

# ***Sudomy: Semi-automated Information Gathering Tools for Subdomain Enumeration and Analysis***

Redho Maland  
Yogyakarta, Indonesia  
screetsec [at] gmail.com

## **ABSTRAK**

*Penilaian keamanan informasi merupakan salah satu bentuk kesadaran terkait serangan dunia maya yang selalu meningkat dari tahun ke tahun. Proses penilaian bisa dilakukan oleh tim internal dan / atau eksternal misalnya tenaga ahli dibidang kemanan informasi (pentester). Tahapan penilaian oleh Tim internal tentu berbeda dengan tim eksternal. Tim eksternal dalam melakukan asesmen perlu mempelajari atau mendapatkan informasi sebanyak mungkin terkait sasaran. Tahap ini biasanya disebut sebagai information gathering/reconnaissance. Oleh karena itu kami membutuhkan aplikasi yang mendukung Pengumpulan Informasi yang efektif dan efisien untuk membantu analisis dan pelaporan. Masih banyak aplikasi information gathering/reconnaissance yang belum melakukan pengintaian secara otomatis serta menyertakan sistem pelaporan dan validasi data. Jadi dalam penelitian ini diusulkan untuk membuat aplikasi untuk mendukung tahapan information gathering/reconnaissance yang mana memudahkan peneliti / analis keamanan siber, penetration tester dan bug hunter.*

## **1. Pendahuluan**

Sebagai seseorang yang ahli dibidang kemanan informasi (pentester) atau bug hunter, sebagian besar waktu yang mereka gunakan adalah melakukan pengumpulan informasi sebanyak mungkin mengenai target (*information gathering/reconnaissance*). Pentester dan bug hunter harus melakukan pengintaian ekstensif untuk menemukan aset menarik seperti server, teknologi dan aplikasi web dari sebuah domain atau subdomain. Mencari dan mengumpulkan subdomain dari domain utama merupakan bagian terpenting dari fase *reconnaissance* dalam kegiatan penilaian keamanan informasi, terutama pada kegiatan *black-box penetration testing* dan *bug hunting*. Pengumpulan informasi tersebut dapat dijadikan sebagai target dalam pengujian untuk mencari kemungkinan bahwa salah satu subdomain memiliki kaitan dengan domain utama dan menemukan aplikasi tersembunyi yang berjalan di subdomain, sehingga dapat meningkatkan peluang dalam menemukan kerentanan.

Dalam melakukan pengumpulan informasi dapat dibagi menjadi dua, yaitu *active reconnaissance* dan *passive reconnaissance*. *Active Reconnaissance* adalah pengumpulan data dengan cara bertatap muka langsung atau berhubungan langsung dengan target/sasaran, sedangkan *passive*

*reconnaissance* adalah menggunakan media informasi yang sudah tersedia seperti berita, internet, dan sebagainya [1]. Pada proses ini dapat dilakukan secara manual dan otomatis, penulis menggabungkan proses tersebut menjadi semi-otomatis, sehingga kegiatan yang dilakukan secara berulang saat proses pengumpulan informasi menjadi lebih efektif dan efisien.

## **2. Tujuan Penulisan**

Memperkenalkan *Sudomy* sebagai salah satu tools yang bisa digunakan dalam pengumpulan subdomain dan analisa secara otomatis. *Sudomy* dibangun untuk mempermudah kegiatan dalam pengumpulan informasi dan melengkapi tools yang diperlukan pentester yang mengikuti kaidah *The National Institute of Standards and Technology* (NIST) dan/atau *Information Systems Security Assessment Framework* (ISSAF).

## **3. Landasan Teori**

### **3.1. Information Gathering/Reconnaissance**

Information Gathering merupakan tahapan pertama dalam penilaian keamanan informasi terutama dibidang kewanaman informasi (pentester) dan bug hunter, yang berguna untuk mendapatkan informasi sebanyak mungkin mengenai sasaran target baik perseorangan maupun perusahaan. Dalam melakukan pengumpulan informasi dapat dibagi menjadi dua:

- 1) *Active Reconnaissance* adalah pengumpulan data dengan cara berhubungan langsung dengan target atau sasaran.
- 2) *Passive Reconnaissance* adalah pengumpulan data dengan cara tidak berhubungan langsung dengan target, melalui sumber-sumber publik seperti yang tersedia di Internet berita, internet, dan media lainnya.

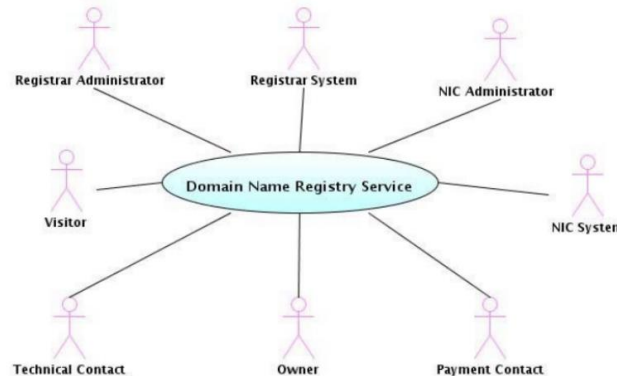
### **3.2 Subdomain**

Subdomain adalah bagian dari sebuah nama domain yang biasanya digunakan sebagai nama website dan subdomain ini tidak dapat berdiri sendiri. Dengan adanya subdomain, pemilik situs dapat membuat halaman atau website tertentu yang terpisah dari domain utama. Sebagai contoh website dengan domain "example.id" memiliki subdomain "blog.example.id" yang berisi informasi khusus yang berhubungan

dengan blog, mail.example.com berisi informasi khusus email dan subdomain “news.example.id” yang berisi informasi khusus yang berhubungan dengan berita saja. Manfaat mencari subdomain sangat bermanfaat dalam kegiatan OSINT, Pentester, Bug hunter dan Red Teamer yang mungkin bisa saja ada informasi yang saling berkaitan antara satu domain dengan subdomain lainnya.

### 3.3 Domain Name System

Domain Name System Domain Name System (DNS) merupakan sistem yang berfungsi mengkonversi nama domain yang mudah diingat ke dalam bentuk IP Address dengan melakukan permintaan informasi ke sistem yang memiliki hierarki dan tersebar. Adanya DNS maka memudahkan menghubungkan sumber daya komputasi baik melalui internet maupun jaringan internal [2]. Implementasinya secara global sistem DNS implementasi tiga peran, yaitu Domain Name Registry Operator, Domain Name Registrar, dan Service Providers dan Customers. Adapun overview of the Domain Name Registry dapat dilihat pada Figure 1 [3].

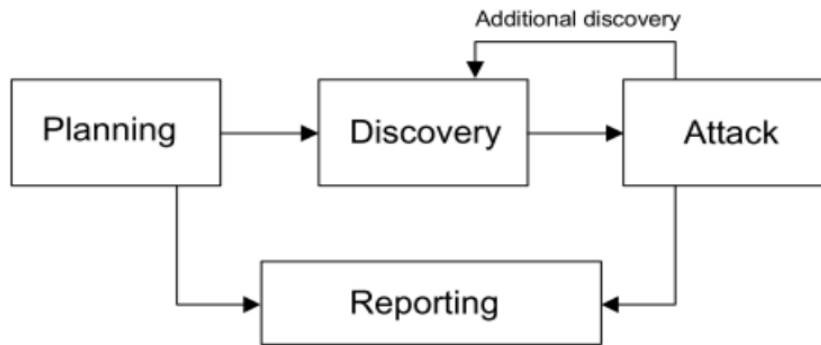


**Figure 1.** Overview of the Domain Name Registry

### 3.4 National Institute of Standards and Technology SP 800-42

US Department of Commerce menerbitkan rekomendasi tentang Network Security Testing yang tertuang pada National Institute of Standards and Technology Special Publication 800-42 (NIST SP 800-42). Metodologi dasar penetration testing menurut NIST SP 800-42 terdapat empat fase, yaitu Planning, Discovery, Attack, dan Reporting, Figure 2 [4]. Pada fase awal Discovery pentester dapat melakukan

