BAB I
PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi informasi pada Kantor Sekretariat Yayasan Masjid Agung Sungailiat telah membawa banyak manfaat, tetapi juga menimbulkan tantangan keamanan. Di Kantor Sekretariat menyimpan data sensitif dan kritis, termasuk data penting, informasi pribadi, dan hak kekayaan intelektual. Ancaman keamanan seperti serangan siber, peretasan, dan kebocoran data dapat menyebabkan dampak serius. Pada Kantor Sekretariat Yayasan Masjid Agung Sungailiat, kerentanan dan celah keamanan dalam sistem jaringan seringkali tidak terdeteksi dengan tepat. Di kantor menghadapi keterbatasan melakukan pengujian keamanan secara menyeluruh.

Selain itu, metode pengujian tradisional seringkali kurang efisien dan efektif dalam mengidentifikasi dan mengatasi kerentanan yang ada. Untuk mengatasi masalah tersebut, diperlukan pendekatan yang komprehensif dan proaktif dalam mengelola keamanan jaringan di Kantor Sekretariat Yayasan Masjid Agung Sungailiat. Pengujian kerentanan dengan metode *Vulnerability Assessment* dan metode NDLC (*Network Devploment Life Cycle*) solusi yang tepat untuk mengidentifikasi, mengukur, dan mengurangi risiko keamanan dalam sistem jaringan. Dengan menggunakan metode ini, Kantor dapat secara aktif mencari dan mengatasi kerentanan sebelum menjadi target serangan yang berbahaya. Metode *Vulnerability Assessment* melibatkan proses pemindaian dan analisis mendalam terhadap sistem jaringan dan aplikasi.

Pengujian dilakukan menggunakan alat-alat khusus seperti Nessus, Wireshark, dan Nmap untuk mengidentifikasi kerentanan yang ada serta menggunakan *router mikrotik* untuk mencegah *port scan* Nmap. Selain itu, proses ini melibatkan pengumpulan informasi dan analisis hasil untuk menilai tingkat risiko yang terkait dengan masing-masing kerentanan. Dalam rangka meningkatkan keamanan dan mengurangi risiko, metode Vulnerability Assessment juga melibatkan rekomendasi mitigasi yang tepat untuk mengatasi kerentanan yang ditemukan. Implementasi langkah-langkah mitigasi ini kemudian diikuti oleh proses verifikasi keamanan untuk memastikan efektivitas langkah-langkah tersebut. Dengan metode *Vulnerability Assessment*, Kantor Sekretariat Yayasan Masjid Agung Sungailiat dapat meningkatkan keamanan sistem jaringan, melindungi data

sensitif, dan menjaga reputasi baik di mata pemangku kepentingan.

Metode ini memungkinkan Kantor untuk menghadapi tantangan keamanan dengan lebih efektif dan menghadirkan lingkungan riset yang aman dan terlindungi. Perkembangan jaringan komputer dan internet yang begitu pesat telah membawa dampak dan manfaat bagi pengguna, baik dari instansi pemerintahan, perusahaan dan perorangan. Setiap perusahaan mengharapkan dengan adanya kehadiran Teknologi informasi dapat membantu perusahaan meningkatkan kinerja mereka. Tidak hanya meningkatkan kinerja tetapi juga untuk meningkatkan keamanan *server-server* yang berisikan data private dari pihak yang tidak berwenang. Hampir semua perusahaan saat ini menjalankan operasionalnya dengan basis Teknologi Informasi. Sehingga kemanaan data menjadi sesuatu yang vital, dimana data rentan serangan dalam bentuk pembobolan, manipulasi, penghilangan para *hacker*. Sayangnya hal ini belum disadari oleh sebagian besar orang, sehingga orang baru menyadari pentingnya keamanan data setelah terjadi serangan. Penelitian dilakukan oleh "*Computer Security Institute*" menunjukkan 90% dari organisasi ikut serta dalam penelitian telah mengalami pelanggaran keamanan dalam 12 bulan terakhir saat riset dibuat. 8% dari organisasi ini menderita kerugian finansial yang besar setelah pelanggaran ini. Banyak dari organisasi ini yang tidak memiliki profesional keamanan bersertifikat, mereka juga tidak menyewa pihak luar untuk memeriksa keamanan jaringan mereka. Dewi Laksmiati 28 Juli 2020 yang berjudul Vulnerability Assesment Pada Pada Situs Www.Hatsehat.Com Menggunakan Openvas [1].

