BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin maju, jaringan komputer menjadi tulang punggung berbagai sektor industri dan layanan publik. Kebutuhan akan konektivitas yang cepat dan andal telah meningkat pesat, mempengaruhi berbagai bidang seperti pendidikan, kesehatan, perdagangan, dan pemerintahan. Universitas, sebagai pusat pendidikan dan penelitian, juga sangat bergantung pada infrastruktur jaringan yang kokoh untuk mendukung aktivitas akademik dan administratif mereka. Layanan jaringan yang tersedia di universitas tidak hanya digunakan oleh staf dan mahasiswa untuk keperluan belajar dan penelitian, tetapi juga untuk akses informasi global yang sangat penting dalam era informasi ini (Stallings & Brown, 2015).

Salah satu layanan jaringan yaitu *web server,* memainkan peran penting dalam penyediaan berbagai layanan *online*, seperti portal akademik, sistem informasi manajemen, dan akses ke materi pembelajaran berbasis *web. Web server* yang dikelola oleh universitas menjadi titik akses utama bagi pengguna internal dan eskternal, memungkinkan interaksi dengan berbagai aplikasi dan layanan berbasis *web.* Namun, seperti jaringan lainnya, *web server* juga rentan terhadap berbagai ancaman siber. Serangan pada *web server* dapat mengakibatkan pencurian data, perusakan website, dan dangguan layanan yang dapat mempengaruhi ribuan pengguna (McDonald, 2020). Oleh karena itu, memastikan keamanan *web server* adalah bagian krusial dari strategi keamanan jaringan secara keseluruhan (Zalewski, 2011).

Masalah keamanan jaringan menjadi perhatian utama karena semakin banyaknya ancaman siber yang mengintai (Khan & Salah, 2018). Serangan siber dapat menyebabkan kerugian besar, mulai dari pencurian data hingga gangguan operasional yang serius (Alsmadi & Zarour, 2017). Oleh karena itu, pemantauan dan pengamanan jaringan publik menjadi tugas penting bagi para insinyur Teknologi Informasi yang bekerja dibidang ini. Mereka bertanggung jawab untuk memastikan bahwa jaringan yang digunakan oleh ribuan pengguna setiap hari aman dari ancaman dan dapat diandalkan untuk mendukung berbagai kegiatan (Anderson, 2020).

Kerentanan jaringan adalah kelemahan dalam sistem komputer yang dapat dieksploitasi oleh penyusup untuk mendapatkan akses yang tidak sah atau mengganggu operasi (Kizza, 2020). Kerentanan ini tidak hanya ada dalam perangkat keras dan perangkat lunak, tetapi juga

dalam kebijakan, prosedur, dan faktor manusia (Kizza, 2020). Infrastruktur jaringan, termasuk *server, firewall, router*, dan perangkat nirkabel, membentuk dasar untuk Sebagian besar masalah keamanan teknis (Basu, 2019). Dengan meningkatnya konektivitas dunia melalui internet, risiko terhadap keamanan informasi telah tumbu secara signifikan (Basu, 2019). Kerentanan dapat didefinisikan sebagai kondisi, kelemahan, atau ketiadaan langkah-langkah keamanan yang dapat dieksploitasi oleh ancaman (Kizza, 2012; Kizza, 2014). Untuk mengurangi risiko ini, sangat penting untuk menguji dan menghilangkan kerentanan kapan pun memungkinkan (Basu, 2019). Peretasan etis dapat digunakan untuk mengidentifikasi potensi kelemahan dalam infrastruktur jaringan, memungkinkan organisasi untuk milenial dan menangani paparan mereka terhadap ancaman (Basu, 2019).

Salah satu metode untuk meningkatkan keamanan jaringan adalah dengan melakukan analisis kerentanan yaitu proses mengidentifikasi dan mengkategorikan semua perangkat dan layanan yang terhubung ke jaringan tersebut (Kaur & Singh, 2017). Metode passive reconnaissance menjadi salah satu teknik yang dapat digunakan dalam enumerasi jaringan. Teknik ini melibatkan pengumpulan informasi tentang jaringan tanpa mengirimkan lalu lintas tambahan yang dapat terdeteksi oleh sistem keamanan jaringan. Ini membuat *passive reconnaissance* menjadi alat yang efektif untuk mengidentifikasi perangkat dan layanan yang ada tanpa menimbulkan gangguan atau kecurigaan (Cole, 2017).

