SATIN – Sains dan Teknologi Informasi
Journal Homepage : http://jurnal.sar.ac.id/index.php/satin

Studi Komparatif Teknik Analisis Keamanan Sistem Informasi e-Government: Penetration Testing VS Vulnerability Assessment

Muhammad Ayyas [1], Ahmad Fauzi[2], Suprih Widodo[3]
[1]Universitas Pendidikan Indonesia, muhammadayyas@upi.edu, Purwakarta, Indonesia.
[2]Universitas Pendidikan Indonesia, ahmadfauzi@upi.edu, Purwakarta, Indonesia.
[3]Universitas Pendidikan Indonesia, supri@upi.edu, Purwakarta, Indonesia.

Informasi Makalah

Submit : Apr 20, 20xx
Revisi : May 20, 20xx
Diterima : May 30, 20xx

Kata Kunci :

Keamanan sistem informasi
Vulnerability assessment
Penetration testing

Abstrak

Keamanan informasi berperan penting dalam melindungi kerahasiaan, integritas, dan ketersediaan data yang vital. Penelitian ini bertujuan untuk membandingkan efektivitas dua teknik keamanan utama, yaitu penetration testing dan vulnerability assessment, dalam mengamankan sistem informasi di instansi pemerintah. Dengan menggunakan metode penelitian kualitatif, penelitian ini menganalisis kedua teknik tersebut berdasarkan standar dan regulasi yang berlaku. Hasil penelitian menunjukkan bahwa penetration testing lebih efektif dalam mengidentifikasi kelemahan yang belum terdeteksi, sementara vulnerability assessment lebih efisien dalam pemetaan dan perbaikan kerentanan yang telah diketahui. Kesimpulan dari penelitian ini adalah bahwa kombinasi kedua teknik tersebut memberikan perlindungan optimal bagi sistem informasi di instansi pemerintah. Implementasi dari hasil penelitian ini diharapkan dapat meningkatkan keamanan informasi dan kualitas pelayanan publik melalui e-Government. Penelitian ini memberikan wawasan mendalam mengenai metode terbaik untuk meningkatkan keamanan informasi.

Abstract

Information security plays a crucial role in protecting the confidentiality, integrity, and availability of vital data. This research aims to compare the effectiveness of two main security techniques, namely penetration testing and vulnerability assessment, in securing information systems within government agencies. Using a qualitative research method, this study analyzes both techniques based on applicable standards and regulations. The research findings indicate that penetration testing is more effective in identifying vulnerabilities that have not been detected, while vulnerability assessment is more efficient in mapping and remediating known vulnerabilities. The conclusion of this study is that the combination of both techniques provides optimal protection for information systems in government agencies. The implementation of these research findings is expected to enhance information security and the quality of public services through e-Government. This research provides in-depth insights into the best methods for improving information security.

Nama Penulis Yang Bertanggung Jawab,
Email: xxx@xx.ac.id.

Sumber pendanaan dapat ditulis disini.
Jika tidak ada, hapus teks ini.

SATIN – Sains dan Teknologi Informasi
Vol. 10, No. 1, Juni 2024, pp. 25-34
ISSSN: 2527-9114, DOI: 10.33372/stn.v9i2.1000

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi yang terus terjadi mengikuti zaman menjadi instrumen penting yang memengaruhi perubahan aktivitas manusia dalam berbagai sektor kehidupan. Tidak terkecuali sektor pelayanan publik yang difasilitasi oleh pemerintah. Digitalisasi pelayanan publik pada instansi pemerintah terus gencar dilakukan. *Electronic Government* atau dikenal dengan istilah *e-Government* mendorong perubahan besar pada pelayanan publik instansi pemerintah yang birokratis dan berbelit-belit menjadi lebih fleksibel, efektif, efisien, dan aman (Hartono et al., 2010).

Pada implementasinya, faktor keamanan informasi pada berbagai sistem informasi menjadi aspek yang sangat krusial untuk dikelola dengan baik. Keamanan informasi merupakan sebuah tindakan menghargai nilai informasi sebagai sebuah aset yang berharga dengan melindungi informasi tersebut dari berbagai ancaman. Sumber daya informasi pada pelayanan publik akan terganggu jika mengalami ancaman yang menyangkut aspek kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability) informasi (Setiawan, 2013). Oleh karena itu, perlu adanya kesiapan dan kewaspadaan terhadap ancaman serangan keamanan informasi pada sistem informasi pelayanan publik di instansi pemerintah.

