BAB II

TINJAUAN PUSTAKA

2.1. Studi Sebelumnya

Penelitian yang dilakukan oleh Herman bertujuan menemukan dan mengetahui serangan-serangan yang mungkin terjadi terhadap kerentanan yang ada pada sistem serta mengetahui dampak suatu jaringan yang diakibatkan dari hasil eksploitasi yang dilakukan oleh penyerang. Penelitian ini berhasil mendeteksi beberapa serangan *Denial of Service* (DoS) menggunakan metode TCP *Ping Flooding,* UDP *Ping Flooding,* dan HTTP *Ping Flooding*. Penelitian ini menggunakan pendekatan penetration testing yang bertujuan melakukan pengujian secara langsung dan mengevaluasi keamanan dari suatu sistem jaringan komputer. Metode ini melibatkan aktivitas pengujian yang dilakukan langsung pada sistem tersebut dengan tujuan menilai tingkat keamanannya [9].

Penelitian yang dilakukan oleh Marzuki bertujuan menguji tingkat keamanan sistem jaringan web server dengan menggunakan uji coba non destruktif yaitu uji coba yang tidak membuat kerusakan sistem. Menunjukkan tingkat kerentanan pada *web server* diva karaoke masih rendah, dibuktikan dengan adanya beberapa *port* TCP yang terbuka, situs web beresiko terhadap serangan *clickjacking*. Selain itu penelitian ini juga dapat menjadi tolak ukur sejauh mana perusahaan yang dievaluasi ini sudah bisa mengamankan data dari pihak yang seharusnya tidak mendapatkan akses terhadap data. Dalam eksperimen ini, penulis menggunakan penetration testing [10].

Penelitian yang dilakukan oleh Ari, untuk pengujian terhadap keamanan jaringan untuk mecari celah dari kelemahan sistem jaringan. Hasil penelitian menunjukkan bahwa uji coba telah dilakukan terhadap keamanan jaringan *hotspot* di kosan dengan metode MITM menggunakan serangan *wireshark, sniffing ping flood,* dan *netcut.* Hal ini berhasil mengidentifikasi potensi celah

keamanan pada jaringan *hotspot* tersebut. Uji coba melibatkan dua klien, dan hasilnya menunjukkan bahwa dengan menggunakan *wireshark*, jaringan dapat dimonitor dengan efektif. Selain itu, hasil dari uji coba juga menunjukkan bahwa serangan tersebut dapat digunakan untuk melakukan kejahatan dengan mendapatkan akses *username* dan *password* dari korban [11].

Penelitian yang dilakukan oleh Tri Yusnanto bertujuan mengidentifikasi serta mengeksploitasi kerentanan pada keamanan jaringan komputer menggunakan metode *penetration testing*. Tujuan analisis dilakukan terhadap keamanan jaringan nirkabel di Laboratorium STMIK Bina Patria. Pengujian dilaksanakan melalui serangkaian aktivitas yang mencakup identifikasi dan eksploitasi kerentanan pada keamanan jaringan komputer. Untuk menganalisis keamanan jaringan WLAN, dilakukan *penetration testing* di mana serangan terhadap jaringan disimulasikan [12].

Penelitian yang dilakukan oleh Anwaruddin bertujuan untuk menganalisis keamanan sistem informasi manajemen aset yang bernama SIMAM milik Muhammadiyah menggunakan *penetration testing* dan ISO 27001:2013. Selain itu, menyusun hasil analisis keamanan SIMAM dari hasil *penetration testing* dan ISO 27001:2013 yang berupa temuan dan rekomendasi guna perbaikan keamanan sistem informasi *asset*. Berdasarkan hasil penelitian, ditemukan 4 *port* yang terbuka pada sistem informasi SIMAM dan 9 kerentanan lainnya. Lalu, melakukan audit keamanan sistem informasi menggunakan ISO 27001 dengan cara *scoring* dan mendapatkan hasil *maturity level* 2.32. Kemudian, membuat rekomendasi dari hasil *penetration testing* dan audit menggunakan ISO 27001:2013 [13].

