BAB II
TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Penelitian terdahulu dari (Silmina et al., 2022) yang berjudul Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test dan ISSAF. Perkembangan teknologi di era industri 4.0 telah berkembang pesat, salah satunya Sistem Informasi Sekolah. Pada MTsN 8 Bantul, telah dibuat Sistem Informasi Sekolah untuk memudahkan pengolahan data sekolah. Sistem ini masih belum diluncurkan karena belum melalui proses pencarian celah keamanan jaringan. Tujuan penelitian ini untuk mencari celah keamanan dan mengetahui tingkat keamanan jaringan untuk menghindari adanya tindakan yang tidak diinginkan seperti pencurian data atau penyalahgunaan hak akses. Metode yang digunakan pada penelitian ini adalah *Information System Security Assessment Framework (ISSAF)*. ISSAF digunakan untuk mengkategorikan penilaian keamanan sistem informasi. Penetration Test juga digunakan untuk pengujian keamanan dengan menggunakan tool yang sudah ditentukan yaitu Kali linux, Nmap, dan WireShark. Hasil dari penetrasi menggunakan 3 tool menunjukkan bahwa tool Kali linux tidak mengeluarkan hasil yang diharapkan, WireShark tidak support untuk capturing pada Localhost, dan Nmap yang menampilkan 11 data pada setiap percobaan sebanyak 10 kali. Hasil dari penetrasi pada Nmap dihitung langsung menggunakan Algoritma Naive Bayes yang menghasilkan nilai akurasi 72,72% dan telah memenuhi Threshold Limit Value sebesar 70%. Hasil akurasi ini menunjukkan bahwa Sistem Informasi Sekolah MTsN 8 Bantul aman dari celah keamanan.

Penelitian terdahulu dari (Agus Rochman, Rizal Rohian Salam, 2021) yang berjudul analisis keamanan *website* dengan *information system security assessment framework (ISSAF)* dan open web application security project (OWASP) di rumah

sakit xyz. Sistem keamanan komputer semakin dibutuhkan seiring dengan meningkatnya pengguna yang terhubung ke jaringan internet, hal ini dapat memicu terjadinya tindak kejahatan *cyber* oleh orang yang tidak bertanggung jawab. Penelitian ini dilakukan pada Sistem Informasi sebuah Rumah Sakit. Salah satunya web server untuk informasi HRD. Sistem ini berisikan data karyawan dan data absensi karyawan. Keamanan webserver biasanya merupakan masalah bagi administrator. Sering kalipermasalahan tersebut terabaikan dan permasalahan dapat ditelusuri ketika terjadi bencana. Berdasarkan latar belakang tersebut, maka dibutuhkan evaluasi mengenai adanya celah keamanan *(vulnerability)* dan kelemahan dari website sistem informasi HRD. Metode penelitian menggunakan Information *System Security.*

Penelitian terdahulu dari (Syarif Revolino & Jatmiko Andri, 2019) yang berjudul Analisis Perbandingan Metode Web Security Ptes, ISSAF Dan OWASP Di Dinas Komunikasi Dan Informasi Kota Bandung. Saat ini perkembangan teknologi di bidang informasi telah merambat ke pelosok bagian di tanah air, baik di desa, kecamatan, kabupaten dan kota sudah mulai memiliki divisi yang menerapkan sistem penyebaran informasi kepada masyarakat dengan menggunakan *website* dan salah satu pihak yang bertanggung jawab di dalam pelayanan penyebaran informasi di Kota Bandung adalah Diskominfo. Namun demikian, dengan digunakannya *website* sebagai media pelayanan informasi masyarakat oleh pemerintah, akan sangat memungkinkan jika *website* tersebut dapat diserang oleh orang-orang yang tidak bertanggung jawab yang dapat menimbulkan kerugian dan terganggunya pelayanan informasi pemerintah ke masyarakat. Salah satu upaya pencegahan hal tersebut ialah *Penetration Testing*. *Penetration Testing,* atau bisa juga disebut *Pen Testing,* merupakan sebuah percobaan untuk menemukan kerentanan pada sistem komputer, jaringan komputer, ataupun aplikasi web, yang dimana kerentanan tersebut dapat dimanfaatkan oleh penyerang. Pada penelitian kali ini akan membandingkan tiga *Penetration Testing Framework,* yaitu PTES, ISSAF, dan OWASP. Hasil dari penelitian inidiharapkan dapat mebantu pihak DISKOMINFO kota Bandung dalam mengelola *website* dan memberikan pemahaman tentang perbedaan ketiga *Framework* tersebut.

