JINTECH: Journal of Information Technology Vol. 4, No. 1
Februari 2023, Halaman : 1 - 15
E-ISSN : 2746-2331
P-ISSN : 2746-234X

UJI *VULNERABILITY ASSESSMENT* DALAM MENGETAHUI TINGKAT KEAMANAN WEB APLIKASI SISTEM INFORMASI LAPORAN DISKOMINFO DAN SANDI ACEH

Irfan Murti Raazi [1], Ima Dwitawati [2], Putri Nabila [3]

[1] *Teknologi Informasi, Universitas Islam Negeri Ar-Raniry, Banda Aceh, irfanmurtiraazi@gmail.com*

[2] *Teknologi Informasi, Universitas Islam Negeri Ar-Raniry, Banda Aceh, ima@ar-raniry.ac.id*

[3] *Teknologi Informasi, Universitas Islam Negeri Ar-Raniry, Banda Aceh, ptriinabilaa01@gmail.com*

Email korespondensi: irfanmurtiraazi@gmail.com

Abstract: Along with the increasing need for information systems in the Districts/Cities of Aceh Province in supporting the development process of a region, the penetration test and evaluation of the system has been delayed. This is due to the limited number of experts in the province as well as the level of dependence on human resources in Districts/Cities who have limited capacity in terms of testing information systems. Therefore, with the presence of the latest web application information system at Diskominfo and Sandi Aceh, it requires system testing to determine the feasibility level of publication of the information system. The testing technique in this study used the VAPT Life Cycle method. Where the VAPT Life Cycle will identify, describe, assess vulnerabilities based on the CVSS (Common Vulnerability Scoring System) and provide solutions for handling vulnerabilities. The vulnerability discovery process in this study uses the Nessus Vulnerability Scanning tool. From the findings there are 4 vulnerabilities, 1 in the high category and 3 in the medium category. This vulnerability data can be used as evaluation material to close or fix existing security holes.

Keywords: Vulnerability Assessment, Information Security System, Penetration Testing.

Abstrak: Seiring dengan meningkatnya kebutuhan sistem informasi di Kabupaten/Kota Provinsi Aceh dalam mendukung proses pembangunan suatu daerah membuat tertahannya uji penetrasi dan evaluasi sistem. Hal ini dikarenakan keterbatasan tenaga ahli di provinsi dan juga tingkat ketergantungan sumber daya manusia di Kabupaten/Kota yang memiliki kapasitas terbatas dalam hal pengujian sistem informasi. Oleh karena itu, dengan hadirnya sistem informasi web aplikasi terbaru pada Diskominfo dan Sandi Aceh memerlukan pengujian sistem untuk mengetahui tingkat kelayakan publikasi sistem informasi tersebut. Teknik pengujian dalam penelitian ini menggunakan metode *VAPT Life Cycle*. Dimana *VAPT Life Cycle* akan melakukan

identifikasi, deskripsi, menilai kerentanan berdasarkan *CVSS* (*Common Vulnerability Scoring System*) serta adanya solusi penanganan kerentanan. Proses penemuan kerentanan pada penelitian ini menggunakan *tool* Nessus *Vulnerability Scanning*. Dari hasil temuan terdapat 4 kerentanan, 1 yang dikategori *high* dan 3 yang dikategori *medium*. Data kerentanan ini dapat jadikan sebagai bahan evaluasi untuk menutup atau memperbaiki celah keamanan yang ada.
Kata kunci: Penilaian Kerentanan, Sistem Keamanan Informasi, Uji Penetrasi.

1. Pendahuluan

Dinas Komunikasi, Informatika dan Persandian Aceh (Diskominfo dan Sandi Aceh) merupakan sebuah instansi yang bertanggung jawab atas pengelolaan aset teknologi dan informasi pada Pemerintah Aceh. Hal ini meliputi urusan pemerintahan pada bidang informasi, komunikasi publik, aplikasi, informatika, persandian serta statistik (Febriani & Juliani, 2022). Dengan begitu, salah satu pekerjaan terkait yang berkenaan dengan pengelolaan sistem keamanan informasi di seluruh Aceh. Tujuannya adalah untuk memperhatikan tingkat keamanan sistem terhadap resiko-resiko yang mungkin timbul dalam sistem manajemen pengamanan informasi di seluruh kabupaten dan kota yang ada di Aceh.

