BAB 2

TINJAUAN PUSTAKA

Pada bab ini penulis menjelaskan penelitian sebelumnya yang menghubungkan penelitian selanjutnya dan juga teori dasar sebagai sistem pendukung penelitan.

2.1. Penelitian Terkait

Pada penyusunan skripsi ini sedikit banyak nya terinspirasi dan mengacu dari penelitian – penelitian yang berkaitan dengan latar belakang masalah pada skripsi ini. Adapun penelitian yang berhubngan dengan skripsi ini antara lain yaitu:

Tabel 2. 1 Penelitian Terkait

Penelitian 1	
Penulis dan Tahun	(Suradji & Chandra, 2014)
Judul	Penetration Testing Sistem Jaringan Komputer Untuk Mengetahui Kerentanan Keamanan Server Dengan Menggunakan Metode Penetration Testing Execuition Standard (PTES) Studi Kasus Rumah Sakit Santa Madiun.
Objek	Keamanan Server Rumah Sakit Sanata Clara Madiun.
Metode	Penetration Testing Execuition Standard (PTES).
Hasil	Dengan menggunakan metode PTES, para peneliti menemukan bahwa server Rumah Sakit Santa Clara memiliki kerentanan signifikan yang dapat digunakan untuk melakukan kejahatan dunia maya. Kerentanan tersebut berasal dari layanan Microsoft Server yang masih penuh dengan bug dan error. Pelaku penyerangan memiliki kemampuan untuk menguasai server, memasang pintu belakang yang memungkinkan akses ke sistem, dan mencuri atau mengubah data yang tersimpan di dalamnya. Meskipun masalah yang ditemukan selama

	penelitian ini telah diperbaiki, firewall server juga harus diaktifkan untuk menghentikan serangan, dan filter jaringan seperti IDS dan IPS harus dipasang untuk memantau dan membatasi akses data ke internet.
Penelitian 2	
Penulis dan Tahun	(Utoro et al., 2020)
Judul	Analisis Keamanan Website E-learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execuition Standard (PTES).
Objek	Keamanan Website E-learning SMKN 1 Cibatu.
Metode	Penetration Testing Execuition Standard (PTES).
Hasil	Metode PTES digunakan dalam penelitian ini untuk mengetahui tingkat kerentanan sistem informasi yang paling berisiko terhadap serangan seperti eavesdropping, cross-site scripting, dan cross-site request forgery, yang dapat menyebabkan kebocoran data yang signifikan. Aplikasi website milik SMKN 1 Cibatu ditemukan rentan.
Penelitian 3	
Penulis dan Tahun	(Fauzan & Syukhri, 2021)
Judul	Analisis Metode Web Security Penetration Testing Execuition Standard (PTES) pada aplikasi E-learning Universitas Negeri Padang.
Objek	Web Security Pada Aplikasi E-learning Universitas Negeri Padang .
Metode	Penetration Testing Execuition Standard (PTES).

Hasil	Kesenjangan keamanan Level 2 atau level menengah pada penelitian ini ditemukan menggunakan pendekatan PTES, artinya serangan apa pun tidak akan berdampak signifikan pada situs web. Selain itu, karena *Secure Socket Layer* digunakan untuk meningkatkan keamanan situs web, eksploitasi *SQL Injection* tidak berhasil.
Penelitian 4	
Penulis dan Tahun	(Adrian & Setiyadi, 2018)
Judul	Analisis Keamanan Jaringan Dengan Menggunakan Metode Penetration Testing Execuition Standard (PTES) DI Dinas Kesehatan Provinsi Jawa Barat.
Objek	Keamanan Jaringan pada Layanan Internet Publik Provinsi Sumatra Selatan.
Metode	Penetration Testing Execuition Standard (PTES).
Hasil	Dinas Kesehatan Provinsi Jawa Barat memiliki sejumlah kerentanan yang perlu diwaspadai oleh Divisi Teknologi Informasi dan Komunikasi organisasinya, berdasarkan hasil penelitian metode PTES. Kerentanan ini membuka banyak kemungkinan kelemahan sistem dalam jaringan, khususnya yang berkaitan dengan keamanan jaringan nirkabel.
Penelitian 5	
Penulis dan tahun	(Pratama & Syamsuar, 2021)
Judul	Analisis Keamanan Jaringan Pada Layanan Internet Publik Menggunakan Metode Penetration Testing Execution Standard (PTES) DPRD Provinsi Sumatra Selatan
Objek	Keamanan Jaringan Pada Layanan Internet Publik Provinsi Sumatra Selatan.

