Jurnal Komtika (Komputasi dan Informatika),
Vol. 5 No. 1| Mei 2021

Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta

Dedy Hariyadi[1*], Faulinda Ely Nastiti[2]
[1]Teknologi Informasi, Universitas Jenderal Achmad Yani Yogyakarta
[1]PT Widya Adijaya Nusantara
[2]Sistem Informasi, Universitas Duta Bangsa Surakarta
*email: dedy@unjaya.ac.id

DOI:https://doi.org/ 10.31603/komtika.v5i1.5134

Received: 12-06-2021, Revised: 25-06- 2021, Accepted:09-07- 2021

ABSTRACT

Hackers are currently not only attacking government agencies like in 2019 but have already carried out attacks on educational institutions. This is in accordance with the monitoring and identification of Badan Siber dan Sandi Negara that 38% of educational institutions have been attacked in 2020. As a form of preventive action related to cyber-attacks on educational institutions, it is necessary to carry out an information security analysis of the installed systems. This article proposes the technical stages of conducting an information security analysis using software with a Free Open Source Software license, namely Sudomy and OWASP ZAP. Using the two software, the results of the analysis of potential security holes in the information system installed at Universitas Duta Bangsa Surakarta were obtained.

Keywords: *Penetration Testing, Vulnerability Identification, Network Mapping, Information Gathering, Web Defacement*

ABSTRAK

Peretas saat ini tidak hanya menyerang instansi pemerintah seperti pada tahun 2019 melainkan sudah melakukan serangan ke instansi pendidikan. Hal ini sesuai dengan pantauan dan identifikasi Badan Siber dan Sandi Negara bahwa instansi pendidikan telah diserang sebanyak 38% pada tahun 2020. Sebagai wujud tindakan preventif terkait dengan serangan siber pada instansi pendidikan perlu dilakukan sebuah tindakan analisis keamanan informasi terhadap sistem-sistem yang terpasang. Pada artikel ini diusulkan tahapan teknis melakukan analisis keamanan informasi menggunakan perangkat lunak dengan lisensi Free Open Source Software, yaitu Sudomy dan OWASP ZAP. Menggunakan kedua perangkat lunak tersebut didapatkan hasil analisis potensi-potensi celah keamanan pada sistem informasi yang terpasang pada Universitas Duta Bangsa.

Kata-kata kunci*:* *Penetration Testing, Vulnerability Identification, Network Mapping, Information Gathering, Web Defacement*

PENDAHULUAN

Evaluasi keamanan suatu sistem informasi pada suatu instansi sektor pendidikan menjadi sangat penting karena ancaman serangan siber pada tahun 2020 menurut Badan Siber dan Sandi Negara sektor pendidikan di Indonesia menjadi target terbesar dibandingkan sektor lainnya [1], seperti pada Tabel 1. Adapun serangan siber yang dimaksud adalah *web defacement*.

Menurut peneliti dari Hague University mengatakan bahwa serangan *web defacement* merupakan tindakan dari peretas yang melakukan perubahan tampilan halaman situs yang tidak semestinya[2]. Contoh server yang telah diretas dengan mengunggah sebuah berkas gambar sehingga tampilannya seperti pada Gambar 1. Hal ini disebabkan karena sebuah sistem yang telah dipublikasikan ke internet memiliki sebuah potensi untuk diserang oleh peretas [3].

Tabel 1. Persentase Serangan Defacement

Kategori instansi	Jumlah Serangan
Perguruan Tinggi	38%
Pemerintah Daerah	32%
Swasta	21%
Sekolah	4%
Personal	3%
Organisasi	2
Pemerintah Pusat	2
Lainnya	1
Kesehatan	0.16%
Keuangan	0.04%