Keamanan informasi dalam organisasi publik memiliki landasan hukum yang penting untuk memastikan kepatuhan terhadap peraturan dan ketentuan yang berlaku di Indonesia. Beberapa landasan hukum tersebut diantaranya Undang-Undang Nomor 11 Tahun 2008 Republik Indonesia tentang Informasi dan Transaksi Elektronik yang memberikan dasar hukum pengaturan aspek keamanan informasi elektronik dan Keputusan Menteri PAN dan Birokrasi Republik Indonesia Nomor 47 Tahun 2018 yang menjadi acuan penting untuk mengamankan sistem informasi instansi pemerintah. Selain itu, pemerintah Indonesia telah mengeluarkan Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Panduan ini mengacu pada SNI ISO/IEC 27001 yang diterbitkan tahun 2009. Standar tersebut berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI).

Dengan adanya panduan dan standar ini, diharapkan implementasi *e-Government* dapat berjalan dengan aman dan efektif. Dengan demikian, penting bagi instansi pemerintah untuk memahami dan menerapkan konsep keamanan informasi dalam implementasi *e-Government*. Hal ini tidak hanya akan membantu instansi pemerintah dalam memberikan pelayanan yang lebih baik kepada masyarakat, tetapi juga akan membantu dalam melindungi aset informasi yang berharga dari berbagai ancaman.

Dalam rangka meningkatkan keamanan informasi, berbagai teknik telah dikembangkan dan diimplementasikan. Di antara teknik-teknik tersebut, dua yang paling menonjol adalah penetration testing dan vulnerability assessment. Penetration testing adalah proses simulasi serangan dunia nyata yang bertujuan untuk mengidentifikasi dan mengeksploitasi kelemahan dalam sistem keamanan. Teknik ini sangat efektif untuk menguji seberapa baik sistem dapat bertahan dari serangan nyata(Antunes & Vieira, 2015).

Sementara itu, vulnerability assessment merupakan proses identifikasi, penilaian, dan mitigasi kerentanan dalam sistem informasi. Teknik ini biasanya digunakan untuk mengidentifikasi kelemahan yang sudah diketahui dan menyediakan rekomendasi untuk perbaikan sebelum kelemahan tersebut dapat dieksploitasi oleh penyerang(Shah & Mehtre, 2015).

Menurut penelitian terbaru, kombinasi kedua teknik ini, yang dikenal sebagai Vulnerability Assessment and Penetration Testing (VAPT), menawarkan pendekatan

yang lebih komprehensif dalam mengamankan sistem informasi. VAPT memungkinkan identifikasi kerentanan yang lebih menyeluruh dan pengujian eksploitasi yang lebih mendalam, sehingga memberikan gambaran yang lebih jelas tentang tingkat keamanan sistem(Goel & Mehtre, 2015).

Dengan dasar hukum dan standar keamanan informasi yang ada, artikel ini akan mencoba melakukan studi komparatif dari kedua teknik tersebut.

2. Metode Penelitian

Pada penelitian ini, metode penelitian yang digunakan adalah penelitian kualitatif. Penelitian kualitatif adalah penelitian yang bermaksud untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian misalnya perilaku, persepsi, motivasi, tindakan, dan lain-lain secara holistic, dan dengan cara deskripsi dalam bentuk kata-kata dan bahasa, pada suatu konteks khusus yang alamiah dan dengan memanfaatkan berbagai metode alamiah (Moelong, 2014).

3. Hasil dan Pembahasan

Ketika berbicara tentang keamanan sistem, dua konsep yang krusial adalah *vulnerability assessment* (penilaian kerentanan) dan penetration testing (pengujian penetrasi). *Vulnerability assessment* membantu dalam mengidentifikasi dan mengevaluasi kelemahan potensial dalam infrastruktur IT, sementara *penetration testing* adalah proses simulasi serangan nyata untuk menguji sejauh mana keamanan sistem tersebut. Namun, yang lebih menarik adalah bagaimana *vulnerability assessment* dapat menjadi bagian integral dari *penetration testing*, memperkaya proses uji coba penetrasi dengan mengetahui kerentanan-kementeran yang telah diidentifikasi sebelumnya.

