CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 4, No. 1, Mei 2021, hlm. 44-48

PENGEMBANGAN APLIKASI *INFORMATION GATHERING* MENGGUNAKAN METODE *HYBRID SCAN* BERBASIS *GRAPHICAL USER INTERFACE*

Mardhani Riasetiawan[1], Akas Wisnuaji[2], Dedy Hariyadi[3], Tri Febrianto[4]

[1]Universitas Gadjah Mada
[2]Komunitas LowSec Indonesia
[3]Universitas Jenderal Achmad Yani Yogyakarta
[4]PT. Widya Adijaya Nusantara
Email: [1]mardhani@ugm.ac.id, [2]akaswisnuaji@gmail.com, [3]dedy@unjaya.ac.id,
[4]tri.febrianto@widyasecurity.com

(Naskah masuk: 10 Mei 2021, diterima untuk diterbitkan: 31 Mei 2021)

Abstrak

Sebagian analis keamanan sistem dan jaringan komputer menyatakan aplikasi atau alat bantu pengujian berbasis Command-line Interface (CLI) sangat mempermudah pekerjaan. Namun, tidak banyak aplikasi tersebut tidak komprehensif baik cara menganalisis maupun hasil laporannya. Laporan pada proses pengujian keamanan sistem dan jaringan komputer diharapkan minimal terdiri dari dua tipe, yaitu keperluan manajemen dan tim teknis. Tulisan ini diusulkan pengembangan aplikasi atau alat bantu pengujian keamanan sistem dan jaringan komputer yang komprehensif dan memiliki laporan yang memudahkan tim manajemen dan tim teknis. Pada pengembangan ini menggunakan bahasa pemrograman Python dengan module TKInter untuk menghasilkan aplikasi berbasis Graphical User Interface (GUI). Dengan menggunakan aplikasi GUI harapannya dapat digunakan oleh siapapun. Fokus pengembangan aplikasi ini yaitu pada tahapan Information Gathering yang menggunakan metode Hybrid Scan,yaitu: Passive dan Active. Passive Scan menggunakan 11 Application Programming Interface (API) sedangkan Active Scan menggunakan Socket Module Python dan berberapa aplikasi native yang berjalan di GNU/Linux.

Kata kunci: *CLI, GUI, Python, TKInter, Information Gathering, Penetration Test, GNU/Linux*

INFORMATION GATHERING APPLICATION DEVELOPMENT USING HYBRID SCAN METHOD BASED ON GRAPHICAL USER INTERFACE

Abstract

Some computer system and network security analysts say that the application or test tool based on Command-line Interface (CLI) makes the job easier. However, not many of these applications are not comprehensive in terms of analyzing and reporting results. Reports on the process of testing computer system and network security are expected to consist of at least two types, namely the needs of management and technical teams. This paper proposes the development of an application or testing tool for computer system and network security testing that is comprehensive and has reports that make it easier for the management team and the technical team. This development uses the Python programming language with the TKInter module to produce a Graphical User Interface (GUI) based application. By using the GUI application, it is hoped that it can be used by anyone. The focus of developing this application is at the Information Gathering stage using the Hybrid Scan method, namely: Passive and Active. Passive Scan uses 11 Application Programming Interfaces (APIs) while Active Scan uses Python Socket Module and several native applications running on GNU / Linux.

Keywords: *CLI, GUI, Python, TKInter, Information Gathering, Penetration Test, GNU/Linux*

1. PENDAHULUAN

Kerangka kerja asesmen keamanan sistem informasi, ISSAF (*Information Systems Security Assessment Framework*) membagi tahapan asesmen menjadi sembilan tahapan, *Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access & Privilegde Escalation, Enumerating Further, Compromise Remote Users/Sites, Maintaining Access,* dan *Covering Tracks* (Open Information Systems Security Group, 2006). Pada proses asesmen, temuan celah keamanan vital dapat ditemukan pada tahapan awal, yaitu **Information Gathering**. Hal ini disebabkan ada sebuah kesalahan dalam proses pengembangan sebuah sistem yang disebut *Misconfiguration* (Sahtyawan, 2019).