Sektor Pendidikan menduduki urutan kedua setelah sektor pemerintah pada jenis serangan *web defacement* [4]. Peretasan web instansi pendidikan harus menjadi perhatian khusus, karena dalam web pendidikan terdapat data-data pribadi yang penting, seperti identitas lengkap pelajar/pengajar dan keluarganya. Universitas Duta Bangsa Surakarta merupakan instansi pendidikan yang memiliki tiga puluh enam layanan sistem informasi berbasis web yang dapat diakses melalui portal https://udb.ac.id/layanan-sistem. Berdasarkan observasi yang dilakukan tanggal 19 Mei 2021 ditemukan bahwa web Universitas Duta Bangsa Surakarta telah diserang, laman ojs.udb.ac.id ter-*deface* seperti pada Gambar 1. Oleh sebab itu, analisis keamanan perlu dilakukan secara terstruktur dan terjadwal, untuk menemukan kelemahan keamanan dan memperbaikinya. Agar proses analisis keamanan sesuai dengan kebutuhan Universitas Duta Bangsa Surakarta, maka dilakukan adopsi teknik analisis kemanan dengan *Information Systems Security Assement Framework* (ISSAF) yang dioptimasi dengan platform Sudomy dan OWASP ZAP.

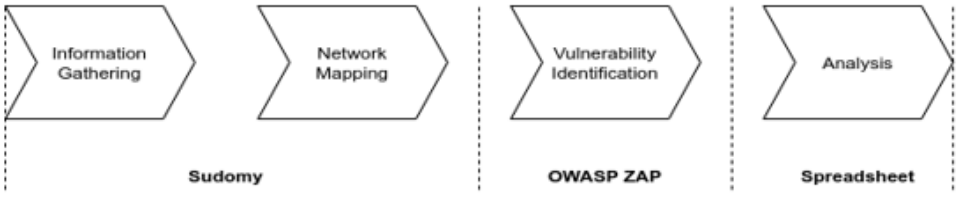
Gambar 1. Contoh Halaman yang Ter-*deface*

METODE

Dalam penelitian ini diusulkan analisis keamanan sistem informasi yang mengadopsi *Information Systems Security Assement Framework* (ISSAF) *dari Open Information Systems Security Group*. ISSAF merupakan kerangka assessmen pada sebuah sistem informasi dengan sembilan tahapan, yaitu: *Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumeratin Further, Compromise Remote Users/Sites, Maintaining Access,* dan *Covering Tracks* [5]. Adapun tahapan yang diadopsi pada artikel ini adalah *Information Gathering, Network Mapping, dan Vulnerability Identification*. Implementasi ketiga tahapan tersebut diterapkan menggunakan Sudomy dan OWASP ZAP.

Information Gathering merupakan tahapan dalam proses asesmen keamanan informasi berdasarkan informasi yang telah tersedia secara terbuka di internet. Contoh informasi yang tersedia diantaranya, IP Address, pendaftar domain, DNS server, status server, sistem operasi yang digunakan, bahkan termasuk *port* yang terbuka [6]. Menggunakan metode *hybrid scan* yang diterapkan pada aplikasi Sudomy menghasilkan sebuah informasi yang beririsan dengan tahapan *Network Mapping*. Hal ini disebabkan aplikasi Sudomy juga menggunakan aplikasi seperti Nmap untuk mengetahui *port* yang terbuka dan memanfaatkan pustaka python pyvis yang menghasilkan pemetaan IP Address yang digunakan [7]. Aplikasi Nmap tidak hanya digunakan untuk melakukan tahapan *Network Mapping,* Nmap dapat digunakan sebagai alat bantu untuk mengidentifikasi potensi celah keamanan secara *helicopter view* yang disebut tahapan *Vulnerability Identification* [8]. Namun, pada penelitian ini tahapan *Vulnerability Identification* menggunakan aplikasi OWASP ZAP untuk mengetahui tingkat potensi keamanan pada suatu aplikasi berbasis web.

Gambar 2. menunjukan tahapan yang digunakan pada penelitian ini yang menggunakan aplikasi Sudomy pada tahapan *Information Gathering* dan *Network Mapping* dan aplikasi OWASP ZAP pada tahapan *Vulnerability Identification.* Informasi yang dihasilkan dari masing-masing aplikasi pada setiap tahapan dianalisis untuk mengetahui potensi kerentanan dari suatu instansi yang memiliki berbagai aplikasi berbasis web. Untuk menganalisis hasil temuan pada tahapan *Vulnerability Identification* menggunakan aplikasi *spreadsheet* dengan hasil sebuah visualisasi yang komparatif [9].



