Perbandingan Tools Vulnerability Scanning Pada Pengujian Sebuah Website

Komang Ayu Suputri [1], Made Donita Maharani [2], Gede Ade Pratama [3], Nyoman Dinda Indira Sudiasta Putri [4], I Made Edy Listartha [5], Gede Arna Jude Saskara [6]
[1,2,3,4,5,6] Program Studi Sistem Informasi, Fakultas Teknik dan Kejuruan
[1,2,3,4,5,6] Universitas Pendidikan Ganesha
[1,2,3,4,5,6] Jl. Udayana No. 11, Banjar Tegal, Singaraja, Kabupaten Buleleng, Bali 81116
ayu.suputri@undiksha.ac.id[1], donita.maharani@undiksha.ac.id[2], ade.pratama.2@undiksha.ac.id[3], dinda.indira@undiksha.ac.id[4], listartha@undiksha.ac.id[5], jude.saskara@undiksha.ac.id[6]

Abstrak. *Cyber Attack* adalah suatu upaya mencuri, mengubah, mengekspos informasi melalui akses tidak sah ke sistem komputer. Terdapat ancaman *cyber attack* yaitu *Phishing, SQL Injection, Man In The Middle, DDOS Attack, Password Attack, XSS, Vulnerability Scanning* dan *Ransomware Attack*. *vulnerability Scanning* adalah suatu proses mengidentifikasi dan menemukan kelemahan atau kerentanan dalam sebuah sistem. Dalam *vulnerability scanning* terdapat tiga tools yaitu *RedHawk, WebKiller,* dan *Rapidscan*. pengujian ini bertujuan untuk membandingkan setiap tools untuk mencari kerentanan pada suatu website. Pada penelitian ini, setiap tools dilakukan percobaan sebanyak 3 kali percobaan dan hasil celah keamanan yang ditemukan pada setiap tool yaitu pada *RedHawk* dan *WebKiller* sejumlah 8 dan pada *RapidScan* sejumlah 12.

Kata Kunci: *Cyber Attack, Vulnerability Scanning*

1. Pendahuluan

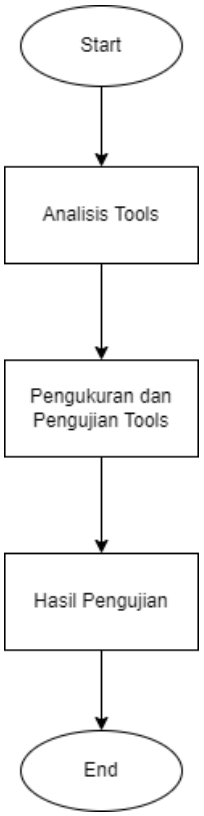
Dengan meningkatnya perkembangan teknologi, kebutuhan manusia saat ini sangat bergantung pada teknologi. Meningkatnya perkembangan teknologi ini memiliki dampak yang banyak baik dalam hal positif maupun negative. Dampak positif dari perkembangan teknologi bisa dilihat dalam komunikasi yang menjadi lebih mudah, praktis dan cepat serta dapat mempermudah pekerjaan dari jarak jauh. Sedangkan dampak negatif dari perkembangan teknologi ini yaitu rentan dalam *cyber crime* atau kejahatan melalui internet. Hal ini sering terjadi di Indonesia dalam beberapa kasus seperti pencurian kartu kredit, hacking situs web, dan menyadap beberapa data orang lain, misalnya email, instagram dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki melalui program komputer. Pencegahan dalam meningkatkan keamanan sebuah sistem dapat dilakukan dengan melakukan uji kerentanan guna membantu dalam proses identifikasi kelemahan pada sistem sebelum adanya serangan. Untuk mendeteksi adanya kerentanan dan melakukan penanganan terhadap kerentanan yang sudah teridentifikasi dapat dilakukan menggunakan *Vulnerability scanner* [1]. Vulnerability adalah suatu kelemahan yang menjadi ancaman nilai integrity, confidentiality, dan availability dari suatu *asse*t [2]. *Dalam cyber crime* terdapat metode yang digunakan dalam melakukan serangan dengan menggunakan teknologi komputer dan internet. Terdapat ancaman *cyber attac*k yaitu *Phishing, SQL Injection, Man In The Middle, DDOS Attack, Password Attack, XSS, Vulnerability Scanning dan Ransomware Attack* [3]. Sedangkan, dalam penelitian ini menggunakan tipe ancaman *Vulnerability Scanner*. *Vulnerability Scanning* merupakan suatu proses mengidentifikasi dan menemukan kelemahan atau kerentanan dalam sebuah sistem [4]. Dalam *vulnerability scanning*, terdapat tiga *tools* yaitu *RedHawk, WebKiller,* dan *Rapidscan*. Artikel ini bertujuan untuk memberikan informasi mengenai konsep dari *Vulnerability Scanning, tools* yang digunakan dalam *Vulnerability Scanning*, serta perbandingan cara kerja dari *setiap tools Vulnerability Scanning*. Pengujianaan dilakukan pada sebuah website bernama *zahranrafif.com* disetiap *tool vulnerability scanning*. *Website* yang tidak memiliki keamanan yang baik memiliki potensi risiko keamanan yang dapat digunakan oleh penyerang [5]. Kerentanan pada aplikasi berbasis web bisa beragam, tergantung dari module, library, CMS, dan database yang dipakai [6]. Keamanan informasi merupakan hal yang harus diperhatikan bagi setiap instansi agar terhindar dari gangguan atau Tindakan kejahatan [7]. Keamanan server web biasanya merupakan masalah administrator [8].

