BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Pada jurnal (Dewanto, 2018) dengan judul "**Penetration Testing pada Domain UII.AC.ID Menggunakan OWASP 10**". Dari hasil penelitian ini dapat diketahui tingginya keamanan sebuah website dalam menghadapi serangan, maka dari itu peneliti menganggap diri sendiri sebagai orang yang sedang mencoba memasuki website dan dari hasil penelitian yang dilakukan dijadikan sebagai saran bagi pengembang sistem.

Pada jurnal (Mushlih, Fitri & Wardiah, 2019) yang berjudul "**Penetration Testing Tool Untuk Menguji Kerentanan SQL Injection Secara Otomatis Berbasis Web**" dari hasil analisisnya yang membuktikan kalau aplikasi website adalah sasaran yang selalu diserang oleh hacker dengan serangan SQL Injection.

Pada jurnal (Tenggono, Purnama, 2018) yang berjudul "**Audit keamanan webserver pada website "www.palcomtech.com"**. Penelitian tersebut untuk menguji dan menganalisis keamanan pada web server yang bertujuan untuk meningkatkan tingkat keamananan pada website tersebut.

Penelitian yang dilakukan oleh (Yunanri, Riadi, Yudhana, 2016) dengan judul "**Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST)**". Yang dimana dengan metode ini dapat memperkirakan dampak dari masing-masing faktor serta membantu para perancang website menyadari resiko kemungkinan terjadinya serangan dan dapat mengambil tindakan yang benar untuk mencegah ataupun mengatasinya.

Suhendi. Analisis Tingkat Kerentanan Keamanan pada Website Simpabu Sistem Monitoring Penyuluhan Agama Buddha Non PNS Kantor Wilayah Kementerian Agama Provinsi Kepulauan Riau Dengan Metode Penetration Testing Execution Standard (PTES).
UIB Repository©2020

Penelitian berjudul "**Auditing Albaha University Network Security using in-house Developed Penetration Tool**" yang dilakukan oleh (Alzahrani, 2017). Dalam menganalis tingkat kerentanan dengan menggunakan aplikasi testing yaitu Nessus untuk mengetahui titik-titik kelemahan dari sebuah website.

Tabel 1 Hasil Penelitian

Peneliti	Judul Penelitian	Tahun	Hasil Penelitian
Yunanri, Riadi, Yudhana	Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST)	2016	Sebuah metode yang dapat memperkirakan dampak dari masing-masing faktor serta membantu para perancang website menyadari resiko kemungkinan terjadinya serangan dan tindakan yang benar untuk menghindari ataupun mengatasinya.
Alzahrani	Auditing Albaha University Network Security using in-house Developed Penetration Tool	2017	Pengujian tingkat keamanan dengan aplikasi Nessus untuk mengetahui titik-titik kelemahan sebuah website.
Dewanto	Penetration Testing pada Domain UII.AC.ID Menggunakan OWASP 10	2018	Dari hasil penelitian ini dapat diketahui tingginya keamanan sebuah website dalam menghadapi serangan.

Suhendi. Analisis Tingkat Kerentanan Keamanan pada Website Simpabu Sistem Monitoring Penyuluhan Agama Buddha Non PNS Kantor Wilayah Kementerian Agama Provinsi Kepulauan Riau Dengan Metode Penetration Testing Execution Standard (PTES).
UIB Repository©2020

Peneliti	Judul Penelitian	Tahun	Hasil Penelitian
Tenggono, Purnama	Audit keamanan webserver pada website "www.palcomtech.com"	2018	Menguji dan menganalisis keamanan pada web server yang bertujuan untuk meningkatkan tingkat keamananan pada website tersebut.
Mushlih, Fitri & Wardiah	Penetration Testing Tool Untuk Menguji Kerentanan SQL Injection Secara Otomatis Berbasis Web	2019	Aplikasi website adalah sasaran yang selalu diserang oleh hacker dengan serangan SQL Injection.

Berdasarkan hasil penelitian di atas maka penulis akan melakukan pengujian dan analisis tingkat kerentanan keamanan pada website Penyuluhan Kementrian Agama dengan metode PTES dan akan memberikan hasil dari pengujian kepada pihak pengembang website supaya meminimalkan resiko masukan serangan dari pihak luar atau *hacker*.

