BAB VI. PENUTUP

6.1. Kesimpulan

Setelah melakukan uji penetrasi terhadap *website* kuliah.uajy.ac.id yang dimiliki oleh Universitas Atma Jaya Yogyakarta, dapat diambil beberapa kesimpulan, yaitu:

1. Pengujian pada *website* Universitas Atma Jaya Yogyakarta dapat dilakukan dengan cara pemindaian dan simulasi penyerangan. Pemindaian dilakukan dengan menggunakan beberapa alat pengujian seperti Nessus, Nmap, Whatweb, dan Whois. Dari pemindaian tersebut dapat diketahui beberapa simulasi penyerangan yang dapat dilakukan terhadap *website* kuliah.uajy.ac.id. Simulasi penyerangan yang dapat dilakukan adalah dengan melakukan *exploit*, *cross site scripting* (XSS), dan DoS.

2. Dari hasil pemindaian menggunakan aplikasi nessus pada *website* kuliah.uajy.ac.id diketahui bahwa *website* kuliah.uajy.ac.id memiliki dua kerentanan pada tingkat '*HIGH*', tiga kerentanan pada tingkat '*MEDIUM*', satu kerentanan pada tingkat '*LOW*', dan 18 kerentanan pada tingkat '*INFO*'. Adapun pemindaian juga dilakukan terhadap *website* ortu.uajy.ac.id. Akan tetapi, dari hasil pemindaian yang diperoleh diketahui bahwa kerentanan yang terdapat pada *website* ortu.uajy.ac.id lebih sedikit dibandingkan dengan *website* kuliah.uajy.ac.id, yaitu dua kerentanan pada tingkat '*MEDIUM*' dan 15 kerentanan pada tingkat '*INFO*', sehingga penguji memutuskan untuk melakukan pengujian pada *website* kuliah.uajy.ac.id. Pada simulasi serangan yang dilakukan pada *website* kuliah.uajy.ac.id menggunakan alat metasploit untuk melakukan *exploit*, diperoleh hasil bahwa terdapat beberapa *file* atau direktori menarik yang ditemukan. Akan tetapi, *file* atau direktori tersebut tidak dapat diakses dan akan langsung dialihkan ke halaman *login* kuliah.uajy.ac.id. Adapun menggunakan modul ssh_login yang memberikan hasil bahwa

upaya *login* berdasarkan tebakan *user* dan *password* yang ada tidak berhasil dilakukan. Dari percobaan yang dilakukan menggunakan metasploit, dapat ditarik kesimpulan bahwa *exploit* yang dilakukan pada *website* kuliah.uajy.ac.id tidak berhasil. Pada simulasi penyerangan menggunakan *cross site scripting* (XSS) juga dianggap tidak berhasil untuk melakukan injeksi *script* karena semua teks akan ubah menjadi *plain text* sehingga *script* tidak berfungsi. Adapun simulasi serangan menggunakan DoS hanya berhasil apabila serangan dilakukan pada domain utama yaitu uajy.ac.id.

6.2. Saran

Berdasarkan pengujian yang telah dilakukan, terdapat beberapa saran untuk melakukan pengembangan pengujian selanjutnya, yaitu:

1. Pemindaian pada uji penetrasi dapat dilakukan dengan beberapa alat pemindaian yang berbeda-beda seperti Acunetix atau alat pemindaian lainnya untuk mengetahui hasil yang diperoleh dari masing-masing alat yang digunakan.

2. Simulasi penyerangan dapat dilakukan dengan beberapa alat atau metode yang berbeda-beda untuk membandingkan hasil yang diperoleh.

3. Rutin melakukan *update* pada *website* kuliah.uajy.ac.id untuk mengantisipasi serangan dari peretas.

DAFTAR PUSTAKA

[1] Wahyudi, "Analisa Pengujian Kerentanan Terhadap Web Server SIMAK (Studi Kasus : STMIK Kharisma Karawang)," *J. Teknol. Inf.*, vol. 5, no. 1, pp. 6–13, 2019.

[2] B. V. Tarigan, A. Kusyanti, and W. Yahya, "Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 3, pp. 206–214, 2017.

[3] S. Sahren, R. A. Dalimuthe, and M. Amin, "Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus," *Pros. Semin. Nas. Ris. Inf. Sci.*, vol. 1, no. September, pp. 994–1001, 2019, doi: 10.30645/senaris.v1i0.109.