Metode	Penetration Testing Execution Standard (PTES).
Hasil	penelitian ini menunjukkan bahwa DPRD Provinsi Sumatera Selatan merupakan salah satu pusat pemerintahan yang memberikan berbagai pelayanan kepada masyarakat. Setiap karyawan dan anggota staf memiliki akses ke satu jaringan *Wireless Area Network* (WLAN) yang menggunakan satu SSID untuk semua aktivitas berbagi data dalam jaringan. Untuk mengetahui celah keamanan pada jaringan WLAN, penulis melakukan percobaan menggunakan metode Penetration Testing Excuition Standard (PTES) dan empat parameter serangan yaitu *Man-in-the-Middle Attack, ARP Spoofing*, *Bypassing MAC Authentication*, dan *Cracking the* Enkripsi. Periksa pengaturan keamanan jaringan WLAN saat ini. Hasil dari empat parameter penyerangan yang digunakan, tiga di antaranya berhasil diselesaikan.
Penelitian 6	
Penulis dan Tahun	(Ningsih, 2021)
Judul	Analisis Pengujian Kerentanan Situs Pemda XYZ Menggunakan Metode PTES.
Objek	Kerentanan Situs Pemda XYZ Menggunakan Metode PTES.
Metode	Penetration Testing Execution Standard (PTES) .
Hasil	Pada penelitiandi peroleh bahwa pemerintah XYZ telah menggunakan website dan penetration testing adalah metode pengujian kerentanan keamanan yang ada pada sebuah website dan penetration testing pada sebuah website. Pada penelitian ini akan di lakukan *vulnerability assessment* dan

	penetration testing pada situs layanan terpadu pemerintah XYZ menggunakan standar PTES dengan beberapa tools yang di gunakan *Acunetix*, dan Paros Kali Linux. Hasil dari kerentanan yang di peroleh pada website layanan terpadu memiliki jenis kerentanan dan tingkat resiko berbeda-beda sesuai tools yang di gunakan.
Penelitian 7	
Penulis dan Tahun	(Andhika et al., 2022)
Judul	Pengujian Penetrasi Pada Windows 10 Menggunakan Metode Penetration Testing Execuition Standard (PTES).
Objek	Pengujian Penetrasi Pada Windows 10.
Metode	Penetration Testing Execuition Standard (PTES).
Hasil	Penelitian ini menemukan bahwa serangan terhadap keamanan sistem informasi dapat dilihat dari sudut pandang peran komputer atau jaringan komputer sebagai penyedia informasi. Jika seseorang mengambil keuntungan dari kelemahan yang ditemukan demi keuntungannya sendiri dan melemahkan sistem sehingga merugikan lembaga atau perusahaan, maka dampaknya mungkin akan merugikan. Karena masalah yang ada sejak Windows 10 pertama kali diinstal oleh konsumen, ditemukan bahwa Windows 10 mengandung kerentanan yang lebih kritis. Kerentanan ini dapat dieksploitasi karena beberapa layanan tidak dapat diakses oleh publik.

Berdasarkan dari hasil penelitian terkait yang di lakukan pengujian dengan menggunakan metode Penetration Testing Execution Standard (PTES) di peroleh bahwa pada

sistem informasi website atau aplikasi masih memiliki sistem keamanan yang lemah seperti *SQL injection* dan keamanan server. Penelitian terkait menggunakan metode PTES telah dilakukan dalam pengujian keamanan sistem. Dari objek pengujian memiliki perbedaan dari tahapannya hasil dan analisis setiap penelitian tersebut. Analisa dari hasil metode ini akan di gunakan dan di rekomendasikan.

2.2. Kajian Teori

2.2.1. Jaringan Komputer

Jaringan komputer adalah sistem yang menghubungkan beberapa komputer untuk bertukar sumber daya dan data. Kemampuan pengguna dalam berkomunikasi akan difasilitasi oleh komputer dan gadget berjaringan lainnya. Beberapa komputer dan perangkat lainnya dihubungkan melalui media kabel atau nirkabel sehingga membentuk suatu jaringan. Selain menggunakan perangkat keras ini, menyiapkan jaringan komputer biasanya memerlukan instalasi perangkat lunak tertentu. Deteksi perangkat jaringan dilakukan oleh perangkat lunak. Sederhananya, jaringan komputer biasanya terdiri dari komputer host untuk operasi pengguna dan komputer server yang berfungsi sebagai pusat kendali.

