BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan dan evolusi dalam dunia komputer, *internet* dan teknologi *web* telah begitu pesatnya berkembang sehingga masuk dalam segala lini kehidupan masyarakat kini masyarakat bergantung pada layanan jaringan komputer melebihi masa sebelumnya. Hal ini dapat dilihat dengan semakin banyaknya pengguna media sosial dan layanan internet saat ini.

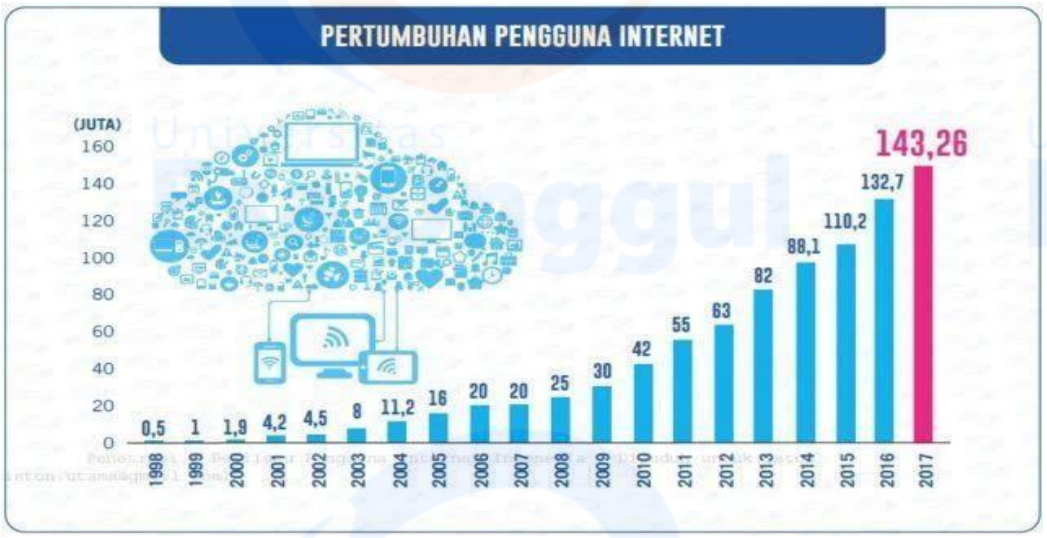
Gambar 1.1 Jumlah pengguna internet menurut APJII pada tahun 2016

Referensi : https://inet.detik.com/telecommunication/d-4551389/pengguna-internet-indonesia-didominasi-milenial

Menurut laporan Asosiasi Penyelenggara Jasa Internet Indonesia(APJII) pada tahun 2016 seperti yang terlihat pada Gambar 1.1 menunjukan jumlah pengguna Internet di Indonesia tahun 2016 adalah 132,7 juta *user* dari total jumlah penduduk Indonesia sebesar 256,2 juta Jika dibandingkan penggunaan internet Indonesia pada tahun 2014 sebesar 88,1 juta *user*, maka terjadi kenaikan sebesar 44,6 juta dalam waktu 2 tahun (2014 – 2016) dan masih didominasi pulau Jawa sebagai pengguna internet terbanyak di Indonesia seperti yang terlihat[1].

Pada Gambar 1.2 di bawah. Pengguna *internet* di Indonesia diprediksi

akan terus meningkat setiap tahun.



Gambar 1.2 Jumlah pengguna internet pada tahun 2016

Referensi : https://marketeers.com/143-juta-internet-user-di-indonesia56566-2/

Dengan semakin bertambahnya pengguna layanan internet maka semakin banyak informasi yang dapat diperoleh dari internet. Informasi sendiri menjadi hal penting di era digital ini baik untuk organisasi, bisnis maupun individu. Begitupun sebaliknya menjadi perhatian khusus bagi para pengembang *web* informasi khususnya sistem informasi berbasis *web* untuk membuat *website* yang dapat menjamin keamanan dan kerahasiaan informasi yang akan dikelola. Aspek-aspek yang harus dipenuhi dalam suatu *web* untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap (*right information*), informasi dipegang oleh orang yang berwenang (*right people*), dapat diakses dan digunakan sesuai dengan kebutuhan (*right time*), dan memberikan informasi pada format yang tepat (*right form*). Dalam membuat keamanan *web* informasi harus mengikuti prisnsip *CIA Triangel* Dasar yang harus dipenuhi agar *website* tersebut handal[2]. Prinsip dasar tersebut diantaranya:

1. *Confidentiality* (kerahasiaan)

Artinya keamanan informasi menjamin hanya orang-orang yang memiliki kewenangan terhadap informasi saja yang dapat mengakses informasi. Sehingga

kerahasiaan informasi terlindungi dari orang-orang yang tidak berwenang terhadap informasi. Contoh kerahasian informasi adalah seorang administrator tidak boleh membuka dan membaca akun email dan *password* pengguna. Selain itu kerahasiaan informasi harus menjamin penggunaan dan penyebarannya baik oleh pengguna maupun administrator, seperti misalnya informasi nama, alamat, tempat tanggal lahir, nomor handphone, nomor kartu kredit, nama ibu kandung, riwayat penyakit yang diderita, dan informasi pribadi lainnya milik pengguna harus dilindungi kerahasiaannya dari pihak-pihak yang tidak berwenang.

2. *Integrity* (integritas)

Artinya keamanan informasi menjamin kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang dapat mengakibatkan adanya perubahan informasi dari aslinya. Salah satu contoh ancaman kelengkapan dan kerusakan informasi adalah virus trojan. Virus tersebut dapat mengubah suatu informasi tanpa seizin dari pemilik informasi yang berwenang. Oleh sebab itu setiap informasi yang dikirim atau ditransimikan sebaiknya dilakukan *enkripsi* data terlebih dahulu untuk melindungi dan menjaga kerahasiaan informasi dari ancaman virus Trojan.

