BAB II
KAJIAN TEORI

2.1. Penelitian Sebelumnya

Pada penelitian ini menggunakan studi literatur sebagai media untuk mencari referensi sekaligus melengkapi data untuk menjelaskan masalah yang akan dikaji. Berdasarkan tema dan metode yang digunakan, maka penulis menggunakan beberapa jurnal yang terkait, yaitu sebagai berikut:

Penelitian sebelumnya yang berjudul "Analisis Keamanan Website *E-Learning* SMKN 1 Cibatu Menggunakan Metode *Penetration Testing Execution Standard* " yang dilakukan oleh Setyo Utoro, Bayu Andi Nugroho, Meinawati, dan Septian Rheno Widianto [3]. Penelitian ini dilakukan karena pada masa pandemi covid-19 ini penyampaian informasi dilakukan secara online serta banyaknya calon siswa yang melakukan pendaftaran secara online di SMKN 1 Cibatu. Dengan adanya hal tersebut, perlu dilakukan pengujian keamanan sistem informasi disekolah itu. Dan penelitian ini menggunakan metode *Penetration Testing Execution Standard* (PTES). Hasil penelitiannya ditemukan kerentanan seperti *Cross Site Scripting, Cross Site Request Forgery,* dan *Eavesdropping* yang dapat berakibat kebocoran data.

Selanjutnya, penelitian yang dilakukan oleh Sahren, Ruri, dan Muhammad Amin yang berjudul "*Penetration Testing* untuk Deteksi *Vulnerability* Sistem Informasi Kampus" [1]. Penelitian menggunakan metode *penetration testing* yang digunakan untuk mengaudit keamanan webserver sistem informasi kampus. Pengujian yang dilakukan pada penelitian ini yaitu untuk mencari *vulnerability* pada webserver dan juga untuk mengurangi resiko terjadinya penyalahgunaan terhadap sumber daya yang ada di suatu perguruan tinggi. Penelitian ini menggunakan beberapa domain yang berbeda dari kampus. Dan hasilnya terdapat dua alamat website yang celahnya memiliki tingkat sedang dan rendah. Serta ditemukan beberapa celah lain yang dapat mengakibatkan terjadinya memanipulasi file, mengganggu kinerja server, *clickjacking,* serta *cross site request forgery.*

Penelitian yang dilakukan oleh Ade Bastian, Harun Sujadi, dan Latiful Abror dengan judul "Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing dan Sql Injection" [5]. Pada penelitian ini masih menggunakan metode yang sama yaitu metode *penetration testing*. Penelitian ini dilakukan untuk mengantisipasi terjadinya serangan dan ancaman seperti pengubahan data, akses yang tidak diijinkan terhadap aplikasi dapodik. Dan dari penelitian tersebut dihasilkan bahwa aplikasi dapodik tidak dapat diserang dengan menggunakan Teknik SQL *injection* dan tingkat ancaman yang terdapat diaplikasi dapodik berada dilevel 0 atau aman. Serta belum ditemukannya celah yang memungkinkan terjadinya ancaman dan akses illegal yang berpotensi merusak sistem.

Kemudian penelitian sebelumnya dengan judul "Evaluasi Keamanan Website Lembaga X Melalui *Penetration Testing* Menggunakan Framework ISSAF" yang dilakukan oleh I Gede Arya, Gusti Made, dan Dewa Made [6]. Penelitian ini masih menggunakan metode *penetration testing.* Penelitian ini dilakukan pada Lembaga pemilihan umum yang memiliki situs berbasis website yang digunakan sebagai media penyampaian informasi dan data pemilih. Situs website pada Lembaga ini sering menjadi sasaran serangan dari pihak luar dan pada tahun 2014 website ini mengalami serangan *deface* yang mengakibatkan website tersebut tidak dapat diakses. Tujuan dari penelitian ini yaitu untuk mengetahui celah keamanan yang terdapat diwebsite sehingga dapat dilakukan peningkatan pada aspek keamanan website. Hasil dari penelitian ini yaitu ditemukan keamanan yang berbahaya seperti SQL *injection,* dan XSS pada website serta port TCP yang terbuka pada website Lembaga X.