Penelitian terdahulu dari (Ojs & Lancang, 2020) yang berjudul Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode ISSAF Dan OWASP (Studi Kasus Ojs Universitas Lancang Kuning). Perkembangan teknologi informasi yang begitu pesat memberikan dampak positif dalam berbagai bidang, salah satunya adalah teknologi internet. Website menjadi alternatif bagi institusi dalam mempromosikan kepada masyarakat umum. Website juga mudah diakses oleh banyak orang, yang tidak kenal tempat maupun waktu. Dengan adanya kemudahan tersebut, banyak instansi membangun web server tanpa memperhatikan apakah web server yang dibangun sesuai dengan standar keamanan atau tidak, apakah sistem yang dibangun sudah aman atau ada gangguan. Universitas Lancang Kuning mempunyai web server yang berisi banyak sistem informasi dan dokumen yangdipublikasi bagi pengguna. Salah satu sistem yang paling krusial adalah sistem Open Journal System (OJS). Menurut informasi dari PDPT Universitas Lancang Kuning, bahwa sistem OpenJournal System (OJS) sudah dua kali terjadi cracking. Kerusakan terhadap OJS ini mengakibatkan data yang terdapatpada sistem OJS hilang, bahkan author sering komlain kepada pengelola jurnal. Pengujian terhadap web server sangatlah penting dilakukan, pengujian ini bertujuan untuk menguji apakah web server sudah aman atau belumdari tindak kejahatan para hacker. Dalam pengujian penetrasi adabeberapa metode yang sering dipakai seperti Information Systems Security Assessment Framework (ISSAF), OWASP. Pada penelitian ini digunakan metode ISSAF dan OWASP versi 4. Metode penelitian yang digunakan pada penelitian ini diantaranya adalah studi literatur, pengumpulan data, pengujian penetrasi menggunakan metode ISSAF dan OWASP, dan analisa dan laporan. Adapun tujuan penelitianini adalah bagaimana menganalisis keamanan sistem Open Journal System (OJS) menggunakan metode ISSAF dan OWASP pada Universitas Lancang Kuning. Berdasarkan pengujian yang telah dilakukan menggunakan metode ISSAF dan OWASP, sistem OJS Universitas Lancang tergolong aman, karena tidak mampu untuk ditembus. Walaupun OJS Universitas Lancang Kuning tergolong aman, serangan bisa saja terjadi dari dalam institusi.

Penelitian terdahulu dari (Zein, 2022) yang berjudul Evaluasi Keamanan Wireless LAN Menggunakan ISSAF (Information System Security Assesment

Framework). Di era teknologi digital, perkembangan teknologi jaringan wireless sangat berperan dalam menunjang kegiatan pada semua bidang pekerjaan baik dikantor-kantor maupun ditempat lainnya. Pada saat initeknologi mengalami booming untuk digunakan sebagai akses jaringan dan internet hotspot. Namun banyak sekali perusahaan, institusi dan perumahan melakukan implementasi jaringan wireless dengan tidak memperdulikan tingkat kemanannya, baik kerentanan potensial yang diakibatkan oleh sistem yang lemah atau konfigurasi sistem yang tidak sesuai atau kelemahan operasional dalam hal teknis. Selain itu, penyerangan jaringan wirelessbegitu sangat mudah dilakukan oleh banyak orang dikarenakan sifat jaringan wireless yang menggunakan teknologi gelombang radio dalam mengirimkan paket datanya sehingga sangat rentan sekali terhadap serangan-serangan.