[4] T. Dirgahayu, Y. Prayudi, and A. Fajaryanto, "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," *J. Ilm. NERO*, vol. 1, no. 3, pp. 190–197, 2015, [Online]. Available: http://nero.trunojoyo.ac.id/index.php/nero/article/download/29/27.

[5] S. Azhar, *Azhar Susanto. 2013. Sistem Informasi Akuntansi. Bandung: Lingga Jaya.* Bandung: Lingga Jaya, 2013.

[6] Mulyadi, *Mulyadi, 2010. Sistem Akuntansi. Jakarta: Salemba Empat*. Jakarta: Salemba Empat, 2010.

[7] Jogiyanto, *Jogiyanto. 2009. Sistem Teknologi Informasi. Yogyakarta. Andi Offset*. Yogyakarta: Andi Offset, 2009.

[8] L. Whitten, D. Bentley, and C. Dittman, *Metode Desain dan Analisis Sistem.* Yogyakarta: CV.Andy offeset, 2011.

[9] dan W. Turban, McLean, *Pengertian Sistem Informasi*. Yogyakarta: Andi Offset, 1999.

[10] E. S. Raymond, *The New Hacker's Dictionary - 3rd Edition eric s Raymond (1996), The MIT press;third edition*. The MIT Press, 1996.

[11] F. Wibowo, H. Harjono, and A. P. Wicaksono, "Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto

Menggunakan OpenVAS dan Acunetix WVS," *J. Inform.*, vol. 6, no. 2, pp. 212–217, 2019, doi: 10.31311/ji.v6i2.5925.

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

[13] E. Cole, *Network security bible*, 2nd ed., vol. 768. John Wiley & Sons, 2011.

[14] M. Chappel, Mike; Solomon, *Information Security Illuminated*. Jones & Bartlett Learning; Illustrated edition, 2011.

[15] Georgia Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*. San Fransisco: William Pollock, 2014.

[16] P. Engebretso and N, *The Basics Of Hacking And Penetration Testing Ethical Hacking And Penetration Testing Made Easy*. USA: Elsevier Inc., 2011.

[17] W. N. Cholifah, Y. Yulianingsih, and S. M. Sagita, "Pengujian Black Box Testing pada Aplikasi Action & Strategy Berbasis Android dengan Teknologi Phonegap," *STRING (Satuan Tulisan Ris. dan Inov. Teknol.*, vol. 3, no. 2, p. 206, 2018, doi: 10.30998/string.v3i2.3048.

[18] Rapid7, "The world's most used penetration testing framework." https://www.metasploit.com/ (accessed Jul. 22, 2021).

[19] R. Seema and N. Ritu, "Penetration Testing Using Metasploit Framework : an Ethical Approach," *Int. Res. J. Eng. Technol.*, vol. 06, no. 08, pp. 538–542, 2019, [Online]. Available: https://www.academia.edu/40379823/IRJET-_PENETRATION_TESTING_USING_METASPLOIT_FRAMEWORK_AN_ETHICAL_APPROACH.

[20] G. Fanani and I. Riadi, "Analysis of Digital Evidence on Denial of Service (DoS) Attack Log Based," *Bul. Ilm. Sarj. Tek. Elektro*, vol. 2, no. 2, p. 70, 2020, doi: 10.12928/biste.v2i2.1065.

[21] Okta, "Low Orbit Ion Cannon (LOIC): Definition, Damage & Defense." https://www.okta.com/identity-101/low-orbit-ion-cannon-loic/ (accessed Jul. 22, 2021).

[22] E. Stephani, Fitri Nova, and Ervan Asri, “Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server,” *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 2, pp. 67–74, 2020, doi: 10.30630/jitsi.1.2.10.

[23] C. Delgado, “How to list Directories and Files of a Website using DirBuster in Kali Linux.” https://ourcodeworld.com/articles/read/417/how-to-list-directories-and-files-of-a-website-using-dirbuster-in-kali-linux (accessed Jul. 22, 2021).

[24] G. Lyon, “Nmap Security Scanner.” https://nmap.org/ (accessed Jul. 22, 2021).

[25] 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 Jul. 22, 2021).

[26] R. Deraison, “THE NESSUS FAMILY Nessus is trusted by more than 30,000 organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment.” https://www.tenable.com/products/nessus (accessed Jul. 22, 2021).

[27] R. Sankar, “whatweb – Tool to Discover Security Vulnerabilities With Your Web Application.” https://kalilinuxtutorials.com/whatweb/ (accessed Jul. 22, 2021).