BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era digital saat ini yang semakin maju berkembang pesat, keamanan jaringan dan sistem informasi menjadi faktor yang penting. Banyak organisasi dan individu mengandalkan jaringan komputer untuk menyimpan dan mengelola data penting. Namun, dengan kemajuan teknologi juga muncul ancaman baru dalam bentuk serangan siber. Serangan ini bisa menyebabkan kerugian yang besar seperti pencurian data sensitif, penipuan online, kerugian finansial, dan pelanggaran privasi.

Dalam rangka melindungi jaringan dan sistem informasi dari serangan siber, penting untuk melakukan analisis kerentanan secara teratur. Analisis ini bertujuan untuk mengidentifikasi kelemahan dan celah kerentanan dalam infrastruktur jaringan. Dengan mengetahui celah-celah ini, langkah-langkah pencegahan yang tepat diambil untuk memperkuat keamanan sistem pada sebuah perusahaan atau organisasi.

"Saat ini, kebanyakan tools pentesting masih menggunakan model Command Line Interface (CLI) sehingga sulit digunakan oleh orang awam. Oleh karena itu, diperlukan tools berbasis Graphical User Interface (GUI) [2]." "Dalam melakukan Vulnerabilities Identification, diperlukan tools untuk mengetahui potensi celah keamanan dalam bentuk laporan. Ini sangat diperlukan untuk mempermudah analisis, penggunaan, dan meminimalisir biaya pentesting [2]."

Selain itu, keberadaan alat yang dapat menghasilkan laporan yang terstruktur dan jelas dalam proses identifikasi kerentanan juga menjadi sangat penting. Laporan ini akan memberikan informasi mengenai celah kerentanan keamanan yang ada dalam sistem jaringan. Dengan melakukan analisis mendalam dan secara berkala, pengguna dapat lebih mudah melakukan evaluasi dan analisis yang lebih terperinci. Selain itu, laporan ini juga akan membantu pengguna dalam mengambil langkah-langkah pencegahan yang tepat dan mengurangi biaya yang

terkait dengan pengujian keamanan. Dengan adanya alat yang efisien dalam menghasilkan laporan, perusahaan atau organisasi dapat mengidentifikasi kerentanan dengan lebih cepat dan segera mengambil keputusan atau tindakan yang diperlukan untuk meningkatkan keamanan pada sistem mereka.

Dengan melakukan analisis kerentanan secara teratur, perusahaan atau organisasi dapat menjaga keamanan jaringan dan sistem informasi dari serangan siber. Pendekatan proaktif dan teratur ini akan membantu mengidentifikasi celah keamanan yang mungkin ada dalam infrastruktur dan sistem yang digunakan. Dengan demikian, perusahaan atau organisasi dapat mengambil langkah-langkah pencegahan yang tepat dan merespons ancaman siber dengan cepat dalam lingkungan yang terus berubah dan kompleks.

1.2 Rumusan Masalah

Penelitian ini bertujuan untuk melakukan analisis kerentanan jaringan dengan menggunakan beberapa alat bantu yang disajikan dalam berbentuk website. Beberapa alat atau tool mencakup nmap, whois, ping icmp, dan lain-lain. Dengan alat atau tool ini, penulis berharap penelitian ini dapat memberikan gambaran yang jelas dan dapat membantu untuk melakukan analisis kerentanan keamanan siber dalam organisasi.

1.3 Batasan Masalah

Dalam penelitian ini, terdapat beberapa batasan masalah yang perlu diperhatikan, antara lain:

1. Lingkup Penelitian: Penelitian ini akan difokuskan pada analisis kerentanan jaringan menggunakan alat atau tool seperti nmap, whois, ping icmp, dan lain-lain yang terintegrasi dalam sebuah website berbasis bahasa pemrograman golang. Penelitian ini tidak akan membahas secara mendalam tentang alat atau tool tersebut, melainkan lebih fokus pada penerapan dan analisis kerentanan jaringan dengan menggunakan alat atau tool tersebut.
2. Pendekatan OWASP: Penelitian ini akan mengadopsi pendekatan OWASP (Open Web Application Security Project) dalam melakukan analisis

kerentanan. Namun, penelitian ini tidak akan membahas secara rinci seluruh aspek dan langkah-langkah yang ada dalam pendekatan OWASP. Fokus penelitian ini adalah penerapan alat atau tool analisis kerentanan yang sesuai dengan pedoman yang diberikan oleh OWASP.

3. Alat yang digunakan: Penelitian ini akan menggunakan beberapa alat seperti nmap, whois, ping icmp, dan lain-lain. Meskipun ada banyak alat lain yang tersedia untuk analisis kerentanan, penelitian ini akan membatasi diri pada alat-alat yang telah disebutkan.
4. Skala Jaringan: Penelitian ini akan memfokuskan pada analisis kerentanan jaringan dalam skala kecil hingga menengah. Meskipun alat atau tool yang digunakan dapat diterapkan pada jaringan yang lebih besar, penelitian ini tidak akan membahas secara mendalam tentang analisis kerentanan dalam skala yang sangat besar.

Dengan memperhatikan batasan-batasan tersebut, penelitian ini diharapkan dapat memberikan gambaran yang jelas dan terstruktur tentang kerentanan jaringan melalui penerapan alat atau tool berbasis website dengan metode pendekatan OWASP.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini sebagai berikut:

1. Membangun sebuah website yang mampu menyajikan alat atau tool analisis kerentanan yang terintegrasi.
2. Mengimplementasikan alat atau tool seperti nmap, whois, ping icmp, dan lain-lain dalam sebuah website.
3. Menganalisis kerentanan jaringan dengan menggunakan alat atau tool yang terdapat pada website.
4. Menyajikan hasil analisis kerentanan secara jelas dan terstruktur.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Memberikan pemahaman yang lebih baik tentang kerentanan

jaringan dan pentingnya analisis kerentanan dalam keamanan sistem informasi.

2. Membangun sebuah alat yang dapat digunakan untuk membantu dan mempermudah dalam analisis kerentanan secara efektif dan efisien.
3. Memberikan kontribusi pada penelitian dan pengembangan bidang keamanan jaringan dan cyber security.

1.6 Sistematika Penulisan

Penelitian skripsi ini terdiri dari lima bab, yaitu:

Bab 1: Pendahuluan

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab 2: Tinjauan Pustaka

Bab ini membahas teori dan konsep-konsep yang berkaitan dengan analisis kerentanan jaringan, keamanan jaringan, alat atau tool yang digunakan dengan menggunakan metode pendekatan OWASP.

Bab 3: Metodologi Penelitian

Bab ini menjelaskan metode yang digunakan dalam penelitian, termasuk perancangan dan implementasi alat atau tool analisis kerentanan, serta prosedur analisis yang akan digunakan.

Bab 4: Hasil dan Pembahasan

Bab ini menyajikan hasil analisis kerentanan yang diperoleh dari penggunaan alat atau tool pada website yang telah dibangun. Hasil tersebut akan dianalisis dan diinterpretasikan secara sederhana.

Bab 5: Kesimpulan dan Saran

Bab ini berisi kesimpulan dari penelitian yang telah dilakukan dan saran-saran untuk pengembangan penelitian lebih lanjut.

Dengan adanya penelitian ini, diharapkan bahwa analisis kerentanan jaringan dapat

dilakukan dengan lebih efektif dan efisien, sehingga upaya perlindungan terhadap serangan siber dapat ditingkatkan.