BAB VI. PENUTUP

6.1. Kesimpulan

Aktifitas identifikasi kerentanan terhadap *website* sikma.uajy.ac.id yang dikelola oleh Kantor Sistem Informasi, Universitas Atma Jaya Yogyakarta, dapat diambil kesimpulan sebagai berikut:

1. Pengujian terhadap *website* sikma.uajy.ac.id dapat dilakukan dengan cara pemindaian atau *scan*. Pemindaian dapat dilakukan dengan beberapa alat pemindaian seperti Whois, Spiderfoot, WhatWeb, Nmap, Nessus, Burp suite dan Metasploit. Berdasarkan pemindaian tersebut dapat diketahui informasi detail mengenai layanan, versi serta kerentanan atau celah keamanan yang dari *website* sikma.uajy.ac.id.

2. Berdasarkan hasil pemindaian menggunakan alat nessus, metasploit dan burp suite, situs sikma.uajy.ac.id memiliki informasi kerentanan yang beragam dan saling melengkapi. Alat nessus menemukan kerentanan tingkat '*HIGH'* berjumlah dua, '*MEDIUM*' berjumlah enam dan '*INFO'* berjumlah 25. Sedangkan untuk alat burp suite ditemukan sembilan kerentanan yang mengandung enam tingkat '*INFORMATION'* dan tiga '*LOW*'. Terakhir, untuk hasil pemindaian dari alat Metasploit terdapat tiga belas (13) *port* yang terbuka, dan memungkinkan menjadi akses kepada peretas untuk dapat masuk ke dalam sistem. Berdasarkan hasil pemindaian dari masing-masing alat yang digunakan, nessus menemukan kerentanan pada situs sikma.uajy.ac.id paling banyak yang berjumlah tiga puluh tiga (33) kerentanan.

3. Perangkat lunak Nessus, Metasploit dan Burp suite merupakan perangkat yang populer dan dapat digunakan untuk mencari kerentanan yang dimiliki oleh sebuah *website*. Ketiga perangkat lunak yang digunakan dalam penelitian ini adalah yang berlisensi gratis dan dapat diakses di berbagai macam *platform* seperti Windows, Linux dan Mac. Untuk versi komersial juga tersedia dengan penambahan fitur pemindaian dan pengujian yang signifikan dari versi gratis. Alat Nessus dan Burp suite langsung memilih tipe pemindaian yang ingin dilakukan, sedangkan metasploit memiliki sintaks-sintaks yang harus dipelajari dan beraneka macam modul yang dapat digunakan. Berdasarkan pengalaman penguji, pemindaian

terhadap *website* sikma.uajy.ac.id bekerja dalam durasi waktu yang beragam dari ketiga alat dalam mendapatkan informasi port yang terbuka, serta celah keamanan.

6.2. Saran

Saran yang dapat menjadi perbaikan pada penelitian di masa yang akan datang:

1. Alat pemindaian kerentanan dapat menggunakan alat yang berbeda seperti Acunetix dan Maltego atau alat pemindaian kerentanan yang berlisensi atau komersial agar dapat diperoleh hasil yang lebih detail dan saling melengkapi.
2. Pemindaian juga dapat menggunakan skrip yang tersedia pada platform kode terbuka seperti GitHub atau membuat kode sumber secara mandiri sehingga dapat menyesuaikan dengan kebutuhan dari pengujian.
3. Pengujian dapat juga dilakukan menggunakan *framework* berbeda selain ISSAF (*Information System Security Assessment Framework*). Hal ini dapat memberikan hasil yang lebih komprehensif dan disesuaikan dengan kebutuhan dari pengujian.
4. Hasil scan Nessus menampilakan satu kerentanan tingkat *HIGH* yang dapat mengakibatkan terambilnya data-data oleh oknum yang tidak bertanggung jawab. Kerentanan ini dapat diatasi dengan mengkonfigurasi ulang SIKMA.

DAFTAR PUSTAKA

[1] F. Fachri, A. Fadlil & I. Riadi, "Analisis Keamanan Webserver Menggunakan Penetration Test," *JURNAL iNFORMATIKA*, vol. 8, p. 183~190, 2021.

[2] A. Rochman, R. R. Salam & S. A. Maulana, "ANALISIS KEAMANAN WEBSITE DENGAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF) DAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP) DI RUMAH SAKIT XYZ," vol. 2, pp. 506-519, 2021.

[3] T. R. Syarif & D. A. Jatmiko, "ANALISIS PERBANDINGAN METODE WEB SECURITY PTES, ISSAF DAN OWASP DI DINAS KOMUNIKASI DAN INFORMASI KOTA BANDUNG".

[4] I. G. A. S. Sanjaya, G. M. A. Sasmita & D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *MERPATI*, vol. 8, pp. 113-124, 2020.

[5] A. Fajaryanto & Y. Prayudi, "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," *NERO*, vol. 1, pp. 190-197, 2015.

[6] N. I. Aspirantama, "Pengujian Keamanan Sistem Informasi UAJY Menggunakan Penetration Testing," 2021.

