Pengembangan Aplikasi *Information Gathering* Berbasis *HybridApps*

Chanief Budi Setiawan[1], Dedy Hariyadi[1*], Adkhan Sholeh[1], Akas Wisnuaji[2]
[1] Program Studi Teknologi Informasi, Universitas Jenderal Achmad Yani Yogyakarta
[2] PT Widya Adijaya Nusantara
[1] dedy@unjaya.ac.id, [1] chanief.b.s@gmail.com, [1] adkhan2006@gmail.com, [2]aji@widyasecurity.com

Abstrak

Information Gathering merupakan tahapan awal dalam melakukan pengujian keamanan sistem dan jaringan komputer. Istilah lain dari *Information Gathering* adalah *Reconnaissance*. Tujuan melakukan *Information Gathering* diantaranya mengumpulkan dan mendapatkan informasi berupa ekosistem yang diterapkan pengguna termasuk kepemilikan domain atau informasi sensitif lainnya. Aplikasi yang digunakan biasanya memanfaatkan pemindaian secara aktif maupun pasif. Sudomy merupakan aplikasi pemindaian yang menggunakan metode aktif dan pasif atau *HybridScan*. Namun, Sudomy masih berbasis *Command Line Interface (CLI)*. Maka pada penelitian ini diusulkan pengembangan aplikasi Sudomy berbasis grafis dengan metode *HybridApps* dengan menggabungkan teknologi *native* dari CLI dan teknologi web sebagai antarmuka grafis. Walaupun menggunakan aplikasi yang dibangun berbasis grafis tetapi secara keseluruhan fitur dan fungsi menggunakan Sudomy. Pengembangan aplikasi menggunakan metode *HybridApps* menggabungkan kelebihan dari dua teknologi atau lebih menjadi satu *platform* yang mempermudah penggunaan aplikasi. Hasil dari penelitian ini berupa aplikasi *Information Gathering* yang berbasis grafis sehingga mempermudah penggunaan dalam proses pengujian keamanan sistem dan jaringan komputer.
Kata kunci: *hybridapps*, *information gathering*, keamanan informasi, *penetration testing*, sudomy

Abstract

Information Gathering is the initial stage in testing the security of computer systems and networks. Another term for Information Gathering is Reconnaissance. The purpose of conducting Information Gathering includes collecting and obtaining information in the form of an ecosystem implemented by users, including domain ownership or other sensitive information. The applications used usually take advantage of active or passive scanning. Sudomy is a scanning application that uses active and passive methods or HybridScan. However, Sudomy is still based on the Command Line Interface (CLI). So in this study, it is proposed to develop a graphical-based Sudomy application using the HybridApps method by combining native technology from the CLI and web technology as a graphical interface. Although using an application that is built based on graphics, but overall the features and functions use Sudomy. Application development using the HybridApps method combines the advantages of two or more technologies into one platform that makes it easier to use applications. The results of this study are in the form of a graphical-based Information Gathering application, making it easier to use in the process of testing computer system and network security.
Keywords: *hybridapps, information gathering, information security, penetration testing, sudomy*