Information Gathering merupakan tahapan yang komprehensif dalam mengidentifikasi target untuk mengetahui beberapa informasi diantaranya, status atau tipe jaringan, jenis sistem operasi yang digunakan, rentang IP Address yang digunakan, port yang terbuka, dan DNS Server yang digunakan. Bahkan tahapan ini bisa digunakan untuk mengidentifikasi kepemilikan sebuah sistem (Zeeshan et al., 2017). Informasi-informasi yang didapatkan ini menjadi hal yang penting sebagai pendukung tahapan asesmen selanjutnya. Alat bantu dalam tahapan *Information Gathering* telah banyak tersedia di sistem operasi yang khusus untuk kegiatan pengujian keamanan informasi atau situs web penyedia layanan jasa pengujian keamanan informasi (Denis, Zena dan Hayajneh, 2016). Namun, alat bantu tersebut kurang memenuhi kebutuhan analis/penguji keamanan siber secara komprehensif (Hariyadi, Wijayanto dan Fazlurrahman, 2020). Oleh sebab itu dikembangkan aplikasi Sudomy sebagai aplikasi yang mendukung tahapan *Information Gathering* lebih komprehensif dengan metode *hybrid scan* (Ramadhan, Aresta dan Hariyadi, 2020).

Walaupun laporan dari aplikasi Sudomy sudah berbasis web tetapi saat ini antarmuka aplikasi masih berbasis skrip sehingga dapat digolongkan sebagai aplikasi berbasis *Command Line Interface* (CLI) (Morris, 2016). Untuk memudahkan penggunaan, pada penelitian ini dikembangkan aplikasi *Information Gathering* yang komprehensif dengan metode *hybrid scan* dan berbasis *Graphical User Interface (GUI)* . Selain antarmuka berbasis GUI, laporan yang akan disajikan dalam bentuk HTML (*Hypertext Markup Languange*) yang dapat dibuka menggunakan peramban web.

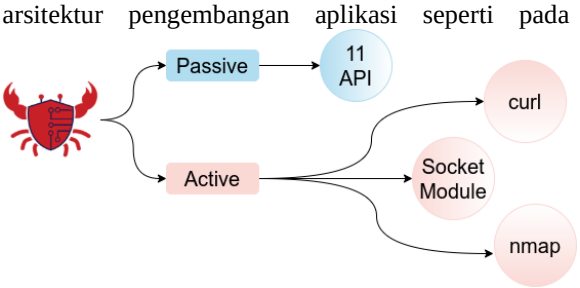
2. METODOLOGI PENELITIAN

Pada penelitian ini mengadopsi metode yang digunakan aplikasi Sudomy dalam melakukan pemindaian. Metode *hybrid scan*, menggabungkan dua metode pemindaian, yaitu pasif dan aktif. Pemindaian pasif yaitu pemindaian yang menggunakan pihak ketiga dalam melakukan proses pemindaian target. Sebaliknya dengan pemindaian aktif yaitu pemindaian yang menggabungkan sumber daya atau aplikasi yang telah terinstall sebelumnya pada komputer (Ramadhan, Aresta dan Hariyadi, 2020). Adapun detil perbedaaan antara Sudomy dan penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Perbandingan Sudomy dan Penelitian Saat Ini

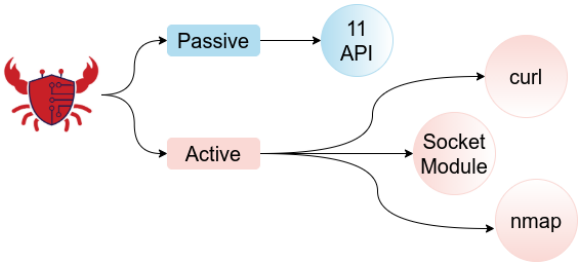
Metode	Sudomy	Penelitian Ini
Pemindaian Pasif		
Censys	V	
Shodan	V	
DNS Bufferover Run	V	
F-Secure Riddler	V	V
Cert Spotter	V	V
Hacker Target	V	V
ThreatMiner	V	
RiskIQ	V	
Certificate Search	V	V
DNS Dumpster	V	V
BinaryEdge	V	
SecurityTrails	V	
Facebook	V	
AlienFault	V	V
Rapid DNS	V	V
Spyse	V	
URL Scan	V	V
DNS DB	V	
Threat Crowd	V	V
Wayback Machine	V	V
Common Crawl		V
Pemindaian Aktif		
Gobuster	V	
Curl		V
Python Socket Module		V
Nmap		V

Berdasarkan Tabel 1 maka disusun sistem arsitektur pengembangan aplikasi seperti pada



Gambar 1. Baik Sudomy dan aplikasi ini adalah memanfaatkan *Application Programmable Interface* (API). Perbedaannya yang mendasar dari Sudomy dan aplikasi ini adalah penggunaan bahasa pemrograman. Pada penelitian ini, aplikasi yang akan dikembangkan menggunakan bahasa pemrograman Python. Bentuk pemanfaatan pustaka Python berupa Socket Module yang diperlukan pada pengembangan aplikasi *Information Gathering*.