Sejauh ini, seluruh proses pengujian sistem dilakukan oleh tenaga ahli bidang *Penetration Testing* untuk mengukur tingkat kelayakan publikasi sistem informasi. Prosesnya, setiap Diskominfo diminta untuk melakukan pengujian berdasarkan kebutuhan sistem informasi dari masing-masing Kabupaten/Kota. Kemudian Diskominfo dan Sandi Aceh akan melakukan tindak lanjut terhadap berbagai permasalahan yang diajukan untuk ditangani oleh tenaga ahli. Oleh karena keterbatasan tenaga ahli di provinsi menyebabkan keterlambatan dalam memberikan hasil kerentanan sistem. Demikian juga, tingkat ketergantungan sumber daya manusia di Kabupaten/Kota yang memiliki kapasitas terbatas dalam hal pengujian sistem informasi menyebabkan tingkat ketergantungan yang amat tinggi terhadap solusi keamanan sistem informasi kepada provinsi. Kondisi ini membuat tertahannya evaluasi sistem serta membutuhkan banyak biaya penanganan.

Berdasarkan uraian diatas, dengan hadirnya sistem informasi web aplikasi terbaru yang akan digunakan untuk merekapitulasi Sistem Informasi

Laporan Keamanan Diskominfo dan Sandi Aceh, maka diperlukan pengujian sistem untuk mengetahui tingkat keamanan web aplikasi dari hasil *vulnerability scanning* akan memberikan evaluasi keamanan terhadap web aplikasi tersebut. Pengujian ini diharapkan dapat membantu dinas dalam menemukan celah keamanan dengan cepat tanpa harus ketergantungan pada tenaga ahli untuk melakukan pengujian sistem. Sementara ini, penulis membatasi pengujian sistem informasi tersebut hanya berfokus pada penemuan jumlah kerentanan, detail tentang setiap temuan, tingkat keparahan resiko, dan dampak pada Web Aplikasi Sistem Informasi Laporan Keamanan Diskominfo dan Sandi Aceh.

2. Kajian Kepustakaan

2.1 Sistem Informasi

Sistem informasi adalah sebuah sistem yang terintegrasi dalam mengumpulkan, memproses, menyimpan dan mendistribusikan informasi dengan tujuan untuk mendukung kebutuhan organisasi. Sehingga sangat penting dalam penentuan kualitas informasi dan penyediaan informasi (Prasetio, 2017).

2.2 Keamanan Informasi

Informasi kini sangat mudah didapatkan dari berbagai macam media di internet. Sehingga dalam mendukung keakuratan informasi dan teknologi harus mempunyai keamanan yang cukup baik. Keamanan informasi adalah suatu kegiatan mengamankan aset informasi dari berbagai ancaman yang mungkin dapat timbul. Dalam hal ini, keamanan informasi memiliki tiga prinsip utama yang dikenal *CIA Triad* sebagai berikut:

1. Kerahasiaan (*Confidentiality*)
   Confidentiality adalah prinsip yang memberikan jaminan kerahasiaan data atau informasi dalam menjaga kerahasiaan suatu informasi dari pihak yang tidak bertanggung jawab.
2. Integritas (*Integrity*)

Integrity adalah prinsip yang mempunyai keterkaitan dengan integritas suatu data dalam menjaga keaslian data dari kegiatan modifikasi tanpa adanya izin pihak yang berwenang.

3. Ketersediaan (*Availability*)

   Availability adalah prinsip yang menjamin penggunaan dan akses data atau informasi sesuai permintaan oleh organisasi yang berwenang. Hal ini jika keamanan berhasil menjalankan availability suatu informasi yang tersedia harus memiliki izin dapat mengakses informasi dari berbagai sumber dengan menggunakan jalur yang aman (Cardwell, 2016).