2. Metode Penelitian

Penelitian ini menggunakan website *zahranrafif.com* untuk melakukan uji kerentanan dengan *tools RedHawk, WebKiller,* dan *RapidScan*. Pada proses ini terdiri dari analisis tools, pengukuran tools, pengujian tools, serta hasil pengujian. Kerangka kerja penelitian adalah suatu tahapan dalam menyelesaikan suatu permasalahan yang

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

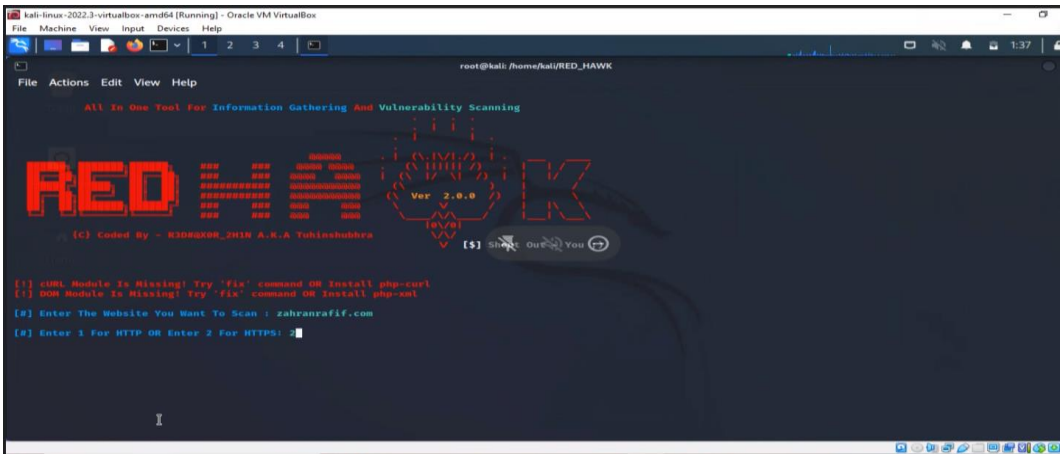
akan dilakukan percobaan [9]. Berikut Alur penelitian dimulai dari analisis, pengukuran, pengujian, dan hasil pengujian tools.



Gambar.1. Alur penelitian diawali dari analisis tools, pengukuran dan pengujian tools, serta hasil pengujian

2.1 Analisis Tools

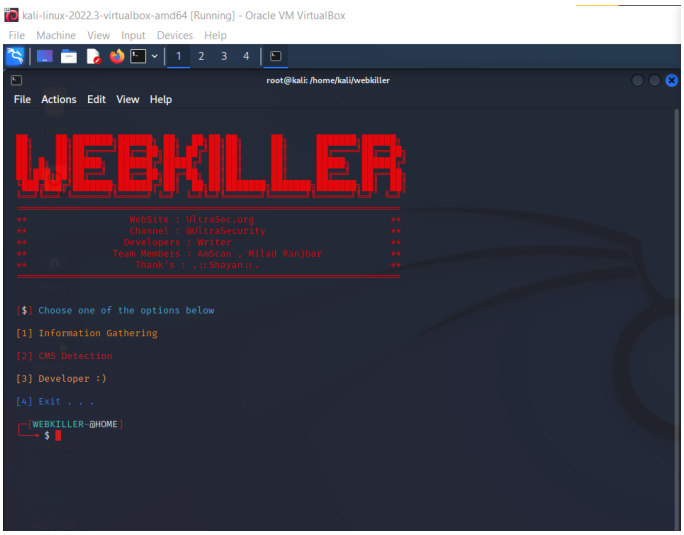
a. RedHawk



Gambar. 2. Tampilan *Tools RedHawk*

RedHawk digunakan sebagai alat untuk memindai situs web yang bertujuan untuk mengumpulkan informasi dan menemukan kerentanan di situs web tersebut [10]. Informasi lengkap mengenai cara install *tools RedHawk* dapat diakses pada link berikut: https://github.com/Tuhinshubhra/RED_HAWK. Tampilan pada *tools RedHawk* memiliki tampilan yang simple, sehingga mudah dipahami oleh pemula. Pada tampilan pertama, tools memberikan daftar fitur yang dapat digunakan dalam *RedHawk*. Bentuk tampilan pada tools *RedHawk* dapat dilihat pada gambar 2 diatas.