Jaringan dan sistem mereka sangat rentan, hal ini bisa menjadi alasan utama keberhasilan serangan. Hal ini tentunya harus ditindak lanjuti, langkah awal yang perlu dilakukan untuk meminimalisir potensi ancaman keamanan dan penyalah gunaan data perlu dilakukan evaluasi secara proaktif terhadap keamanan server yang ada sehingga ancaman dapat dihilangkan dan celah diblokir sebelum kerusakan dapat dilakukan pada sistem. *Vulnerability Assessment* mencakup proses analisa teknologi yang digunakan dalam organisasi, mencari kelemahan apa pun yang dapat dieksploitasi oleh penyerang, dan memberikan rekomendasi tentang bagaimana Kantor dapat meningkatkan keamanan data. Zirawan A 23 April 2020 yang berjudul Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner [2].

Pada fase pertama, fokus ditempatkan pada sistem keamanan agar lebih memahami jenis perangkat lunak dan perangkat yang digunakan oleh bisnis serta penggunaannya setiap hari. Fase kedua melibatkan memeriksa sistem infrastruktur saat ini. Pada langkah

ini, kelemahan dalam sistem keamanan diidentifikasi dan diperbaiki. Pada fase terakhir *Vulnerability Assessment*, perbaikan diuji un- tuk memastikan bahwa semuanya ada di tempat yang tepat. Jika ada kebutuhan untuk per- baikan, proses dimulai kembali dari fase dua dan setelah penilaian selesai, pemilik sistemakan diberikan penjelasan terperinci tentang apa yang diubah dan mengapa itu diubah. Syahab A.S 3 September 2021 yang berjudul Penggunaan Wireshark dan Nessus untuk Analisis Ssl/Tls Keamanan data[3].

proses identifikasi, analisis, dan prioritisasi kerentanan yang ada pada sistem komputer. pengujian ini bertujuan untuk menemukan kelemahan pada sistem dan memberikan rekomendasi untuk mengatasi masalah tersebut. *Vulnerability Assessment* dapat membantu perusahaan dalam mengidentifikasi risiko keamanan yang ada pada sistem mereka dan mengevaluasi tingkat keamanan jaringan komputer. Melakukan uji kerentanan akan mampu membantu proses identifikasi kelemahan dalam sistem sebelum serangan dapat terjadi serta dapat menjadi langkah pencegahan dalam meningkatkan keamanan terhadap sebuah sistem. Juliharta, 2021 yang berjudul *Vulnerability Assesment* sistem menejemen keamanan informasi [4]

Menggunakan vulnerability scanner memungkinkan untuk pendeteksian dini dan sekaligus dapat dilakukan penanganan yang sudah diketahui kerentanannya serta mudah untuk mengidentifikasi kerentanan yang ada pada jaringan. Kerentanan tersebut memungkinkan timbulmya resiko yang berpotensi dieksploitasi. Penilitian ini akan menyajikan tentang pengendalian terhadap ancaman serangan pada sistem dengan memberikan rekomendasi perbaikan untuk menahan resiko melalui vulnerability assessment. penilaian kerentanan mendapat perhatian dikarenakan dampak yang tidak menentu terhadap Kantor. Pemetaan kerentanan sistem jaringan komputer dapat mengidentifikasi dan menerapkan kebijakan yang perlu dilakukan untuk pengurangan risiko kerentanan dalam sistem. Kajian penelitian ini membuat penilaian secara kualitatif tidak berfokus pada pengukuran angka atau statistik, tetapi lebih mengutamakan pemahaman konteks, makna, dan interpretasi subjektif dari perspektif individu yang terlibat di wilayah penelitian. Penelitian ini berfokus pada Pengujian kerentanan Sistem jaringan komputer menggunakan metode *Vulnerability Assesment*. Salim Y.A.N 2023 yang berjudul Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning [5].