Penelitian terdahulu dari (Boke, 2022) yang berjudul Web SecurityVulnerability Analysis In Selected Ethiopian Governmental Offices (Using White Box And Black Box Testing). Keamanan dunia maya adalah tindakan untuk memastikan data dan sistem data dengan langkah-langkah keamanan prosedural dan inovatif yang sesuai. Ancaman keamanan siber berkembang dari waktu ke waktu. Kerentanan keamanan web adalah ketidaksempurnaan atau kekurangan dalam sistem komputer, strategi keamanan, kontrol internal, atau rencana dan pelaksanaannya, yang dapat disalahgunakan untuk menyalahgunakan kebijakan keamanan kerangka kerja. Kerentanan keamanan web dapat memengaruhi negara dan dapat mengganggu bidang sosial, keuangan, dan politik pemerintah. Analisis kerentanan adalah serangkaian latihan yang dilakukan untuk mengenali kekurangan dan celah untuk mengeksploitasi kerentanan keamanan.

Penelitian terdahulu dari (Abu-Dabaseh & Alshammari, 2018) yang berjudul Automated Penetration Testing: An Overview. Penggunaan sumber daya teknologi informasi yang meningkat pesat di organisasi, bisnis, dan bahkan pemerintahan, menyebabkan munculnya berbagai serangan, dan kerentanan di lapangan. Semua sumber daya menjadikannya suatu keharusan untuk sering melakukan uji penetrasi (PT) untuk lingkungan dan melihat apa yang dapat diperoleh penyerang dan apa

kerentanan lingkungan saat ini. Makalah ini mengulas beberapa teknik pengujian penetrasi otomatis dan menyajikan peningkatannya atas pendekatan manual tradisional. Sepengetahuan kami, ini adalah penelitian pertama yang mempertimbangkan konsep pengujian penetrasi dan standar di area tersebut. Penelitian ini menangani perbandingan antara pengujian penetrasi manual dan otomatis, alat utama yang digunakan dalam pengujian penetrasi. Selain itu, bandingkan beberapa metodologi yang digunakan untuk membangun platform pengujian penetrasi otomatis.

Penelitian terdahulu dari (Collins, 2021) yang berjudul Pen Testing Framework for IoT Devices. Kerangka Pen-Testing saat ini fokus pada menemukan cacat dalam desain Aplikasi Web dan server Jaringan, mengidentifikasi vektor serangan yang paling mungkin, dan memperkenalkan strategi mitigasi untuk meminimalkan potensi kerusakannya. Tantangannya adalah mengadaptasi kerangka Pen-Testing yang cocok untuk digunakan dengan perangkat IoT. Penelitian ini mengusulkan untuk membuat Pen-Testing Framework yang akan ditujukan untuk perangkat IoT yang karena kendala memori dan daya pemrosesan yang lebih kecil perlu ditangani secara berbeda dalam uji penetrasi. Kerangka Pen-Testing diterapkan ke jaringan Mikrokontroler ESP32 dalam proyek IoT yang digunakan untuk mengumpulkan data suhu dan kelembapan dari sensor, memeriksa status sakelar tombol tekan, dan memantau output dari Mikrokontroler. Ini adalah proyek IoT tipikal dengan standar pengkodean dasar dan berisi pertimbangan keamanan minimal. Kerangka Pen-Testing akan digunakan untuk mengevaluasi masalah yang diuraikan dalam tinjauan pustaka dengan memberikan perhatian khusus pada standar dan pedoman peraturan yang berkembang.

Penelitian terdahulu dari (Rusdan et al., 2020) yang berjudul Evaluation of Wireless Network Security Using Information System Security Assessment Framework (ISSAF) (Case Study: PT. Keberlanjutan Strategis Indonesia). Tujuan penelitian ini dilakukan untuk mengetahui tingkat kerentanan jaringan nirkabel menggunakan ISSAF dengan pengujian penetrasi dan membuat rencana, penilaian, dan laporan evaluasi keamanan jaringan nirkabel yang dapat digunakan sebagai