2.3 *Vulnerability Assessment*

Vulnerability Assessment merupakan suatu proses identifikasi kerentanan pada sistem keamanan yang ada pada ekosistem teknologi informasi. kerentanan dalam hal teknologi informasi terdapatnya celah keamanan ataupun jika dieksploitasi dapat mengakibatkan relasi serangan pada sistem (Aziz, 2021). Adapun jenis aktivitas serangan terhadap sistem dapat digolongkan sebagai berikut (Ketaren, 2016):

1. *Unauthorised Access*

   Unauthorised Acces adalah suatu tindakan kejahatan yang dapat terjadi pada saat *attacker* melakukan penyusupan ke dalam suatu sistem jaringan komputer secara tidak sah. Misalkan seperti *probing* atau *port scanning*.

2. *Cyber Espionage, Sabotage and Extortion*

   Cyber Espionage adalah suatu tindakan kejahatan yang memata-matai target tertentu dengan memanfaatkan jaringan internet untuk mengumpulkan informasi mengenai suatu organisasi atau hanya ingin memperoleh kesenangan bagi pelaku. Adapun *Sabotage and Extortion* adalah suatu tindakan kejahatan yang membuat gangguan, perusakan atau memodifikasi suatu data, dan sistem komputer. Hal ini segala aktivitas yang ingin dilakukan tidak dapat digunakan semestinya atau dapat berjalan sesuai kehendak oleh pelaku.

3. *Sniffing*

   Sniffing adalah tindakan kejahatan yang dilakukan pada jaringan internet dengan tujuan mengambil data dan informasi target dari hasil kegiatan capturing paket yang melewati jaringan tertentu.

4. *Defacing*

   Suatu tindakan kejahatan yang terjadi pada website atau program *application* untuk mengubah konten dan konfigurasi program aplikasi dengan menyisipkan file pada server, teknik ini terjadi karena adanya celah keamanan pada sistem.

5. *Pharming*

   Pharming adalah tindakan kejahatan dari serangan rekayasa sosial dengan memanipulasi lalu lintas situs web untuk memperoleh informasi pengguna atau menyisipkan malware ke dalam komputer target melalui situs web palsu

2.4 *Penetration Testing*

Penetration testing adalah bagian dari *ethical hacking* yang mempunyai metode dan prosedur untuk melindungi sebuah keamanan organisasi. Menurut Baloch dalam buku *Ethical Hacking and Penetration Testing Guide* menyatakan bahwa *Penetration Testing* terbukti dapat membantu dan menemukan celah keamanan yang terdapat di dalam sebuah organisasi dan mampu memeriksa apakah penyerang mendapatkan akses yang tidak sah terhadap suatu informasi (Baloch, 2017). Dalam hal ini, pengujian suatu sistem pada institusi atau organisasi harus memiliki izin dari pemilik objek sehingga diperlukan persetujuan dalam menentukan batasan-batasan dalam ruang lingkup terhadap metode dan target yang akan dilakukan *Vulnerability Assessment*.

2.5 Nessus

Nessus merupakan *tool scanning* yang bersifat *open source* untuk melihat celah keamanan sistem. Dimana *tool* ini dapat mengaudit keamanan sebuah sistem, seperti *vulnerability*, *misconfiguration*, *security path* yang belum diaplikasikan

dan *denial of service* yang digunakan *tool* Nessus untuk monitoring lalu lintas jaringan. Dengan begitu, penggunaan Nessus dapat mendeteksi adanya kelemahan atau pun cacat dari suatu sistem.

Dalam *tool* Nessus memiliki penilaian yang disebut *CVSS* (*Common Vulnerability Scoring System*). *CVSS* adalah sebuah proses kegiatan penilaian yang digunakan untuk menilai kerentanan pada pengujian sistem. Berdasarkan peringkat kerentanan skor *CVSS* dapat dilihat pada Tabel 1 (Kumar, 2014).

