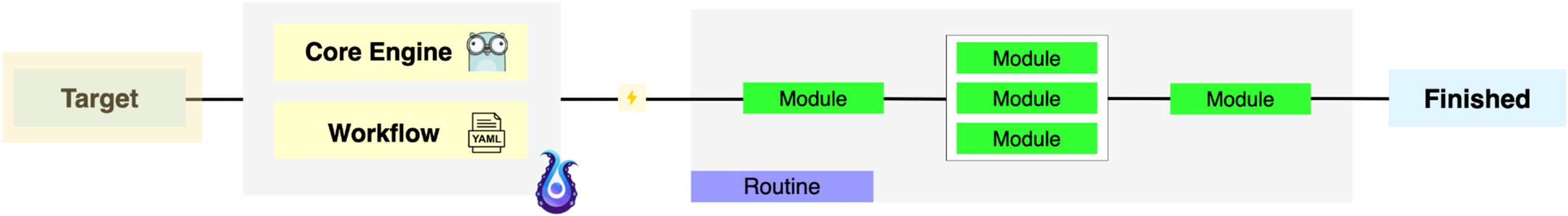
Written in Golang which is responsible for handling all the complex logic and provide a lot of built-in utilities to run your workflow much more efficient

Workflow

A collection of YAML files that describe your methodology

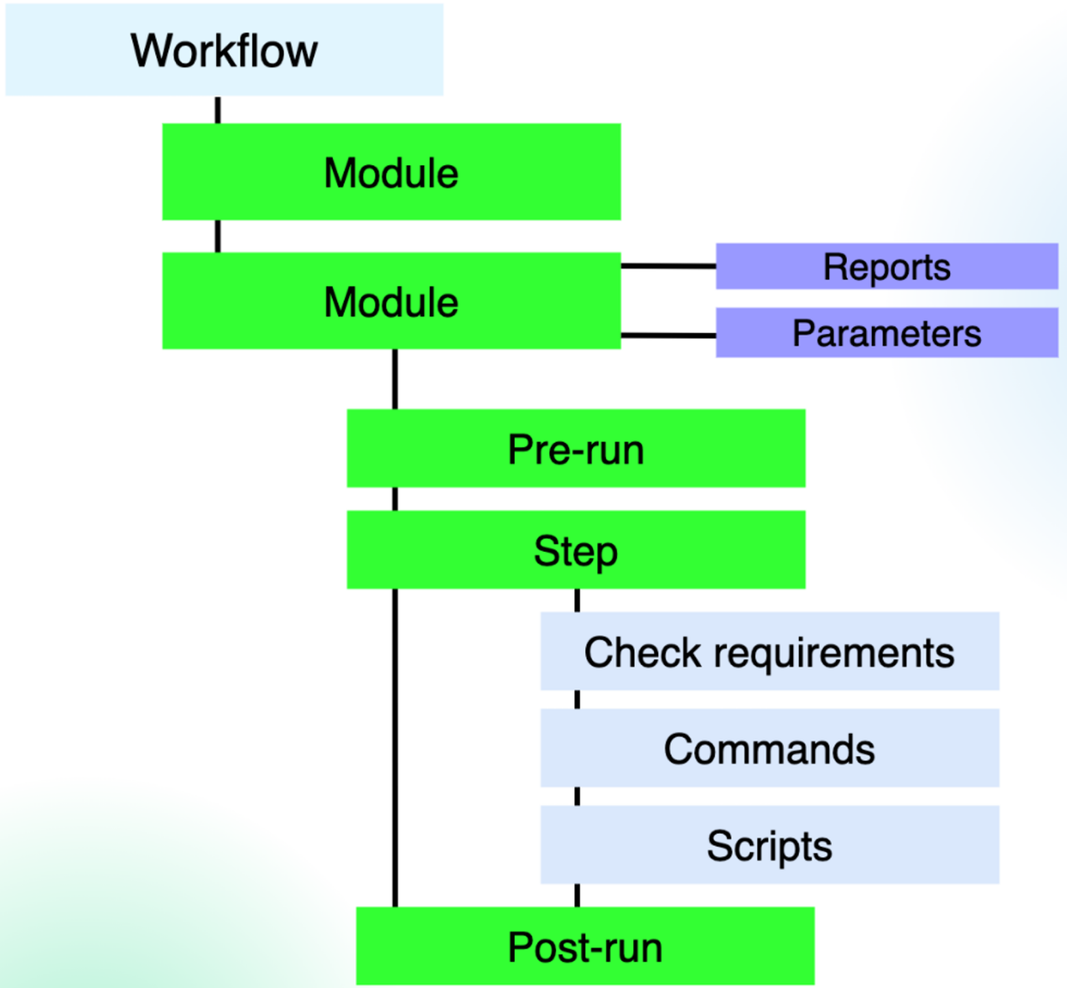


Routine Overview



Target can be URL, domain, IP or anything fit with your workflow provided from cli or web UI

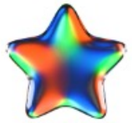
Workflow Breakdown



Understand the Workflow

Flow

Flow contains multiple module and also define order how to run these modules.

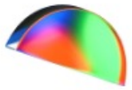


Module

Contains detail of multiple step

Target

can be domain, url, IP, CIDR or anything that fit your workflow



Step

Step is smallest part of the Osmedeus workflow

EXPLORER ···

OSMEDEUS-WORKFLOW

- .github
- cidr
- custom
- default-modules
- extensive
- general
- sync
- test
- urls
  - cidr.yaml
  - domains.yaml
  - extensive-vuln.yaml
  - extensive.yaml
  - fast.yaml
  - general.yaml
  - quick-cidr.yaml
  - README.md
  - sync.yaml
  - test.yaml
  - urls.yaml
  - vuln-and-dirb.yaml
  - vuln.yaml

general.yaml

general.yaml

```yaml
name: general
desc: Running default reconnaissance routine
type: general
validator: domain

routines:
  - modules:
      - subdomain
  - modules:
      - probing
  - modules:
      - fingerprint