pedoman untuk melakukan pengujian penetrasi pada suatu organisasi atau perusahaan. Penelitian dilakukan dengan pendekatan penelitian tindakan yang dibagi menjadi beberapa tahapan yaitu diagnosa, perencanaan tindakan, intervensi, evaluasi, dan refleksi. Kemudian untuk proses evaluasi keamanan jaringan wireless dengan menerapkan ISSAF Penetration Testing. Hasil pengujian tingkat kerentanan jaringan wireless PT. Keberlanjutan Strategis Indonesia menggunakan ISSAF dengan pengujian penetrasi menunjukkan bahwa hasil keseluruhan dari keempat jenis pengujian menunjukkan rata-rata tingkat kerentanan adalah 0,8 dengan kata lain keseluruhan jaringan nirkabel di PT. Keberlanjutan Strategis Indonesia memiliki tingkat kerentanan yang tinggi. Keluaran dari setiap tahapan yaitu tahap perencanaan dan persiapan menghasilkan dokumen kebijakan dan kesepakatan, tahap penilaian menghasilkan dokumen penilaian, dan tahap pelaporan, pembersihan, dan pemusnahan artefak menghasilkan dokumen evaluasi. Keluaran yang dihasilkan pada setiap fase menentukan fase selanjutnya sehingga ketiga fase tersebut merupakan rangkaian proses yang tidak dapat dipisahkan.

Penelitian terdahulu dari (van den Hout, 2019) yang berjudul Standardised penetration testing? Examining the usefulness of current penetration testing methodologies. Sebuah studi kasus industri pengujian penetrasi Belanda. Pengujian penetrasi adalah salah satu pendekatan utama yang diambil oleh perusahaan untuk mendapatkan jaminan keamanan teknologi informasi mereka. Tes penetrasi mencakup simulasi penyerang dan pengujian persyaratan keamanan negatif (pada dasarnya menguji apakah ada sesuatu yang tidak mungkin dikompromikan) yang dapat membuat hasil yang andal menjadi sangat sulit, jika bukan tidak mungkin. Beberapa metodologi telah dibuat dan diterbitkan untuk membantu penguji dalam melakukan tes penetrasi berkualitas tinggi. Metodologi ini, bagaimanapun, tampaknya digunakan sampai batas yang sangat terbatas. Tidak jelas mengapa hal ini terjadi dan bagaimana hal ini mempengaruhi kualitas tes penetrasi.

Penelitian terdahulu dari (Nasser et al., 2020) yang berjudul On The Standardization Practices of the Information Security Operations in Banking Sector: Evidence from Yemen. Makalah ini bertujuan untuk membahas keefektifan

kontrol standardisasi operasi keamanan informasi di bank-bank Yaman dengan menyelidiki persyaratan utama penerapannya untuk menjalankan peran keamanan mereka secara efektif. Juga untuk menentukan kelemahan utama praktik standardisasi dalam sistem manajemen keamanan informasi (ISMS) sektor perbankan dan untuk memberikan rekomendasi perbaikan yang diperlukan berdasarkan standar keamanan internasional ISO 27002-2013. Para peneliti merancang kuesioner yang dibagikan kepada pekerja yang bertanggung jawab atas pernyataan keamanan informasi di 13 bank yang diatur oleh bank sentral Yaman, di Sana'a. Hasilnya menunjukkan bahwa tingkat kematangan aktual praktik-praktik tersebut adalah 3,66 dari 5, yang berarti praktik-praktik terbaik tidak diikuti secara konsisten. Kesenjangan antara tingkat kematangan aplikasi nyata praktik keamanan informasi dan tingkat yang kuat ditemukan; sama dengan 1,34, yang berarti ISMS di sektor ini tidak memiliki sebagian besar persyaratan keamanan yang diperlukan untuk fungsinya yang praktis dan kuat. Dua titik kekuatan signifikan ditentukan. Tiga kekurangan dan kelemahan utama ditemukan, dan tindakan perbaikan serta rekomendasi telah disarankan untuk meningkatkan praktik standardisasi operasi keamanan informasi di sektor ini. Skema pemetaan matriks implementasi tambahan dan panduan implementasi berbasis ISO untuk setiap bank telah direkomendasikan.