Tabel 1. Daftar *Common Vulnerability Scoring System*

No	*CVSS Score*	*Criticality*
1	0,0	*None*
2	0,1 – 3,9	*Low*
3	4,0 – 6,9	*Medium*
4	7,0 – 8,9	*High*
5	9,0 – 10,0	*Critical*

Pada Tabel 1 merupakan bagian yang menjadi rujukan dari temuan kerentanan berdasarkan masing-masing *score* pada tingkat penilaian untuk *None*, *Low*, *Medium*, *High*, dan *Critical*. Hal ini *CVSS* menilai kerentanan suatu sistem dari beberapa aspek yang dibagi menjadi 8 bagian yaitu *Attack Vector, Attack Complexity, Privilege Required, User Interaction, Scope, Confidentiality, Integrity*, dan *Availability* (CVSS, 2018). Dengan demikian, yang menjadi fokus utama penilaian dari kerentanan suatu sistem berdasarkan *Confidentiality*, *Integrity*, dan *Availability*. Apabila ketiga aspek tidak mengancam maka skor kerentanannya akan tetap 0 karena tidak terdeteksi aspek apapun (Yohan, 2018).

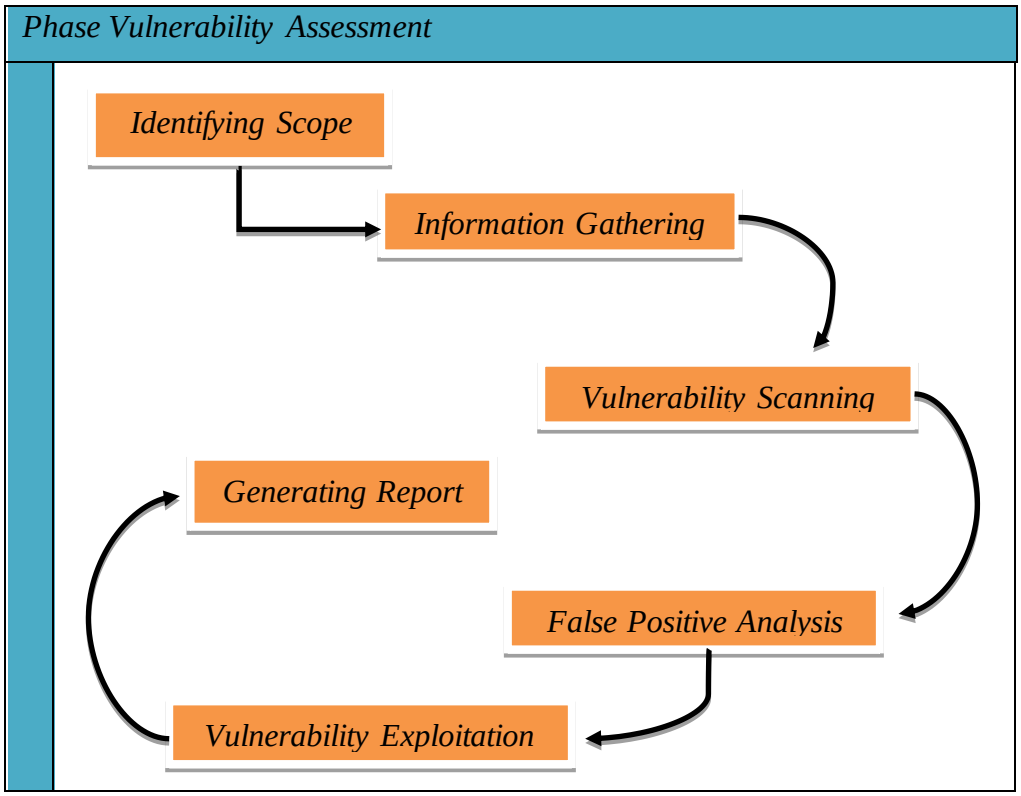
3. Metode Penelitian

3.1 Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah *Vulnerability Assessment dan Penetration Testing Life Cycle* (*VAPT Life Cycle*), yang

E-ISSN : 2746-2331
P-ISSN : 2746-234X

merupakan bagian arus aktivitas secara keseluruhan dari pengujian sistem. Gambar 1 urutan dari prosedur yang terdapat di dalam pengujian sistem.