Pada penelitian yang berjudul "Analisis Keamanan Webserver Menggunakan *Penetration Testing*" oleh Fahmi Fachri, Abdul Fadlil, dan Imam Riadi" [7]. Penelitian ini masih menggunakan metode yang sama yaitu *penetration testing* dan dilakukan pada web server dari sistem informasi akademik perguruan tinggi. Penenilitan ini dilakukan dikarenakan seringnya terjadi permasalahan seperti *hacking sistem,* dirubah file index hingga menginjektkan file backdoor dalam sistem, dan serangan yang terus menerus pada website akademik. Penelitin ini

dilakukan dengan tujuan untuk mencari kelemahan keamanan pada web server. Hasil dari penelitin ini yaitu didapatkan tiga kategori level hight, medium, dan low. Bagian yang dilakukan penyeranga yaitu pada port 22 mengenai ssh. Dan terdapat bug pada sistem yang dapat dimanfaatkan penyerang sebagai celah keamanan.

Ringkasan penelitian terdahulu pada table dibawah ini:

Table 2.1 Penelitian Terdahulu

No	Peneliti, Tahun	Judul Penelitian	Metode	Hasil
1	Setyo Utoro, Bayu Andi Nugroho, Meinawati, dan Septian Rheno Widianto, 2020	Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard	*Penetration Testing*	Hasil dari penelitian ini yaitu ditemukan celah serangan yang paling tinggi seperti *Cross Site Scripting, Cross Site Request Forgery*, dan *Eavesdropping* yang berpotensi mengakibatkan kebocoran data.
2	Sahren, Ruri Ashari Dalimuthe, dan Muhammad Amin, 2019	Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus	*Penetration Testing*	Hasil dari pengujian tersebut terdapat dua domain yang *threat* levelnya medium dan satu domain yang *threat* levelnya high. Serta ditemukan beberapa celah kelemahan pada sistem informasi kampus yang nantinya dapat digunakan untuk memanipulasi file, mengganggu kinerja server, *clickjacking*, serta *cross site request forgery*.
3	Ade Bastian, Harun Sujadi, dan Latiful Abror, 2020	Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing Dan Sql Injection	*Penetration Testing* dan SQL *Injection*	Dari penelitian tersebut dihasilkan bahwa aplikasi dapodik tidak dapat diserang dengan menggunakan Teknik SQL *injection* dan tingkat ancaman yang terdapat diaplikasi dapodik berada dilevel 0 atau aman. Serta belum ditemukannya celah yang

No	Peneliti, Tahun	Judul Penelitian	Metode	Hasil
				memungkinkan terjadinya ancaman dan akses illegal yang berpotensi merusak sistem.
4	I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, dan Dewa Made Sri Arsa, 2020	Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF	*Penetration Testing* dan *Framework* ISSAF	Hasil dari penelitian ini yaitu ditemukan keamanan yang berbahaya seperti SQL *injection*, dan XSS pada website serta port TCP yang terbuka pada website Lembaga X.
5	Fahmi Fachri, Abdul Fadlil, dan Imam Riadi, 2021	Analisis Keamanan Webserver Menggunakan Penetration Test	*Penetration Testing*	Hasil dari penelitin ini yaitu didapatkan tiga kategori level hight, medium, dan low. Bagian yang dilakukan penyeranga yaitu pada port 22 mengenai ssh serta terdapat bug dalam website.

2.2. Dasar Teori

2.2.1. Website

Website adalah salah satu media informasi yang ada di internet. Website sendiri mempunyai pengertian yaitu sebutan dari kumpulan halaman web yang merupakan bagian dari nama domain atau subdomain di *World Wide Web* (WWW). Sebuah halaman web adalah sebuah dokumen yang ditulis dalam format html yang dapat diakses melalui http atau https. Halaman dari situs web dapat diakses melaui URL yang disebut beranda. Web dapat dibuka dengan browser baik pada komputer maupun smartphone. Diantaranya seperti mozilla, internet explorer, firefox, opera, google chrome, dan lain-lain. [8]

2.2.2. Web server

Menurut Effendi Yusuf, web server adalah perangkat lunak yang menyediakan layanan data berfungsi untuk menerima permintaan *Hypertext Transfer Protocol* (HTTP) oleh pengguna dan mengirimkan kembali hasilnya dalam baik berupa teks, gambar, animasi, dan video [9]. Selain berfungsi untuk mengolah data, webserver juga berfungsi untuk mengirimkan data baik dalam bentuk foto, video, dan teks sesuai dengan permintaan dari client.