3.1 *Vulnerability Assessment*

Kerentanan atau *vulnerability* yang dimiliki oleh sistem maupun program komputer memungkinkan pelaku kejahatan (peretas) untuk mengakses sistem secara ilegal dan mencuri informasi berharga yang ada di dalamnya. Untuk mencegah hal tersebut terjadi, kerentanan atau kelemahan tersebut harus segera diidentifikasi dan diperbaiki. Memperbaiki kerentanan yang ada pada suatu sistem dengan cepat adalah salah satu upaya untuk memperkuat keamanan informasi dari sistem tersebut sehingga informasi berharga yang ada di dalamnya dapat terlindungi dengan baik. Organisasi-organisasi penting seperti bank, rumah sakit, dan pemerintah punya aturan (kebijakan) untuk melindungi data dan sistem mereka. Organisasi harus segera memperbaiki kerentanan dalam perangkat lunak dan sistem mereka untuk melindungi data, layanan, dan informasi rahasia mereka dari peretas (Russo et al., 2019).

Vulnerability Assessment (VA) merupakan proses untuk mengidentifikasi kerentanan atau celah keamanan dalam suatu sistem komputer (Shinde & Ardhapurkar, 2016). Proses VA terbagi ke dalam tiga tahap utama yaitu pengumpulan informasi, analisis kerentanan, dan pelaporan seperti yang ditunjukkan oleh Gambar 1 (Al Shebli & Beheshti, 2018)(Patel, 2019)

Tahap pengumpulan informasi diawali dengan mengidentifikasi tujuan dan sumber daya yang dibutuhkan untuk melakukan serangkaian proses VA. Proses VA dapat dilakukan secara manual maupun otomatis untuk mempercepat proses identifikasi agar lebih efisien. Di tahap ini, informasi rinci terkait perangkat lunak maupun perangkat keras yang membangun sistem yang akan diuji dikumpulkan. Seluruh informasi yang dibutuhkan untuk analisis keamanan seperti konfigurasi sistem, versi perangkat lunak, desain jaringan, data yang tersimpan, hingga riwayat celah keamanan yang sebelumnya

SATIN – Sains dan Teknologi Informasi
Vol. 10, No. 1, Juni 2024, pp. 25-34
ISSSN: 2527-9114, DOI: 10.33372/stn.v9i2.1000

pernah teridentifikasi pun perlu diidentifikasi pada tahap ini.

Gambar 1. Proses *Vulnerability Assessment*

Proses selanjutnya adalah analisis kerentanan. Tahap analisis kerentanan melibatkan identifikasi kerentanan dalam sistem atau jaringan. Proses ini dapat dilakukan dengan memanfaatkan berbagai alat identifikasi kerentanan. Fokus utama pada tahap ini adalah menemukan celah keamanan yang ada pada target sistem. Pada penelitian (Al Shebli & Beheshti, 2018), tahap analisis kerentanan ini dibagi ke dalam dua jenis, yaitu *code analysis* dan *vulnerability analysis*.

Code analysis dilakukan untuk menemukan kelemahan keamanan dengan menganalisis kode program dari perangkat lunak atau sistem yang dianalisis. Proses tersebut memungkinkan untuk mengidentifikasi sumber utama penyebab kerentanan suatu sistem. Teknik tersebut digunakan untuk menemukan jenis celah keamanan atau kerentanan yang belum pernah teridentifikasi sebelumnya, begitupun dengan solusinya. *Vulnerability analysis* menggunakan alat yang berfungsi untuk mengidentifikasi berbagai jenis kerentanan yang sudah diketahui baik jenis maupun solusinya atau dikenal dengan istilah *Common Vulnerabilities and Exposures* (CVE).

Tahap terakhir dalam proses VA adalah membuat laporan yang berisi daftar kerentanan yang ditemukan beserta tingkat risiko dan rekomendasi perbaikan atau mitigasinya. Rekomendasi perbaikan tersebut dapat berupa pembaruan perangkat lunak atau perbaikan konfigurasi.

Proses VA mengidentifikasi kerentanan dalam suatu sistem berdasarkan pola dari berbagai jenis kerentanan. Banyak pola kerentanan yang umum ditemui di berbagai sistem telah didokumentasikan. Oleh karena itu, proses VA dapat diotomatisasi (Nagpure & Kurkure, 2017). Alat yang digunakan untuk menjalankan VA secara otomatis dapat memindai kerentanan sistem dengan cepat dan efisien, sehingga menghemat waktu.