[7] A. Elanda & R. L. Buana, "ANALISIS KEAMANAN SISTEM INFORMASI BERBASIS WEBSITE DENGAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) VERSI 4: SYSTEMATIC REVIEW," *Journal of Computer Engineering System and Science*, vol. 5, pp. 185-191, 2020.

[8] A. I. Rosadi, "ANALISIS KEAMANAN SISTEM INFORMASI AKADEMIK DENGAN WEB PENETRAION TESTING".

[9] Syukhri & F. Y. Fauzan, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang," *Jurnal Vocational Teknik Elektronika dan Informatika*, vol. 9, 2021.

[10] S. Sauda, M. Fatoni & Y. N. Kunang, "PENGUJIAN CELAH KEAMANAN

PADA CMS (Content Management System)," 2013.

[11] Djahir & Pratita. 2015. Bahan Ajar Sistem Informasi Manajemen. Yogyakarta: Budi Utama.

[12] Mulyani, Sri. 2016. Sistem Informasi Manajemen. Bandung: Abdi Sistematika.

[13] Hutahaean, Jeperson. 2015. Konsep Sistem Informasi. Yogyakarta: Deepublish.

[14] Sutanta, Edhy.2011. Basis data dalam tinjauan konseptual. Jakarta: Andi.

[15] Susanto, Azhar. 2017.Sistem Informasi Manajemen: Konsep dan Pengembangan Secara Terpadu. Bandung: Lingga Jaya.

[16] Rusdiana, H.A., dan Irfan, M. (2014).”Sistem Informasi Manajemen”. Bandung: CV. Pustka Setia.

[17] Arbie, E., 2000, Pengantar Sistem Informasi Manajemen, Edisi Ke-7, Jilid 1, Bina Alumni Indonesia, Jakarta.

[18] O’Brein, James A., (2005), ”Pengantar Sistem Informasi”, Penerbit : Salemba 4, Jakarta.

[19] Jogianto2 HM. 2005. Sistem Teknologi Informasi. Andi. Yogyakarta.

[20] B. Sugiantoro, "Ethical Hacking," 2019.

[21] J. Simarmata, Pengenalan teknologi computer dan informasi, Janner Simarmata,yogyakarta,Andi 2006. Yogyakarta: Andi Offset, 2006.

[22] EC-Council. Certified Ethical Hacker v8 : Module 20 Penetration Testing. Amerika : EC-Council, 2012.

[23] P. Engebretson, “The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy,” Vasa, 2011.

[24] Rizky. Soetam. 2011. “Konsep Dasar Rekayasa Perangkat Lunak”.jakarta: Prestasi Pustaka.

[25] Budi Rahardjo. Keamanan Perangkat Lunak. PT Insan Infonesia, 2016.

[26] Daqiqil, Ibnu. 2011. Framework CodeIgniter Sebuah Panduan dan Best Practice. Makalah kumpulan tutorial komputer.

[27] B. Ratore *et al.*, *Information System Security Assessment Framework (ISSAF) Draft 0.2.1B*. OISSG, 2005.

[28] R. H. Hutagalung, L. E. Nugroho, and R. Hidayat, “Analisis Uji Penetrasi Menggunakan ISSAF,” *Hacking Digit. Forensics Expo.*, pp. 32–40, 2017.

[29] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss," *Int. J. Informatics Vis.*, vol. 4, no. 4, pp. 225–230, 2020.

[30] T. Syarif Revolino and D. Jatmiko Andri, "Analisis Perbandingan Metode Web Security Ptes , Issaf Dan Owasp Di Dinas Komunikasi Dan Informasi Kota Bandung," p. 8, 2018.

[31] A. Kili, "How to Get Domain and IP Address Information Using WHOIS Command." https://www.tecmint.com/whois-command-get-domain-and-ip-address-information/ (accessed Apr. 22, 2022).

[32] GIJN (Global Investigation Journalism Network) Indonesia" Analisis Jaringan Antarsitus Mencurigakan" https://jaring.id/analisis-jaringan-antarsitus-mencurigakan/ (accessed Apr.22, 2022).

[33] R. Sankar, "whatweb – Tool to Discover Security Vulnerabilities With Your Web Application." https://kalilinuxtutorials.com/whatweb/ (accessed Apr. 22, 2022).

[34] M. Zakaria, "Pengertian NMAP Beserta Fungsi dan Cara Kerjanya yang Perlu Diketahui" https://www.nesabamedia.com/pengertian-nmap/ (accessed Apr. 22, 2022).

[35] L. Obbayi, "A brief introduction to the Nessus vulnerability scanner" https://resources.infosecinstitute.com/topic/a-brief-introduction-to-the-nessus-vulnerability-scanner/ (accessed Apr. 22, 2022).

[36] Jess H, "Burp Suite Documentation" https://portswigger.net/burp/documentation/scanner (accessed Apr. 22, 2022).

[37] J. Petters, "What is Metasploit? The Beginner's Guide" https://www.varonis.com/blog/what-is-metasploit (accessed Apr. 22, 2022).