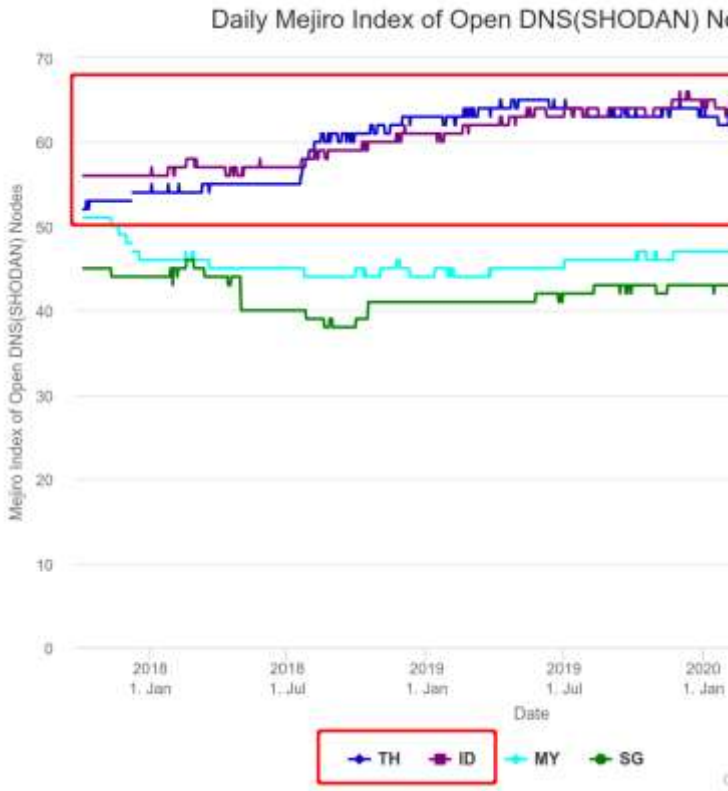
1. PENDAHULUAN

Domain Name System (DNS) merupakan layanan fundamental di jaringan internet yang memetakan alamat IP dan nama domain seluruh dunia (Dooley & Rooney, 2017). DNS merupakan bagian dari Layer Aplikasi pada TCP/IP Layer yang mentransfer data antara server dan klien. Terdapat ratusan protokol pada Layer Aplikasi ini sehingga terdapat beberapa informasi penting di dalamnya, termasuk DNS (Kent et al., 2006). Perkembangan sistem berbasis daring mengalami pertumbuhan termasuk di dalamnya terdapat informasi penting melekat. Hal ini tidak menutup kemungkinan terjadi pada konfigurasi DNS (Van Heugten, 2018). Maka dari itu, fase asesmen pada *Information Systems Security Assessment Framework (ISSAF)* diawali dengan

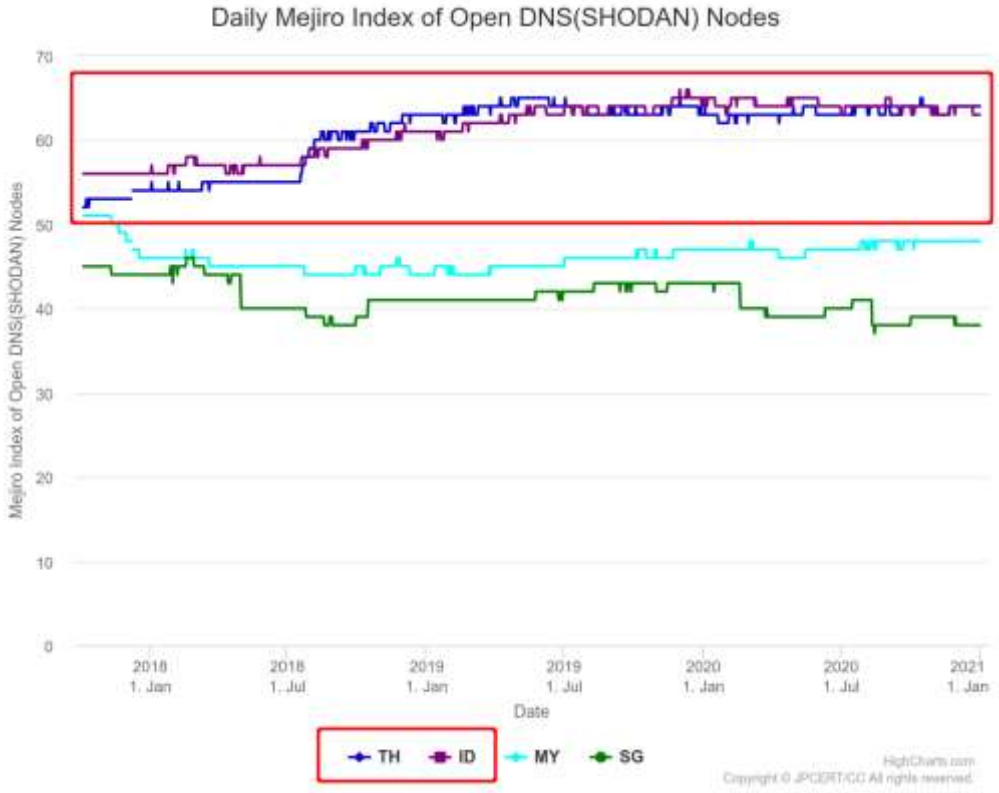
fase *Information Gathering*. Pada fase *Information Gathering* teknik yang digunakan untuk mengetahui informasi dari target asesmen memanfaatkan informasi pada DNS seperti diantaranya, informasi registar, pengelola teknis, pengelola finansial, IP, dan sub-domain (Open Information Systems Security Group, 2006).