Kekurangannya dari implementasi proses VA menggunakan alat otomatis adalah alat pendeteksi terkadang dapat keliru mendeteksi sesuatu sebagai kerentanan atau celah keamanan padahal sebenarnya tidak. Hal tersebut dapat terjadi karena alat tersebut mengandalkan pola dan tanda-tanda umum yang sangat mungkin untuk salah interpretasi. Jika itu terjadi, ada waktu dan sumber daya yang terbuang untuk menyelidiki kerentanan yang sebetulnya tidak ada pada sistem (Patel, 2019).

Berbagai alat otomatis untuk mengidentifikasi kerentanan pada proses VA semakin berkembang. Salah satunya adalah pemanfaatan kecerdasan buatan atau *artificial intelligence* (AI). Pemanfaatan AI dalam proses otomatisasi VA memberikan kinerja yang lebih baik dalam mendeteksi kerentanan. (Russo et al., 2019) menciptakan alat bernama CVErizer dengan memanfaatkan pengolahan bahasa alami yang secara otomatis mengidentifikasi dan mengkategorikan kerentanan yang ditemukan. (Pan & Mishra, 2021) mengusulkan alat otomatis untuk mendeteksi *trojan hardware* dalam sirkuit elektronik menggunakan *reinforcement learning*. *Trojan hardware* adalah perangkat pada sirkuit yang ditanam secara ilegal dan

Gambar 2. Proses *Penetration Testing*

dapat membahayakan keamanan dan fungsionalitas sistem. (Li et al., 2022)mengusulkan SySeVR, sebuah *framework* berbasis *deep learning* untuk secara otomatis mendeteksi kerentanan dalam perangkat lunak. SySeVR menggunakan

convolutional neural network (CNN) dan *recurrent neural network* (RNN), untuk menganalisis kode program dan secara otomatis mengidentifikasi potensi kerentanan suatu perangkat lunak.

3.2 *Penetration Testing*

Tak ada yang lebih vital dalam dunia keamanan digital daripada memahami kerentanan sistem. *Penetration testing* adalah salah satu aspek krusial dalam memastikan keamanan sebuah sistem komputer atau jaringan. Melalui serangkaian teknik dan metode, *penetration testing* menggali celah keamanan yang dapat dieksploitasi oleh pihak yang tidak berwenang.

Penetration testing atau pengujian penetrasi adalah teknik pengujian untuk menemukan pemahaman, dan mendokumentasikan semua lubang keamanan yang dapat ditemukan dalam suatu sistem. Ini adalah upaya yang sah untuk melanggar batasan-batasan tertentu yang dinyatakan dalam bentuk kebijakan keamanan atau integritas sebuah data atau sistem (Shravan et al., 2014). Pengujian penetrasi digunakan untuk memeriksa eksploitasi dan kerentanan sistem sebuah dan membantu *developers* untuk membangun sistem yang lebih terlindungi (Abu-Dabaseh & Alshammari, 2018), kemudian pengujian penetrasi juga merupakan langkah penting dalam pengembangan sistem pertahanan berbasis komputer server yang aman dan terhubung dalam suatu jaringan dalam hal apapun karena tidak hanya menekankan operasi, tetapi implementasi serta desain sistem, ini adalah tindakan resmi dan dijadwalkan yang memisahkan tester penetrasi dari penyerang dan telah banyak diadopsi oleh organisasi dan lembaga (Zen et al., 2020).

Proses pengujian penetrasi ditunjukkan pada gambar 2 berikut. Secara garis besar, proses ini dapat dibagi menjadi empat fase (Bechtsoudis & Sklavos, 2012) seperti yang diilustrasikan oleh Gambar 2.

3.2.1 *Planning*

Yang pertama dilakukan pada tahap perencanaan adalah penentuan ruang lingkup pengujian. Persetujuan manajemen, dokumen dan perjanjian seperti NDA (*Non-Disclosure Agreements*) ditandatangani terlebih dahulu di bawah bimbingan departemen hukum dan pengacara yang bertanggung jawab. Setelah persetujuan manajemen, tim pengujian penetrasi mengumpulkan masukan penting tentang prosedur operasional organisasi dan kebijakan keamanan dalam menentukan ruang lingkup pengujian.