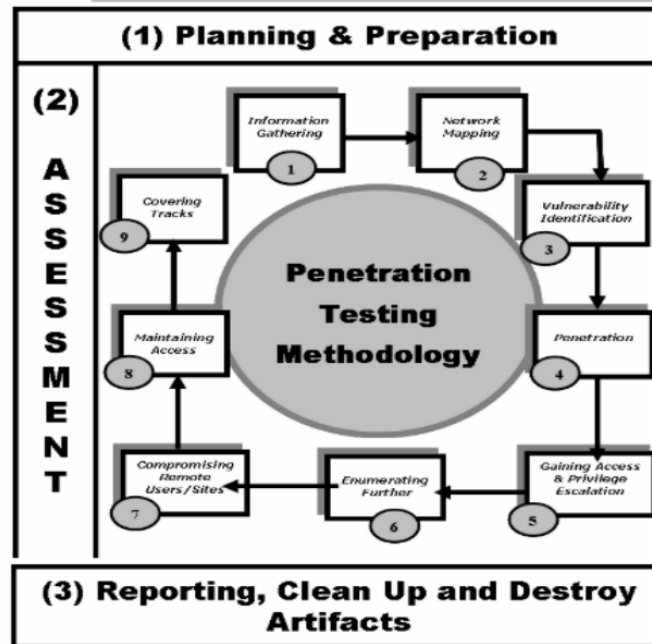
identifikasi dan pengumpulan informasi yang potensial terkait target. Information gathering dapat dilakukan berbagai teknik diantaranya: Domain Name System interrogation, InterNIC queries, Search of the target organization's web server(s) for information, Search of the organization's Lightweight Directory Access Protocol server(s) (LDAP) for information, Packet capture, NetBIOS enumeration, Network Information System, and Banner grabbing.



**Figure 2.** NIST: Penetration Testing Methodology

### 3.5 Information Systems Security Assessment Framework (ISSAF)

Information Systems Security Assessment Framework (ISSAF) memiliki tiga fase methodology, yaitu Planning and Preparation, Assessment, dan Reporting, Clean-up, Destroy Artefacts. Sedangkan pada fase Assessment terdapat sembilan langkah yaitu: Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access & Privilege Escalation, Enumerating Further, Compromise Remote Users/Sites, Maintaining Access, and Covering Tracks, Figure 3 [5].



**Figure 3.** ISSAF: Penetration Testing Methodology

Pada langkah Information Gathering pencarian informasi dari target dapat dilakukan secara teknis, non-teknis atau gabungan keduanya. Hal ini bertujuan untuk mendapatkan informasi yang potensial terkait dengan celah dari target. Information Gathering dapat dibagi menjadi dua bagian, yaitu passive dan active. Pada bagian Passive Information Gathering teknik yang digunakan untuk mendapatkan informasi tidak secara langsung berhubungan dengan target. Bisa juga pada bagian Passive Information Gathering memanfaatkan pihak ketiga untuk mendapatkan informasi. Sedangkan pada bagian Active Information Gathering dalam proses mendapatkan informasi berhubungan langsung dengan target. Maka hal ini di beberapa negara dinyatakan ilegal [5].

### 3.6 Web Application Programming Interfaces

Kelebihan pengembangan menggunakan Web Application Programming Interfaces (Web APIs) adalah mempercepat dalam pengembangan sebuah aplikasi. Oleh sebab itu implementasi Web APIs dalam rentang waktu 2005 – 2013 selalu meningkat, Figure 4 [6]. Web APIs menggunakan protokol HTTP/HTTPS dalam berkomunikasi dengan aplikasi utama dengan penyedia Web APIs [7]. Pengembangan aplikasi Information Gathering yang bersifat Passive memanfaatkan Web APIs untuk mempercepat mendapatkan informasi dari pihak ketiga, seperti SecurityTrails, BinaryEdge, VirusTotal, Censys, dan Shodan.

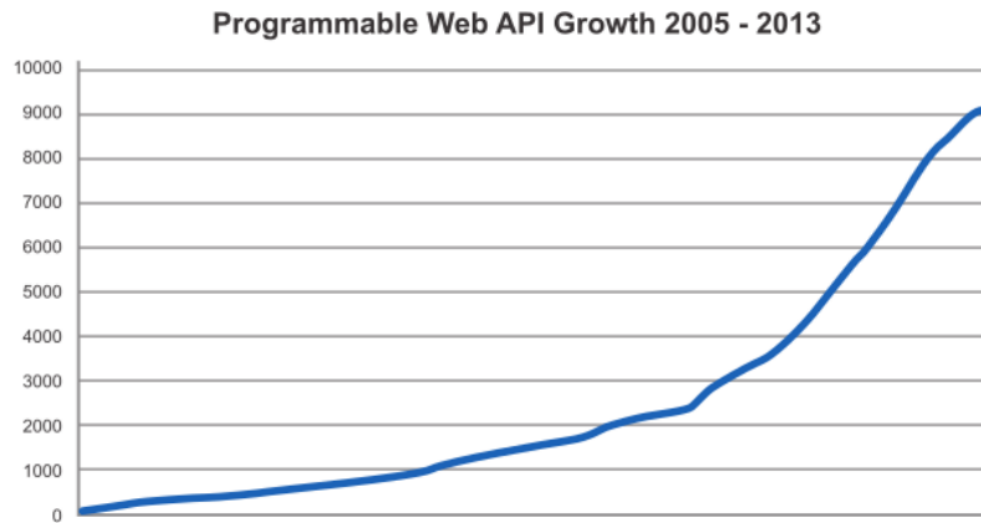


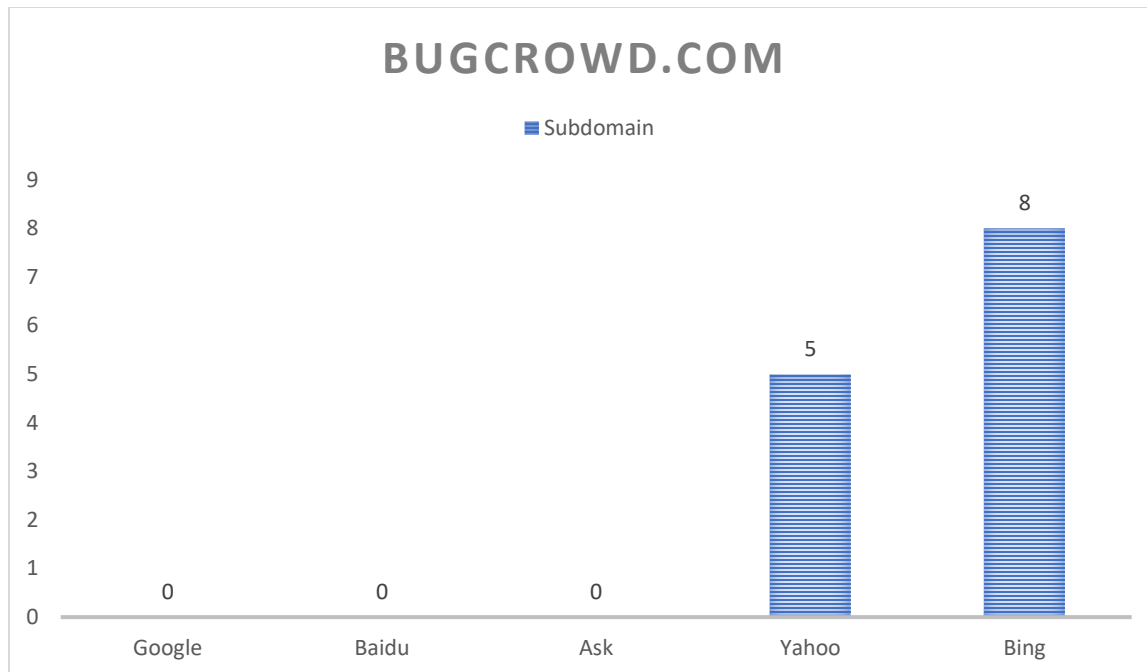
Figure 4. Programmable Web API Growth 2005-2013

## 4. Pembahasan

### 4.1 Perkenalan Sudomy

*Sudomy* adalah alat bantu subdomain *enumeration* untuk mengumpulkan subdomain dan menganalisis domain dengan melakukan *automated reconnaissance*. Alat ini juga dapat digunakan untuk aktivitas OSINT. Pengembangan aplikasi Information Gathering mengikuti kaidah ISSAF[5] dengan menerapkan dua teknik, yaitu passive dan active. Teknik passive mendapatkan informasi melalui beberapa cara dengan memanfaatkan sumber daya pihak ketiga seperti menggunakan Web API, pustaka Information Gathering atau melalui OSINT Source dengan proses scraping [8]. Sedangkan teknik active menggunakan aplikasi yang terinstall dengan fitur serupa yaitu fungsi Information Gathering baik dengan cara brute force, wordlists ataupun metode baru lainnya.