Informasi-informasi tersebut dapat ditemukan di internet dengan sangat mudah. Hal ini tergantung dari konfigurasi keamanan DNS di setiap organisasi (Wang et al., 2018). Lembaga atau Tim Tanggap Insiden Siber di Jepang, JPCERT/CC merancang sebuah indeks risiko internet dalam bentuk visualisasi tentang beberapa kerentanan protokol pada internet di seluruh dunia. Indeks ini disebut dengan Mejiro yang mengolah sumber data dari Shodan, Censys, dan CGI (Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara, 2020). Indeks Mejiro mencatat berdasarkan sumber-sumber tersebut beberapa celah keamanan DNS, yaitu *Open DNS Resolver* yang memungkinkan diserang dan digunakan tanpa otoritas resmi (Park et al., 2019).

JPCERT/CC mencatat celah *Open DNS Resolver* di Indonesia cukup tinggi dibanding negara tetangga seperti Singapura dan Malaysia. Berdasarkan *Index Time Series Graph* Mejiro pada



Gambar 1 bahwa potensi celah keamanan DNS Open Resolver di Indonesia dan Thailand masih cukup tinggi. Data tersebut dicatat sejak 1 Januari



Gambar 1. Perbandingan OpenDNS Berdasarkan Mejiro Index

2018 sampai dengan 1 Januari 2021.

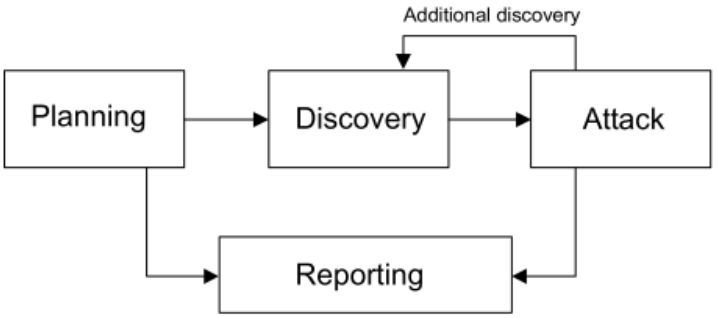
Informasi yang didapatkan dari DNS dapat dikategorikan dalam dalam fase asesmen *Information Gathering* (Hariyadi & Nastiti, 2021). Aplikasi yang digunakan pada fase asesmen diantaranya adalah Sudomy. Aplikasi Sudomy merupakan aplikasi yang dikembangkan menggunakan metode *active scan* dan *passive scan* untuk mendukung proses pengujian keamanan informasi pada fase *Information Gathering* dan *Network Mapping*. Adapun fitur utama Sudomy diantaranya adalah pemeriksaan Host pada subdomain *active*, informasi HTTP status *code response*, konversi dari subdomain list ke *Resolver IP*, *port scanning* dari *Resolver IP*, pemeriksaan serangan *Subdomain Take-Over*, *screenshots* melalui domain list, serangan DNS *Bruteforce Subdomain*, dan laporan interaktif. Namun, kekurangan aplikasi Sudomy belum menggunakan antarmuka grafis yang memudahkan pengguna. Penggunaan aplikasi Sudomy saat ini masih berbasikan perintah text atau *CLI (Command Line Interface)* (Ramadhan et al., 2020).

Aplikasi Sudomy masih perlu pengembangan terutama dari sisi antarmuka. Oleh sebab itu pada penelitian ini diusulkan pengembangan aplikasi Sudomy berbasis *Graphical User Interface* (GUI) menggunakan metode *HybridApps* yang memadukan dua teknologi CLI dan GUI. Aplikasi keamanan informasi yang pengembangannya menggunakan metode *HybridApps*, yaitu Bangkolo. Aplikasi Bangkolo merupakan aplikasi yang digunakan pada fase *Vulnerbility Identification* yang menggabungkan keunggulan aplikasi berbasis CLI, Nmap dengan kerangka pengembangan aplikasi *multiplatform* yang berbasis Javascript, ElectronJS sehingga menghasilkan aplikasi berbasis GUI (Hariyadi et al., 2020).