  - modules:
      - screenshot
  - modules:
      - spider
  - modules:
      - sto
      - archive
      - ipspace
  - modules:
      - vulnscan
  - modules:
      - dirbscan
  - modules:
      - portscan
```

Flow

general > subdomain.yaml

```yaml
name: subdomain
desc: Scanning for subdomain

report:
  final:
    - "{{Output}}/subdomain/final-{{Workspace}}.txt"
    - "{{Output}}/subdomain/more-{{Workspace}}.txt"

# {{Output}} == {{Workspaces}} + {{Workspace}} but strip "/" char
pre_run:
  - CreateFolder("{{Output}}/subdomain/")

params:
  - amassTimeout: "3h"
  - subfinderThreads: "{{threads * 5}}"

steps:
  - required:
      - "{{Binaries}}/amass"
      - "{{Binaries}}/subfinder"
      - "{{Binaries}}/assetfinder"
      - "{{Binaries}}/findomain"
    commands:
      - "timeout -k 1m {{amassTimeout}} {{Binaries}}/amass enum -config {{Data}}/configs/amass.ini -d {{Target}} -o {{Output}}/subdomain/{{Workspace}}-amass.txt >/dev/null 2>&1"
      - "{{Binaries}}/assetfinder -subs-only {{Target}} > {{Output}}/subdomain/{{Workspace}}-assetfinder.txt"
  # these two commands will run in parallels
  - commands:
      - "{{Binaries}}/findomain -u {{Output}}/subdomain/{{Workspace}}-findomain.txt -t {{Target}} >/dev/null 2>&1"
      - "{{Binaries}}/subfinder -d {{Target}} -t {{subfinderThreads}} -o {{Output}}/subdomain/{{Workspace}}-subfinder.txt >/dev/null 2>&1"