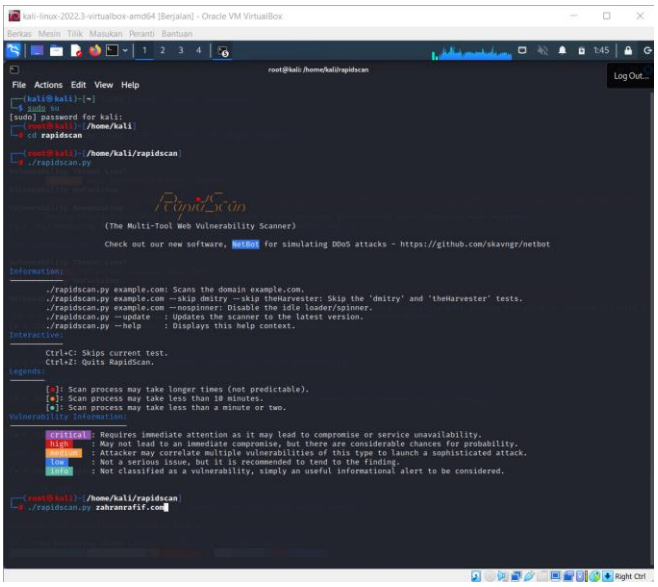
b. WebKiller



Gambar. 3. Tampilan Tools *WebKiller*

WebKiller merupakan salah satu *tool vulnerability scanner* yang digunakan untuk memindai dan mengumpulkan informasi dan menemukan kerentanan di situs *website* tersebut[11]**.** Mengenai informasi lengkap mengenai cara install tools *WebKiller* dapat diakses pada link github berikut: https://github.com/vardhanadi/WebKiller . Pada Proses Scanning menggunakan tool WebKiller. Pada gambar 3, memberikan gambaran tampilan pada *tools WebKiller*. Tampilan yang dimiliki oleh tools ini adalah tampilan yang *to the point* yang memberikan kesan langsung. Namun, dapat dipahami oleh pengguna dengan baik.

c. RapidScan



Gambar. 4. Tampilan *Tools RapidScan*

RapidScan merupakan tools *vulnerability scanner open-source* dan gratis yang tersedia di GitHub yang didasarkan pada kecerdasan open-source (OSINT)[12], *RapidScan* adalah tools yang berguna dalam melakukan pemindaian dan mengumpulkan informasi dan menemukan kerentanan di situs web tersebut. Mengenai cara instal tool *RapidScan* dapat diakses pada link berikut: https://www.geeksforgeeks.org/rapidscan-the-multi-tool-web-vulnerability-scanner-in-kali-linux/. Pada gambar 4 di atas, memberikan informasi mengenai bagaimana gambaran tampilan pada tools Webiller. Tampilan yang dimilkki oleh tools WebKiller memberikan kesan penuh informasi yaitu dalam bentuk keterangan yang harus diperhatikan ketika akan melakukan scanning dengan menggunakan tools WebKiller. Celah keamanan yang didapatkan dari proses scanning tersebut sejumlah 8 saat dideteksi dengan menjalankan

tool ini di kali linux. Website yang diuji dalam pengujian ini adalah *zahranrafif.com.* Dalam *tools RapidScan* terdapat fitur yang menjelaskan *Vulnerability Information* yang terdiri dari:

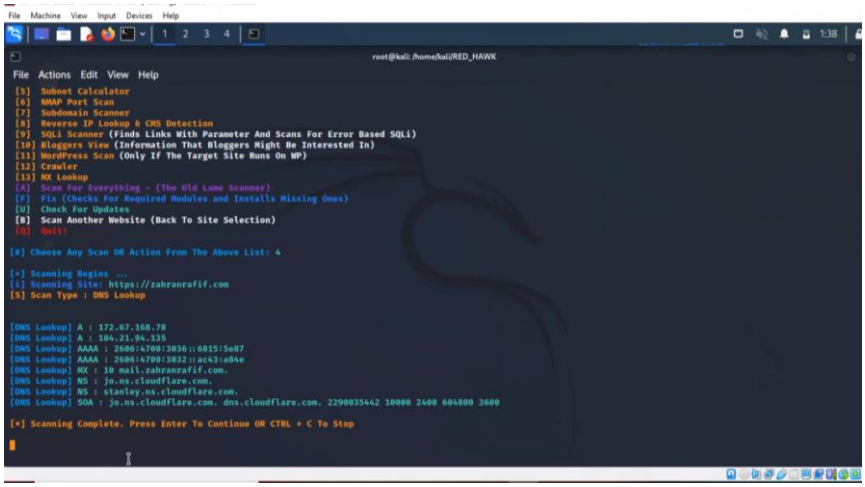
Tabel 1. *Vulnerability Information* pada *RapidScan*

Type	*Vulnerability Information*
Critical	Diperlukan tindakan segera karena dapat menyebabkan ketidaksediaan layanan
High	Terdapat peluang besar untuk probabilitas
Medium	Dapat mengkorelasikan beberapa kerentanan untuk meluncurkan serangan
Low	Bukan masalah serius, tapi dianjurkan untuk cenderung menemukan
Info	Tidak diklasifikasikan sebagai kerentanan

Dapat dilihat pada tabel 1, pengguna akan mendapatkan informasi mengenai type kerentanan yang akan diperoleh setelah melakukan proses *scanning* menggunakan *tools RapisScan*. Jenis atau type tersebut memudahkan pengguna untuk mengetahui jenis kerentanan apa yang diperoleh. Fitur *Vulnerability Information* pada *RapidScan*, juga memberikan pengalaman yang baik untuk pemula yang akan menggunakan *tools RapidScan*. Sehingga pengguna baru tidak kebingungan ketika pertama kali menggunakan *tools RapidScan*.