Gambar 2. Tahapan Penelitian

HASIL DAN PEMBAHASAN

Information Gathering

Studi kasus dalam penelitian ini adalah sebuah perguruan tinggi di Surakarta, Universitas Duta Bangsa. Pemilihan obyek penelitian dari perguruan tinggi sesuai dengan hasil temuan Badan Siber dan Sandi Negara pada tahun 2020 yang menyatakan instansi perguruan tinggi merupakan target serangan *web defacement* tertinggi seperti terlihat pada Tabel 1.

Pertimbangan lainnya yaitu Universitas Duta Bangsa Surakarta menjadi korban peretasan dengan menyisipkan suatu berkas gambar sehingga menurut Zone-H dapat dikategorikan sebagai korban *web defacement* seperti tampak pada Gambar 1 [9]. Obyek dari penelitian ini telah memiliki validasi informasi dasar yang dapat dipertanggungjawabkan, adapun ciri-cirinya adalah penggunaan *Top Level Domain* .ac.id sesuai ketentuan dari Pengelola Nama Domain Indonesia (PANDI) [10]. Domain yang digunakan Universitas Duta Bangsa Surakarta adalah udb.ac.id. Berdasarkan penelusuran alamat fisik dari perguruan tinggi secara manual menggunakan layanan Google Maps yang berdasarkan domain udb.ac.id bahwa Universitas Duta Bangsa Surakarta memiliki tiga kampus, yaitu kampus I yang beralamat di Jln. Bhayangkara No.55 Tipes, kampus II yang beralamat di Jln. Kiyai Samanhudi No.93 Sondakan , dan kampus yang beralamat di Jln. Pinangraya No 47, seperti pada Gambar 3. Proses penelusuran ini juga masih dikategorikan sebagai tahapan *Information Gathering*. Tahapan selanjutnya adalah melakukan penelusuran sub-domain yang dikelola oleh Universitas Duta Bangsa Surakarta menggunakan aplikasi Sudomy seperti disajikan dalam Tabel 2.

Gambar 3. Penelusuran Alamat Kampus

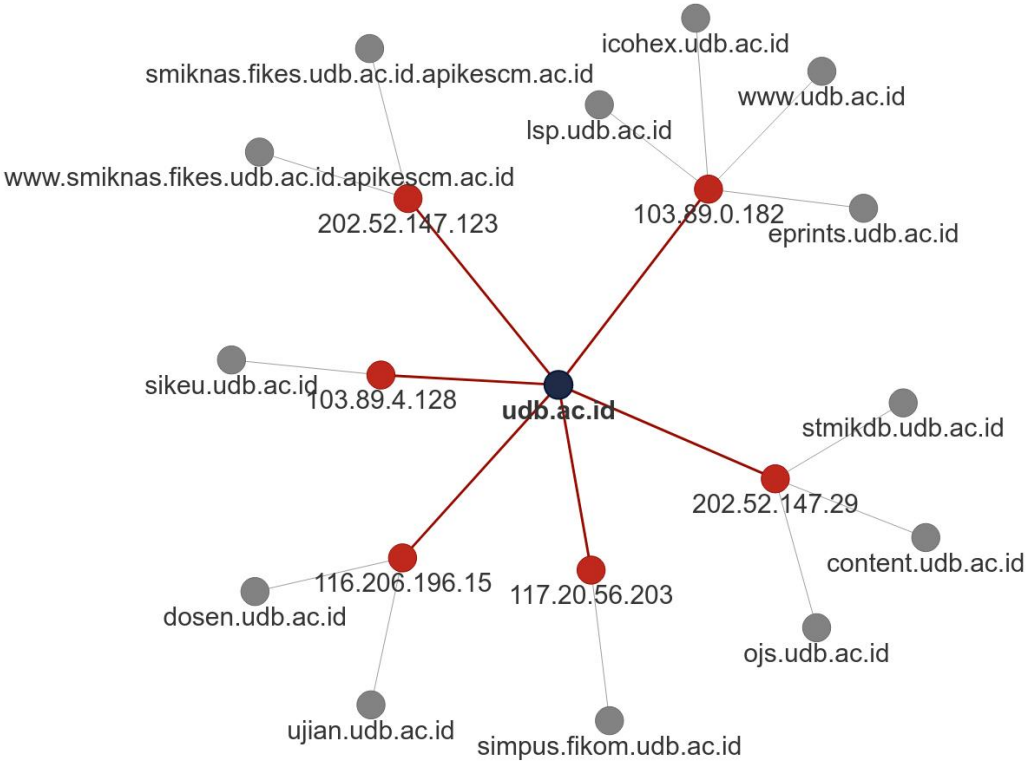
Tabel 2. Daftar Domain/Sub-Domain Hasil Pemindaian Sudomy