2.2.2. Keamanan jaringan Komputer

Keamanan jaringan merupakan salah satu hal penting dalam memonitoring komponen dan mencegah.

a. Confidentiality

Confidentiality yaitu, menuntut hanya pihak yang berwenang yang dapat mengakses informasi atau data.

b. Intergrity

Intergrity yaitu, menuntut pemilik informasi menjadi satu-satunya yang dapat mengubahnya.

c. Availability

Availability yaitu menuntut agar informasi dapat diakses oleh pihak yang berwenang pada waktu yang tepat.

d. Authentication

Authentication yaitu menuntut agar pengirim informasi diidentifikasi secara akurat dan terdapat bukti bahwa identifikasi yang diperoleh adalah asli..

e. Nonrepudiation

Nonrepudiation yaitu menuntut agar informasi dikirim dan diterima tanpa pengirim atau penerima dapat menarik kembali tindakannya.

2.2.3. **Website**

Menurut (Lukmanul hakim, 2004) Halaman web adalah sumber daya online yang menghubungkan dokumen secara lokal dan global. Halaman web dokumen yang ditemukan di situs web. Pengguna dapat berpindah antar halaman (hiperteks) di server yang sama atau di server lain di seluruh dunia dengan menggunakan tautan di situs web. Pengguna yang menggunakan browser seperti *Google Chrome*, *Mozilla Firefox*, dan lainnya dapat melihat dan membaca halaman.

2.2.4. **Webserver**

Mesin yang menyimpan, memproses, dan mengirimkan file halaman web ke browser web disebut server web. Server web terdiri dari perangkat keras dan perangkat lunak yang merespons permintaan dari pengguna web di World Wide Web menggunakan HTTP (Hypertext Transfer Protocol). Halaman yang diminta dimuat dan dikirimkan oleh server web melalui prosedur ini untuk ditampilkan di browser pengguna, seperti *Google Chrome*. Dari segi *hardware*, web server terhubung dengan internet sehingga file atau data dapat dibagikan ke perangkat lain yang terhubung. Apa pun dapat dimasukkan dalam data ini, termasuk foto, lembar gaya CSS, file *JavaScript*, dan file HTML. Perangkat lunak server web, yang mengatur cara pengguna online mengakses file yang disimpan, juga ditempatkan pada perangkat keras ini. Perangkat lunak ini terdiri dari beberapa bagian,.

2.2.5. **IP Address (Internet Protocol Address)**

Alamat IP, atau alamat Protokol Internet, adalah pengidentifikasi numerik yang digunakan setiap perangkat komputer yang terhubung ke internet untuk mengidentifikasi dirinya sendiri. Alamat IP sering kali digambarkan sebagai seperangkat pedoman yang mengontrol aktivitas internet dan memfasilitasi penyelesaian tugas online. Alamat IP terdiri dari beberapa digit. Empat adalah ekspresi angka. Ada satu hingga tiga digit di setiap kelompok bilangan bulat. Alamat IP dapat berupa angka antara 0 dan 255. Alamat IP diwakili oleh notasi 192(dot)168(dot)38.1. ID Jaringan dan ID Host adalah dua komponen yang membentuk alamat IP. Bagian alamat IP yang dikenal sebagai ID jaringan menunjukkan lokasi jaringan aktif. Dalam ilustrasi.

2.2.6. **Penetration Testing**

Pengujian penetrasi adalah mengirim atas otoritas yang sah dengan cara mengidentifikasi kerentanan dan memanfaatkannya untuk keuntungan pribadi. Peretasan yang terkontrol dapat digunakan untuk mengetahui tingkat keamanan suatu jaringan. Karena pengujian penetrasi tidak selalu membuktikan adanya kerentanan, pengujian ini cenderung lebih menekankan pada seni daripada ilmu peretasan. Selain itu, pengujian penetrasi yang tidak efektif tidak selalu menjadi penyebab pengujian gagal mengidentifikasi kerentanan.

2.2.7. **Penetration Testing Execuition Standard (PTES)**

Standar Eksekusi Pengujian Penetrasi (PTES) yang baru, yang terdiri dari tujuh komponen utama, diciptakan untuk memberikan perusahaan dan penyedia layanan keamanan kosakata dan ruang lingkup yang konsisten untuk melaksanakan tes penetrasi. menjelaskan tahap awal pengujian penetrasi dan motivasi di baliknya. Hal ini juga mencakup pengumpulan informasi, pemodelan ancaman, dan penelitian kerentanan, eksploitasi, dan pasca-eksploitasi, di mana penguji melakukan pengujian