Suhendi. Analisis Tingkat Kerentanan Keamanan pada Website Simpabu Sistem Monitoring Penyuluhan Agama Buddha Non PNS Kantor Wilayah Kementerian Agama Provinsi Kepulauan Riau Dengan Metode Penetration Testing Execution Standard (PTES).
UIB Repository©2020

2.2 Landasan Teori

2.2.1 Keamanan Informasi

Merupakan perlindungan informasi terhadap segala ancaman yang mungkin terjadi dan dapat menjamin berjalannya bisnis dengan lancar, meminimalisir resiko-resiko bisnis serta pengembalian asset yang stabil (Ali, Sabir & Ullah, 2019).

Berikut terdapat 3 prinsip dasar dari keamanan informasi sebagai berikut:

1. *Integrity*

   Menjaga serta menjamin kelengkapan dari sebuah data yang tidak dapat diubah secara tidak sah (Ali, Sabir & Ullah, 2019).

2. *Availability*

   Ketersedian informasi yang dapat diakses pada saat dibutuhkan dan yang di mana sistem tersebut dapat menyimpan data serta memproses informasi (Ali, Sabir & Ullah, 2019).

3. *Confidentiality*

   Sebuah tempat penyimpanan informasi yang dimana informasi tersebut tidak dapat diketahui kepada orang yang tidak memiliki wewenang (Ali, Sabir & Ullah, 2019).

2.2.2 *E-Government*

Merupakan sebuah program dari pemerintah yang di mana bertujuan untuk mengembangkan implementasi tata kelola dalam berbasis elektronik dan transfomasi untuk kegiatan masyarakat dan bisnisnya (Huda, 2020).

Suhendi. Analisis Tingkat Kerentanan Keamanan pada Website Simpabu Sistem Monitoring Penyuluhan Agama Buddha Non PNS Kantor Wilayah Kementerian Agama Provinsi Kepulauan Riau Dengan Metode Penetration Testing Execution Standard (PTES).
UIB Repository©2020

2.2.3 *Consumer To Government* (C2G)

Merupakan sebuah proses transaksi bersifat elektronik yang dilakukan oleh seseorang terhadap pemerintah (Putra, Muhazir, Hutahaean, Syah, 2020).

2.2.4 Website

Merupakan salah satu aplikasi yang di mana berisi teks, gambar, suara, animasi dan video yang menggunakan protokol HTTP untuk mengaksesnya dari browser (Hasugian, 2018).

2.2.5 Penyuluhan Agama

Merupakan seseorang yang diberikan wewenang serta tanggung jawab dalam melaksanakan bimbingan keagamaannya dari pemerintah (Kadir, 2017).

2.2.6 *Web Server*

Merupakan salah satu bagian penting bagi sebuah website, *Web Server* ini gunanya adalah melayani segala request dari website selama 24 jam dan ketika *Web Server* mati maka layanan website tidak akan dapat diakses (Sumbogo, Data, Siregar, 2018).

2.2.7 *Flowchart*

Merupakan sebuah bagian yang berfungsi sebagai menunjukan diagram dari sebuah proses dengan simbol dalam menyelesaikan masalah (Halik, Budiyanto, Benedicta, 2019).

2.2.8 *Penetration Testing*

Merupakan sebuah kegiatan yang dilakukan untuk menguji sebuah kerentanan keamanan pada sebuah aplikasi dan mengetahui resiko yang akan terjadi kedepannya (Yunanri, 2016). Dan dibawah ini terdapat 3 model pentest sebagai berikut:

Suhendi. Analisis Tingkat Kerentanan Keamanan pada Website Simpabu Sistem Monitoring Penyuluhan Agama Buddha Non PNS Kantor Wilayah Kementerian Agama Provinsi Kepulauan Riau Dengan Metode Penetration Testing Execution Standard (PTES).
UIB Repository©2020

1. *Black Box*

   Merupakan sebuah tipe pengujian yang lebih berfokus terhadap sudut pandang external, disini pengujian hanya mencari *input* dan *output* dari sebuah sistem (Robertus, 2017).

2. *White Box*

   Merupakan sebuah tipe pengujian yang lebih berfokus terhadap sudut pandang internal, disini pengujian terhadap kesalahan terhadap fungsional yang spesifik (Robertus, 2017).

3. *Gray Box*

   Merupakan sebuah tipe pengujian yang didapatkan dari kombinasi dari *black box* dan *white box*, disini pengujian tersebut menggunakan *framework* yang digunakan oleh aplikasi (Robertus, 2017).

2.2.9 *Penetration Testing Execution Standard* (PTES)

Merupakan kegiatan di mana seseorang harus mencoba menyerang sebuah aplikasi atau sistem untuk menemukan celah atau kelemahan keamanan yang terdapat dalam sebuah aplikasi (Kholiq & Khoirunnisa, 2019). Berikut terdapat 7 tahapan yang harus dilakukan dalam melakukan pengujian testing.