```

Module

```
- scripts:
    - Append("{{Output}}/subdomain/sum-{{Workspace}}.txt", "{{Output}}/subdomain/{{Workspace}}-amass.txt")
    - Append("{{Output}}/subdomain/sum-{{Workspace}}.txt", "{{Output}}/subdomain/{{Workspace}}-subfinder.txt")
    - Append("{{Output}}/subdomain/sum-{{Workspace}}.txt", "{{Output}}/subdomain/{{Workspace}}-assetfinder.txt")
    - Append("{{Output}}/subdomain/sum-{{Workspace}}.txt", "{{Output}}/subdomain/{{Workspace}}-findomain.txt")
    # remove junk subdomain like sample@subdomain.com and 1-2-3.subdomain.com format
    - ExecCmd("cat {{Output}}/subdomain/sum-{{Workspace}}.txt | {{Binaries}}/cleansub -t '{{Target}}' > {{Output}}/subdomain/final-{{Workspace}}.txt")
- scripts:
    - SortU("{{Output}}/subdomain/final-{{Workspace}}.txt")
```

```
# for Cleaning output of some tools or module
Cleaning, CleanAmass, CleanGoBuster, CleanMassdns, CleanWebanalyze

# for Notification
StartNoti, DoneNoti, ReportNoti, DiffNoti

# for Push result to git Storages
PushResult, PushFolder, DiffCompare