Gambar 1. Tahapan Penelitian

Pada Gambar 1 menjelaskan tahapan pengujian sistem informasi pada Diskominfo dan Sandi Aceh didalam penelitian ini. Berikut penjelasan dari tahapan-tahapan pengujian tersebut adalah:

A. *Identifying Scope*

Tahap pertama yang berfungsi untuk menentukan ruang lingkup pengujian yang akan diuji, pada pengujian ini penulis menggunakan alamat IP (*Internet Protocol*) 123.xx.xx.221 pada Diskominfo dan Sandi Aceh sebagai objek dari pengujian yang akan dilakukan.

B. *Information Gathering*

Tahap kedua yang berfungsi sebagai pengumpulan informasi tentang sistem target. Berikut tools yang digunakan untuk mengumpulkan informasi target:

a) *Whois*

Whois adalah layanan untuk mengakses informasi spesifik tentang target termasuk alamat IP atau nama *host* dari target server, DNS dan informasi kontak yang biasanya berisi alamat dan nomor telepon.

b) *NMAP*

Network Mapper (*NMAP*) adalah sebuah *tool open source* untuk melakukan eksplorasi dan audit keamanan jaringan dalam mengidentifikasi *port* sebuah *host.* Dimana akan mengidentifikasi kondisi *port* berdasarkan tiga kondisi yaitu *open*, *filtered,* dan *closed* (Kamilah & Hendri Hendrawan, 2019). Dengan demikian, *port* digunakan untuk menjalankan servis yang dibutuhkan oleh sistem maka kondisi *open port* menjadi salah satu jalur eksploitasi sistem.

C. *Vulnerability Scanning*

Tahap ketiga yang berfungsi untuk mencari kerentanan pada alamat IP 123.xx.xx.221 dengan menggunakan *tool* Nessus.

D. *False Positive Analysis*

Tahap keempat menemukan daftar kerentanan dari hasil pemindaian pada tahap ketiga. Dalam hal ini, kegiatan utama yang harus dilakukan yaitu memfilter daftar kerentanan yang didapatkan bukan kerentanan yang salah.

E. *Vulnerability Exploitation*

Tahap kelima yang berfungsi untuk menembus sistem target berdasarkan eksploitasi kerentanan yang dapat diakses secara publik untuk dimanfaatkan oleh pihak yang tidak berwenang.

F. *Generating Report*

Tahap keenam bagian tahapan akhir yaitu pembuatan laporan yang berisi tentang kerentanan pada alamat IP 123.xx.xx.221, dan memberikan rekomendasi untuk memperbaiki kerentanan pada target uji tersebut.

3.2 Pengujian

Pada penelitian ini dalam melakukan *vulnerability assessment* terhadap alamat IP 123.xx.xx.221 pada Diskominfo dan Sandi Aceh, dengan menggunakan

E-ISSN : 2746-2331
P-ISSN : 2746-234X

tool Nessus untuk melakukan pengujian *vulnerability scanning* dalam memperoleh daftar hasil kerentanan beserta penjelasan, persentase kerentanan, dan solusi untuk mengatasi temuan kerentanan guna untuk mengevaluasi serta meningkatkan keamanan terhadap Web Aplikasi Sistem Informasi Laporan Keamanan dengan alamat IP 123.xx.xx.221 Diskominfo dan Sandi Aceh.

4. Hasil dan Pembahasan

4.1 *Vulnerability Scanning*

Pada tahap ini dilakukan *Vulnerability Scanning* kerentanan pada Web Aplikasi Sistem Laporan Diskominfo dan Sandi Aceh menggunakan *tool* Nessus. Dimana hasil *Vulnerability Scanning* pada web aplikasi tersebut dapat dilihat pada Gambar 2.