2.2 Pengukuran dan Pengujian Tools

a. RedHawk



Gambar. 5. Tampilan hasil dari scanning RedHawk DNS Lookup

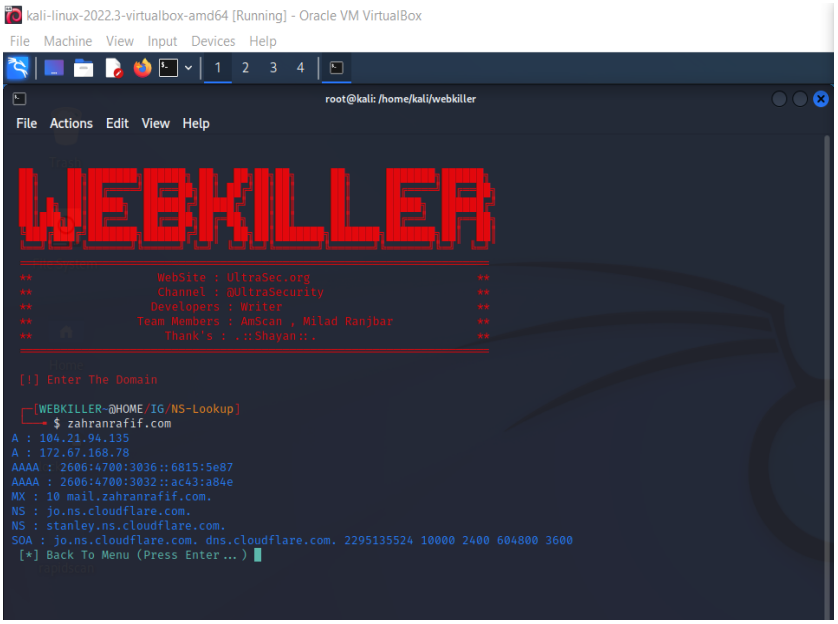
Pada gambar 5. Menampilkan hasil yang diperoleh dari scanning RedHawk dengan menggunkan fitur DNS Lookup, hasil yang diperoleh yaitu IP, MX, NS dari website yang diujikan yang dapat dilihat pada gambar di atas. Pada Proses *Scanning* menggunakan tool *RedHawk* dilakukan sebanyak 3 kali percobaan untuk membuktikan seberapa efektif tool ini. *zahranrafif.com* adalah website yang akan digunakan sebagai pengujian scanning.

Tabel 2. Hasil Percobaan RedHawk

RedHawk	Percobaan 1	Percobaan 2	Percobaan 3
Waktu Scanning	2 Menit	2 Menit	2 Menit
Celah Keamanan	8	8	8

Setelah melakukan pengujian, waktu yang dibutuhkan untuk menyelesaikan sekali percobaan yaitu membutuhkan waktu yang cukup singkat yaitu 2 menit. Pada 3 kali pengujian yang dilakukan, menghasilkan waktu dengan hasil yang sama yaitu selama 2 menit saat melakukan scanning hingga selesai. Tool *RedHawk* termasuk tool yang cukup efektif dengan menyelesaikan proses scanning dalam durasi 2 menit, dimana dalam waktu yang singkat tersebut tool ini dapat melakukan scanning *DNS Lookup* dengan celah keamanan yang didapatkan sejumlah 8 pada saat melakukan *detected* dengan menjalankannya di kali linux. Dalam percobaan ini, celah keamanan yang dapat di *detected* yaitu salah satunya alamat IP dari website yang diujikan. Pada *tools RedHawk*, jaringan internet tidak terlalu berpengaruh karena terganggu atau tidaknya jaringan internet akan menghasilkan output yang sama dengan percobaan-percobaan yang sebelumnya telah dilakukan.

b. WebKiller



Gambar. 6. Hasil dari percobaan *tools WebKiller*

Dapat dilihat pada gambar 6. Hasil yang didapatkan dari percobaan tools WebKiller sama dengan hasil yang diperoleh dari pengujian dengan menggunakan tools RedHawk dimana hasil yang diperoleh yaitu diantaranya IP, MX, NS dari website yang diujikan. Dari percobaan tersebut dapat diperoleh sebuah pengukuran proses scanning yang dilakukan sebanyak 3 kali percobaan.