# for Remote control
ExecCmd, ExecLoop, RemoteLogin, RemoteUpload, ExecRemote, ExecScheduleRemote


# for I/O utility and others
Cleaning, CreateFolder, DeleteFile, DeleteFolder, Copy, Append, Unique, Sort, StripName, EmptyDir, EmptyFile, Printf, SplitFile
```

Scripts used as a shortcut for specific task

general > subdomain.yaml

```yaml
name: subdomain
desc: Scanning for subdomain

report:
  final:
    - "{{Output}}/subdomain/final-{{Workspace}}.txt"
    - "{{Output}}/subdomain/more-{{Workspace}}.txt"

# {{Output}} == {{Workspaces}} + {{Workspace}} but strip "/" char
pre_run:
  - CreateFolder("{{Output}}/subdomain/")

params:
  - amassTimeout: "3h"
  - subfinderThreads: "{{threads * 5}}"
```

Reports

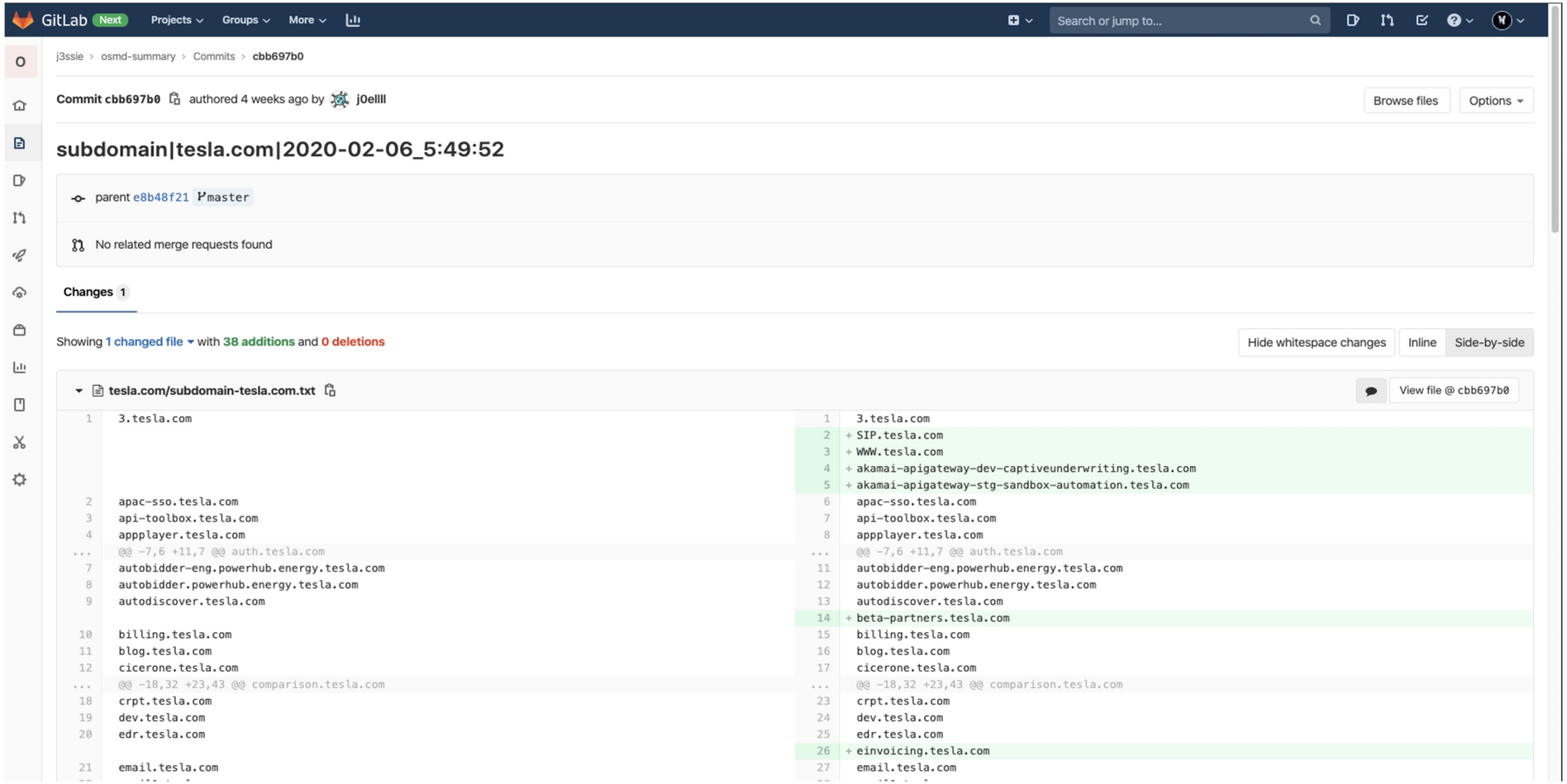
Parameters

```yaml
# these two commands will run in parallels
- commands:
  - "{{Binaries}}/findomain -u {{Output}}/subdomain/{{Workspace}}-findomain.txt -t {{Target}} >/dev/null 2>&1"
  - "{{Binaries}}/subfinder -d {{Target}} -t {{subfinderThreads}} -o {{Output}}/subdomain/{{Workspace}}-subfinder.txt >/dev/null 2>&1"
```