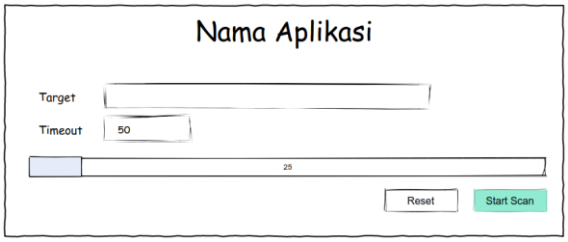
Struktur aplikasi terdiri dari dua bagian, yaitu *backend* dan antarmuka. Bagian *backend* berisi kode inti berupa bahasa pemrogram python yang memanfaatkan 11 API untuk mendapatkan informasi suatu domain. Adapun 11 API yang digunakan adalah F-Secure Riddler, Cert Spotter, Hacker Target, Certificate Search, DN Dumpster, AlienFault, Rapid DNS, URL Scan, Threat Crowd, Wayback Machine, dan Common Crawl. Sedangkan



Gambar 1. Arsitektur Hybrid Scan

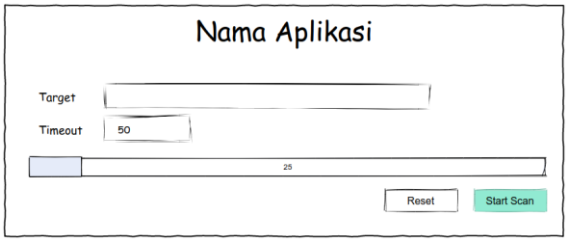
pengembangan antara muka menggunakan TKInter yang merupakan modul pengembangan berbasis GUI pada bahasa pemrograman Python (Surya Gunawan et al., 2020).

Pengembangan aplikasi Information Gathering ini dibuat untuk memudahkan pengguna dalam pencarian informasi. Pengguna cukup memasukan domain dari target dan nilai batas waktu pemindaian per-API. Standar batas waktunya maksimal 50 detik.



Gambar 2 menunjukan rancangan antarmuka dari pengembangan aplikasi ini.

Jika penulisan target ada kesalahan dapat memanfaatkan tombol reset untuk mengulangi entri nama target. Penggunaan API sebanyak 11 maka akan memiliki dampak waktu proses pemindaian. Selain itu proses pemindaian juga memiliki ketergantungan akses internet dari pengguna maupun dari target.



Gambar 2. Rancangan Antarmuka Aplikasi

3. HASIL DAN PEMBAHASAN

Bahasa pemrograman Python pada prinsipnya telah menerapkan model Object Oriented Prrogramming (OOP) (Goldwasser dan Letscher, 2007). Oleh sebab itu pada aplikasi ini menerapkan prinsip OOP yang sederhana dengan memisahkan kode *backend* dan antarmuka. Kode *backend* melakukan proses information gathering dengan metode pemindaian pasif dan aktif. Metode pemindaian pasif memanfaatkan sumber daya pihak ketiga dengan memanfaatkan 11 API. Adapun cuplikan kode backend yang memanfaatkan 11 API dapat dilihat pada Kode 1.

```
def get_domain(self):
api = [
"http://web.archive.org/cdx/search/cdx?url=*."+self.url+"/&output=text&fl=original&collapse=urlkey",
"https://threatcrowd.org/searchApi/v2/domain/report/?domain="+self.url,
"https://urlscan.io/api/v1/search/?q="+self.url,
"https://rapiddns.io/subdomain/"+self.url,
"https://otx.alienvault.com/api/v1/indicators/domain/"+self.url+"/passive_dns",
"https://dnsdumpster.com/",
"https://crt.sh/?q="+self.url+"&output=json",
"https://api.threatminer.org/v2/domain.php?q="+self.url+"&rt=5",
"https://api.certspotter.com/v1/issuances?domain="+self.url+"&include_subdomains=true&expand=dns_names",
"https://api.hackertarget.com/hostsearch/?q="+self.url,
"https://riddler.io/search/exportcsv?q=pld:"+self.url,
"http://index.commoncrawl.org/CC-MAIN-2020-50-index?url=*."+self.url+"&output=json",
]

Y = Pool(12)

Y.map(self.scan_domain, api)
```