2. METODE

2.1 NIST SP 800-115

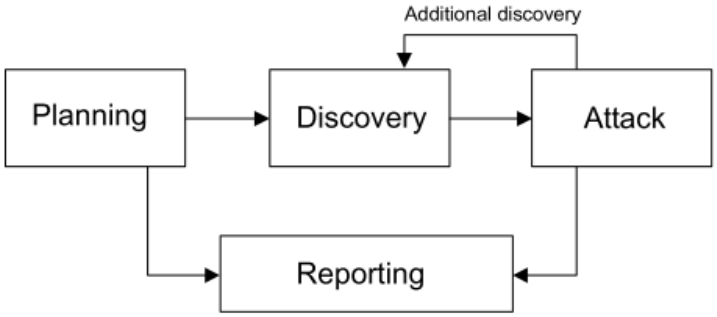
Kementerian perdagangan Amerika Serikat melalui *National Institute of Standards and Technology* mengeluarkan petunjuk standar pengujian dan asesmen keamanan informasi dengan kode NIST SP 800-115. Standar NIST 800-115 merupakan penyempurnaan standar NIST SP 800-42. Namun, tahapan melakukan metode asesmennya masih sama yaitu *Planning, Discovery, Attack* dan *Report*, seperti tampak pada



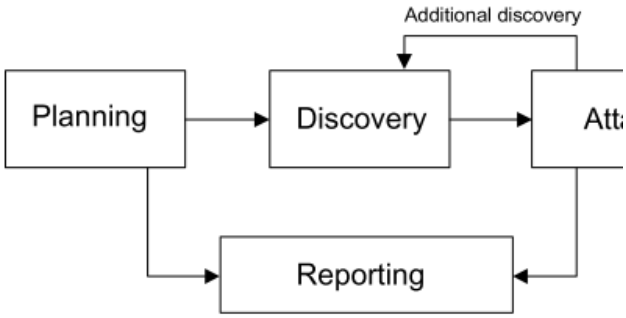
Gambar 2. Pada penelitian ini menitikberatkan pada tahapan *Discovery*, yaitu suatu tahapan mengidentifikasi target yang berpotensi untuk mendapatkan informasi seperti *hostname*, alamat IP, staff yang bertanggung jawab terhadap domain, informasi dari layanan aplikasi, dan kondisi atau status dari sebuah server (Scarfone et al., 2008). Tahapan semacam ini juga disebut sebagai tahapan *information gathering* pada *Information Security Assessment Framework* (Open Information Systems Security Group, 2006).

2.2 *Information Gathering*

Berdasarkan pada



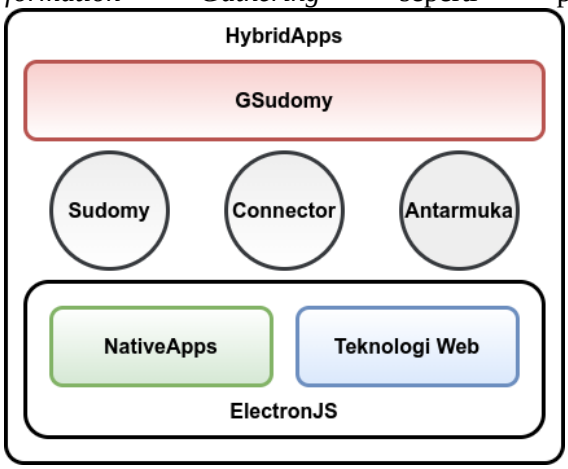
Gambar 2. Tahapan Asessmen Berdasarkan NIST SP 800-115



Gambar 2 tahapan *Discovery* atau *Information Gathering* tidak hanya dilakukan diawal saja. Namun, tahapan ini bisa dilakukan ulang setelah proses *Attack* dengan tujuan mendapatkan informasi tambahan dalam mengakses target yang berpotensi. Walaupun *information gathering* pada tahapan awal terkadang mendapatkan celah keamanan berupa *misconfiguration* seperti informasi username dan password (Sahtyawan, 2019). Sehingga tahapan *Information Gathering* merupakan tahapan penting yang tidak boleh ditinggalkan. Aplikasi Sudomy merupakan aplikasi yang dikategorikan sebagai pendukung tahapan *Information Gathering* dengan menganalisis subdomain. Sudomy dikembangkan menggunakan dua metode, yaitu *passive scan* dan *active scan*. Pada *metode passive scan*, Sudomy memanfaatkan pustaka pihak ketiga seperti DNSdumpster, WebArchive, Shodan, Total Virus, Certsh, BinaryEdge, SecurityTrails, Certspotter, Censys, Threatminer, Bufferover, Hackertarget, Entrust, ThereatCrowd, dan Riddler. Sedangkan metode *active scan* menggabungkan aplikasi yang telah terinstall di komputer seperti Gobuster (Ramadhan et al., 2020).