Run in Parallel

```yaml
# cleaning some result
- scripts:
  - Append("{{Output}}/subdomain/sum-{{Workspace}}.txt", "{{Output}}/subdomain/{{Workspace}}-amass.txt")
  - Append("{{Output}}/subdomain/sum-{{Workspace}}.txt", "{{Output}}/subdomain/{{Workspace}}-subfinder.txt")
  - Append("{{Output}}/subdomain/sum-{{Workspace}}.txt", "{{Output}}/subdomain/{{Workspace}}-assetfinder.txt")
  - Append("{{Output}}/subdomain/sum-{{Workspace}}.txt", "{{Output}}/subdomain/{{Workspace}}-findomain.txt")
```

Run in Serial



Git Storages

#reports

1 | 0 | Add a topic

Search

Today

jbot APP 4:20 PM

/private/tmp/Osmedeus/workspaces/duckduckgo.com/subdomain/final-duckduckgo.com.txt

```
1  aaron.duckduckgo.com
2  abeyang.duckduckgo.com
3  about.duckduckgo.com
4  ac.duckduckgo.com
5  andrey.duckduckgo.com
6  answers.duckduckgo.com
7  api.duckduckgo.com
8  ashish.duckduckgo.com
9  audio.duckduckgo.com
10 b2.duckduckgo.com
11 bartek.duckduckgo.com
12 bastion.duckduckgo.com
13 beta.duckduckgo.com
14 bhall.duckduckgo.com
15 blake.duckduckgo.com
16 blog.duckduckgo.com
17 brad.duckduckgo.com
18 brian.duckduckgo.com
19 brindy.duckduckgo.com
20 bttf.duckduckgo.com
```

osm-reports

2 subscribers

04 January

osm-reports 2 23:39

```
[weblogic-console-rce-probe][Tentative-Critical] - https://comply08.mavent.com/console/css/%252e%252e%252fconsole.portal?_nfpb=false&_pageLabel=&handle=com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime.getRuntime().exec('whoami')") - /root/.osmedeus/workspaces/mavent.com/vuln/active/comply08.mavent.com/weblogic-console-rce-probe-1fac2a8099aae4ff7df1529c0d4a634c3f5c2de2
[weblogic-console-rce-probe][Tentative-Critical] - https://comply08.mavent.com/console/css/%252e%252e%252fconsole.portal?_nfpb=false&_pageLabel=&handle=com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime.getRuntime().exec('whoami')") - /root/.osmedeus/workspaces/mavent.com/vuln/active/comply08.mavent.com/weblogic-console-rce-probe-e5d1675f2de64aa1d1163d3d3eebe60e8a419b14
```