Dengan menyeleksi situs pihak ketiga yang digunakan, proses enumerasi dns dapat dilakukan secara efektif dan efisien, sehingga hasil yang didapatkan lebih banyak tetapi waktu yang dibutuhkan lebih sedikit. Sebagai contoh *sudomy* tidak menggunakan resource mesin pencari seperti Google, Baidu, Ask Yahoo dan Bing, dikarenakan hasil yang didapat kurang maksimal dan adanya faktor lainnya seperti terhambat oleh captcha,



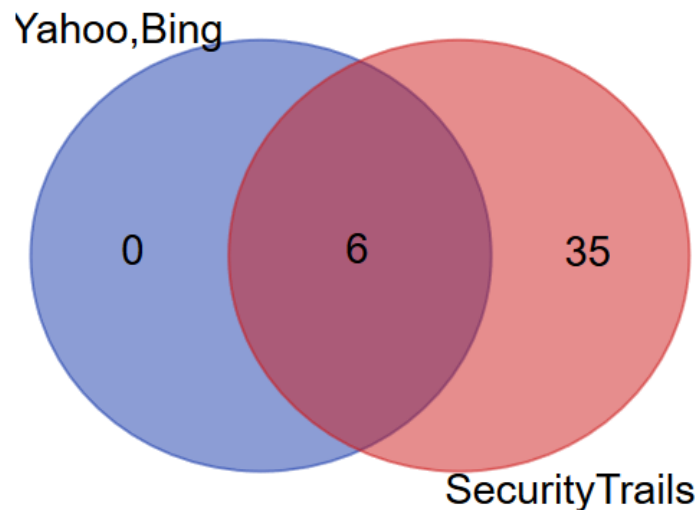
**Figure 5.** Proses pengumpulan data hasil Scanning

Selain itu hasil yang didapatkan dari mesin pencari Yahoo dan Bing, sudah terhimpun disalah satu resource seperti SecurityTrails .

Resource	Totals	Subdomain
Yahoo & Bing	6	assetinventory.bugcrowd.com docs.bugcrowd.com events.bugcrowd.com forum.bugcrowd.com levelup.bugcrowd.com researcherdocs.bugcrowd.com
SecurityTrails	35	a.bugcrowd.com api.bugcrowd.com assetinventory.bugcrowd.com blog.bugcrowd.com bounce.bugcrowd.com collateral.bugcrowd.com concourse.bugcrowd.com crowdcontrol.bugcrowd.com docs.bugcrowd.com documentation.bugcrowd.com email.assetinventory.bugcrowd.com email.bugcrowd.com email.bugs.bugcrowd.com email.crowdcontrol.bugcrowd.com

		email.forum.bugcrowd.com email.submit.bugcrowd.com events.bugcrowd.com forum.bugcrowd.com forum-new.bugcrowd.com gemstash-mattress.a.bugcrowd.com go.bugcrowd.com gslink.bugcrowd.com hello.bugcrowd.com hooks.bugcrowd.com itmoah.bugcrowd.com levelup.bugcrowd.com omnidb.a.bugcrowd.com otter.bugcrowd.com pages.bugcrowd.com p.bugcrowd.com portal.bugcrowd.com production-sandbox.a.bugcrowd.com proxilate.a.bugcrowd.com proxilate.bugcrowd.com researcherdocs.bugcrowd.com sandbox-crowdcontrol.a.bugcrowd.com stargate.a.bugcrowd.com submissions.bugcrowd.com tableau.a.bugcrowd.com tracker.bugcrowd.com tracker.production-sandbox.a.bugcrowd.com
--	--	--

Oleh karena itu penulis tidak memasukan search engine sebagai resource dalam pengumpulan data subdomain, berikut tampilan data dalam bentuk diagram venn, lihat pada Figure 6.





**Figure 6.** Data dalam bentuk himpunan

## 4.2 System Design

Pengembangan aplikasi Information Gathering menggunakan kombinasi dari Bash (Bourne-Again Shell) Script [9] dan bahasa pemrograman Python karena sudah mendukung object-oriented programming [8] dan dukungan pustaka yang mempermudah pengembangan. Penggunaan Bash Script memiliki tiga komponen utama: lexical analysis and parsing, text expansion, and command execution, Figure 7 [10]. Input dapat bermula dari antarmuka interaktif melalui console atau Bash Script file. Komponen pertama merupakan analisis lexical dan mem-parsing masing perintah ke dalam struktur data. Selanjutnya komponen kedua melakukan serangkaian ekspansi dan mengganti variabel



**Figure 7.** Architecture of Bash

dari masing-masing parsing perintah dengan mengikuti sophisticated rules. Setiap eksekusi perintah kemudian diinterpretasikan.

## 4.3 Tujuan Pembuatan Sudomy

Sudomy dibangun untuk mempermudah kegiatan dalam pengumpulan informasi dan melengkapi tools yang diperlukan pentester/bug hunter dengan membuat proses menjadi lebih efektif dan efisien.

## 4.4 Fitur Sudomy

Saat ini *sudomy* memiliki 19 fitur, yaitu:

1. Mudah, cepat, ringan dan powerfull. Bash script tersedia secara default di semua distro linux. Dengan memanfaatkan fitur multiprocessing (multiprocessing) yang dimiliki oleh bash script, maka semua prosesor akan terpakai secara optimal.
2. Pengujian enumerasi dns menggunakan metode aktif atau pasif

- **Metode aktif**

Sudomy memanfaatkan tools Gobuster, karena Gobuster sangat cepat dalam melakukan serangan DNS Subdomain Bruteforce (wildcard support). Wordlist yang dipakai berasal dari SecList (Discover/DNS). Beberapa file wordlist pada SecList kemudian disatukan menjadi sebuah file dengan total wordlist mencapai 3 juta entri.

- **Metode Pasif**

Dengan menyeleksi situs pihak ketiga yang digunakan, proses enumerasi dns dapat dilakukan secara efektif dan efisien, hasil yang didapatkan lebih banyak tapi waktu yang dibutuhkan lebih sedikit. Sudomy dapat mengumpulkan data dari ke-20 situs pihak ketiga yang telah melalui proses seleksi sebagai berikut:

By selecting the good third-party sites (resources)	
Shodan	<a href="http://developer.shodan.io">http://developer.shodan.io</a>
VirusTotal	<a href="https://www.virustotal.com">https://www.virustotal.com</a>
Censys	<a href="http://censys.io">http://censys.io</a>
Certspotter	<a href="https://api.certspotter.com">https://api.certspotter.com</a>
BinaryEdge	<a href="https://docs.binaryedge.io/">https://docs.binaryedge.io/</a>
Hackertarget	<a href="https://api.hackertarget.com">https://api.hackertarget.com</a>
Threatminer	<a href="https://api.threatminer.org">https://api.threatminer.org</a>
CrtSH	<a href="https://crt.sh">https://crt.sh</a>
DnsDB	<a href="https://www.dnsdb.info">https://www.dnsdb.info</a>
BufferOver	<a href="http://dns.bufferover.run">http://dns.bufferover.run</a>
Sypse	<a href="https://spyse.com">https://spyse.com</a>
Threatcrowd	<a href="http://threatcrowd.org">http://threatcrowd.org</a>
Dnsdumpster	<a href="https://dnsdumpster.com">https://dnsdumpster.com</a>
Riddler	<a href="http://riddler.io">http://riddler.io</a>
Webarchive	<a href="http://web.archive.org">http://web.archive.org</a>
SecurityTrails	<a href="http://securitytrails.com">http://securitytrails.com</a>
RapidDNS	<a href="https://rapiddns.io">https://rapiddns.io</a>
AlienVault	<a href="https://otx.alienvault.com">https://otx.alienvault.com</a>
CommonCrawl	<a href="http://index.commoncrawl.org">http://index.commoncrawl.org</a>
FBcert	<a href="https://graph.facebook.com">https://graph.facebook.com</a>
URLScan	<a href="https://urlscan.io">https://urlscan.io</a>
RiskIQ	<a href="https://community.riskiq.com">https://community.riskiq.com</a>

3. Pengujian terhadap daftar subdomain yang ditemukan untuk memastikan http atau https server berfungsi dengan baik atau tidak. Fitur ini menggunakan tools pihak ketiga yaitu, httpprobe.
4. Pengecekan subdomain berdasarkan Ping Sweep dan/atau mendapatkan HTTP status code
5. Mampu mendeteksi virtualhost (beberapa subdomain yang berbagi satu alamat IP). Dari daftar subdomain yang ditemukan, *sudomy* akan menerjemahkannya menjadi alamat IP, mengurutkan serta menggolongkannya apabila beberapa subdomain ternyata resolve ke alamat IP yang sama.