2.3 Arsitektur Aplikasi

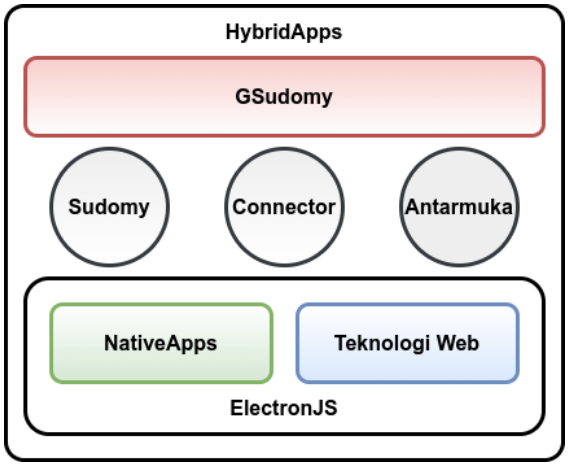
Pengembangan aplikasi berbasis GUI yang mengkombinasikan pengembangan aplikasi web dan aplikasi *native* yang dapat diartikan sebagai pengembangan aplikasi berbasis *HybridApps*. Pada *HybridApps* memanfaatkan kelebihan masing-masing pengembangan, misal aplikasi web memiliki kelebihan tampilan yang interaktif sedangkan aplikasi *native* memiliki performa yang cepat (Hariyadi & Irawan, 2014). Kerangka pengembangan yang mendukung *HybridApps* diantaranya ElectronJS yang dikembangkan oleh pengembang dari Github, Cheng Zhao (Cai et al., 2019). Adopsi kerangka ElectronJS yang dikembangkan Cheng Zao diimplementasikan pada pengembangan *Information Gathering* seperti pada



Gambar 3.

2.4 Rancangan Antarmuka

Antarmuka yang dikembangkan pada aplikasi *Information Gathering* ini menerapkan tampilan *dual-pane*. Sebuah aplikasi dengan tampilan *dual-pane* selain memiliki rancangan yang sederhana, memiliki fungsi mempermudah pengguna dalam mengamati setiap fungsi dari aplikasi (Sciore, 2019). Adapun rancangan aplikasi *Information Gathering* dengan *dual-pane* dapat dilihat pada 6.



Gambar 3. Arsitektur *Information Gathering* Berbasis *HybridApps*

3. HASIL DAN PEMBAHASAN

Sudomy sebagai aplikasi *Information Gathering* dengan metode *HybridScan* memiliki kelebihan menggabungkan beberapa metode pemindaian. Walaupun menggunakan metode *HybridScan*, Sudomy merupakan aplikasi yang bersifat *native*. Bahkan Sudomy tidak memiliki antarmuka grafis. Untuk mengoperasikan atau menggunakan perintah Linux atau dikenal *Command Linux Interface (CLI).*

Supaya memiliki antarmuka grafis dan mudah digunakan, aplikasi Sudomy dikombinasikan dengan teknologi web yang memiliki antarmuka mudah dipahami. Menggabungkan kedua teknologi tersebut menggunakan ElectronJS yang merupakan bagian pengembang aplikasi berbasis *HybridApps*.