05 January

osm-reports 4 06:24

```
[oracle-equola-flash-xss][Tentative-Low] - http://images.seemore.zebra.com/Web/FifthThirdBank/player.swf?playerReady=1-location.replace`javascript:alert%2528document.location%2529` - /root/.osmedeus/workspaces/zebra.com/vuln/active/images.seemore.zebra.com/oracle-equola-flash-xss-785793a66a58d2ac4ab6a8c27cfee943ee472899
[pingidentity-opendirect][Certain-Low] - https://dev-pi.zebra.com/sp/startSLO.ping?TargetResource=https://bing.com - /root/.osmedeus/workspaces/zebra.com/vuln/active/dev-pi.zebra.com/pingidentity-opendirect-f6a327af9f1385e13280f8bcdf356cbd9d0e64d9
[pingidentity-opendirect][Certain-Low] - https://pi.zebra.com/sp/startSLO.ping?TargetResource=https://bing.com - /root/.osmedeus/workspaces/zebra.com/vuln/active/pi.zebra.com/pingidentity-opendirect-538d7a57b94607665a1da8f0f4627ee0df3017c5
[route-disclosure-01][Certain-Low] - https://fts.zebra.com/%ff - /root/.osmedeus/workspaces/zebra.com/vuln/active/fts.zebra.com/route-disclosure-01-ffef3a90fa30ffd44febdf475f37c2f2374e4701
[route-disclosure-01][Certain-Low] - https://qa-fts.zebra.com/%ff - /root/.osmedeus/workspaces/zebra.com/vuln/active/qa-fts.zebra.com/route-disclosure-01-8227c638633280aea794acbaa2d478304d9b51c0
[oracle-equola-flash-xss][Tentative-Low] - http://images.seemore.zebra.com/Web/FifthThirdBank/player.swf?playerReady=1-location.replace`javascript:alert%2528document.location%2529` - /root/.osmedeus/workspaces/zebra.com/vuln/active/images.seemore.zebra.com/oracle-equola-flash-xss-cd7b031a89c803080a78c3b5e2b8e02457d5c37f
[pingidentity-opendirect][Certain-Low] - https://dev-pi.zebra.com/sp/startSLO.ping?TargetResource=https://bing.com - /root/.osmedeus/workspaces/zebra.com/vuln/active/dev-pi.zebra.com/pingidentity-opendirect-766d15e844af904a698e2872b69e7819193ba6a4
[pingidentity-opendirect][Certain-Low] - https://pi.zebra.com/sp/startSLO.ping?TargetResource=https://bing.com - /root/.osmedeus/workspaces/zebra.com/vuln/active/pi.zebra.com/pingidentity-opendirect-c9550ca3750223f9b34cebf92598a2ba6ecb0e13
[route-disclosure-01][Certain-Low] - https://fts.zebra.com/%ff - /root/.osmedeus/workspaces/zebra.com/vuln/active/fts.zebra.com/route-disclosure-01-ee940f9e24c0b83c4b8b14b2585abb3b006d3f2a
[route-disclosure-01][Certain-Low] - https://qa-fts.zebra.com/%ff - /root/.osmedeus/workspaces/zebra.com/vuln/active/qa-fts.zebra.com/route-disclosure-01-8d7e8b4b9c4f42b7eb60aca4830d8520ae0d7257
[pingidentity-opendirect][Certain-Low] - https://test-pi.zebra.com/sp/startSLO.ping?TargetResource=https://bing.com - /root/.osmedeus/workspaces/zebra.com/vuln/active/test-pi.zebra.com/pingidentity-opendirect-b051737f2fa27d383581467496f745d8236c48f7
[pingidentity-opendirect][Certain-Low] - https://test-pi.zebra.com/sp/startSLO.ping?TargetResource=https://bing.com - /root/.osmedeus/workspaces/zebra.com/vuln/active/test-pi.zebra.com/pingidentity-opendirect-97e3bfe882fbbb090131e153179b024141d86211
```