Fitur ini akan sangat bermanfaat dalam proses pentest/bug bounty berikutnya, misal dalam melakukan port scanning, satu alamat ip tidak akan discan berulang-ulang.

6. Melakukan port scanning dari alamat IP subdomain/virtualhost yang telah ditemukan
7. Melakukan pengujian serangan Subdomain TakeOver (CNAME Resolver, DNSLookup, Detect NXDomain, Check Vuln)
8. Mengambil Tangkapan Layar dari subdomain default menggunakan gowitness atau Anda dapat memilih alat tangkapan layar lain, seperti (-ss webscreenshot)
9. Mengidentifikasi teknologi di situs web (kategori, aplikasi, versi)
10. Mendeteksi urls, ports, title, content-length, status-code, response-body probing.
11. Sebagai default menggunakan auto fallback dari https ke http
12. Pengumpulan Data & Scraping terhadap port terbuka dari pihak ke-3 defaultnya adalah Shodan. Untuk saat ini hanya menggunakan Shodan [Future: Censys, Zoomeye]. Lebih efisien dan efektif untuk mengumpulkan port dari daftar ip pada target [[Subdomain> IP Resolver> Crawling> ASN & Open Port]]
13. Mengumpulkan dan Mengekstrak URL & Parameter yang menarik, resource yang digunakan WebArchive, CommonCrawl dan UrlScanIO
14. Mengumpulkan path, url dan file yang menarik seperti api, git, admin, file javascript (js|node) dan dokumen (doc|pdf)
15. Menentukan output saat file scanning telah selesai berjalan
16. Memeriksa apakah IP dimiliki/dilindungi oleh Cloudflare
17. Mengumpulkan dan membuat wordlist berdasarkan pengumpulan sumber daya url (wayback, urlscan, commoncrawl. Untuk membuatnya, kami Ekstrak Semua parameter dan jalur dari pengintaian domain kami
18. Output laporan dalam format HTML atau CSV
19. Mengirim pemberitahuan ke Channel Slacks apabila automated recon telah selesai

#### 4.5 Cara kerja Sudomy

Disini penulis akan menjelaskan cara kerja/proses recon disaat *sudomy* dijalankan menggunakan perintah argumen terbaik dalam mengumpulkan subdomain dan menganalisis dengan melakukan automatic recon. Perintah

```
root@maland: Sudomy -d bugcrowd.com -dP -eP -rS -cF -pS -tO -gW --httpx --dnsprobe -al webanalyze -sS -  
-slack
```

Recon Workflow Sudomy v1.1.8#dev, lihat Figure 8.

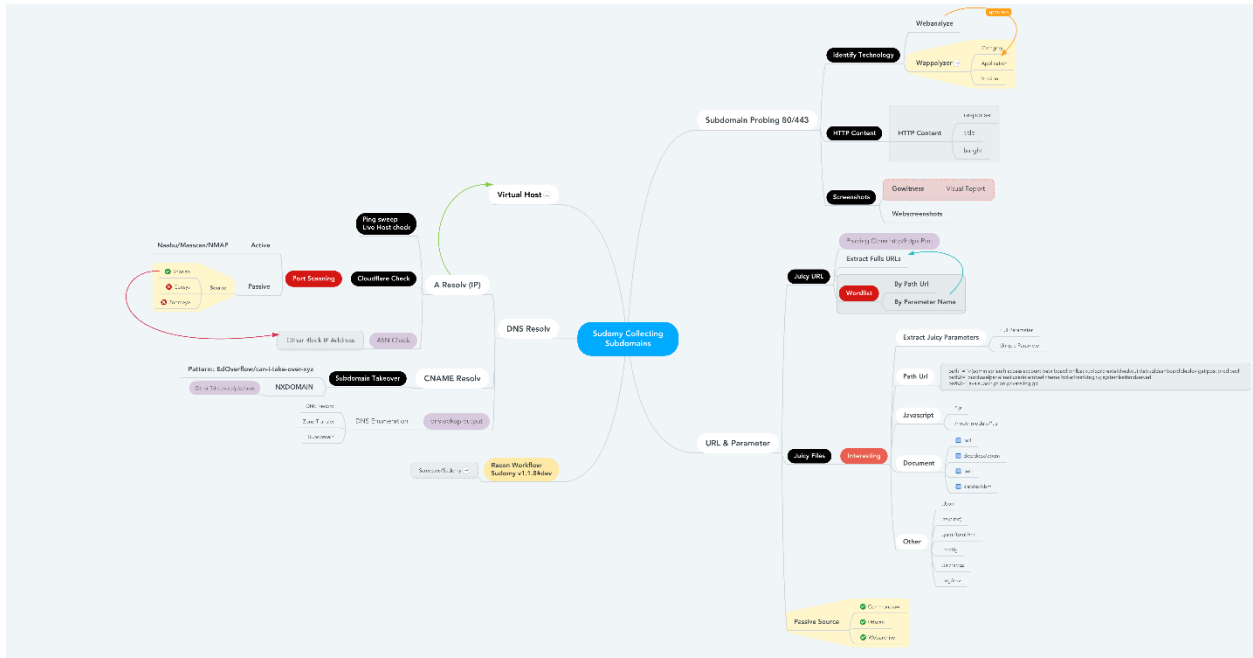


Figure 8. Recon Worflow Sudomy

<https://raw.githubusercontent.com/Screetsec/Sudomy/master/doc/Sudomy%20-%20Recon%20Workflow%20v1.1.8%23dev.png>

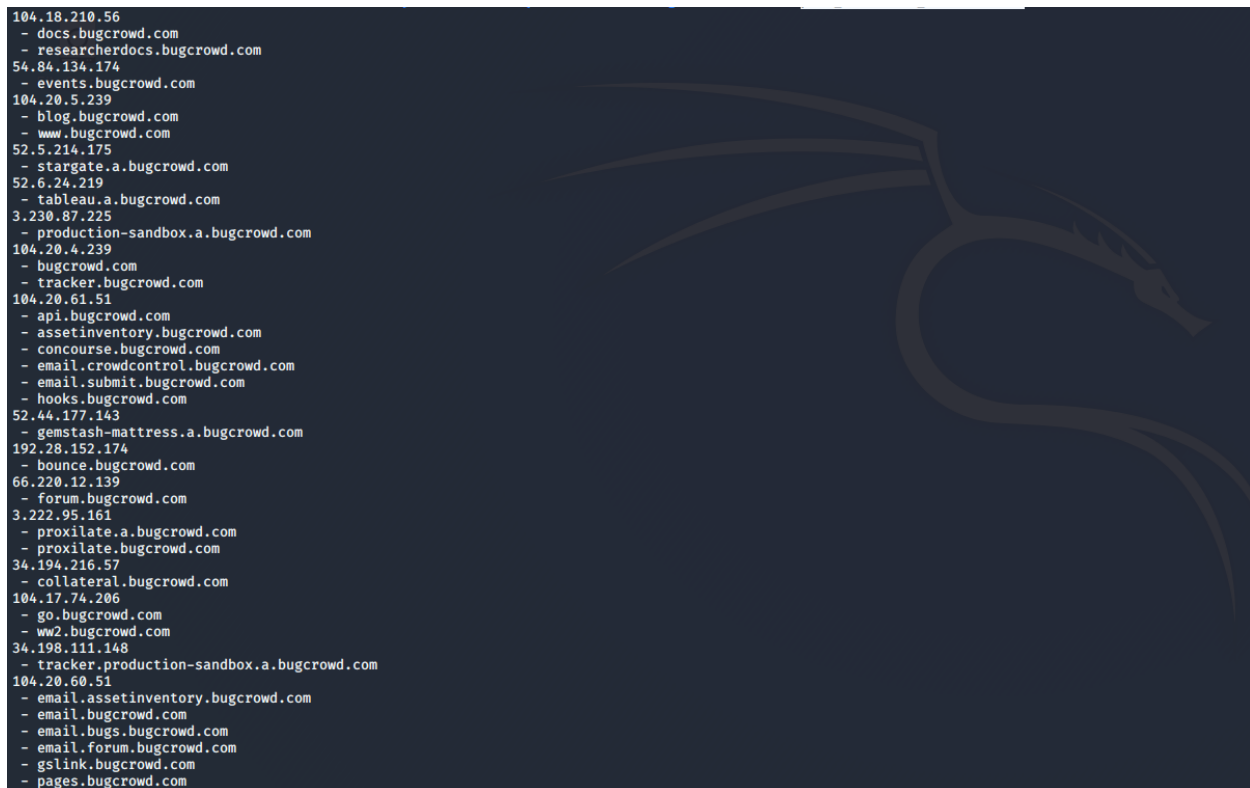
Hal pertama, *sudomy* akan melakukan pengumpulan subdomain dari domain utama menggunakan metode pasif melalui resource yang telah di seleksi seperti dnsdumpster, webarchive, shodan, virustotal, crt.sh, binaryedge, securitytrails, certspotter, censys, threatminer, bufferover, hackeertarget, entrust, threatcrowd, riddler, findsubdomains, rapiddns, alienvault, commoncrawl, dan urlscan.io. Untuk meningkatkan hasil enumerasi, aplikasi *sudomy* perlu menambahkan API Key untuk Shodan, Censys, Virus Total, BinaryEdge, dan SecurityTrails pada bagian **sudomy.api**.