Tabel 3. Hasil Percobaan *WebKiller*

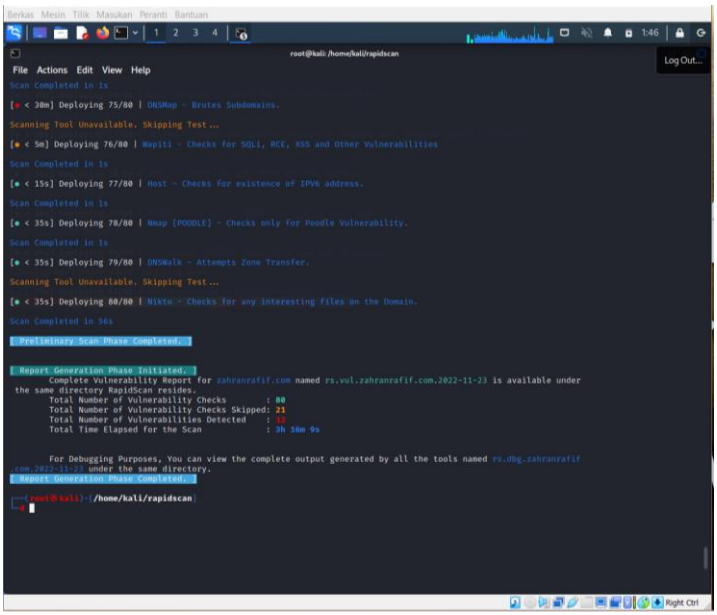
Webiller	Percobaan 1	Percobaan 2	Percobaan 3
Waktu Scanning	3 Menit	3 Menit	3 Menit
Celah Keamanan	8	8	8

Hasil pengukuran yang diperoleh yaitu waktu scanning yang sama, yaitu *WebKiller* memerlukan waktu scanning selama 3 menit untuk melakukan proses scanning hingga selesai. Selain itu, tool *WebKiller* termasuk tool yang efektif dalam proses scanning, dimana waktu yang dibutuhkan begitu cepat dalam melakukan *scanning* yaitu dalam kurun waktu 3 menit dan mampu melakukan scan *DNS Lookup* sebuah website. Namun, untuk tools *Webkiller* hanya dapat mendeteksi kerentanan dalam sebuah website dengan jumlah *detected* yang sedikit sehingga tools ini masih kurang efektif. Perlu diketahui, *Webkiller* memberikan laporan keamanan namun tidak begitu rinci dan menurut kami tidak terlalu memuaskan. Pada *tools WebKiller*, jaringan internet tidak terlalu berpengaruh dengan hasil yang diperoleh sama dengan *tools RedHawk*.

c. RapidScan

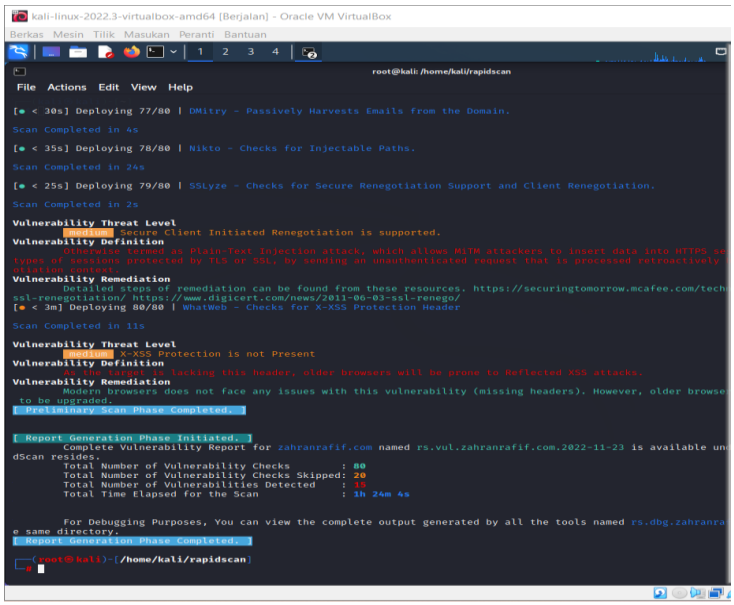
Proses scanning menggunakan website *zahranrafif.com* yang akan dilakukan pengujian scanning. Proses scanning pada tools *RapidScan* dilakukan sebanyak tiga kali pengujian untuk membuktikan seberapa efektif tool tersebut. Pada pengujian pertama dengan menggunakan tool *RapidScan* memerlukan waktu selama 3 jam 16 menit 9 detik, pada pengujian kedua memerlukan waktu selama 1 jam 24 menit 4 detik dan pada pengujian ketiga memerlukan waktu selama 1 jam 27 menit 7 detik. Tool *Rapidscan* termasuk tool yang cukup efektif sebab tools ini bisa mendeteksi cukup banyak kerentanan pada *website* namun proses *scanning* dalam tools ini memerlukan waktu yang cukup lama.