Notification

```
root@osmedeus ▶ ~ osmedeus server
[+] Osmedeus v4.4.0 by @j3ssiejjj
[+] Web UI available at: https://0.0.0.0:8000/ui/
[+] Static Content available at: https://0.0.0.0:8000/21523

                   Fiber v2.42.0
                 https://[::]:8000

 Handlers ............ 30  Processes ........... 1
 Prefork ....... Disabled  PID ............. 30901

15:42:05 | 400 |      0s | 171.232.109.139 | GET      | /api
15:42:39 | 200 |      0s | 171.232.109.139 | POST     | /api
15:43:15 | 200 |     2ms | 171.232.109.139 | GET      | /api
15:43:15 | 200 |      0s | 171.232.109.139 | GET      | /api

root@osmedeus ▶ ~ cat ~/.osmedeus/config.yaml | grep 'pass'
    password: 5667f81ac75c7cc
    db_pass: DB_PASS
    password: GITLAB_PASS
    master_pass: ""
root@osmedeus ▶ ~
```

https://demo.osmedeus.local:8000/ui/index.html#/workspaces

Osmedeus **Next Generation UI** | Workspaces | Utilities

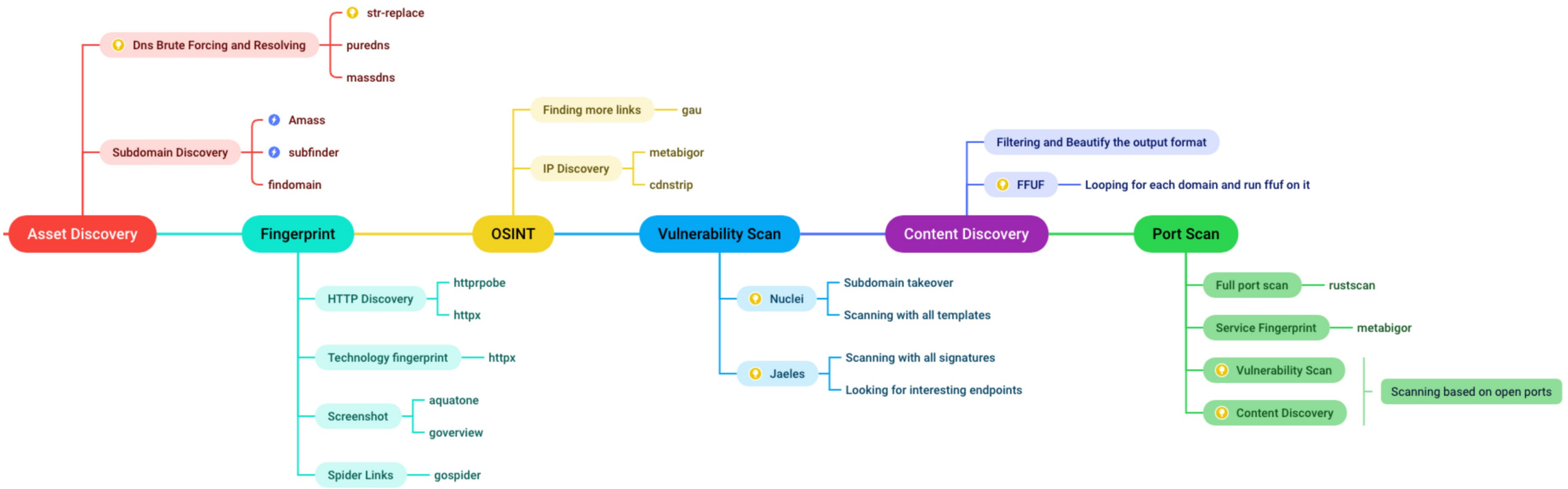
Index of all workspaces

Filter table | New Scan + | Raw View

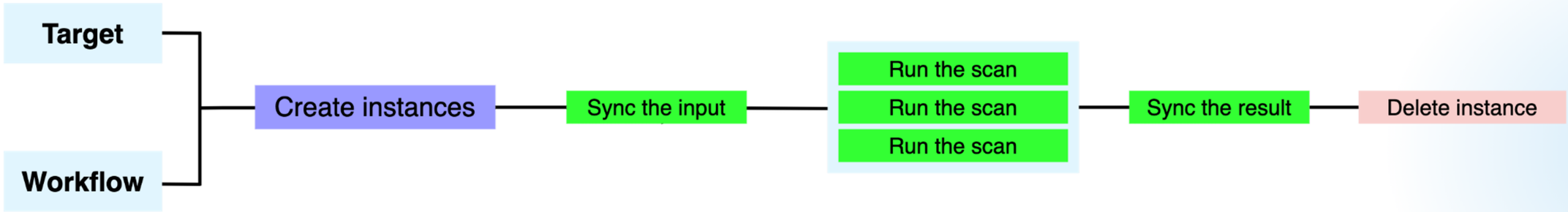
Target	Detail	Routine	Progress	Running Time	Statistics	Updated
sample-urls.txt	Reports (12)	flow/urls	14/14	0.369 h	subdomains/0 dns/0 directory/211 vuln/0 screenshots/0 archive/0 links/0	4/8/2023
spotify.net	Reports (N/A)	flow/general	0/44	0.000 h	subdomains/0 dns/0 directory/0 vuln/0 screenshots/0 archive/0 links/0	1/1/1
103.120.231.1_24	Reports (24)	flow/cidr	23/23	2.299 h	subdomains/0 dns/0 directory/0 vuln/0 screenshots/0 archive/0 links/0	4/8/2023
202.181.69.1_24	Reports (24)	flow/cidr	23/23	0.579 h	subdomains/0 dns/0 directory/0 vuln/0 screenshots/0 archive/0 links/0	4/8/2023
opensea.io	Reports (20)	flow/vuln	26/26	3.470 h	subdomains/4 dns/8 directory/16073 vuln/2 screenshots/0 archive/0 links/0	4/8/2023
tesla.com	Reports (54)	flow/general	59/59	36.201 h	subdomains/5 dns/11 directory/663 vuln/0 screenshots/325 archive/10658 links/0	3/26/2023