Kode 1. *API Backend*

Metode pemindaian aktif memanfaatkan sumber daya yang telah pasang pada sistem operasi atau pustaka pada bahasa pemrograman. Ada tiga sumber daya yang dimanfaatkan pada aplikasi ini, yaitu cURL, socket module, dan nmap. Aplikasi cURL yang telah terinstall pada sistem operasi berfungsi sebagai perintah dalam bentuk baris untuk mentransfer data (Hutagalung, Nugroho dan Hidayat, 2017). cURL pada aplikasi ini digunakan untuk memastikan status aktif atau non-aktif dari sebuah server yang menjadi target. Kode 2 menunjukan sebuah fungsi dari bahasa pemrograman python yang pemanfaatan cURL dalam memastikan status sebuah target.

```
def scan_livehost(self, url):
try:
time.sleep(1)
cmd = subprocess.getoutput("curl -Is "+url)
if cmd:
self.livehost += [url]
except:
pass
```

Kode 2. *Live Host Scan*

Untuk mendapatkan nama hostname dari sebuah target menggunakan socket module yang tertuang dalam fungsi scan_IP, seperti pada Kode 3. Sumber daya lainnya adalah memanfaatkan Nmap yang telah terpasang pada sistem operasi. Nmap sesuai fungsi dasarnya yaitu sebagai aplikasi pemindai *port* dari sebuah komputer/server (Gordon

Lyon, 2011). Begitu pula pada aplikasi ini, Nmap juga berfungsi sebagai pemindai port yang tertuang seperti pada Kode 4.

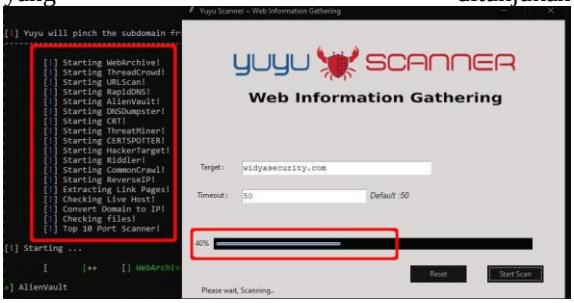
```
1  def scan_IP(self, url):
2  try:
3  ip = socket.gethostbyname(url)
4  if ip not in self.ips:
5  self.ips += [ip]
6  except:
7  pass
```

Kode 3. *IP Scan*

```
1  def scan_port(self,ip):
2  try:
3  if "*." not in ip:
4  if ":" not in ip:
5  cmd = subprocess.getoutput("nmap -F --top-ports 10 "+ip)
6  self.port += [{'url':ip, 'result':cmd}]
7  except:
8  pass
```

Kode 4. *Port Scan*

Kode antarmuka yang menggunakan modul Tkinter pada Python selain berfungsi untuk membangun aplikasi berbasis *Graphical User Interface* (GUI), pada bagian antarmuka juga untuk memproses temuan menjadi sebuah laporan dalam bentuk berkas HTML, seperti pada Kode 5. Adapun proses pemindaian sebuah target pada *mode debug* yang ditunjukan



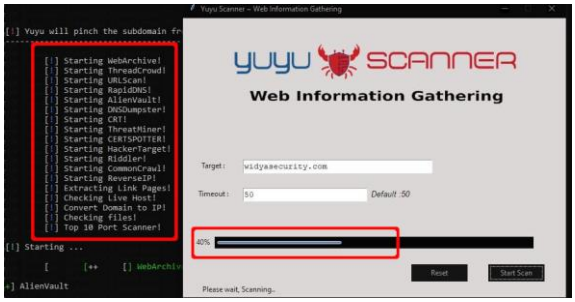
Gambar 4 bahwa pada saat proses pemindaian terlihat melakukan pemindaian dengan metode pemindaian aktif. Sedangkan pada antarmuka berbasis GUI yang diperuntukan pengguna tidak menunjukan proses latar dalam bentuk *mode debug* sehingga dalam melakukan tahapan Information Gathering yang mengintegrasikan seluruh temuan dari 11 API dapat mempermudah pengguna, seperti pada

Gambar 3.

```
1  try:
2  import Tkinter as tk
3  except ImportError:
4  import tkinter as tk
5  try:
6  import ttk
7  py3 = False
8  except ImportError:
9  import tkinter.ttk as ttk
10 py3 = True
11 def vp_start_gui():
12 '''Starting point when module is the main routine.'''
13 global val, w, root
14 root = tk.Tk()
15 top = Toplevel1 (root)
16 root.mainloop()
```

Kode 5. Implementasi TKInter

Gambar 3. Antarmuka Aplikasi



Gambar 4. Proses Pemindaian pada *Mode Debug*

4. KESIMPULAN

Aplikasi yang dihasilkan dari penelitian ini diberi nama Yuyu Scanner yang merupakan alat bantu dalam proses pengujian sistem dan keamanan jaringan, yaitu pada tahapan *Information Gathering*. Dengan memanfaatkan metode pemindaian active dan passive, Yuyu Scanner memeliki tujuh proses utama, yaitu:

1. Sub-Domain Enumeration, tahapan mencari sub-domain dari target dari berbagai sumber.
2. Reverse IP, tahapan mencari informasi IP Address yang digunakan dalam 1 mesin.
3. Page Link Extraction, tahapan mencari parameter yang tercatat pada URL (Uniform Resource Locator).
4. Check Live Host, memastikan mesin dari sub-domain yang ditemukan dalam kondisi menyala.
5. Convert Domain to IP, melakukan konversi sub-domain yang ditemukan dalam bentuk IP Address.
6. Port Scanning, melakukan pemindaian protokol dari mesin domain utama dan sub-domain yang dalam kondisi menyala.
7. Reporting, menyajikan temuan proses pemindaian dalam format HTML (HyperText Markup Language) yang mudah dipahami.

Yuyu Scanner memudahkan pentester atau analis keamanan informasi dengan tampilan berbasis GUI dan memiliki kemudahan dalam penggunaannya dalam memberikan laporan pemindaian dibandingkan alat bantu serupa yang berlisensi *Free Open Source Software* seperti Sudomy, DNSDumspter, Subslist3r, Subfinder,, dan Findomain yang masih berbasis *Command-line Interface*. Walaupun sudah berbasis GUI, Yuyu Scanner perlu dikembangkan kembali seperti laporan hasil pemindaian dalam bentuk PDF atau diintergrasikan dengan sistem pengujian keamanan lainnya. Yuyu Scanner juga masih punya potensi untuk dikembangkan dengan menambahkan metode-metode baru pemindaian yang lebih lengkap. Harapannya kekurangan tersebut dapat dikembangkan pada penelitian berikutnya.

5. UCAPAN TERIMA KASIH

Terima kasih kepada PT. Widya Adijaya Nusantara (Widya Security) yang telah memberikan pendanaan pada penelitian ini. Publikasi ini merupakan bentuk kolaborasi Industri, Perguruan Tinggi dan Komunitas. Widya Security sebagai perusahaan jasa analisis keamanan siber berkomitmen berkolaborasi antar *stakeholder* untuk mewujudkan Indonesia lebih baik.

DAFTAR PUSTAKA

DENIS, M., ZENA, C. DAN HAYAJNEH, T., 2016. Penetration testing: Concepts, attack methods, and defense strategies. *2016 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2016*.

GOLDWASSER, M.H. DAN LETSCHER, D., 2007. Teaching object-oriented programming in python. *ACM SIGCSE Bulletin*, 39(3), hal.365–366.

GORDON LYON, 2011. *Nmap Network Scanning*. [daring] Tersedia pada: <https://nmap.org/book> [Diakses 6 Jul 2018].

HARIYADI, D., WIJAYANTO, H. DAN FAZLURRAHMAN, 2020. Bangkolo : Aplikasi Vulnerability Identification Berbasis Hybrid Apps. *Cyber Security dan Forensik Digital*, 3(1), hal.39–44.

HUTAGALUNG, R.H., NUGROHO, L.E. DAN HIDAYAT, R., 2017. Analisis Uji Penetrasi Menggunakan ISSAF. In: *Hacking and Digital Forensics Exposed (H@DFEX)*. Yogyakarta: Universitas Islam Indonesia.hal.32–40.

MORRIS, H.D., 2016. *IDC's Worldwide Software Taxonomy, 2016*.

Open Information Systems Security Group, 2006. *Information Systems Security Assessment Framework (ISSAF)*. Draft 0.2. ed.

RAMADHAN, R.A., ARESTA, R.M. DAN HARIYADI, D., 2020. Sudomy: Information Gathering Tools for Subdomain Enumeration and Analysis. In: *IOP Conference Series: Materials Science and Engineering*. [daring] Tersedia pada: <https://iopscience.iop.org/article/10.1088/1757-899X/771/1/012019>.

SAHTYAWAN, R., 2019. Penerapan Zero Entry Hacking Didalam Security Misconfiguration Pada Vapt (Vulnerability Assessment and Penetration Testing). *Journal of Information System Management*, 1(1), hal.18–22.

SURYA GUNAWAN, T., ALEAH JEHAN ABDULLAH, N., KARTIWI, M. DAN IHSANTO, E., 2020. Social Network Analysis using Python Data Mining. *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*.

ZEESHAN, M., NISA, S.U., MAJEED, T., NASIR, N. DAN ANAYAT, S., 2017. Vulnerability Assessment and Penetration Testing: A proactive approach towards Network and Information Security. *International Journal of Digital Information and Wireless Communications*, 7(2), hal.124–142.