Disaat proses pengumpulan subdomain, *sudomy* juga mengambil raw data (tanpa penyaringan) dari resource tertentu seperti CommonCrawl, UrlScan, Webarchive dan Shodan. Dikarenkan raw data dari resource tersebut dapat diolah dan dimanfaatkan sekaligus dalam mendapatkan informasi lainnya. Contohnya informasi port, asn number, path, url, paremeter dan file menarik lainnya seperti api, git,

admin, javascript (js, node\_module) dan dokumen (doc, pdf, pub, xlsx) yang bisa digunakan untuk pembuatan wordlist.

Dari daftar subdomain yang didapatkan, *sudomy* akan melakukan validasi terhadap subdomain yang aktif dengan memeriksa protokol http / https secara otomatis. Fitur ini menggunakan alat pihak ketiga, httpprobe. Tidak hanya disitu, *sudomy* juga akan melakukan pengecekan terhadap title, content-length, status-code dan response-body pada masing-masing subdomain yang aktif. Kemudian/Dari daftar subdomain yang aktif, *sudomy* akan melanjutkan proses enumerasi dengan mengidentifikasi teknologi web yang digunakan seperti Content Management System (CMS), Bootstrap, Web Server, Operating System dan Database yang digunakan oleh website tersebut.

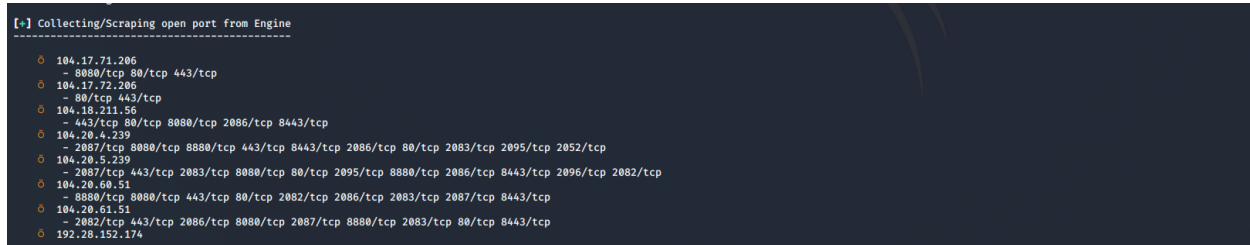
Kumpulan subdomain yang telah berhasil dikumpulkan, *sudomy* akan mendeteksi beberapa subdomain yang terbagi dalam satu alamat IP (virtualhost) dan menggolongkannya serta menyeleksi apabila beberapa subdomain resolve ke alamat IP yang sama, Figure 9.



```
104.18.210.56
- docs.bugcrowd.com
- researcherdocs.bugcrowd.com
54.84.134.174
- events.bugcrowd.com
104.20.5.239
- blog.bugcrowd.com
- www.bugcrowd.com
52.5.214.175
- stargate.a.bugcrowd.com
52.6.24.219
- tableau.a.bugcrowd.com
3.230.87.225
- production-sandbox.a.bugcrowd.com
104.20.4.239
- bugcrowd.com
- tracker.bugcrowd.com
104.20.61.51
- api.bugcrowd.com
- assetinventory.bugcrowd.com
- concourse.bugcrowd.com
- email.crowdcontrol.bugcrowd.com
- email.submit.bugcrowd.com
- hooks.bugcrowd.com
52.44.177.143
- gemstash-mattress.a.bugcrowd.com
192.28.152.174
- bounce.bugcrowd.com
66.220.12.139
- forum.bugcrowd.com
3.222.95.161
- proxilate.a.bugcrowd.com
- proxilate.bugcrowd.com
34.194.216.57
- collateral.bugcrowd.com
104.17.74.206
- go.bugcrowd.com
- ww2.bugcrowd.com
34.198.111.148
- tracker.production-sandbox.a.bugcrowd.com
104.20.60.51
- email.assetinventory.bugcrowd.com
- email.bugcrowd.com
- email.bugs.bugcrowd.com
- email.forum.bugcrowd.com
- gslink.bugcrowd.com
- pages.bugcrowd.com
```

**Figure 9.** Subdomain yang telah di kelompokkan berdasarkan IP dan Subdomain

Setelah daftar IP terkumpul, *sudomy* akan melakukan pengecekan terhadap host berdasarkan ping sweep dan juga memeriksa apakah IP dimiliki/dilindungi oleh Cloudflare. Kemudian *sudomy* melakukan port scanning melalui daftar alamat original ip yang telah di filter, disini *sudomy* menggunakan dua metode dalam melakukan port scanning. Dalam pemindai aktif *sudomy* menggunakan nmap dan untuk pemindai secara pasif, untuk sekarang sumber utamanya adalah shodan, kedepannya akan ditambahkan resource lainnya seperti censys dan zoomeye. Figure 10