B. Landasan Teori

1. Analisis

Pengertian analisis secara umum adalah sebuah kemampuan memecahkan atau menguraikan suatu materi atau informasi menjadi komponen-komponen yang lebih kecil sehingga lebih mudah dipahami. Analisis dapat diartikan sebagai usaha dalam mengamati sesuatu secara mendetail dengan cara menguraikan komponen pembentuknya atau menyusun sebuah komponen untuk kemudian dikaji lebih mendalam.

Pengertian analisis menurut Dwi Prastowo Darminto adalah penguraian suatu pokok atas berbagai bagiannya dan penelaahan bagian itu sendiri, serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan. (Dwi Prastowo Darminto, 2022)

2. Website

Website adalah kumpulan halaman web yang saling terhubung dan seluruh file saling terkait. Web terdiri dari page atau halamandan kumpulan halaman yang dinamakan *homepage*. *Homepage* berada pada posisi teratasdengan halaman-halaman terkait berada di bawahnya. Biasanya, setiap halaman di bawah *homepage (child page)* berisi *hyperlink*ke halaman lain dalam web. (Puspitasari, 2020)

Dalam pengaksesan website pengguna hanya perlu menggunakan *smartphone* ataupun perangkat komputer dalam mengakses. Website terdiridari dua jenis yaitu :

a. *Website* Statis (*Static Website*) adalah *web* yang biasanya *user* tidak bisa mengubah *content* dari *web* tersebut secara langsung menggunakan *browser*. Interaksi yang terjadi hanya seputar pemrosesan *link* yang ada.

b. *Website* Dinamis (*Dynamic Website*) adalah *web* yangbiasanya *user* dapat mengubah *content* dari halaman tertentu dengan menggunakan *browser.*

3. Informasi System Security Assessment Framework

Information System Security Assessment Framework (ISSAF) adalah standar pengujian penetrasi yang digunakan untuk menguji ketahanan situs web, yang memiliki beberapa keunggulan dibandingkan control keamanan lainnya, dan berfungsi sebagai jembatan antara pandangan teknis dan manajerial. (Yudiana et al., 2021)

4. Penetration Testing

Penetration Testing adalah suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan organisasi atau perusahaan tertentu untuk menemukan kelemahan yang adapada sistem jaringan tersebut.

Penetration Testing adalah metode penilaiandengan cara menguji kelemahan dari keamanan sistem, jaringan komputer ataupun kelemahan program aplikasi web. Dengan melakukan serangan langsung terhadap target atau sistem yang akan diuji. Hasil dari pengujian ini dapat menjadi masukan untuk memperbaiki kelemahan sistem yang terdeteksi, sehingga dapat meningkatkan keamanan dan guna menghindari serangan cyber yang dapat terjadi kapan saja.

Metode ini memiliki 3 metode yang berbeda berdasarkan jangkauan lingkungan dan jenis target yaitu *black box testing*, *white box* testing dan *grey box testing*. (Hanafi et al., 2019)

Berikut penjelasan 3 metode pentest sebagai berikut :

a. Black box Testing

Dalam metode ini, penguji melakukan serangan tanpa mengetahui infrastruktur yang digunakan oleh target. Penguji harus mencari tahu semua kerentanan dalam keamanan sistem berdasarkan kemampuan serta pengetahuan mereka. Metode *black box* ini digunakan untuk mengaudit keamanan sistem dengan penyerang eksternal untuk melakukan serangan pada celah kerentanan yang ditemukan.

b. White Box Testing

Dalam metode ini, penguji diberikan semua informasi terkait infrastruktur keamanan sistem target yang akan diuji dan dilakukannya audit keamanan sistem dari internal. Serangan yang dilakukan dengan mensimulasikan jika bahaya terjadi dalam lingkungan internal.

c. Greybox Testing

Dalam metode ini, metode *grey box* merupakan gabungan dari 2 metode yaitu *black box* dan *white box*. Penguji diberikan informasi terkait infrastruktur keamanan sistem tapi juga harus mencari informasi sendiri untuk menemukan celah kerentanan sistem.