Gambar 2. Hasil *Vulnerability Scanning*

Dari hasil *Vulnerability Scanning* yang didapatkan pada Web Aplikasi Sistem Informasi Laporan Keamanan Diskominfo dan Sandi Aceh. Adapun daftar kerentanan dapat dilihat berdasarkan tingkatan kategori kerentanan pada Tabel 2.

Tabel 2. Daftar Kerentanan

No	Nama Kerentanan	*Base Score*	Tingkat Kerentanan
1	*DNS Server Spoofed Request Amplification DDoS*	7.5	*High*
2	*SSL Certificate Cannot Be Trusted*	6.5	*Medium*
3	*DNS Server Cache Snooping Remote Information Disclosure*	5.3	*Medium*
4	*DNS Server Recursive Query*	5.0	*Medium*

	Cache Poisoning Weakness		

Pada daftar kerentanan yang telah didapatkan dari hasil *Vulnerability Scanning* tentunya mempunyai dampak kerentanan yang berbeda-beda di setiap kerentanan. Adapun penjelasan dari setiap kerentanan yang ditemukan sebagai berikut:

1) DNS Server Spoofed Request Amplification DDoS

Kerentanan ini didapatkan berdasarkan dengan *spoofing* IP sumber alamat, dimana penyerang dapat memanfaatkan amplifikasi ini untuk melakukan serangan penolakan layanan terhadap *host* dengan menggunakan *remote* DNS server. Dengan demikian, kerentanan tersebut ditemui pada *port* 53/udp/dns yang merupakan dengan *base score CVSS* 7.5 dan tingkat kerentananya adalah *high*.

2) SSL Certificate Cannot Be Trusted

Kerentanan dari sertifikat server tidak dapat dipercaya akibat rantai sertifikat ke otoritas publik tidak mendapat persetujuan atau ditanda tangani oleh *authority* sertifikat yang terpercaya. Hal dapat mempermudah untuk melakukan serangan *man-in-the middle* terhadap *host* jarak jauh. Dengan demikian, kerentanan tersebut ditemui pada *port* 110/tcp/pop3, 143/tcp/imap, 993/tcp/imap dan 995/tcp/pop3 yang merupakan dengan *base score* CVSS 6.5 dan tingkat kerentananya adalah *medium*.

3) DNS Server Cache Snooping Remote Information Disclosure

Domain Name System (DNS) adalah suatu kegiatan yang bertugas mengubah IP *Address* suatu situs menjadi domain agar mudah di *search engine*. Sehingga *snooping* ini memungkinkan dilakukan pemantauan elektronik terhadap jaringan untuk memperoleh *password* atau data lainnya. Pada kerentanan ini ditemukan layanan DNS server untuk mencari tahu bahwa DNS server mempunyai *record cached* DNS tertentu. Dari kerentanan ini dengan mudah menemukan informasi tentang pemilik DNS server. Dengan demikian, kerentanan tersebut ditemui pada *port* 53/udp/dns yang merupakan dengan *base score* CVSS 5.3 dan tingkat kerentananya adalah *medium*.

E-ISSN : 2746-2331
P-ISSN : 2746-234X

4) DNS Server Recursive Query Cache Poisoning Weakness

Kerentanan ini mengizinkan host untuk melakukan q*uery* rekursif melalui *User Datagram Protocol* (UDP). Pemanfaatan UDP dapat berlangsung lebih cepat meskipun tidak akurat, namun pertukaran informasi tanpa perlu melakukan negosiasi saat pertukaran data karena data yang saling ditransferkan telah sesuai dengan settingan UDP. Oleh sebab itu, penyerang dapat memasukkan catatan alamat palsu untuk domain internet ke dalam DNS, sehingga jika server menerima DNS maka entri palsu di *cache* oleh server akan terhubung ke alamat server DNS yang disusupi. Dengan demikian, kerentanan tersebut ditemui pada *port* 53/udp/dns yang merupakan dengan *base score* CVSS 5.0 dan tingkat kerentananya adalah *medium*.