Di Universitas Muhammadiyah Yogyakarta (UMY), jaringan publik memainkan peran penting dalam mendukung berbagai kegiatan akademik dan administratif. Namun, dengan meningkatnya penggunaan jaringan publik, risiko terhadap keamanan jaringan juga meningkat. Penelitian ini bertujuan untuk melakukan analisis keamanan jaringan publik UMY menggunakan metode *passive reconnaissance*, dengan tujuan mengidentifikasi potensi celah keamanan yang ada dan memberikan rekomendasi untuk peningkatan keamanan jaringan (Scarfone & Mell, 2007).

Sebagai insinyur Teknologi Informasi, peran kita sangat krusial dalam memastikan bahwa jaringan publik yang digunakan aman dan efisien. Dengan menggunakan metode *passive reconnaissance*, kita dapat memperoleh gambaran yang jelas tentang perangkat dan layanan yang aktif di jaringan tanpa menimbulkan gangguan pada operasional jaringan. Hasil dari penelitian ini diharapkan dapat membantu UMY dalam memperkuat pertahanan jaringan mereka dan mengurangi risiko terhadap serangan siber (Anderson, 2020).

1.2 Rumusan Masalah

Berdasarkan pembahasan diatas, rumusan masalah dalam penelitian ini ada: Bagaimana analisis keamanan *web server* Universitas Muhammadiyah Yogyakarta (UMY) menggunakan Shodan.io dapat mengidentifikasi celah keamanan yang ada, dan apa rekomendasi yang dapat diberikan untuk meningkatkan keamanan *web server* tersebut?

1.3 Batasan Masalah

Batasan masalah dari penelitian ini adalah pencarian kerentanan keamanan melalui Shodan.io yang menunjukkan banyak *sekali Common Vulnerabilities and Exposures* (CVE) yang ditemukan. Karena keterbatasan waktu, hanya beberapa CVE yang dapat dimasukkan dan dianalisis dalam penelitian ini.

1.4 Tujuan Tugas Akhir

1. Mengidentifikasi potensi celah keamanan pada *web server* Universitas Muhammadiyah Yogyakarta (UMY) dengan menggunakan Shodan.io untuk mendapatkan gambaran menyeluruh mengenai kerentanan yang mungkin ada dalam sistem
2. Menganalisa hasil identifikasi celah keamanan untuk menentukan tingkat kritikalitas dan dampaknya terhadap keamanan dan integritas *web server* UMY.
3. Menyusun dan memberikan rekomendasi perbaikan yang spesifik dan praktis untuk mengatasi kerentanan yang ditemukan, guna meningkatkan keamanan dan perlindungan *web server* UMY dari potensi ancamana siber.

1.5 Manfaat Tugas Akhir

Penelitian ini diharapkan dapat memberikan rekomendasi yang tepat untuk meningkatkan keamanan layanan jaringan seperti *web server*, sehingga dapat mengurangi risiko serangan siber dan memastikan layanan yang digunakan oleh staf dan mahasiswa tetap aman dan andal untuk mendukung berbagai kegiatan akademik dan administratif.

1.6 Sistematika Penulisan

Dalam penelitian ini terdapat beberapa bab, setiap bab terdiri dari beberapa sub-bab. Setiap bab menyajikan rincian yang komprehensif mengenai subjek penelitian. Berikut adalah ringkasan dari setiap bab:

Bab I Pendahuluan

Bab pendahuluan ini memberikan gambaran tentang informasi latar belakang, kesulitan penelitian termasuk rumusan masalah dan batasan masalah, serta tujuan dan manfaat dari penelitian.

Bab II Tinjauan Pustaka dan Dasar Teori

Bab ini menyajikan tinjauan pustaka dan kerangka teoritis, menjelaskan tentang jurnal penelitian dan teori yang dijadikan referensi dalam proses penulisan penelitian.

Bab III Metodologi Penelitian

Bab metodologi penelitian menjelaskan teknik-teknik yang digunakan dalam menyelesaikan tantangan. Metodologi penelitian ini juga menjelaskan rancangan desain yang dapat diimplementasikan selanjutnya.

Bab IV Hasil dan Pembahasan

Bab hasil dan pembahasan memberikan penjelasan tentang temuan penelitian, melakukan pengujian terhadap hasil desain dan implementasi, serta membahas analisis sistem yang sesuai dengan desain.

Bab V Kesimpulan dan Saran

Pada bab kesimpulan dan saran ini merupakan bagian penutup yang berisikan suatu kesimpulan dan saran yang dimuat dari berdasarkan penelitian.