IP Address	Domain/Sub-domain
103.89.0.182	eprints.udb.ac.id
	icohex.udb.ac.id
	lsp.udb.ac.id
	udb.ac.id
103.89.4.128	sikeu.udb.ac.id
116.206.196.15	dosen.udb.ac.id
	ujian.udb.ac.id
117.20.56.203	simpus.fikom.udb.ac.id
202.52.147.123	smiknas.fikes.udb.ac.id.apikescm.ac.id
202.52.147.29	content.udb.ac.id
	ojs.udb.ac.id
	stmikdb.udb.ac.id

Adapun hasil pemindaian dari aplikasi Sudomy pada tahapan ini adalah daftar sub-domain berserta alamat IP Address yang digunakan dengan status aktif digunakan berdasarkan ping sweep. Teknik ping sweep berfungsi untuk mendeteksi suatu *host* yang berstatus atau dalam kondisi aktif/menyala [11]. Selanjutnya hasil dari temuan menggunakan teknik Ping Sweep dilakukan penyaringan berdasarkan HTTP Status dengan kode 200 karena pengujian yang dilakukan menggunakan sistem informasi yang berbasis web [12]. Tabel 2 merupakan informasi sub-domain hasil pemindaian Sudomy yang menggunakan metode Hybrid Scan pada tanggal 6 Juni 2021.

Network Mapping

Berdasarkan Tabel 2 yang menunjukan bahwa 1 IP Address dapat memiliki beberapa sub-domain. Informasi hasil pemindaian Sudomy tersebut kemudian dipetakan menggunakan pustaka Python pyvis menjadi sebuah jejaring yang menunjukan distribusi penggunaan dan alokasi IP Address yang digunakan serta visualisasi sub-domain dari udb.ac.id seperti pada Gambar 4. Oleh sebab itu hasil visualisasi ini dapat dikategorikan tahapan *Network Mapping* yang dapat memberikan informasi kepada analis keamanan informasi terkait pemetaan infrastruktur berdasarkan pemanfaatan IP Address dan sub-domain.