3.2.2 *Discovery*

Fase ini disebut juga fase *information gathering*. Selama proses pengumpulan informasi, tim penguji penetrasi meluncurkan prosedur pemindaian dan pencacahan untuk mendapatkan informasi sebanyak mungkin tentang jaringan target dan sistem serta layanan yang berpartisipasi. Fase pengumpulan dapat dibagi lagi menjadi *non-intrusive (public repositories, documents, mailing lists, web profiles* dll.*)* dan *intrusive (port scanning, firewall rules, matching OS fingerprints* dll.*)*. Dengan jumlah informasi yang cukup, tim penguji dapat membuat profil jaringan target dan menghitung kemungkinan atau basis pengetahuan keamanan pribadi target.

3.2.3 *Exploitation*

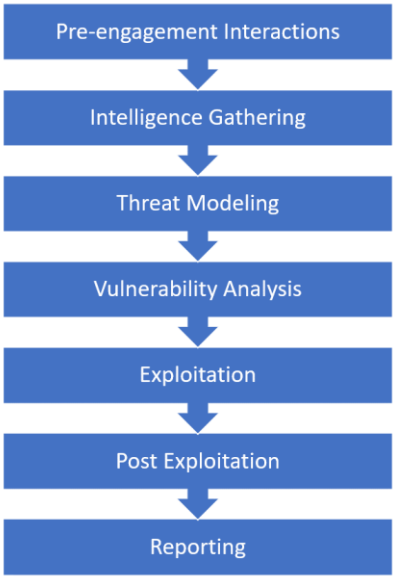
Fase ketiga dan yang paling penting dari uji penetrasi adalah fase eksploitasi. Dengan menggunakan masukin dan data dari kerentanan yang ditemukan dari fase sebelumnya, tim uji penetrasi merevisi bukti konsep eksploitasi yang sesuai dan dapat mengarah ke

SATIN – Sains dan Teknologi Informasi
Vol. 10, No. 1, Juni 2024, pp. 25-34
ISSN: 2527-9114, DOI: 10.33372/stn.v9i2.1000

keamanan atau layanan jaringan. Tergantung pada kesepakatan dengan manajemen dan tingkat implikasi eksploitasi, serangan dapat diluncurkan dalam kerentanan jaringan yang sama dan kesalahan konfigurasi, tim penguji dapat menemukan informasi tambahan yang dapat memberi umpan balik pada fase *discovery*. fase *discovery*, menghasilkan skenario serangan dan eksploitasi baru. Interaksi antara fase *discovery* dan fase eksploitasi terus berlanjut selama pengujian yang sebenarnya.

3.2.4 *Reporting*

Tahap terakhir yang melengkapi proses *penetration test* adalah tahap pelaporan. Penulisan laporan dapat dimulai secara paralel dengan tiga tahap lainnya, meskipun harus diselesaikan setelah tahap eksploitasi selesai. Laporan yang sukses adalah yang merinci semua temuan dan dampaknya terhadap organisasi dengan mempertimbangkan aspek teknis dan



Gambar 3. *Penetration Testing Execution Standard* (PTES)

manajemen untuk membuat laporan yang lengkap dan terdokumentasi dengan baik untuk menginformasikan kepada manajemen tentang risiko keamanan dan memberikan rincian teknis dan rekomendasi tingkat tinggi kepada departemen *ICT*.

Model pengujian penetrasi dikategorikan menjadi tiga bagian; *white box*, *grey box*, dan *black box*. *White box* menggambarkan pengujian yang di mana penguji memiliki pengetahuan lengkap tentang infrastruktur yang akan diuji (Liu et al., 2012). *Black* box, sebaliknya, mengasumsikan bahwa tidak ada pengetahuan sebelumnya tentang lingkungan yang akan diuji atau *environment test*-nya. Sebagian besar studi dan makalah penelitian, terutama seputar *vulnerability discovery tools* melakukan pengujian dengan model *black box* (Antunes & Vieira, 2015b). Sementara itu *grey box test* mewakili jalan tengah antara *black box* dan *white box* di mana jumlah informasi tentang target kerap kali tidak lengkap atau bahkan tidak ada. Adapun *tools* yang terkategorikan memenuhi untuk melakukan pengujian penetrasi ini terbilang cukup banyak dan beragam, diantaranya yaitu: *Wireshark*, *Metasploit*, *Nmap*, *Webinspect* dan lain sebagainya (Dalalana Bertoglio & Zorzo, 2017).