Tabel 1. Perbandingan Penelitian Sebelumnya

No	Penulis	Tahun	Subjek	Tujuan	Metode	Hasil
1	Herman, dkk	2023	Jaringan LAN kampus	menemukan dan mengetrahui serangan-serangan yang mungkin terjadi terhadap kerentanan yang ada pada sistem serta mengetahui dampak suatu jaringan yang diakibatkan dari hasil eksploitasi yang dilakukan oleh penyerang.	*Penetration Testing*	Mendeteksi beberapa serangan *Denial of Service* (DoS) menggunakan metode TCP *Ping Flooding*, UDP *Ping Flooding*, dan HTTP *Ping Flooding.*
2	Hasibuan	2022	*Web server* diva karaoke	Menguji tingkat keamanan sistem jaringan *web* server dengan menggunakan uji coba non destruktif yaitu uji coba yang tidak membuat kerusakan sistem.	*Penetration Testing*	Menunjukkan tingkat kerentanan pada *web* server diva karaoke masih rendah, dibuktikan dengan adanya beberapa *port* TCP yang terbuka, situs *web* beresiko terhadap serangan *clickjacking*.

No	Penulis	Tahun	Subjek	Tujuan	Metode	Hasil
3	Anggraini, dkk.	2022	Sistem keamanan jaringan *hotspot*	Pengujian terhadap keamanan jaringan untuk mecari celah dari kelemahan sistem jaringan	*Penetration Testing*	Menunjukkan bahwa serangan tersebut dapat digunakan untuk melakukan kejahatan dengan mendapatkan akses *username* dan *password* dari korban.
4	Yusnanto	2022	*Laboratorium* STMIK Bina Patria	Analisis dilakukan terhadap keamanan jaringan nirkabel di Laboratorium STMIK Bina Patria	*Penetration Testing*	Berhasil melakukan serangan *Cracking The Ecryption, Attacking The Infrastructure* dan MITM.
5	Ibrahim	2019	Keamanan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM)	Melakukan analisis keamanan penggunaan Sistem Informasi Manajemen Aset Muhammadiyah (SIMAM) dengan metode *penetration testing* dan ISO 27001:2013.	*Penetration testing* dan ISO 27001:2013	Menemukan 4 *port* yang terbuka pada sistem informasi SIMAM dan 9 kerentanan lainnya. Lalu, melakukan audit keamanan sistem informasi menggunakan ISO 27001 dengan cara scoring dan mendapatkan hasil *maturity level* 2.32. Kemudian, membuat rekomendasi dari hasil *penetration testing* dan audit menggunakan ISO 27001:2013.

2.2. Dasar Teori

2.2.1. *Penetration Testing*

Terdapat berbagai jenis metode untuk identisikasi kerentanan jaringan, yakni metode *penetration testing, vulnerability assessment, vulnerability scanning.* Penetration testing dapat membantu dalam menemukan kerentanan spesifik yang mungkin tidak terdeteksi oleh metode lain seperti *vulnerability assessment dan vulnerability scanning*. Hal ini karena serangan yang dilakukan dalam pengujian penetrasi menyerupai serangan asli yang dilakukan oleh penyerang yang berpotensi merusak. Penetration Testing secara aktif mencoba mengeksploitasi kerentanan yang ada dalam sistem. Ini membantu organisasi untuk memahami seberapa efektif pengendalian keamanan yang telah diimplementasikan dalam melindungi sistem mereka [14].

2.2.2. Jaringan Komputer

Jaringan komputer adalah suatu sistem yang terdiri dari beberapa komponen komputer dan perangkat yang saling berhubungan melalui transmisi kabel atau nirkabel [15]. Dalam suatu jaringan komputer, komponen utamanya meliputi server dan klien yang digunakan oleh pengguna. Kedua pihak berinteraksi untuk berbagi informasi, sumber daya, dan layanan. Selain itu, jaringan juga mencakup perangkat keras seperti *router, switch,* dan *modem* yang berperan sebagai perantara dalam pengiriman data antar komputer [16]. Transmisi data dalam jaringan dapat dilakukan dengan menggunakan berbagai teknologi, mulai dari kabel fisik hingga teknologi nirkabel seperti *Wi-Fi*. Semua ini membantu memungkinkan komunikasi yang efisien dan berbagi sumber daya antara komputer yang terhubung ke jaringan komputer. Jaringan komputer memainkan peran penting dalam banyak aspek kehidupan modern, mulai dari bisnis hingga hiburan, dan telah menjadi fondasi penting dalam revolusi *digital* saat ini.