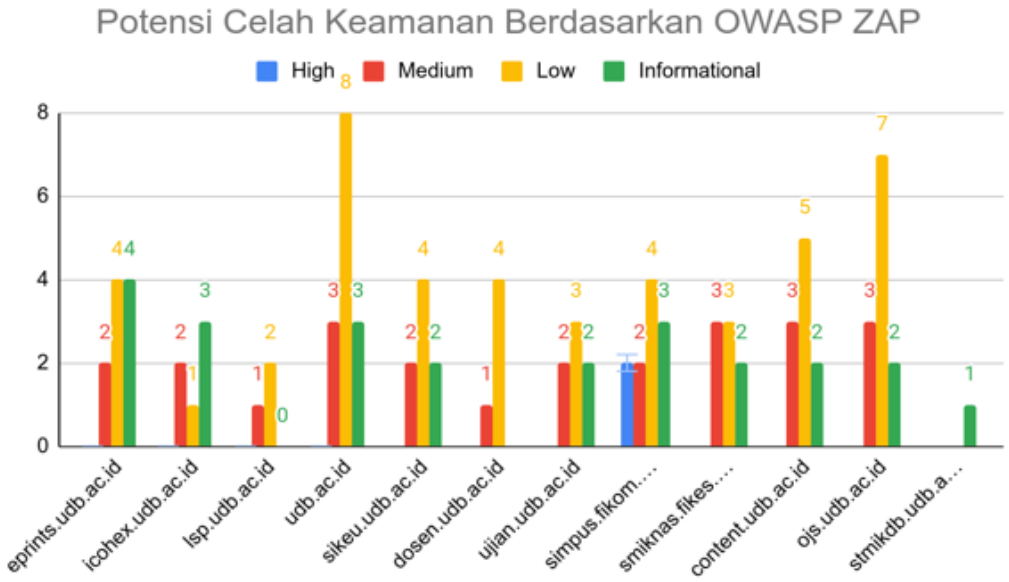


Gambar 4. *Network Mapping* dari Sudomy

Vulnerability Identification

Tahapan selanjutnya adalah melakukan *Vulnerability Identification* menggunakan OWASP ZAP dengan sumber data *berdasarkan Network Mapping*. Pemindaian target berdasarkan dari Network Mapping menggunakan aturan OWASP ZAP yang paling dasar (*default scan policy*). Adapun *default scan policy* tersebut diantaranya: *Cross Site Scripting* (DOM Based), *httaccess Information Leak*, *Directory Browsing*, ELMAH *Information Leak*, *Source Code Disclosure – WEB-INF folder, Buffer Overflow, CRLF Injection, Cross Site*

Scripting (Persistent), Cross Site Scripting (Persistent) – Prime, Cross Site Scripting (Persistent) – Spider, Cross Site Scripting (Reflected), Forma String Error, Paramater Tampering, Remote OS Command Injection, Server Side Code Injection, Server Side Include, SQL Injection, External Redirect, Script Active Scan Rules, SOAP Action Spoofing, SOAP XML Injection, Path Traversal, dan Remote File Inclusion. Hasil *Vulnerability Identification* pada domain dan sub-domain berdasarkan Tabel 2 menghasilkan grafik potensi celah keamanan informasi dengan kategori *High, Medium, Low,* dan *Informational* seperti pada Gambar 5.



Gambar 5. *Network Mapping* dari Sudomy

Walaupun sebagian besar domain dan/atau sub-domain dari Universitas Duta Bangsa Surakarta tidak memiliki celah keamanan dengan kategori *high*, kecuali simpus.fikom.udb.ac.id tetapi berdasarkan penelusuran di zone-h.org ditemukan sebuah celah yang memungkinkan seorang penyerang dapat mengunggah sebuah berkas yang dapat dikategorikan sebagai *web defacement* seperti tampak pada Gambar 1. Hal ini menunjukan bahwa proses *Vulnerability Identification* dalam melakukan pemindaian celah keamanan secara *helicopter view*. Berdasarkan hasil pemindaian dari hasil *Vulnerability Identification* sebaiknya ditindaklanjuti dengan *Penetration Testing*, sesuai dengan kerangka *Information System Security Assement Framework* [13].

KESIMPULAN

Evaluasi terkait dengan sistem informasi pada sebuah instansi pendidikan sebaiknya dilakukan secara berkala sebagai wujud implementasi dan mengukur kesiapan keamanan informasi dari serangan siber. Berdasarkan data dari Badan Siber dan Sandi Negara peretas mulai mengubah target serangan dari instansi pemerintah ke instansi pendidikan. Oleh sebab pemindaian secara berkala dan singkat dapat menggunakan Sudomy sebagai alat bantu *Information Gathering* dan *Network Mapping* dan OWASP ZAP sebagai alat bantu *Vulnerability Identification.*

Sudomy yang memiliki penggaya pihak ketiga dapat mengidentifikasi dan memetakan aset digital sebuah domain dari sudut pandang pihak luar atau pihak ketiga seperti eksternal *Penetration Tester*. Walaupun dilakukan oleh pihak internal instansi, informasi yang disajikan Sudomy memberikan laporan yang infomatif sebagai pendukung keputusan pihak manajemen. Laporan OWASP ZAP harus diolah kembali supaya mempermudah manajemen dalam mengambil keputusan terkait celah keamanan yang ditemukan. Baik Sudomy dan OWASP ZAP memiliki lisensi yang selaras dengan *Free Open Source Software* sehingga mudah didapatkan dan rendah biaya.