3.3 Penerapan *Vulnerability Assessment* pada *Penetration Testing*

VAPT adalah metode keamanan informasi yang menggabungkan dua teknik untuk menemukan dan memperbaiki kerentanan pada sistem. VA adalah teknik untuk menemukan kerentanan, sedangkan PT adalah teknik untuk menguji kerentanan tersebut. PT memanfaatkan kerentanan yang ditemukan VA untuk mencoba mengeksploitasi sistem dan mengukur dampak yang akan terjadi. Laporan PT kemudian memberikan rekomendasi perbaikan untuk memperkuat keamanan sistem (Patel, 2019).

Pada penelitian (Haubris & Pauli, 2013), (Al Shebli & Beheshti, 2018), (Patel, 2019), *vulnerability analysis* atau *vulnerability identification* menjadi bagian dari proses PT. menunjukkan tahapan pada proses PT sesuai dengan PTES atau *Penetration Testing Execution Standard* (Haubris & Pauli, 2013). Pada standar tersebut, proses *penetration testing* mencakup fase *assessment* yang salah satu aktivitasnya adalah mengidentifikasi kerentanan yang ada pada sistem.

Proses VA dapat menjadi langkah awal yang dapat dilakukan untuk mengidentifikasi kelemahan dari keamanan yang terdapat pada sistem. Proses ini dapat dilakukan secara rutin untuk mengetahui potensi kerentanan di sistem. Namun, jika dibutuhkan evaluasi yang lebih menyeluruh, mengkombinasikan VA dengan PT (atau VAPT) adalah pilihan yang lebih baik. Dengan melakukan *vulnerability exploits* dari hasil yang telah diperoleh pada proses VA, risiko akibat kerentanan yang ada dapat dianalisis dan dievaluasi secara mendalam. Kerusakan sistem yang dapat terjadi karena kerentan tersebut juga dapat diminimalisir (Al Shebli & Beheshti, 2018).

3.4 Penerapan teknik analisis keamanan sistem informasi yang efektif untuk digunakan pada pelayanan publik

Dalam konteks pelayanan publik, seperti yang sebelumnya dipaparkan pada awal pendahuluan, keamanan sistem informasi menjadi sangat penting. Hal ini dikarenakan banyaknya informasi yang harus dikelola dengan tingkat sensitivitas yang cukup tinggi (Solms, 2001). Oleh karena itu, sektor keamanan harus menjadi fokus utama dalam melakukan penerapan layanan publik (Ibrahim et al., 2020).

E-Government atau Sistem Pemerintahan Berbasis Elektronik (SPBE) adalah salah satu contoh implementasi sistem informasi dalam pelayanan publik. SPBE diharapkan mampu memberikan layanan kepada masyarakat dengan lebih efektif dan efisien. Namun, seiring dengan perkembangan teknologi, sering kali terjadi penyalahgunaan oleh beberapa pihak yang tidak bertanggung jawab yang dapat menimbulkan ancaman keamanan (Hassan & Khalifa, 2016).

Untuk itu, dibutuhkan pemetaan serius tentang bagaimana kondisi aman dalam pengembangan implementasi SPBE. Salah satu cara yang dapat dilakukan adalah dengan menerapkan teknik analisis keamanan sistem informasi, seperti Penetration Testing dan Vulnerability Assessment, dengan sebagaimana sudah dipaparkan pada bahasan sebelumnya. Kedua teknik ini memiliki peran penting dalam memastikan keamanan sistem informasi pada pelayanan publik. Dengan menerapkan kedua teknik ini, pemerintah dapat memprioritaskan lebih banyak faktor keselamatan dalam menerapkan SPBE (Hassan & Khalifa, 2016).

Sebagaimana sebelumnya disampaikan bahwa *penetration testing* dan *vulnerability assessment* memiliki perbedaan mendasar dalam pendekatan mereka terhadap analisis keamanan sistem informasi. *Penetration testing* lebih berfokus pada penemuan celah keamanan dan mencoba mengeksploitasi celah tersebut, sedangkan *vulnerability assessment* lebih berfokus pada identifikasi dan penilaian kerentanan sistem (Goel & Mehtre, 2015).