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)



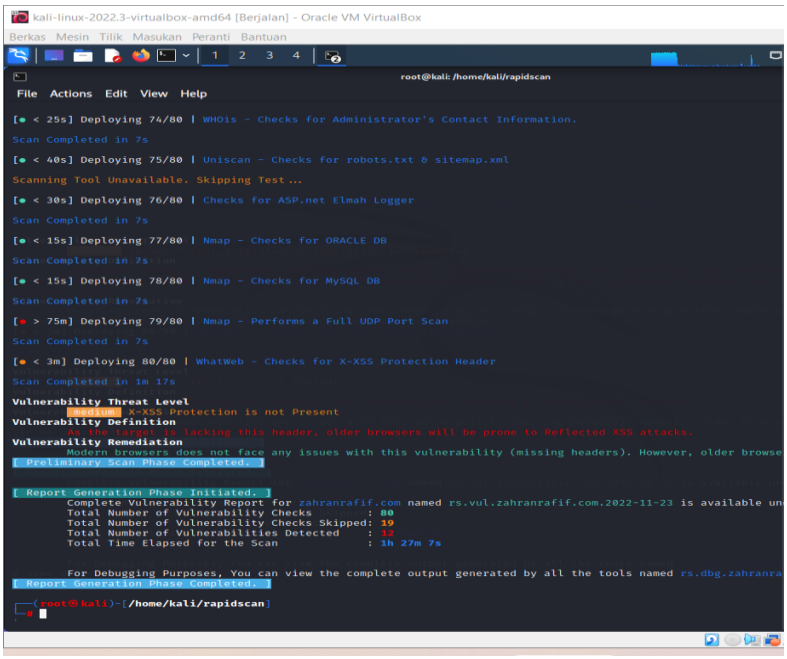
Gambar. 7. Laporan Keamanan *RapidScan* Hasil Percobaan 1

Pada gambar 7 diatas, terdapat laporan keamanan yang muncul, ketika sebuah proses scanning selesai dilakukan, diperoleh bahwa jumlah kerentanan yang dicek yaitu 80, jumlah kerentanan yang di skip yaitu 21, jumlah kerentanan yang di deteksi yaitu berjumlah 12 dan total waktu yang digunakan untuk scanning yaitu selama 3 jam 16 menit 9 detik. Jumlah kerentanan suatu website berkorelasi dengan tingkat kematangan [13]. Dari laporan keamanan tersebut dapat dilihat bahwa laporan tersebut sangat detail mengenai hasil yang peroleh selama scanning dilakukan. Oleh karena itu, *RapidScan* ini tergolong efektif karena dari laporan keamanan, celah keamanan yang dihasilkan memberikan tingkat kerentanan yang diperoleh dalam pengujian tersebut. Dalam proses *Scanning* menggunakan *tools RapidScan* dilakukan *scanning* dengan mengecek 80 celah keamanan pada website yang akan di scanning.



Gambar. 8. Laporan Keamanan RapidScan Hasil Percobaan 2

Gambar 8 di atas merupakan laporan keamanan yang muncul ketika sebuah proses scanning selesai dilakukan, diperoleh bahwa jumlah kerentanan yang dicek yaitu 80, jumlah kerentanan yang di *skip* yaitu 20, jumlah kerentanan yang di deteksi yaitu berjumlah 15 dan total waktu yang digunakan untuk *scanning* yaitu selama 1 jam 24 menit 4 detik.



Gambar 9. Laporan Keamanan *RapidScan* Hasil Percobaan 3

Pada gambar 9, laporan keamanan yang muncul ketika sebuah proses scanning selesai dilakukan, diperoleh bahwa jumlah kerentanan yang akan dicek yaitu 80, jumlah kerentanan yang di *skip* yaitu 19, jumlah kerentanan yang di deteksi yaitu berjumlah 12 dan total waktu yang digunakan untuk scanning yaitu selama 1 jam 27 menit 7 detik.

Tabel 4. Hasil percobaan *RapidScan*

RapidScan	Percobaan 1	Percobaan 2	Percobaan 3
Waktu Scanning	3 Jam 16 Menit 9 Detik	1 Jam 24 Menit 4 Detik	1 Jam 27 Menit 7 Detik
Celah Keamanan	12	15	12

Dari 3 kali proses percobaan yang dilakukan pada *RapidScan*, diperoleh kesamaan celah keamanan. Setiap proses percobaan memiliki hasil *detected* yang sama yaitu berjumlah 12. Namun, hasil waktu scanning memiliki perbedaan setiap percobaan. Setelah tahap pemindaian hasilnya ditampilkan ke pengguna dan mereka dapat disimpan untuk analisis nanti [14].

Dari Pengujian menggunakan *tools RapidScan* pada website *zahranrafif.com.* Diperoleh 80 kerentanan yang akan di scanning pada website, 80 kerentanan tersebut adalah total atau jumlah celah keamanan yang akan di scanning dengan *RapidScan*. Setiap proses scanning, tools akan memberikan informasi mengenai jumlah celah keamanan yang akan di scanning dan dalam proses scanning menggunakan website *zahranrafif.com*. *RapidScan* memberikan informasi bahwa akan melakukan scanning sebanyak 80 kerentanan. Dari pengujian ini, dapat diketahui bahwa dalam proses scanning menggunakan tools *Rapidscan* secara otomatis akan melakukan *skip* pada saat proses berlangsung jika pada proses scanning jaringan internet mengalami gangguan dan akan melakukan scanning ke celah kerentanan selanjutnya. Selain itu, dalam proses scanning dengan *rapidscan* diperoleh jumlah kerentanan yang dapat di *detected* pada website *zahranrafif.com.* Pada tool *RapidScan*, jaringan internet salah satu hal yang berpengaruh dalam proses scanning karena dapat dilihat pada percobaan pertama, bertepatan dengan jaringan yang mengalami gangguan menghasilkan waktu scanning yang cukup lama dan jumlah skip kerentanan yang berjumlah banyak. Sedangkan pada percobaan kedua dan ketiga, proses scanning dilakukan pada jaringan yang cukup bagus sehingga menghasilkan waktu scanning yang cepat dan jumlah skip yang sedikit.