2.2.3. IP *Address*

Identitas unik komputer dalam bentuk alamat logis dikenal sebagai IP *addres*. Lalu lintas data dapat diidentifikasi dan diatur menggunakan alamat IP ini di seluruh jaringan internet [17]. Setiap perangkat yang terhubung ke internet memiliki alamat IP yang unik, yang memungkinkan mereka berkomunikasi dengan baik dan efisien satu sama lain. Alamat IP juga sangat penting dalam perutean data, karena memastikan bahwa data dikirimkan ke perangkat yang tepat di seluruh dunia. *Address* IP adalah alamat logika yang diberikan ke peralatan jaringan yang menggunakan protokol TCP/IP [18]. Alamat IP terdiri dari angka biner 32-bit yang disusun dalam empat kelompok, masing-masing terdiri dari oktat delapan bit yang terpisah oleh titik. Sebagai contoh, 10000.00001010.00000001, atau dalam empat kelompok dengan angka desimal 0-255, seperti 192.16.10.1. Nilai yang sama ditunjukkan dalam biner dan angka desimal, tetapi alamat IP ditulis dalam angka desimal lebih mudah dipahami. Pengulangan bilangan panjang 0 dan 1 adalah masalah menggunakan bilangan biner karena kemungkinan kesalahan meningkat. Alamat IP versi 4 (IPv4) memberikan alamat komputer lengkap yang terdiri dari gabungan alamat jaringan dan host karena IP address terdiri dari dua bagian yaitu *network* ID dan *host* ID. *Network* ID menentukan alamat jaringan, sedangkan *host* ID menentukan alamat komputer atau *host*. Jumlah kelompok angka yang termasuk dalam *network* ID dan *host* ID bervariasi berdasarkan kelas.

2.2.4. Firewall

Firewall adalah sistem atau perangkat yang sangat penting untuk memastikan keamanan jaringan komputer dengan mengontrol lalu lintas data yang masuk dan keluar [19]. Misalnya, *firewall* dapat dikonfigurasi oleh sebuah perusahaan untuk memungkinkan pekerjanya mengakses internet, tetapi memblokir situs *web* berbahaya atau konten yang melanggar kebijakan perusahaan. Contoh tambahan adalah ketika firewall digunakan dalam jaringan rumah, mereka memungkinkan perangkat seperti komputer dan *smartphone*

untuk terhubung ke internet sambil mencegah akses yang tidak diinginkan atau potensi serangan dari luar jaringan [20]. Dengan demikian, *firewall* berfungsi sebagai penghalang yang efektif untuk mencegah akses yang tidak diinginkan atau ancaman ke jaringan, menjaga keamanan data dan informasi yang ada di dalamnya.

2.2.5. Keamanan Jaringan Komputer

Dalam dunia *digital* yang terus berkembang, keamanan jaringan sangat penting. Untuk mengurangi risiko penyalahgunaan oleh *hacker*, hal ini perlu ditingkatkan dengan tindakan yang tepat. Saat data menjadi aset penting dan jaringan komunikasi menjadi bagian penting dari kehidupan sehari-hari, keamanan jaringan adalah kebutuhan dan kewajiban[21]. *Hacking* dapat berdampak besar pada individu, organisasi, dan bahkan masyarakat pada umumnya. Oleh karena itu, kita dapat yang tidak berwenang melalui pendidikan dan pelatihan keamanan, pemantauan jaringan yang aktif, *firewall* yang kuat, dan enkripsi data. Oleh karena itu, menjaga keamanan jaringan harus menjadi prioritas utama di dunia digital yang semakin kompleks ini.

Sistem keamanan jaringan ada *firewall*, filter perutean, kontrol akses, sistem pencegahan intrusi, sistem deteksi intrusi, dan *honeypots* [22]. *Administrator* jaringan komputer juga dapat membangun *Intrusion Detection System* (IDS) untuk menemukan ancaman jaringan. IDS akan memberikan peringatan kepada manajer jaringan jika terjadi serangan atau gangguan jaringan. Dibandingkan dengan berbagai anomali dan teknologi baru yang digunakan oleh penyerang, metode deteksi intrusi saat ini bergantung pada deteksi berbasis tanda tangan atau model berbasis anomali.