1. *Pre-engagement*

   Tahap di mana seorang tester akan menjelaskan semua kegiatan yang akan dilakukannya kepada client atau user (Kholiq & Khoirunnisa, 2019).

Suhendi. Analisis Tingkat Kerentanan Keamanan pada Website Simpabu Sistem Monitoring Penyuluhan Agama Buddha Non PNS Kantor Wilayah Kementerian Agama Provinsi Kepulauan Riau Dengan Metode Penetration Testing Execution Standard (PTES).
UIB Repository©2020

2. *Intelligence gathering*

   Tahap di mana seorang tester akan mengumpulkan sebanyak mungkin informasi yang dapat membantu dalam proses pengujiannya (Kholiq & Khoirunnisa, 2019).

3. *Threat modeling*

   Tahap di mana seorang tester mencoba mencari kelemahan dari informasi yang dikumpulkan sebelumnya (Kholiq & Khoirunnisa, 2019).

4. *Vulnerability analysis*

   Tahap di mana seorang tester mencoba menggabungkan informasi mengenai kelemahan aplikasi yang ada dengan serangan yang bisa dilakukan untuk melakukan serangan yang efektif (Kholiq & Khoirunnisa, 2019).

5. *Exploitation*

   Tahap di mana seorang tester melakukan proses serangan terhadap aplikasi (Kholiq & Khoirunnisa, 2019).

6. *Post exploitation*

   Tahap di mana seorang tester melakukan analisis ketika berhasil memasuki ke dalam sistem aplikasinya (Kholiq & Khoirunnisa, 2019).

7. *Reporting*

   Tahap di mana seorang tester akan membuat laporan mengenai pengujian yang dilakukan dari hasil yang didapatkan dan dijelaskan kepada client atau user (Kholiq & Khoirunnisa, 2019).

Suhendi. Analisis Tingkat Kerentanan Keamanan pada Website Simpabu Sistem Monitoring Penyuluhan Agama Buddha Non PNS Kantor Wilayah Kementerian Agama Provinsi Kepulauan Riau Dengan Metode Penetration Testing Execution Standard (PTES).
UIB Repository©2020

2.2.10 *Vulnerabilty Assessment*

Merupakan sebuah bentuk kontrol terhadap insiden yang akan terjadi pada sebuah sistem (Wibowo, Harjono, Wicaksono, 2019).

2.2.11 *Secure Socket Layer* (SSL)

Protokol yang digunakan untuk mengakses sebuah web dengan aman serta tindakan protokol untuk mengamankan secara langsung komunikasi antara client dan server (Aditya, Farida, Ramadhani, 2018).

2.2.12 *Framework*

Sebuah kerangka yang dipergunakan dalam pengembangan sistem yang di mana dapat menghemat waktu dan usaha bagi perancang (Aini, Rahardja, Madiistriyatno, Setiaji, 2018).

2.3 Tools yang digunakan

2.3.1 *Geekflare*

Merupakan sebuah alat bantu yang digunakan untuk mengaudit sebuah performa dari sebuah website (Kurniawan, 2020).

2.3.2 *Wappalyzer*

Merupakan alat yang mengungkapkan teknologi yang digunakan pada situs website target pada umumnya (Ondrackova, 2018).

2.3.3 *Nessus*

Merupakan perangkat lunak pemindaian yang bisa dipergunakan untuk mengaudit keamanan suatu sistem, contohnya kerentanan, kesalahan konfigurasi, patch keamanan yang masih belum diterapkan, kata sandi tetap, serta penolakan layanan,

Suhendi. Analisis Tingkat Kerentanan Keamanan pada Website Simpabu Sistem Monitoring Penyuluhan Agama Buddha Non PNS Kantor Wilayah Kementerian Agama Provinsi Kepulauan Riau Dengan Metode Penetration Testing Execution Standard (PTES).
UIB Repository©2020

Fungsi utama dari *Nessus* adalah memantau lalu lintas jaringan. *Nessus* adalah sebuah alat pengujian yang andalan ketika melakukan pengujan keamanan pada sebuah sistem.

Suhendi. Analisis Tingkat Kerentanan Keamanan pada Website Simpabu Sistem Monitoring Penyuluhan Agama Buddha Non PNS Kantor Wilayah Kementerian Agama Provinsi Kepulauan Riau Dengan Metode Penetration Testing Execution Standard (PTES).
UIB Repository©2020