4.2 *Vulnerability Port Service*

Adapun *port service* yang terdapat pada *vulnerability* Web Aplikasi Sistem Informasi Laporan Keamanan Diskominfo dan Sandi Aceh dapat dilihat pada Tabel 3.

Tabel 3. *Vulnerability Port Service*

Service Port	*Threat Level*
53/udp/dns	*High*
110/tcp/pop3	*Medium*
143/tcp/imap	*Medium*
993/tcp/imaps	*Medium*
995/tcp/pop3s	*Medium*

Dari Tabel 3 menjelaskan bahwa kerentanan Web Aplikasi Sistem Informasi Laporan Keamanan pada *port* 53 (udp/dns) memiliki dua kerentanan, dimana pada setiap kerentanan memiliki *base score* 7.5, 5.3, dan 5.0 dengan tingkat kerentanan *high, medium*, dan *medium*. Kemudian pada *port* 110 (tcp/pop3), 143 (tcp/imap), 993 (tcp/imaps), dan 995 (tcp/pop3s) memiliki satu kerentanan, dimana kerentanan memiliki *base score* 6.5 dengan tingkat

kerentanan medium. Sehingga dapat diketahui bahwa pada Web Aplikasi Sistem Informasi Laporan Keamanan memiliki satu kerentanan *high* yaitu amplifikasi DNS di *port* 53, amplifikasi DNS adalah jenis serangan refleksi yang memanipulasi sistem nama domain publik dapat diakses, yang membuat terjadinya penyerangan berulang kepada target (Triyana & Eka, 2017). Kerentanan pada amplifikasi DNS ini memiliki dampak yang menyebabkan seorang penyerang dapat membanjiri SYN klasik sehingga *respons* dari server melipat gandakan ukuran yang dapat membanjiri bandwidth yang dikonsumsi dan juga membuat sumber serangan sangat sulit untuk dilacak, karena pada amplifikasi DNS tidak dikonfigurasi dalam penggunaan sumber daya jarak jauh maka dapat memalsukan alamat IP sumber dalam melakukan penyerangan.

4.3 *Generating Report*

Generating report merupakan tahapan terakhir untuk membuat laporan dari hasil kegiatan *Vulnerability Assessment*. Dimana tahapan pelaporan ini bagian yang paling penting untuk memberikan rekomendasi tentang penemuan hasil identifikasi celah keamanan kepada pihak Diskominfo dan Sandi Aceh tentang kerentanan pada Web Aplikasi Sistem Informasi Laporan Keamanan yang dimilikinya.

Dalam proses identifikasi adanya beberapa tingkat celah keamanan pada Web Aplikasi Sistem Informasi Laporan Keamanan yaitu *high*, dan *medium*. Setiap kerentanan tentunya mempunyai dampak yang berbeda-beda, maka dari itu pembuatan laporan ini akan mendokumentasikan setiap kerentanan yang didapatkan untuk memberikan rekomendasi dalam bentuk laporan seperti yang terdapat pada Tabel 4.

Tabel 2. Laporan *Vulnerability Assessment*

No	Nama Kerentanan	Dampak	Solusi
1	*DNS Server Spoofed Request Amplification DDoS*	Penyerang dapat memanfaatkan amplifikasi untuk membanjiri bandwidth.	Membatasi akses server DNS dari jaringan publik atau dapat mengkonfigurasi ulang untuk menolak

			kueri tersebut.
2	*SSL Certificate Cannot Be Trusted*	Penyerang dapat mencuri data dan informasi karena tidak tersedianya sertifikat dari otoritas terpercaya.	Membeli atau membuat sertifikat SSL.
3	*DNS Server Cache Snooping Remote Information Disclosure*	Penyerang akan dengan mudah menemukan informasi tentang pemilik DNS Server.	Melakukan perbaikan pada perangkat lunak DNS.
4	*DNS Server Recursive Query Cache Poisoning Weakness*	Penyerang dapat memasukkan catatan alamat palsu untuk *domain* internet ke dalam DNS.	Membatasi kueri rekursif ke host yang harus menggunakan nama server dengan mengelompokkan alamat internal.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil dari uji *Vulnerability Assessment* terhadap Web Aplikasi Sistem Informasi Laporan Diskominfo dan Sandi Aceh, maka dapat disimpulkan:

1. Kerentanan Sistem Informasi pada web aplikasi dapat diketahui dengan menggunakan metode *VAPT Life Cycle* dengan tahapan *Identyfing Scope*, *Information Gathering*, *Vulnerability Scanning*, *False Positive Analysis*, *Vulnerability Exploitation*, dan *Generating Report*. Kemudian untuk mengukur tingkat kerentanannya menggunakan *Common Vulnerability Scoring System* (*CVSS*) sehingga dapat dipetakan tingkat kerentanannya ke dalam kategori *critical, high*, *medium*, *low*, dan *none*.
2. Setelah dilakukan pengujian kerentanan terhadap Web Aplikasi Sistem Informasi Laporan Diskominfo dan Sandi Aceh memiliki 4 kerentanan. Dari 4 kerentanan tersebut 1 yang masuk kategori *high* dan 3 yang masuk kategori *medium* sehingga perlu segera diperbaiki. Adapun kerentanan tersebut ialah *DNS Server Spoofed Request Amplification DDoS*, *SSL Certificate Cannot Be*

Trusted, DNS Server Cache Snooping Remote Information Disclosure, dan *DNS Server Recursive Query Cache Poisoning Weakness*.

5.2 Saran

Berdasarkan dari kesimpulan dan hasil pembahasan yang telah diuraikan, maka pada laporan ini disarankan hal-hal berikut:

1. Proses pemeriksaan sebaiknya dilakukan dengan sistem terjadwal yang berbatas waktu.
2. Ditemukan kerentanan pada Laporan hasil uji *Vulnerability Assessment* maka disarankan kepada bagian terkait untuk segera melakukan proses evaluasi keamanan terhadap web aplikasi tersebut. Hal ini untuk memastikan tindakan pengamanan sistem tetap terjaga.
3. Mengingat kegiatan *Vulnerability Assessment* memerlukan keahlian yang spesifik maka kegiatan pelatihan dan peningkatan SDM dalam hal *Vulnerability Assessment* perlu dilakukan.

Daftar Kepustakaan

Aziz, M. (2021). Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas Xyz. *Jecsit*, *1*(1), 101–109.

Baloch, R. (2017). *Ethical hacking and penetration testing guide*. CRC Press.

CVSS. (2018). *CVSS v3.0 Specification Document*. https://www.first.org/cvss/v3.0/specification-document

Febriani, D. L., & Juliani, R. (2022). Strategi Komunikasi Pemerintah Daerah Dalam Mensosialisasikan Informasi Publik Di Kabupaten Aceh Barat. *At-Tanzir: Jurnal Ilmiah Prodi Komunikasi Penyiaran Islam*, 19–38. https://doi.org/10.47498/tanzir.v13i1.970

Kamilah, I., & Hendri Hendrawan, A. (2019). Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika. *Prosiding Semnastek*, *16*(0), 1–9.

https://jurnal.umj.ac.id/index.php/semnastek/article/view/5233

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Times*, *5*(2), 35–42. http://stmik-time.ac.id/ejournal/index.php/jurnalTIMES/article/viewFile/556/126

Kumar, H. (2014). *Learning Nessus for Penetration Testing*. https://books.google.com/books?id=hhuxAgAAQBAJ&pgis=1

Prasetio, N. (2017). Sistem Informasi Penyewaan Kendaraan Berbasis Web (Studi Kasus Chandra Trans Bali). *Jurnal Ilmiah Methonomi*, *3*(2), 28–29.

Triyana, N., & Eka, A. (2017). Analisis DNS Amplification Attack. *Jurnal of Education and Information Communication Technology*, *1*(1), 17–22.

Yohan, M. (2018). *Mengenal Istilah Common Vulnerability Scoring System*. https://socs.binus.ac.id/2018/12/13/mengenal-istilah-common-vulnerability-scoring-system/