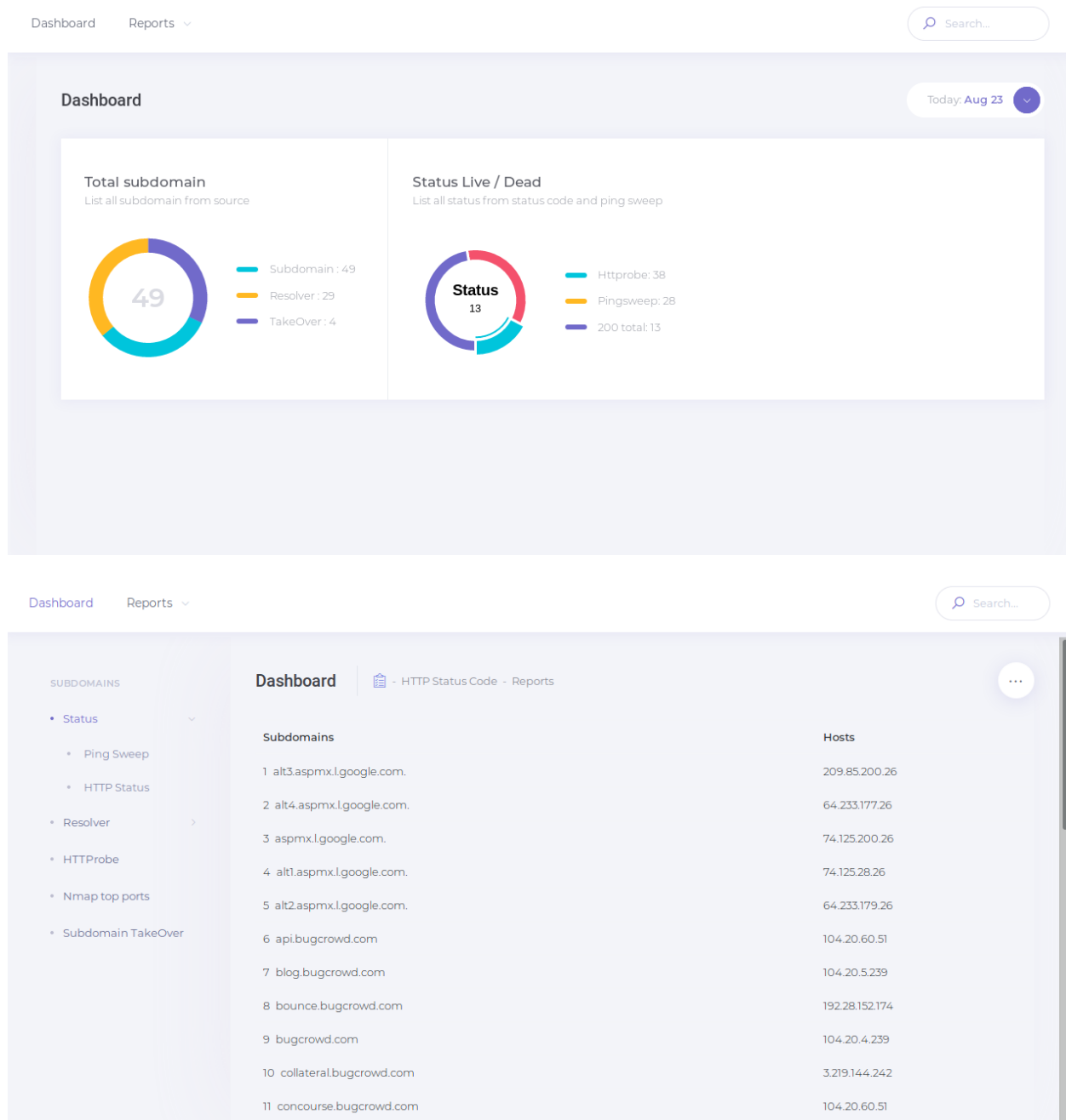


```
[+] Collecting/Scraping open port from Engine
-----
o 104.17.71.206
  - 8880/tcp 80/tcp 443/tcp
o 104.17.72.206
  - 80/tcp 443/tcp
o 104.18.211.56
  - 443/tcp 80/tcp 8080/tcp 2086/tcp 8443/tcp
o 104.20.4.239
  - 2087/tcp 8080/tcp 8880/tcp 443/tcp 8443/tcp 2086/tcp 80/tcp 2083/tcp 2095/tcp 2052/tcp
o 104.20.5.239
  - 2087/tcp 443/tcp 2083/tcp 8080/tcp 80/tcp 2095/tcp 8880/tcp 2086/tcp 8443/tcp 2096/tcp 2082/tcp
o 104.20.60.51
  - 8880/tcp 8080/tcp 443/tcp 80/tcp 2082/tcp 2086/tcp 2083/tcp 2087/tcp 8443/tcp
o 104.20.61.51
  - 2082/tcp 443/tcp 2086/tcp 8080/tcp 2087/tcp 8880/tcp 2083/tcp 80/tcp 8443/tcp
o 192.28.152.174
```

**Figure 10.** Hasil Scraping & Collecting Port menggunakan Shodan

Tak hanya disitu, *sudomy* juga melakukan pengecekan subdomain takeover dan pembuatan wordlist kustom secara otomatis berdasarkan informasi yang telah dikumpulkan. Dalam pembuatan wordlist, *sudomy* memanfaatkan resource seperti CommonCrawl, UrlScan, Webarchive dan Shodan untuk mendapatkan informasi Path, Url dan Parameter mengenai target. Sehingga wordlist yang digunakan lebih spesifik, menghemat waktu dan tepat sasaran.

Jika tahapan pengumpulan informasi sudah selesai, *sudomy* akan merekam tangkapan layar (screenshot) dari daftar subdomain dan membuat laporan dengan output berformat HTML dan CSV yang dapat memudahkan peneliti dan/atau analisis cyber security dalam menganalisa. Pada laporan berformat HTML tersebut ditampilkan grafik hasil enumerasi subdomain diantaranya: Ping Sweep, HTTP status, IP Address, sepuluh teratas protokol yang terbuka, pemeriksaan Subdomain TakeOver, dan grafik hasil enumerasi, Figure 11



**Figure 11.** Dashboard Report sudomy

Apabila tahapan screenshot dan pembuatan laporan selesai, maka selanjutnya akan masuk ketahapan akhir yaitu pemberitahuan bahwa scanning telah selesai menggunakan slack alert, lihat pada Figure 12.



**Sudomy** APP 5:31 PM

**Sudomy - Subdomain Enumeration & analysis:**

Information: Automated Recon Done !!

- Domain: [tiket.com](https://tiket.com)

- Date: 10-13-2020

**Figure 12.** Slack Notifications

## 4.6 Pemasangan Sudomy

Dalam melakukan pemasangan, *sudomy* membutuhkan beberapa dependensi agar tools dapat berjalan dengan baik. Petunjuk tentang cara menginstal sebagai berikut:

Untuk Mengunduh Sudomy Dari Github:

```
git clone --recursive https://github.com/screetsec/Sudomy.git
```

Untuk Menginstall depedensi

```
pip install -r requirements.txt
```

Sudomy membutuhkan jq dan beberapa tools lainnya untuk menjalankan dan melakukan parse data.

```
# Pengguna Linux
apt-get update
apt-get install jq nmap phantomjs npm chromium parallel
npm i -g wappalyzer wscat

# Pengguna Mac
brew cask install phantomjs
brew install jq nmap npm parallel
npm i -g wappalyzer wscat

# Note
Yang Anda perlukan hanyalah pemasangan Google Chrome atau Chromium
terbaru
```

## 4.7 Berjalan di Docker Container

Sudomy juga support dan berjalan di Docker Container, sehingga tidak perlu melakukan melakukan instalasi dan dependensi. Petunjuk tentang cara penggunaan

```
# Pull an image from DockerHub
docker pull screetsec/sudomy:v1.1.8
```



```
# Run an image, you can run the image on custom directory but you must
copy/download config sudomy.api on current directory
docker run -v "${PWD}/output:/usr/lib/sudomy/output" -v
"${PWD}/sudomy.api:/usr/lib/sudomy/sudomy.api" -it --rm
screetsec/sudomy:v1.1.8 [argument]

or define API variable when executed an image.

docker run -v "${PWD}/output:/usr/lib/sudomy/output" -e
"SHODAN_API=xxxx" -e "VIRUSTOTAL=xxxx" -it --rm screetsec/sudomy:v1.1.8
[argument]
```

## 4.8 Konfigurasi tambahan

API Key diperlukan untuk melakukan query pada situs pihak ketiga seperti Shodan, Censys, SecurityTrails, Virustotal, dan BinaryEdge yang bertujuan untuk meningkatkan hasil enumerasi. Pengaturan API key dapat dilakukan melalui file **sudomy.api**

```
# Shodan
# URL : http://developer.shodan.io
# Example :
# - SHODAN_API="VGhpc1M0bXBsZWwKVGHmcGxlbAo"

SHODAN_API=""

# Censys
# URL : https://censys.io/register

CENSYS_API=""
CENSYS_SECRET=""

# Virustotal
# URL : https://www.virustotal.com/gui/
VIRUSTOTAL=""

# Binaryedge
# URL : https://app.binaryedge.io/login
BINARYEDGE=""

# SecurityTrails
# URL : https://securitytrails.com/
SECURITY_TRAILS=""
```

YOUR\_WEBHOOK\_URL diperlukan juga sebelum menggunakan pengiriman notifikasi ke slack. Pengaturan URL dapat dilakukan melalui file **slack.conf**

```
# Configuration Slack Alert
# For configuration/tutorial to get webhook url following to this site
# - https://api.slack.com/messaging/webhooks
# Example:
# -
YOUR_WEBHOOK_URL="https://hooks.slack.com/services/T01CGNA9743/B02D3BQNJM
6/MRSpVUxgvO2v6jtCM6lEejme"

YOUR_WEBHOOK_URL=""
```