3 Hasil dan Pembahasan

Dari proses *scanning* yang dilakukan dengan menggunakan tiga tools dari *vulnerability scanning* yang terdiri dari *Redhawk, WebKiller* dan *RapidScan.* Dalam pengujian yang telah dilakukan, menghasilkan sebuah perbandingan data yang diperoleh antar *tools* tersebut. Hasil penelitian yang diperoleh merupakan suatu perbandingan antar *tools* yang didapatkan dari proses metode penelitian yaitu menganalisis, mengukur, dan menguji.

Tabel 5. Hasil Perbandingan Data antar *Tools*

Tools	Waktu Scanning	Laporan	Fitur yang digunakan	Celah Keamanan	Keefektifan
RedHawk	2 Menit	Ada	*DNS Lookup*	8	60%
WebKiller	3 Menit	Ada	*DNS Lookup*	8	60%
RapidScan	3 Jam 16 Menit 9 Detik	Ada	*DNS Lookup*	12	80%

Dari Tabel diatas, memberikan gambaran perbandingan antar *tools* dalam proses scanning. Hal yang menjadi perbandingan yaitu dimulai dari laporan keamanan, *fitur*, celah keamanan dan keefektifan serta waktu scanning. Pada *Tools RedHawk*, waktu scanning yang diperlukan yaitu selama 2 menit dan terdpat laporan yang menjelaskan berapa jumlah kerentanan yang di *detected* pada *website zahranrafif.com* tidak terlalu jelas namun dapat dipahami. Fitur dalam *RedHawk* yang digunakan dalam pengujian ini yaitu fitur *DNS Lookup*. Selain itu, celah keamanan yang dihasilkan dari pengujian tersebut yaitu mendapatkan 8 celah keamanan. Sementara untuk keefektifan, *RedHawk* memiliki keefektifan sebesar 60% karena dari sisi waktu *RedHawk* unggul namun dari sisi celah keamanan dan laporan keamanan *RedHawk* hanya dapat mendeteksi sedikit kerentanan dalam sekali proses scanning. Pada *tools RedHawk*, jaringan internet tidak terlalu berpengaruh karena terganggu atau tidaknya jaringan internet akan menghasilkan output yang sama dengan percobaan-percobaan yang sebelumnya telah dilakukan.

Sedangkan. pada tool *Webkiller* memerlukan waktu scanning selama 3 menit dalam satu kali scanning. Laporan yang menjelaskan berapa jumlah kerentanan yang di *detected* pada *website* tersebut tidak terlalu jelas namun dapat dipahami sama seperti RedHawk. Dalam proses pengujian, *WebKiller* menggunakan *fitur DNS Lookup* dan mendapatkan celah keamanan sejumlah 8 kerentanan. Dari pengujian ini, diketahui bahwa setiap *fitur* dalam *tools* tersebut memiliki bentuk laporan yang berbeda-beda. Pada *tool WebKiller* memiliki keefektifan yang sama dengan *RedHawk* karena dari fitur, laporan keamanan, dan celah keamanan memiliki hasil sama. Pada *tools WebKiller*, jaringan internet tidak terlalu berpengaruh dengan hasil yang diperoleh sama dengan *tools RedHawk.*

Sementara itu, pada tool *RapidScan* memerlukan waktu 3 Jam 16 Menit dalam pertama kali proses scanning dan setelah *scanning complete* akan muncul sebuah laporan keamanan yang berisi jumlah waktu, jumlah kerentanan yang dicek, kerentanan yang di *skip* dan kerentanan yang di *detected.* Pada *RapidScan* menemukan celah keamanan sejumlah 12, dan *RapidScan* memiliki sejumlah 80% dalam kategori keefektifan karena dari fitur, laporan keamanan, celah keamanan, dan fitur tool *RapidScan* menghasilkan jumlah *detected* paling banyak serta pada *RapidScan*, *scanning* yang dihasilkan memiliki tingkatan seperti *high, medium* dan *low. Vulnerability Scanning* menghasilkan jumlah kerentanan yang sudah ditemukan terdapat kerentanan dengan tingkat kerentanan yang berbeda-beda. Namun hanya terdapat satu kerentanan yang bersifat *critical* (krisis) [15]. Pada tool *RapidScan*, jaringan internet salah satu hal yang berpengaruh dalam proses scanning karena dapat dilihat pada percobaan pertama, bertepatan dengan jaringan yang mengalami gangguan menghasilkan *waktu* scanning yang cukup lama dan jumlah skip kerentanan yang berjumlah banyak. Sedangkan pada percobaan kedua dan ketiga, proses scanning dilakukan pada jaringan yang cukup bagus sehingga menghasilkan waktu scanning yang cepat dan jumlah skip yang sedikit.