Sudomy memanfaatkan berbagai API untuk melakukan pemindaian. Adapun API yang digunakan diantaranya: Facebook, Spyse, Shodan, DNSDB, Security Trails, Binary Edge, Censys, dan VirusTotal. API tersebut pada aplikasi Sudomy tersimpan di berkas konfigurasi API. Namun, hal ini menjadi tidak praktis saat menambahkan kode atau token API. Pada penelitian ini untuk menambahkan kode atau token API telah dipermudah. Adapun kode yang digunakan untuk menambahkan beberapa API menggunakan algoritma percabangan IF yang disimpan dalam sebuah function, seperti pada potongan Gambar 4Gambar 4. Algoritma Percabangan pada Konfigurasi API

.

```
1 if ($_POST['type'] == "setting") {
2 $template = '';
3 if (!empty($_POST['SHODAN_API'])) {
4 $template .=
5 'SHODAN_API="'.$_POST['SHODAN_API'].'"
6 ';
7 }
8 if (!empty($_POST['CENSYS_API'])) {
9 $template .=
10'CENSYS_API="'.$_POST['CENSYS_API'].'"
11';
12}
13if (!empty($_POST['CENSYS_SECRET'])) {
14$template .=
15'CENSYS_SECRET="'.$_POST['CENSYS_SECRET'].'
16';
17}
18...
19$h = fopen("Sudomy/sudomy.api", "w");
20fwrite($h, $template);
21}
```

Gambar 4. Algoritma Percabangan pada Konfigurasi API

Perintah CLI dari aplikasi Sudomy sebagai aplikasi *native* dikombinasikan dengan teknologi web berupa kode bahasa pemrograman PHP pada kerangka ElectronJS. Adapun potongan kode pemrograman PHP terlihat pada Gambar 5. Aplikasi Sudomy tetap tersedia di dalam satu direktori kerangka ElectronJS. Hal ini untuk mempermudah mengakses perintah CLI dari aplikasi Sudomy.

```
1   public function run($arg){
2   $cmd = shell_exec("cd Sudomy && ./sudomy
3   ".$arg." --html");
4   if (preg_match("/output\//", $cmd)) {
5   echo "sukses";
6   }
7   else{
8   echo "gagal";
9   }
10  }
```

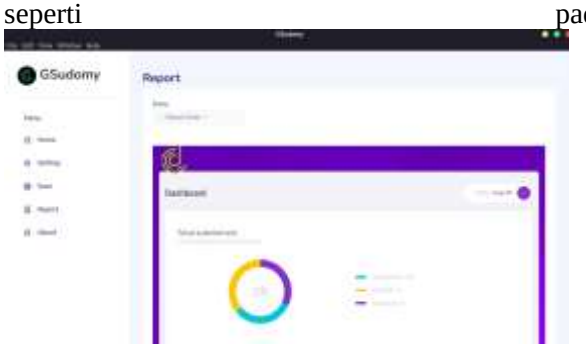
Gambar 5. Implementasi *HybridApps* pada ElektronJS

Rancangan antarmuka dari aplikasi ini terdapat beberapa pilihan diantaranya :

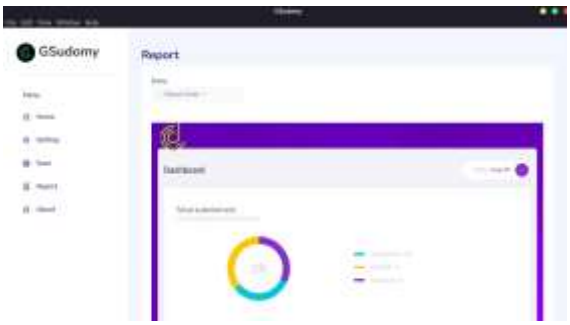
1. *Setting*, berfungsi untuk melakukan konfigurasi kode atau token API dari pihak ketiga.
2. *Scan*, merupakan fungsi utama dari aplikasi untuk melakukan pemindaian dari suatu domain.
3. *Report*, merupakan fitur laporan berdasarkan dari proses Scan.
4. *About*, merupakan halaman informasi dari aplikasi Information Gathering.

Gambar 6. Antarmuka Konfigurasi API

Gambar merupakan contoh peroses memasukan kode atau token API pada bagian *Setting*. Hasil laporan dari aplikasi Sudomy yang berbasis HTML telah dikonversi dan disisipkan dalam aplikasi ini, seperti pada



Gambar 7. Sehingga pengguna lebih mudah menggunakan aplikasi yang terintegrasi. Selain itu juga laporan dapat diunduh sesuai dengan fitur dasarnya aplikasi Sudomy.