Items per page 10 | 1–6 of 6 items | 1 of 1 page

Web UI

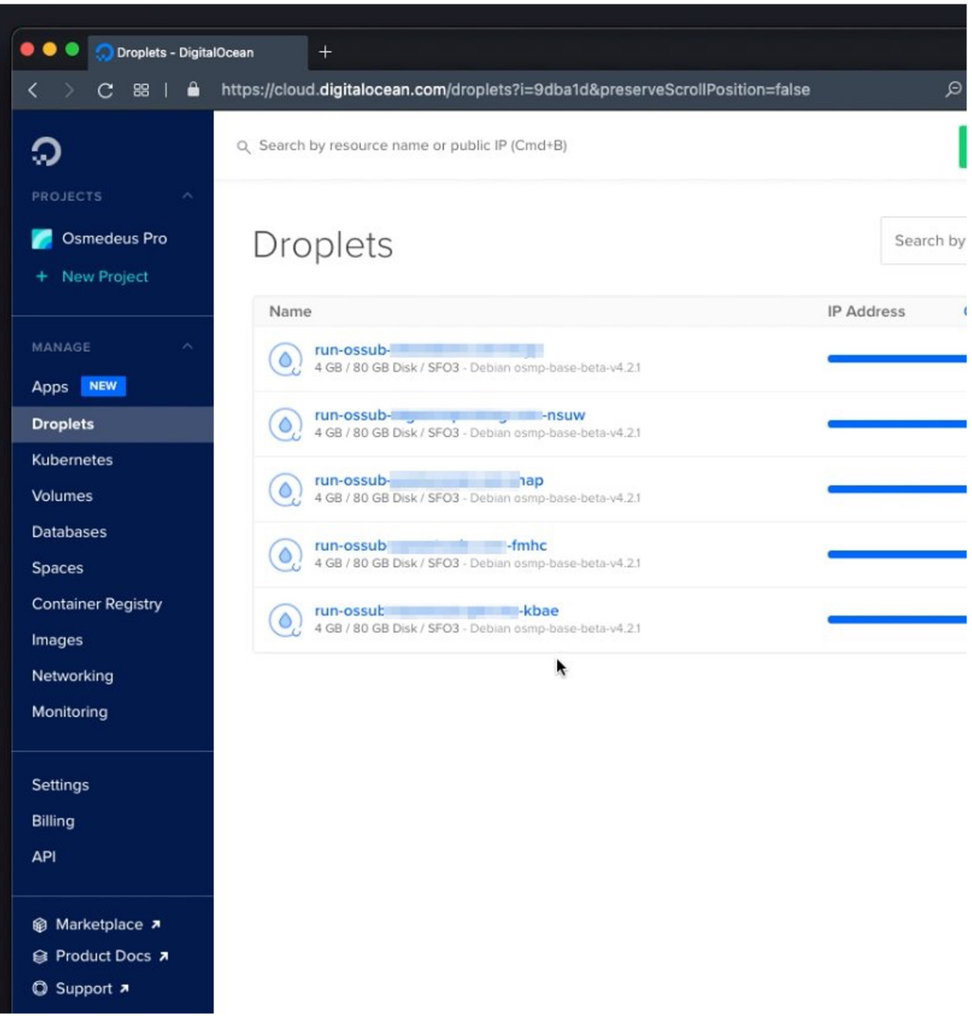


General Workflow Scan



Distributed Scan

```
j3ssie ▶ /tmp/demo $ osmedeus cloud -c 5 -f ossub -T domains
[2021-07-09T19:37:42]  INFO Store log file to: /tmp/osm-log/osmedeus-282372100.log
[2021-07-09T19:37:45]  INFO Finding base snapshot: osmp-base-beta-v4.2.1
[2021-07-09T19:37:50]  INFO Found base image snapshot with ID: 87534007
[2021-07-09T19:37:50]  INFO Found snapshot ID: 87534007
[2021-07-09T19:37:50]  INFO Finding SSH Key for droplet
[2021-07-09T19:37:50]  INFO Found SSH Key ID: 30778277
[2021-07-09T19:37:50]  INFO Prepared number of clouds in queue: 1
[start-scan] [redacted]
[2021-07-09T19:37:53]  INFO Creating instance: run-ossub-[redacted]-kbae
[start-scan] [redacted]
[2021-07-09T19:37:53]  INFO Creating instance: run-ossub-[redacted]-fmhc
[start-scan] [redacted]
[2021-07-09T19:37:53]  INFO Creating instance: run-ossub-[redacted]-jhap
[start-scan] [redacted]
[2021-07-09T19:37:53]  INFO Creating instance: run-ossub-[redacted]-nsuw
[start-scan] [redacted]
[2021-07-09T19:37:54]  INFO Creating instance: run-ossub-[redacted]-bvyp
[2021-07-09T19:38:11]  INFO Created Droplet with ID: 254148672 -- 143.198.150.61
[2021-07-09T19:38:11]  INFO Sync input of [redacted] to root@143.198.150.61
[2021-07-09T19:38:11]  INFO Created Droplet with ID: 254148670 -- 143.198.150.17
[2021-07-09T19:38:11]  INFO Sync input of [redacted] to root@143.198.150.17
[2021-07-09T19:38:11]  INFO Created Droplet with ID: 254148677 -- 143.198.158.9
[2021-07-09T19:38:11]  INFO Sync input of [redacted] to root@143.198.158.9
[2021-07-09T19:38:11]  INFO Created Droplet with ID: 254148671 -- 143.198.150.124
[2021-07-09T19:38:11]  INFO Sync input of [redacted] to root@143.198.150.124
[2021-07-09T19:38:11]  INFO Created Droplet with ID: 254148673 -- 143.198.158.60
[2021-07-09T19:38:11]  INFO Sync input of [redacted] to root@143.198.158.60
```



https://youtube.com/playlist?list=PLiifzv5MjIo3JqKeG5EXbSKDBlqa7v14P

Demo

Planned Features

1. Make experimental features more stable.
2. Integrate with more other tools.
3. Add more workflows.
4. Add more providers for cloud distributed scan.
5. Added more documentations ¯_(ツ)_/¯

Acknowledgments

- @theblackturle for his significant contributions in the form of feature requests and ideas.
- Special Thanks to all authors of the binaries tool that's being used in the workflow.
- Quang Ngo has been an early tester who provided incredibly valuable feedback.
- Thank you to all users of my open-source tools for your support and motivation.

Thank you for your attention!

For additional details, visit https://docs.osmedeus.org

@j3ssiejjj

@OsmedeusEngine