Hasil dari evaluasi Sudomy dan OWASP ZAP perlu ditindaklanjuti dengan tahapan berikutnya yaitu *Penetration Testing* oleh eksternal *Penetration Tester*. Hal ini untuk mendapatkan informasi yang komprehensif dan bersifat netral. Artinya penelitian selanjutnya dapat melakukan tahapan *Penetration Testing* pada sistem yang lebih spesifik dengan celah keamanan sesuai temuan atau laporan pada *Vulnerability Identification* menggunakan OWASP ZAP.

DAFTAR PUSTAKA

[1] BSSN, "Laporan Tahunan Monitoring Keamanan Siber," Jakarta, 2021.
[2] M. Romagna and N. J. Van Den Hout, "Hacktivism and website defacement : Motivations, capabilities and potential threats," 2017.
[3] W. P. Ono, *Keamanan Jaringan*. 2011.
[4] Fazzlurrahman and H. Dedy, "Analisis Serangan Web Defacement pada Situs Web Pemerintah Menggunakan ELK Stack," *I. Inf. Sunan Kalijaga*, vol. 4, no. 1, pp. 1–8, 2019.
[5] OISSG, *Information Systems Security Assessment Framework (ISSAF), Draft 0.2*. 2006.
[6] M. Riasetiawan, A. Wisnuaji, D. Hariyadi and T. Febrianto, "Pengembangan Aplikasi Information Gathering menggunakan Metode Hybrid Scan berbasis Graphical User Interface," *Cyber Secur. dan Forensik Digit*, vol. 4, no. 1, 2021.
[7] G. Perrone, J. Unpingco, and H. Lu, "Network visualizations with Pyvis and VisJS," in *Proc. 19th Python Sci. Conf.*, 2020, pp. 58–62, doi: doi: 10.25080/majora-342d178e-008.
[8] D. Hariyadi, H. Wijayanto, and Fazlurrahman, "Bangkolo : Aplikasi Vulnerability Identification Berbasis Hybrid Apps," *," Cyber Secur. dan Forensik Digit*, vol. 3, no. 1, 2020.
[9] A. Azam, K. A. Alam, and H. Ali, "Version detection in spreadsheets based on headers similarity," 2019, doi: doi: 10.1109/ICET48972.2019.8994397.
[10] H. M. Jumhur, "Perbandingan Bentuk Kelembagaan Pengelola Nama Domain di Indonesia dengan Lembaga Pengelola Nama Domain di Beberapa Negara between Indonesia and Other Countries A . Pendahuluan Peraturan perundang-undangan yang menjadi dasar dari pengelolaan nama domain," *J. Illmu Huk. Padjadjaran*, vol. 1, no. 4, 2014.
[11] G. Bagyalakshmi *et al.*, "Network Vulnerability Analysis on Brain Signal/Image Databases Using Nmap and Wireshark Tools," *EEE Access*, vol. 6, 2018, doi: 10.1109/ACCESS.2018.2872775.
[12] S. Alam, M. Weigle, M. Nelson, F. Melo, D. Bicho, and D. Gomes, "MementoMap framework for flexible and adaptive web archive profiling," 2019, doi:

10.1109/JCDL.2019.00033.

[13] R. H. Hutagalung, L. E. Nugroho, and R. Hidayat, "Analisis Uji Penetrasi Menggunakan ISSAF," in *in Hacking and Digital Forensics Exposed (H@DFEX*, 2017, pp. 32–40.