Dalam konteks pelayanan publik, kedua teknik ini dapat digunakan secara bersamaan untuk memberikan gambaran yang lebih komprehensif tentang keamanan sistem informasi. *Penetration testing* dapat digunakan untuk mengetahui sejauh mana sistem dapat bertahan terhadap serangan, sedangkan *vulnerability assessment* dapat digunakan untuk mengetahui area mana yang paling rentan dan memerlukan perbaikan (Goel & Mehtre, 2015).

Selanjutnya, dalam memilih antara *penetration testing* dan *vulnerability assessment*, beberapa faktor perlu dipertimbangkan. Pertama, tujuan dari analisis keamanan sistem informasi. Jika tujuannya adalah untuk mengetahui sejauh mana sistem dapat bertahan terhadap serangan, maka *penetration testing* mungkin lebih cocok. Namun, jika tujuannya adalah untuk mengetahui area mana yang paling rentan dan memerlukan perbaikan, maka *vulnerability assessment* mungkin lebih

cocok. Kedua, sumber daya yang tersedia. Penetration Testing biasanya memerlukan lebih banyak sumber daya dibandingkan dengan *vulnerability assessment*, baik dari segi waktu maupun tenaga kerja. Oleh karena itu, jika sumber daya terbatas, *vulnerability assessment* mungkin menjadi pilihan yang lebih baik. Ketiga, tingkat keahlian tim keamanan sistem informasi. *Penetration testing* biasanya memerlukan tingkat keahlian yang lebih tinggi dibandingkan dengan *vulnerability assessment*. Oleh karena itu, jika tim keamanan sistem informasi tidak memiliki keahlian yang cukup, maka *vulnerability assessment* mungkin menjadi pilihan yang lebih baik (Shah & Mehtre, 2015).

Namun, dalam penerapannya, perlu diperhatikan bahwa tidak semua teknik analisis keamanan sistem informasi cocok untuk setiap jenis pelayanan publik. Oleh karena itu, penting untuk melakukan evaluasi dan penyesuaian terhadap teknik yang digunakan berdasarkan karakteristik dan kebutuhan spesifik dari pelayanan publik yang bersangkutan.

4. Simpulan

Pada penelitian ini, dapat disimpulkan bahwa keamanan informasi merupakan aspek yang krusial dalam era digital saat ini. Dua teknik utama dalam menangani keamanan sistem, yaitu Vulnerability Assessment (VA) dan Penetration Testing (PT), memiliki peran penting dalam melindungi sistem dan data dari ancaman peretas. VA membantu dalam mengidentifikasi kerentanan yang ada dalam sistem secara lebih terinci, sedangkan PT membantu menguji kerentanan tersebut dengan mencoba mengeksploitasi sistem guna mengukur dampak yang mungkin terjadi. Kedua teknik ini saling melengkapi: VA sebagai langkah awal dalam mengidentifikasi kelemahan keamanan, sementara PT sebagai uji coba seberapa kuat sistem melawan potensi serangan. Kombinasi keduanya, yang dikenal sebagai Vulnerability Assessment and Penetration Testing (VAPT), memberikan pemahaman yang lebih dalam tentang kerentanan sistem dan memberikan rekomendasi perbaikan yang konkrit. Metode ini dapat diterapkan secara rutin untuk memastikan sistem terlindungi secara optimal. Namun, perlu diingat bahwa proses ini bukanlah solusi akhir, melainkan sebuah langkah yang harus terus menerus diperbarui dan disempurnakan seiring evolusi teknologi dan serangan yang semakin kompleks. Kesadaran terhadap risiko dan upaya yang berkelanjutan dalam meningkatkan keamanan sistem sangatlah penting untuk melindungi informasi berharga dari ancaman yang terus berkembang di dunia digital saat ini. Sementara itu, pemilihan implementasi kedua teknik analisis keamanan sistem tersebut pada konteks pelayanan publik harus disesuaikan dengan kebutuhan yang ada berdasarkan aspek-aspek yang satu sama lain juga berhubungan.