#### 4.9 Petunjuk Pemakaian

```

/ _ | _ _ _ | ( ) ( ) _ _ _ _ _
\ _ \ | | / _ \ / _ \ ' \ | | |
| _ \ / _ \ , \ _ \ , \ _ \ / _ \ | | \ , |
| _ \ / v{1.1.0#dev} by @screetsec

SudÖmy - Fast Subdomain Enumeration and Analyzer
http://github.com/screetsec/sudomy

Usage: sudÖmy.sh [-h [--help]] [-s[--source]][-d[--domain=]]

Example: sudÖmy.sh -d example.com
        sudÖmy.sh -s Shodan,VirusTotal -d example.com
        sudÖmy.sh -pS -rS -sC -nT -sS -d example.com

Optional Arguments:
-a, --all                Running all Enumeration, no nmap & gobuster
-b, --bruteforce         Bruteforce Subdomain Using Gobuster (Wordlist:
ALL Top SecList DNS)
-d, --domain             domain of the website to scan
-h, --help              show this help message
-o, --html               Make report output into HTML
-s, --source             Use source for Enumerate Subdomain
-tO, --takeover          Subdomain TakeOver Vulnerabilty Scanner
-pS, --ping-sweep       Check live host using methode Ping Sweep
-rS, --resolver          Convert domain lists to resolved IP lists without
duplicates
-sC, --status-code       Get status codes, response from domain list
-nT, --nmap-top          Port scanning with top-ports using nmap from
domain list
-sS, --screenshot       Screenshots a list of website
-nP, --no-passive        Do not perform passive subdomain enumeration
--no-probe              Do not perform httprobe

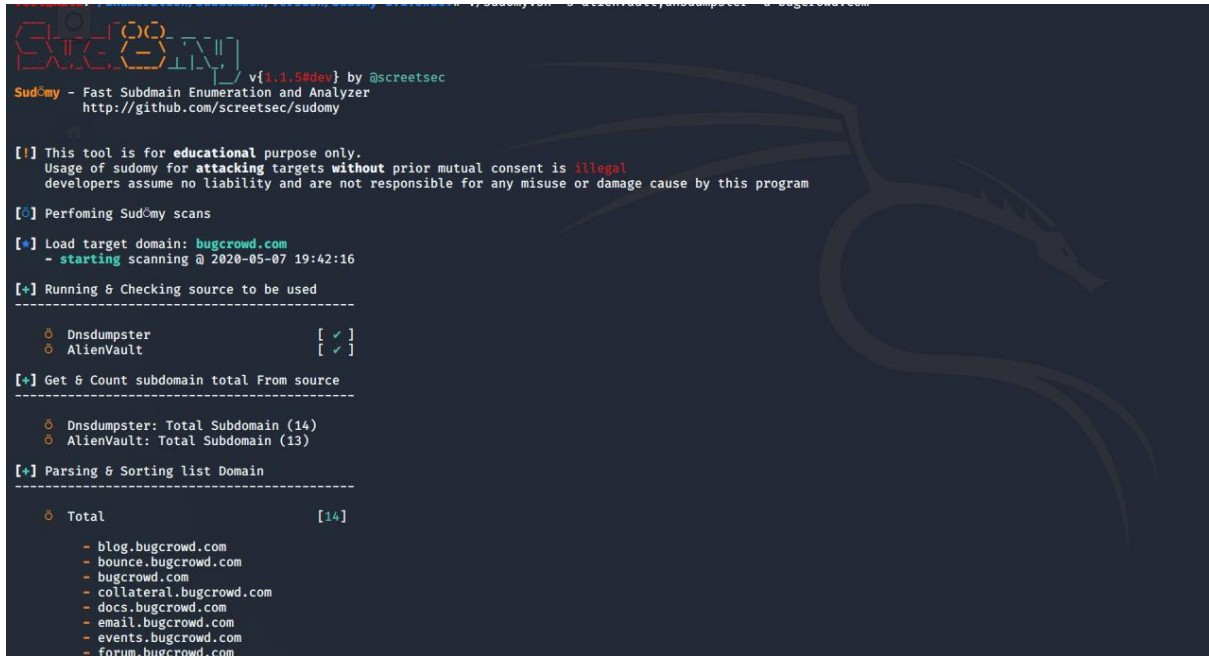
```

Menggunakan seluruh situs pihak ketiga, kemudian melakukan pengujian apakah http/https server berfungsi dengan baik:

```
$ sudomy -d bugcrowd.com
```

Menggunakan salah satu situs pihak ketiga atau lebih:

```
sudomy -s shodan,dnsdumpster,webarchive -d bugcrowd.com
```



```

Sudomy - Fast Subdomain Enumeration and Analyzer
http://github.com/screetsec/sudomy

v{1.1.5#dev} by @screetsec

[!] This tool is for educational purpose only.
Usage of sudomy for attacking targets without prior mutual consent is illegal
developers assume no liability and are not responsible for any misuse or damage cause by this program

[+] Performing Sudomy scans

[+] Load target domain: bugcrowd.com
- starting scanning @ 2020-05-07 19:42:16

[+] Running & Checking source to be used
-----
o Dnsdumpster [✓]
o AlienVault [✓]

[+] Get & Count subdomain total From source
-----
o Dnsdumpster: Total Subdomain (14)
o AlienVault: Total Subdomain (13)

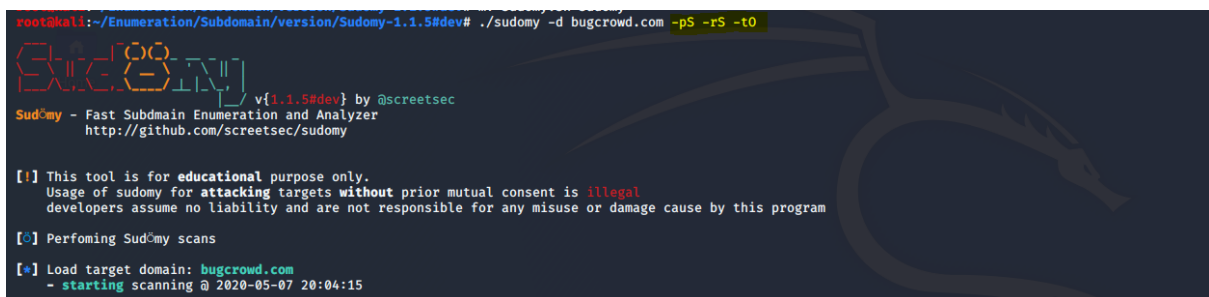
[+] Parsing & Sorting list Domain
-----
o Total [14]

- blog.bugcrowd.com
- bounce.bugcrowd.com
- bugcrowd.com
- collateral.bugcrowd.com
- docs.bugcrowd.com
- email.bugcrowd.com
- events.bugcrowd.com
- forum.bugcrowd.com
```

Figure 13. Menggunakan salah satu resources/situs pihak ketiga atau Lebih

Menggunakan satu atau lebih Plugin:

```
$ sudomy -d bugcrowd.com -pS -rS -tO
```



```

root@kali:~/Enumeration/Subdomain/version/Sudomy-1.1.5#dev# ./sudomy -d bugcrowd.com -pS -rS -tO

Sudomy - Fast Subdomain Enumeration and Analyzer
http://github.com/screetsec/sudomy

v{1.1.5#dev} by @screetsec

[!] This tool is for educational purpose only.
Usage of sudomy for attacking targets without prior mutual consent is illegal
developers assume no liability and are not responsible for any misuse or damage cause by this program

[+] Performing Sudomy scans

[+] Load target domain: bugcrowd.com
- starting scanning @ 2020-05-07 20:04:15
```

Figure 14. Menggunakan satu plugin atau Lebih

Menggunakan seluruh Plugin , seperti pengecekan status host, status code, subdomain takeover, screenshots

```
sudomy -d bugcrowd.com --all
```