2.2.3. Sistem Informasi

Menurut Jogiyanto (2009) sistem informasi adalah sistem dalam organisasi yang memproses transaksi sehari-hari, mendukung operasi, manajemen dan aktivitas strategi organisasi serta memenuhi kebutuhan penyediaan informasi spesifik, bersama dengan laporan yang diperlukan kepada pihak eksternal [10]. Sistem informasi adalah sistem yang menggabungkan aktivitas manusia dan teknologi untuk kegiatan manajemen serta operasional. Tujuan dari sistem informasi adalah untuk menciptakan produk yang berisi kumpulan informasi. Sistem informasi bisa berupa website, aplikasi, blog.

2.2.4. Keamanan Jaringan

Keamanan jaringan adalah pendekatan untuk mengendalikan sumber daya jaringan. Tujuan dari pengontrolan akses jaringan yaitu supaya jaringan tersebut hanya bisa diakses oleh pihak tertentu yang memiliki hak untuk mengaksesnya [5].

2.2.5. Cyber Attack

Cyber attack adalah serangan yang dapat terjadi dalam dunia maya baik yang ditunjukkan untuk melakukan serangan atau pertahanan yang mengakibatkan terjadinya kerusakan pada objek yang dituju [11]. Ada banyak *cyber attck* yang dapat menyerang sebuah website, diantaranya yaitu *sql injection* (teknik *hacking* dimana penyerang memasukkan perintah sql melalui url untuk dieksekusi oleh database), *remote code/command execution* (jenis serangan dimana penyerang melakukan eksekusi kode dari jarak jauh), *cross site scripting attacks* (merupakan serangan yang dilakukan dengan cara penyerang memasukkan kode pemrograman tertentu ke dalam situs tersebut), dan banyak lagi jenis *cyber attack* lainnya [12].

2.2.6. Penetration testing

Penetration testing atau uji penetrasi adalah sebuah upaya untuk mengetahui kelemahan dari sistem informasi dengan tujuan agar sistem informasi tersebut lebih aman dengan secara legal dan berwenang [13]. *Penetration testing* merupakan suatu kegiatan berupa simulasi yang dilakukan oleh pihak yang sudah memiliki ijin untuk melakukan eksploitasi suatu sistem berdasarkan celah keamanan yang ada. *Penetration testing* berbeda dengan hacking, dimana kegiatan hacking tidak memiliki ijin untuk melakukan serangan terhadap sistem tersebut. Tujuan dari *penetration testing* adalah untuk mengidentifikasi kerentanan dalam sistem keamanan. Pengujian penetrasi dapat digunakan untuk pengujian kebijakan keamanan sistem yang terdapat pada perusahaan atau organisasi untuk melakukan identifikasi dan penanganan jika masalah tersebut mengancam keamanan sistem[6]. Proses *penetration testing* terdiri dari pengumpulan informasi, identifikasian celah-celah keamanan, dan melakukan pelaporan terhadap hasil dari pengujian yang dilakukan.

2.2.7. *Information Sistem Security Assessment Framework* (ISSAF)

ISSAF (*Information Sistem Security Assessment Framework*) adalah framework yang pengguanannya terarah dan terdiri dari langkah dalam pengelompokkan informasi, penilaian dan laporan hasil pengujian sistem keamanan terhadap domain yang diuji serta melakukan Analisa terhadao

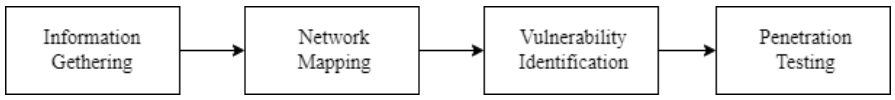
hasilnya[14]. Dalam ISSAF ini memiliki tiga fase pendekatan, diantaranya adalah sebagai berikut:

1. Fase *planning and preparation*

   Tahapan awal yang terdiri dari persiapan serta pengumpulan informasi dari web target yang akan dilakukan *penetration testing* [15].

2. Fase *Assessment*

   Langkah pengujian pada sistem informasi yang terdiri dari empat langkah yaitu :



Gambar 2. 1 *Fase Assesment*

   Berikut adalah penjelasan dari masing-masing langkah pada gambar diatas:

   a. *Information Gethering*

      Pengumpulan informasi umum terkait sistem informasi target seperti alamat ip, informasi domain, email, dan lain-lain.

   b. *Network Mapping*

      Tahap ini dilakukan untuk mengetahui informasi seperti nama port, jenis, serta versi port yang terbuka.

   c. *Vulnerability Identification*

      Yaitu mengidentifikasi kerentanan atau kelemahan pada sistem informasi target.

   d. *Penetration*

      Yaitu dengan melakukan pengujian terhadap sistem keamanan target [16].