5. Referensi

Abu-Dabaseh, F., & Alshammari, E. (2018). *Automated Penetration Testing : An Overview*. https://doi.org/10.5121/csit.2018.80610

Al Shebli, H. M. Z., & Beheshti, B. D. (2018). A study on penetration testing process and tools. *2018 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2018*. https://doi.org/10.1109/LISAT.2018.8378035

Antunes, N., & Vieira, M. (2015a). Assessing and Comparing Vulnerability Detection Tools for Web Services: Benchmarking Approach and Examples. *IEEE Transactions on Services Computing*, *8*(2), 269–283. https://doi.org/10.1109/TSC.2014.2310221

Antunes, N., & Vieira, M. (2015b). Assessing and Comparing Vulnerability Detection Tools for Web Services: Benchmarking Approach and Examples. *IEEE Transactions on Services Computing*, *8*(2). https://doi.org/10.1109/TSC.2014.2310221

Bechtsoudis, A., & Sklavos, N. (2012). Aiming at higher network security through extensive penetration tests. *IEEE Latin America Transactions*, *10*(3). https://doi.org/10.1109/TLA.2012.6222581

Dalalana Bertoglio, D., & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer*

Society, *23*(1). https://doi.org/10.1186/s13173-017-0051-1

Goel, J. N., & Mehtre, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science*, *57*, 710–715. https://doi.org/10.1016/j.procs.2015.07.458

Hartono, Utomo, D., & Mulyanto, E. (2010). Electronic Government Pemberdayaan Pemerintahan Dan Potensi Desa Berbasis Web. *Jurnal Teknologi Informasi*, *6*(April).

Hassan, R. G., & Khalifa, O. O. (2016). E-Government-an Information Security Perspective. *International Journal of Computer Trends and Technology*, *36*(1). http://www.ijcttjournal.org

Haubris, K. P., & Pauli, J. J. (2013). Improving the efficiency and effectiveness of penetration test automation. *Proceedings of the 2013 10th International Conference on Information Technology: New Generations, ITNG 2013*. https://doi.org/10.1109/ITNG.2013.135

Ibrahim, A., Arief, A., & Do Abdullah, S. (n.d.). PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE): SEBUAH KAJIAN PUSTAKA SISTEMATIS SECURITY FOR E-GOVERNMENT IN PUBLICK SERVICES IMPLEMENTATION: A SYSTEMATIC LITERATURE REVIEW. In *IJIS Indonesian Journal on Information System*.

Li, Z., Zou, D., Xu, S., Jin, H., Zhu, Y., & Chen, Z. (2022). SySeVR: A Framework for Using Deep Learning to Detect Software Vulnerabilities. *IEEE Transactions on Dependable and Secure Computing*, *19*(4). https://doi.org/10.1109/TDSC.2021.3051525

Liu, B., Shi, L., Cai, Z., & Li, M. (2012). Software vulnerability discovery techniques: A survey. *Proceedings - 2012 4th International Conference on Multimedia and Security, MINES 2012*, 152–156. https://doi.org/10.1109/MINES.2012.202

Moelong, L. J. (2014). Metodologi Penelitian Kualitatif. In *PT. Remaja Rosdakarya*.

Nagpure, S., & Kurkure, S. (2017). Vulnerability Assessment and Penetration Testing of Web Application. *2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017*. https://doi.org/10.1109/ICCUBEA.2017.8463920

Pan, Z., & Mishra, P. (2021). Automated Test Generation for Hardware Trojan Detection using Reinforcement Learning. *Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC*. https://doi.org/10.1145/3394885.3431595

Patel, K. (2019). A survey on vulnerability assessment penetration testing for secure communication. *Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019*. https://doi.org/10.1109/ICOEI.2019.8862767

Russo, E. R., Di Sorbo, A., Visaggio, C. A., & Canfora, G. (2019). Summarizing vulnerabilities' descriptions to support experts during vulnerability assessment activities. *Journal of Systems and Software*, *156*. https://doi.org/10.1016/j.jss.2019.06.001

Setiawan, A. B. (2013). Kajian Kesiapan Keamanan Informasi Instansi Pemerintah dalam Penerapan E-government. *Masyarakat Telematika Dan Informasi*, *4*(2), 109–126.

Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, *11*(1), 27–49. https://doi.org/10.1007/s11416-014-0231-x

Shinde, P. S., & Ardhapurkar, S. B. (2016). Cyber security analysis using vulnerability assessment and penetration testing. *IEEE WCTFTR 2016 - Proceedings of 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare*. https://doi.org/10.1109/STARTUP.2016.7583912

Shravan, K., Neha, B., & Pawan, B. (2014). Penetration Testing : A Review. *Compusoft*, *3*(Iv).

Zen, B. P., Gultom, R. A. G., & Reksoprodjo, A. H. S. (2020). Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara. *Jurnal Teknologi Penginderaan*, *2*(1).