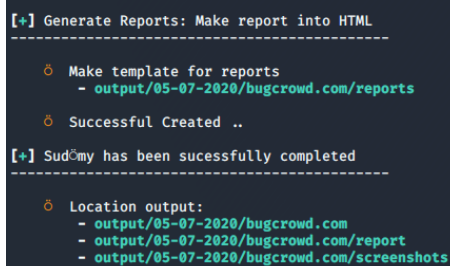
Dalam hal ini, plugin untuk Nmap, Gobuster dan wappalyzer tidak disertakan. Jadi Anda bisa menambahkan lebih banyak argumen untuk plugin itu, misalnya

```
sudomy -d bugcrowd.com --all -aI webanalyze
```

Membuat output laporan dalam format html

```
sudomy -d bugcrowd.com --all --html
```

Jika program sudah selesai dijalankan maka output dan report akan berada di folder output /

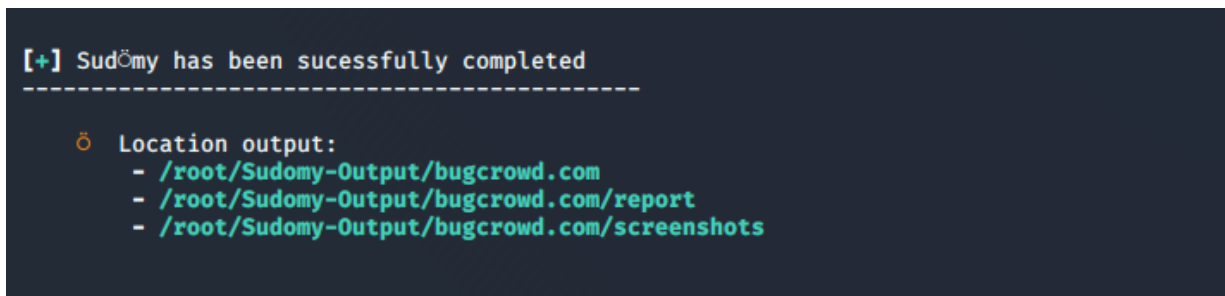


```
[+] Generate Reports: Make report into HTML
-----
  o Make template for reports
    - output/05-07-2020/bugcrowd.com/reports
  o Successful Created ..
[+] Sudomy has been sucessfully completed
-----
  o Location output:
    - output/05-07-2020/bugcrowd.com
    - output/05-07-2020/bugcrowd.com/report
    - output/05-07-2020/bugcrowd.com/screenshots
```

**Figure 15.** Hasil scanning

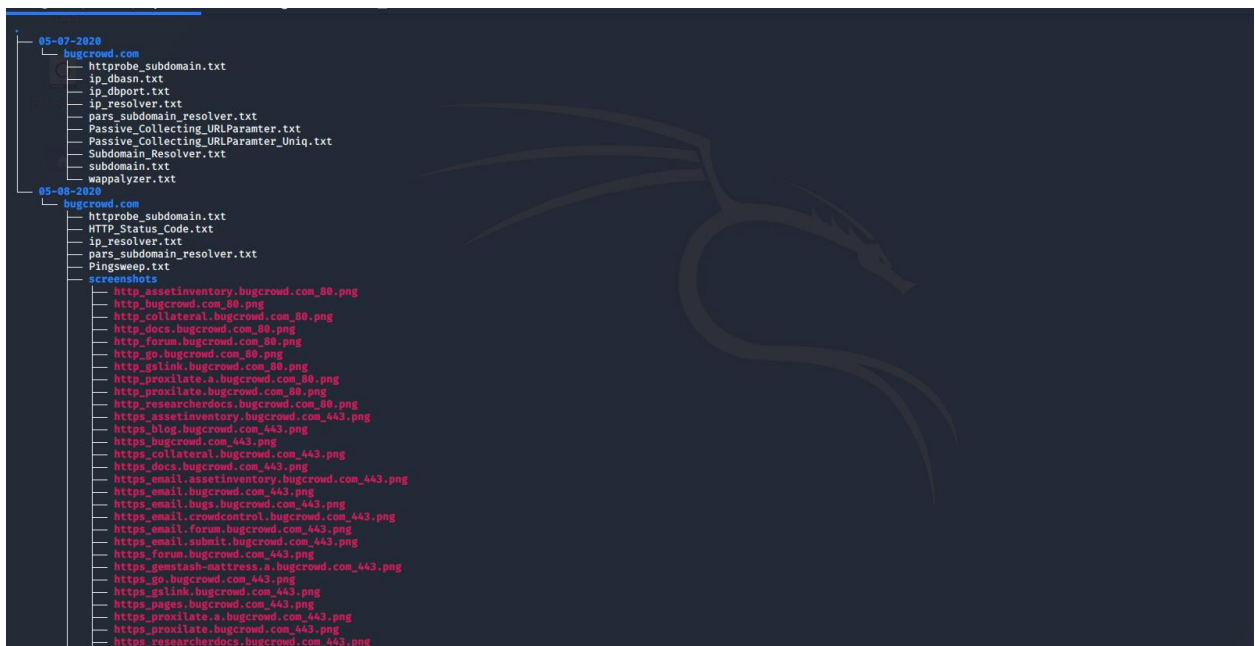
Kita juga dapat menentukan jalur untuk file keluaran (tentukan file keluaran setelah selesai) dengan argumen

```
sudomy -d bugcrowd.com --all -outfile /root
```



**Figure 16.** Hasil scanning dengan output yang telah ditentukan

Struktur Folder Output berdasarkan nama domain dan tanggal disaat melakukan scanning, seperti gambar berikut



**Figure 17.** Stuktur folder hasil scanning sudomy

Mengirim Notifikasi ke Slack Channels

```
sudomy -d bugcrowd.com --slack
```

Untuk menggunakan argumen terbaik untuk mengumpulkan subdomain & menganalisis dengan melakukan pengintaian otomatis dan mengirimkan pemberitahuan ke slack

```
./sudomy -d bugcrowd.com -dP -eP -rS -cF -pS -tO -gW --httpx --dnsprobe  
-aI webanalyze --slack -sS
```

#### 4.10 Kesimpulan

Berdasarkan pengujian dengan tools yang serupa, *sudomy* masih lebih cepat dalam proses enumerasi pencarian subdomain. Selain itu *sudomy* juga dilengkapi fitur-fitur otomatisasi yang sangat membantu peneliti dan/atau analis Cyber Security dalam mempermudah kegiatan pengumpulan informasi serta melengkapi tools yang diperlukan pentester/bug hunter dengan membuat proses menjadi lebih efektif dan efisien. Aplikasi *sudomy* juga dapat diunduh secara bebas di <https://github.com/Screetsec>. Pengembangan selanjutnya diharapkan *sudomy* dapat terintegrasi dengan aplikasi information security assessment lainnya.

#### References

- [1] Kalsum, T. U., & Kurniawan, A. (2016). Analisa Implementasi Teknik *Reconnaissance* Pada Webserver (Studi Kasus: Upt Puskom Universitas Dehasen). *Jurnal Media Infotama*, 12(1)
- [2] Mockapetris P V. 1987 *RFC 1035: Domain Names - Implementation and Specification*
- [3] Sinaci A A, Sehitoglu O T, Yondem M T, Fidan G and Tatli I 2010 SEMbySEM in Action: Domain Name Registry Service Through a Semantic Middleware *eChallenges*, 2010 1–8
- [4] Scarfone K, Souppaya M, Cody A and Orebaugh A 2015 *NIST SP 800-42: Guideline on Network Security Testing* vol 115 (Gaithersburg, MD)
- [5] Open Information Systems Security Group 2006 *Information Systems Security Assessment Framework (ISSAF)*
- [6] Rudrakshi C, Varshney A, Yadla B, Kanneganti R and Somalwar K 2014 API-fication
- [7] Mendoza A and Gu G 2018 *Mobile Application Web API Reconnaissance: Web-to-Mobile Inconsistencies & Vulnerabilities Proc.* - IEEE Symp. Secur. Priv. 2018-May 756–69
- [8] Hariyadi D and Fazlurrahman 2019 Membangun Telegram untuk Crawling Malware OSINT Menggunakan Raspberry Pi *Indones. J. Bus. Intell.* 2 18–24
- [9] Ramey C and Fox B 2019 *Bash Reference Manual* (Free Software Foundation, Inc.)
- [10] Davis I J, Wexler M, Zhang C, Holt R C and Weber T 2015 Bash2py: A bash to Python translator 2015 *IEEE 22nd Int. Conf. Softw. Anal. Evol. Reengineering, SANER 2015 - Proc* 508–11