3. Fase *Reporting*

   Pada fase ini yaitu membuat laporan dari hasil yang sudah didapatkan dari fase sebelumnya.

2.2.8. Kali Linux

Linux adalah sistem operasi yang bersifat terbuka atau *open source*, yang memiliki arti bahwa sistem operasi ini dapat dikembangkan oleh siapa saja.

Sistem operasi ini diciptakan oleh Linus Benedict Torvolds, yang mana beliau 17ini adalah seorang *hacker*. Kali linux merupakan salah satu jenis linux. Kali linux banyak digunakan untuk *penetration testing* baik terhadap website maupun jaringan komputer. Kali linux ini dikembangkan oleh *Offensive Security* [12].

2.2.9. Virtual Box

Virtualbox adalah sebuah program *open source* yang berkaitan dengan virtualisasi. Virtualisasi sendiri merupakan sebuah teknologi yang bisa digunakan oleh pengguna untuk memiliki komputer beserta dengan sistem operasi yang seoalah-olah seperti nyata[17]. Virtualbox dikeluarkan oleh innotec GmbH yang kemudian dibeli oleh Sun Microsistems pada tahun 2008 yang sekarang dikembangkan oleh Oracle. Perangkat lunak ini diinstall dalam sistem operasi utama sebagai sebuah aplikasi. Yang mana aplikasi ini dapat memungkinkan sistem operasi utama untuk menginstall sistem operasi tambahan pada host OS, masing-masing dikenal dengan istilah Guest OS.

2.2.10. OWASP ZAP

Owasp zap merupakan sebuah *tools* untuk membantu mendeteksi kerentanan keamanan pada *web application*. Menurut website resmi Owasp zap, Owasp zap didefinisikan sebagai komunitas terbuka yang memungkinkan untuk bisa dikembangkan oleh masing-masing individua tau organisasi. Owasp zap dapat diinstall dalam berbagai jenis sistem operasi seperti windows, linux, maupun macOs.

2.2.11. Jenis-Jenis Serangan

Berikut ini ada beberapa jenis serangan yang mungkin dapat menyerang sebuah sistem keamanan website dianataranya sebagai berikut:

1. Serangan DDos (Denial of Service)

   DDoS merupakan sebuah serangan yang bekerja dengan cara membajiri permintaan dari pengguna ke sumber daya server. Hal ini bertujuan agar server tidak mampu untuk menangani banyaknya permintaan pengguna. Sehingga server tidak dapat bekerja dengan benar [18].

2. Serangan Brute Force

Serangan *brute force* merupakan teknik serangan pada sebuah sistem keamanan komputer yang dilakukan dengan cara melakukan percobaan terhadap semua kunci yang memunyai kemungkinan benar [19]. *Brute force* ini digunakan untuk melakukan pembobolan akses ke suatu host (server/network/workstation) atau terhadap data yang terenkripsi. *Brute force* ini banyak dipakai oleh penyerang untuk mendapatkan akun secara tidak sah. Serangan *brute force* ini akan memakan banyak waktu apabila suatu pengguna menggunakan kombinasi password yang sulit untuk ditebak. Lama tidaknya serangan ini bergantung pada tingkat kerumitan pengguna dalam membuat password. Semakin rumit paswordnya maka akan semakin lama waktu yang dibutuhkan penyerang.

3. Serangan Clickjacking

   Adalah jenis serangan yang terjadi pada aplikasi berbasis website. Serangan ini akan membuat korbannya secara tidak sengaja mengklik sebuah elemen pada halaman web yang seharusnya tidak ingin diklik. Serangan ini biasanya dilakukan dengan memanipulasi tampilan halaman website.

4. Serangan SQL Injection

   SQL sendiri merupakan kepanjangan dari *Structured Query Language.* SQL adalah sebuah bahasa tingkat empat yang mempunyai fungsi untuk menampilkan hasil atau melakukan sesuatu terhadap data yang tidak diinginkan. Sedangkan SQL *injection* merupakan sebuah teknik *hacking* yang memiliki tujuan untuk menyusup ke dalam sistem agar bisa mengetahui isi dari database sebuah website. Serangan ini terjadi karena terdapat sebuah kode program lemah serta keamanan yang kurang dari pengelola website [20].