2.2.6. IP *Scanning*

IP *scanning* adalah proses untuk mengidentifikasi alamat IP yang aktif dalam suatu jaringan komputer. Metode ini digunakan untuk mengeksplorasi jaringan, mengumpulkan informasi tentang perangkat yang terhubung, dan menentukan ketersediaan serta keamanan jaringan. Dengan menggunakan perangkat lunak

khusus atau alat jaringan, seperti Nmap atau *Wireshark*, IP *scanning* dapat dilakukan dengan berbagai teknik, termasuk *ping sweeps, port scanning,* dan *protocol-specific scans.* Informasi yang diperoleh dari hasil *scanning* ini dapat membantu administrator jaringan dalam memonitor dan mengelola infrastruktur jaringan mereka serta mengidentifikasi potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak berwenang.

2.2.7. *Port Scanning*

Port scanning adalah proses yang digunakan untuk mengidentifikasi *port* yang terbuka pada sebuah sistem komputer atau jaringan. Tujuan utama dari *port scanning* adalah untuk mengeksplorasi infrastruktur jaringan, mengidentifikasi layanan yang berjalan di setiap *port*, serta menentukan tingkat keamanan sistem tersebut. Dengan menggunakan perangkat lunak seperti Nmap atau *tools* kustom, *port scanning* dapat dilakukan dengan berbagai teknik, termasuk TCP *connect scans*, SYN *scans*, dan UDP *scans*. Informasi yang diperoleh dari hasil *port scanning* ini dapat membantu administrator jaringan untuk mengamankan sistem mereka dengan menutup *port* yang tidak diperlukan atau menyesuaikan konfigurasi *firewall* agar hanya mengizinkan akses yang sesuai. Namun, *port scanning* juga dapat digunakan oleh pihak yang tidak berwenang untuk memetakan jaringan dan mencari celah keamanan, sehingga penting bagi organisasi untuk secara teratur memantau dan mengaudit aktivitas *port scanning* dalam upaya untuk menjaga keamanan jaringan mereka [23].

2.2.8. *Packet Sniffing*

Packet Snifiing adalah proses untuk menganalisis paket data yang dikirimkan melalui jaringan komputer dengan tujuan untuk mengidentifikasi informasi tertentu, memantau lalu lintas jaringan, atau mendeteksi serangan keamanan. Metode ini memungkinkan para pengguna untuk menginspeksi dan mengambil sampel data yang dikirim melalui jaringan, seperti protokol, alamat sumber dan tujuan, serta isi paket. *Packet sniffing* umumnya dilakukan dengan menggunakan perangkat lunak atau perangkat keras khusus, seperti *sniffer* atau *packet analyzer*,

yang memungkinkan pengguna untuk memonitor dan menganalisis lalu lintas jaringan secara *real-time*. Informasi yang diperoleh dari hasil *packet sniffing* ini dapat digunakan untuk memantau kinerja jaringan, mendeteksi aktivitas mencurigakan atau serangan, serta melakukan *troubleshooting* pada masalah jaringan. Namun, penting untuk dicatat bahwa penggunaan packet *scanning* juga dapat melibatkan privasi dan keamanan data, sehingga perlu diimplementasikan dengan kebijakan dan tindakan perlindungan yang tepat [24].

2.2.9. Keamanan Informasi

Keamanan informasi mencakup upaya perlindungan terhadap informasi dan sistem informasi dari berbagai potensi risiko seperti akses yang tidak sah, penggunaan yang tidak diotorisasi, penyebaran informasi, pengoperasian yang tidak sah, modifikasi data, dan bahkan pengungkapan oleh pihak yang tidak berwenang. Fokusnya adalah memastikan tiga aspek kunci: kerahasiaan, integritas, dan ketersediaan informasi [25].

Dalam konteks keamanan informasi, empat bidang utama menjadi fokus, yaitu organisasi, orang, proses, dan teknologi. Organisasi memerlukan kebijakan dan praktik manajemen risiko yang efektif, serta keinginan dalam membangun budaya keamanan. Orang, sebagai bagian manusia dalam ekosistem keamanan informasi, memerlukan pemahaman dan kesadaran akan kebijakan serta tanggung jawabnya dalam menjaga keamanan informasi. Proses, termasuk prosedur operasional dan langkah-langkah keamanan yang diterapkan, menjadi landasan untuk menjalankan operasional sehari-hari secara aman. Terakhir, teknologi mencakup solusi dan sistem keamanan yang digunakan untuk melindungi infrastruktur dan data dari berbagai ancaman.