Gambar 7. Antarmuka Pelaporan

4. KESIMPULAN

Aplikasi *native* yang berbasis CLI dapat dikembangkan lebih lanjut menggunakan metode *HybridApps* supaya memiliki antarmuka grafis. Oleh sebab itu aplikasi *Information Gathering* seperti Sudomy yang dikembangkan lebih lanjut dengan antarmuka berbasiskan teknologi web pada penelitian ini disebut GSudomy. Aplikasi GSudomy pada prinsipnya tetap memiliki fitur utama dari Sudomy. Perbaikannya adalah dari sisi antarmuka yang berbasis grafis.

Pengembangan GSudomy saat ini belum menggunakan pendekatan UI/UX. Harapannya penelitian selanjutnya dapat dikembangkan dengan pendekatan UI/UX sehingga antarmukanya lebih menarik. Selain itu GSudomy memiliki potensial pengembangan lebih lanjut untuk diintegrasikan dengan aplikasi pengujian keamanan informasi lainnya.

UCAPAN TERIMA KASIH

Penelitian ini didukung oleh Universitas Jenderal Achmad Yani Yogykarta pada program Hibah Penelitian Dosen Internal. Universitas Jenderal Achmad Yani Yogyakarta bekerjasama dengan PT Widya Adijaya Nusantara (Widya Security) berserta Komunitas LowSec Indonesia menjalin kerjasama dalam penelitian ini sebagai wujud implementasi Kampus Merdeka.

DAFTAR PUSTAKA

Cai, R., Rao, Y., Wang, J., Guan, H., Shi, X., & Wang, Y. (2019). NetPadBrowser : An Offline Browser for Web-Based Dynamic Geometric Resources. *2019 14th International Conference on Computer Science & Education (ICCSE)*, *Iccse*, 434–438.

Dooley, M., & Rooney, T. (2017). Introduction to the Domain Name System (DNS). In *DNS Security Management* (First Edit, pp. 17–29). John Wiley & Sons, Inc. https://doi.org/10.1002/9781119328292.ch2

Hariyadi, D., & Irawan, E. T. (2014). Purwarupa Forensik BBM di Telepon Seluler Android Menggunakan IGN-SDK. In *Indonesia Security Conference 2014* (pp. 2–8). https://doi.org/10.13140/RG.2.1.2771.3764

Hariyadi, D., & Nastiti, F. E. (2021). Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta. *Jurnal Komtika (Komputasi Dan Informatika)*, *5*(1), 35–42.

Hariyadi, D., Wijayanto, H., & Fazlurrahman. (2020). Bangkolo : Aplikasi Vulnerability Identification Berbasis Hybrid Apps. *Cyber Security Dan Forensik Digital*, *3*(1), 39–44.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. National Institute of Standards and Technology.

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

Park, J., Khormali, A., Mohaisen, M., & Mohaisen, A. (2019). Where Are You Taking Me? Behavioral Analysis of Open DNS Resolvers. *Proceedings - 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2019*, 493–504. https://doi.org/10.1109/DSN.2019.00057

Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara. (2020). Indonesia Cyber Security Monitoring Report 2019. In *Indonesia Security Incident Response Team On Internet Infrastructure*.

Ramadhan, R. A., Aresta, R. M., & Hariyadi, D. (2020). Sudomy: Information Gathering Tools for Subdomain Enumeration and Analysis. *IOP Conference Series: Materials Science and Engineering*, *771*. https://doi.org/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), 18–22.

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *NIST SP 800-115: Technical Guide to Information Security Testing and Assessment Recommendations*. http://books.google.com/books?hl=en&lr=&id=EHrf6q7GobUC&oi=fnd&pg=PR7&dq=Technical+Guide+to+Information+Security+Testing+and+Assessment+Recommendations+of+the+National+Institute+of+Standards+and+Technology&ots=FTcnroLXL8&sig=DE

Sciore, E. (2019). Model, View, and Controller. In *Java Program Design* (pp. 389–443). Apress. https://doi.org/10.1007/978-1-4842-4143-1_11

Van Heugten, J. H. C. (2018). *Privacy analysis of DNS resolver solutions*. https://www.nlnetlabs.nl/downloads/publications/privacy-analysis-of-dns-vanheugten.pdf

Wang, M., Zhang, Z., & Xu, H. (2018). DNS Configurations and Its Security Analyzing via Resource Records of the Top-Level Domains. *Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID*, *2017-Octob*, 21–25. https://doi.org/10.1109/ICASID.2017.8285736