4 Kesimpulan

Tools *Vulnerability Scanning* memberikan informasi celah kerentanan atau kelemahan yang dimiliki oleh suatu *website* yang digunakan saat proses *scanning*. Penelitian ini menunjukkan kelebihan dan kekurangan dari

ketiga tools tersebut. Dalam penelitian ini, sudah dilakukan pengujian beberapa tools *Vulnerability Scanning*, diantaranya yaitu *RedHawk, WebKiller, dan RapidScan.* Dari pengujian tersebut, telah diperoleh perbandingan setiap toolnya. Dapat dilihat hasil perbandingan yang didapatkan yaitu perbandingan waktu Scanning, Keefektifan, Laporan, celah keamanan, dan fitur dari ketiga tools tersebut untuk mengetahui fitur, cara kerja dan hasil dari pengujian pada setiap tools *Vulnerability Scanning*. Dari pengujian ini, dari tiga tools yang diujikan, hasil yang diperoleh dapat dijadikan referensi untuk memilih tools yang akan digunakan dalam melakukan *vulnerability Scanning.*

5 Saran

Penelitian yang telah kami lakukan ini belum sempurna dan perlu ditingkatkan untuk mengetahui kegunaan dari berbagai tools dalam *Cyber Attack* dengan menggunakan topik tertentu, khususnya dalam penelitian ini dalam menganalisis dan meneliti beberapa *tools Vulnerability Scanning,* diantaranya yaitu *RedHawk, WebKiller,* dan *RapidScan.*

Referensi

[1] T. Astriani, A. Budiyono, dan A. Widjajarto, "Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar Nist 800-115," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 8, no. 4, hal. 2041–2050, Dec. 2021, doi: 10.35957/JATISI.V8I4.1232.

[2] K. Subandi dan V. I. Sugara, "Analisa Serangan Vulnerabilities Terhadap Server Selama Periode WFH di Masa Pandemi Covid-19 Sebagai Prosedur Mitigasi," dalam *Seminar Nasional Sains dan Teknologi*, November 2021, hal, 1-4.

[3] S. Sahren, R. A. Dalimuthe dan M. Amin, "Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus," dalam *Prosiding Seminar Nasional Riset Information Science (SENARIS)*, vol. 1, 2019.

[4] A. I. Rafeli, H. B. Seta, dan I. W. Widi, "Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ," *Informatik: Jurnal Ilmu Komputer*, vol. 18, no. 2, hal. 97–103, Augustus 2022.

[5] I. Riadi, R. Umar, dan W. Sukarno, "Vulnerability of injection attacks against the application security of framework based websites open web access security project (OWASP)," *Jurnal Informatika*, vol. 12, no. 2, hal. 53–57, Jul. 2018, doi: 10.26555/JIFO.V12I2.A8292.

[6] A. Budiman, S. Ahdan, dan M. Aziz, "Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment," *Jurnal Komputasi*, vol. 9, no. 2, Oct. 2021, doi: 10.23960/KOMPUTASI.V9I2.2800.

[7] M. Yunus, "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4," *Jurnal Ilmiah Informatika Komputer*, vol. 24, no. 1, hal. 37–48, Aug. 2019, doi: 10.35760/IK.2019.V24I1.1988.

[8] D. C. Angir, A. Noertjahyana, dan J. Andjarwirawan, "Vulnerability Mapping pada Jaringan Komputer di Universitas X," *Journal Infra*, vol. 3, no. 2, 2015

[9] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," *Jurnal Informasi dan Teknologi*, hal. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.

[10] "Red Hawk - Information Gathering and Vulnerability Scanning Tool in Kali Linux - GeeksforGeeks." Diambil dari https://www.geeksforgeeks.org/red-hawk-information-gathering-and-vulnerability-scanning-tool-in-kali-linux/ (diakses Nov. 25, 2022).

[11] "Webkiller v2.0 - Tool Information Gathering tool in Kali Linux - GeeksforGeeks." Diambil dari https://www.geeksforgeeks.org/webkiller-v2-0-tool-information-gathering-tool-in-kali-linux/ (diakses Nov. 25, 2022).

[12] "RapidScan – The Multi-Tool Web Vulnerability Scanner in Kali Linux - GeeksforGeeks." Diambil dari https://www.geeksforgeeks.org/rapidscan-the-multi-tool-web-vulnerability-scanner-in-kali-linux/ (diakses Nov. 24, 2022).

[13] I. G. N. Mantra, M. S. Hartawan, H. Saragih, dan A. A. Rahman, "Web vulnerability assessment and maturity model analysis on Indonesia higher education," dalam *Procedia Computer Science*, 2019, vol. 161, pp. 1165–1172. doi: 10.1016/j.procs.2019.11.229.

[14] J. Fonseca, M. Vieira and H. Madeira, "Testing and Comparing Web Vulnerability Scanning Tools for SQL Injection and XSS Attacks," dalam *13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007)*, 2007, hal. 365-372, doi: 10.1109/PRDC.2007.55.

[15] M. A. Aziz, "Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas XYZ," *Journal of Engineering, Computer Science and Information Technology (JECSIT)*, vol. 1, no. 1, pp. 101–109, Apr. 2021, doi: 10.33365/JECSIT.V1I1.13.