1.2 Rumusan Masalah

Adapun Rumusan Masalah dari judul "Pengujian Kerentanan Keamanan Pada Sistem Jaringan Komputer Menggunakan Metode Vulnerability Assesment Pada Kantor Sekretariat Yayasan Masjid Agung Sungailiat". Sebagai berikut:

1. Bagaimana Pengujian Kerentanan Keamanan dapat dilakukan dengan menggunakan Tools yang tersedia Pada Kantor Sekretariat Yayasan Masjid Agung Sungailiat?
2. Apa saja manfaat yang diperoleh dari Pengujian Kerentanan Keamanan Pada Sistem Jaringan Komputer Menggunakan Metode Vulnerability Assesment Pada Kantor Sekretariat Yayasan Masjid Agung Sungailiat?
3. Apa saja kendala atau kerentanan yang dihadapi dalam pengujian di Kantor Sekretariat Yayasan Masjid Agung Sungailiat?

1.3 Batasan Masalah

Adapun batasan masalah yang dibuat adalah sebagai berikut:

1. Penelitian ini terbatas pada kantor Sekretariat Yayasan Masjid Agung Sungailiat sebagai studi kasus.
2. Data yang digunakan dalam penelitian ini akan didapatkan melalui observasi, wawancara, dan dokumentasi di kantor Sekretariat Yayasan Masjid Agung Sungailiat.
3. Analisis data akan dilakukan dengan menggunakan metode Vulnerability Assesment dan NDLC (Network Devploment Life Cycle).

1.4 Tujuan dan Manfaat Penelitian

Adapun Tujuan dan manfaat dari penelitian tentang "Pengujian Kerentanan Keamanan Pada Sistem Jaringan Komputer Menggunakan Metode *Vulnerability Assessment* Pada Kantor Sekretariat Yayasan Masjid Agung Sungailiat", sebagai berikut:

1.4.1 Tujuan

Adapun Tujuan dari Penelitian ini antara lain:

1. Untuk mengetahui sejauh mana kerentanan atau celah keamanan yang ada pada sistem jaringan komputer pada kantor dan dapat mengetahui kerentanan tersebut
2. Untuk menggambarkan serta meningkatkan keamanan sistem dan jaringan Kantor Sekretariat
3. dengan mengidentifikasi dan mengatasi kerentanan.

1.4.2 Manfaat

Adapun manfaat dari penelitian ini antara lain:

1. Dapat menambah pemahaman tentang Pengujian kerentanan keamanan dalam sistem jaringan komputer Pada Kantor Sekretariat.
2. Dapat menemukan kelemahan dan celah kerentanan dari sistem yang dikelola oleh Kantor Sekretariat Yayasan Masjid Agung Sungailiat.
3. Dapat memberi saran, rekomendasi atau informasi untuk menangani kerentanan yang ada Pada Kantor.

1.5 Sistematika Penulisan Laporan

Sistematika laporan ini bertujuan agar proses dokumentasi pembuatan laporan secara terstruktur mudah dipahami. Adapun sistematika dalam penulisan laporan ini terdiri dari 5 (lima) bab, yaitu sebagai berikut:

BAB I :PENDAHULUAN

Berisi tentang latar belakang, rumusan masalah, Batasan masalah, tujuan penelitian dan manfaat penelitian, dan sistematika penulisan.

BAB II :LANDASAN TEORI

Bersis tentang pembahasan teori-teori yang menjadi dasar dalam penulisan skripsi ini seperti teori tentang konsep yang akan di terapakan, teori tentang pengembagan sistem dan tentang peralatan

yang di gunakan.

BAB III **:METODOLOGI PENELITIAN**

Pada bab ini berisi tentang penjelasan mengenai model pengembangan sistem, metode pengembangan perangkat lunak dan tools pengembangan perangkat lunak pada penelitian ini atau alat bantu dalam mengenai proses yang menggunakan metode NDLC (*Network Devploment Life Cycle*) Dan *Vulnerability Assesment*

BAB IV **:HASIL DAN PEMBAHASAN**

Pada bab ini berisi tentang struktur organisasi, jabaran tugas dan wewenang, analisa permasalahan, analisa sistem berjalan, analisa sistem usulan yang terjadi, serta rancangan sistem, rancangan basis data, menyajikan Pengujian kerentanan keamanan pada jaringan komputer beserta penjelasannya.

BAB V **:PENUTUP**

Pada bab ini berisi tentang kesimpulan dan saran terkait dengan pengujian kerentanan yang telah dibuat oleh penulis dan untuk keperluan pengembangannya lebih lanjut, yang di proleh dari pembahasan pada bab-bab sebelumnya.