3. *Availability* (ketersediaan)

Artinya keamanan informasi menjamin pengguna atau pihak berwenang dapat mengakses dan menggunakan informasi kapanpun, dimanapun tanpa adanya gangguan kegagalan akses informasi. Salah satu hambatan dalam ketersediaan ini adalah adanya serangan *DoS* (*Denial of Service Attack*). *DoS* adalah serangan yang ditujukan ke server dalam bentuk pengiriman permintaan dalam jumlah yang sangat banyak sekali dan biasanya palsu sehingga menyebabkan server tidak sanggup lagi melayani permintaan karena tidak sesuai dengan kemampuan yang mengakibatkan server menjadi *down* bahkan *error*[3].

Universitas Esa Unggul sebagai salah satu lembaga pendidikan perguruan tinggi terkemuka di Indonesia memanfaatkan jaringan internet yaitu *web* sebagai media dalam menyampaikan informasi kepada pihak luar dan menghubungkan

civitas-civitas yang ada guna memudahkan dalam penyampaian informasi. Pertukaran informasi yang terjadi dalam jaringan internet dapat berupa informasi penting atau pribadi yang hak aksesnya hanya dapat dilakukan oleh orang-orang tertentu[4]. Jika 3 faktor dasar dalam keamanan informasi di atas itu tidak dapat terpenuhi maka suatu jaringan dapat dikategorikan tidak aman dan rawan tersusupi oleh pihak yang tidak bertanggung jawab. Dalam mengatasi masalah ini salah satu langkah yang dapat ditempuh adalah dengan melakukan analisis terhadap *web* dan jaringan yang terdapat pada Esa Unggul dari persepektif luar atau jaringan publik. Penelitian ini berfokus pada pengumpulan informasi dan pengujian *web* yang ada dengan metode *penetration testing* (*pentest*) berdasarkan pada metode *Open Web Application Security Project Top 10* (*OWASP 10*).

Salah satu pusat perhatian terhadap keamanan adalah dengan begitu cepatnya perkembangan internet yang menjadikan seluruh server terhubung satu dengan yang lainnya. Menjaga keamanan menjadi hal yang menakutkan ketika melihat begitu banyak peralatan perentas yang dapat digunakan untuk melancarkan serangan ke server secara automatis[5]. Meskipun proses peretasan tersebut berhasil dilakukan, dalam waktu yang singkat pula perangkat lunak baru bermunculan guna mengatasi serangan tersebut. Melakukan pencegahan secara aktif terhadap kerentanan dapat membantu mengidentifikasi layanan atau kerentanan yang tidak diinginkan secara dini sebelum dapat membahayakan sistem yang ada. Tidak sedikit untuk mengamankan data/asset yang dimiliki perusahaan merekrut para ahli keamanan yang lebih baik dikarenakan sumber daya yang ada belum dapat menanganinya.

Dasar Pengelolaan terhadap keamanan dapat dilihat dari sisi pengelolaan resiko (*risk management*). Lawrie Brown dalam menyarankan menggunakan "*Risk Management* Model" untuk menghadapi ancaman (*managing threats*). Ada tiga komponen yang memberikan kontribusi kepada *risk*, yaitu Asset, *Vulnerabilities*, dan *Threats*[6].

Langkah besar dalam mengukur tingkat risiko adalah menentukan dampak buruk yang dihasilkan dari analisa kerentanan. Hasil dari analisa kerentanan dapat membantu pengelola dan pengembang sistem untuk mencegah dan mengatasi

dampak risiko yang ditemukan pada sistem.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan di atas maka rumusan masalah yang ditetapkan:

a. Bagaimana menganalisis tingkat keamanan sistem informasi akademik di Universitas Esa Unggul dengan menggunakan metode *Web Penetration Testing*.
b. Bagaimana hasil dari pengujian tingkat keamanan *web* informasi akademik di Universitas Esa Unggul dengan *Penetration Testing*.
c. Bila terdapat celah kerentanan yang dapat ditembus, apa solusi atau saran untuk menutupi kerentanan tersebut.

1.3 Batasan Masalah

Batasan masalah pada penelitian tingkat keamanan sistem informasi akademik di Universitas Esa Unggul adalah sebagai berikut:

a. Penelitian ini hanya untuk menguji tingkat keamanan sistem informasi domain *web* akademik yang ada di Universitas Esa Unggul.
b. Hanya menggunakan metode *black* dan *white hat* yaitu metode penetration testing yang serupa dengan yang dilakukan aslinya karena peneliti hanya mengetahui domain saja dan informasi mengenai jaringan maupun informasi lainnya harus dicari sendiri oleh peneliti.
c. Uji coba yang digunakan pada penelitian ini adalah menggunakan uji coba non destruktif, yaitu uji coba yang tidak membuat kerusakan sistem.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian pengujian tingkat keamanan sistem informasi akademik di Universitas Esa Unggul ini adalah sebagai berikut :

a. Untuk mengetahui tingkat keamanan sistem informasi akademik yang ada di Universitas Esa Unggul.
b. Untuk mengetahui hasil dari pengujian tingkat keamanan sistem informasi akademik di Universitas Esa Unggul.
c. Untuk mengetahui solusi atau saran dari kerentanan yang dapat ditembus selama proses pengujian.

1.5 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian pengujian tingkat keamanan *web* informasi akademik di Universitas Esa Unggul ini adalah dapat mengembangkan dan meningkatkan keamanan sistem informasi akademik yang dimiliki oleh Universitas Esa Unggul sehingga kegiatan civitas akademika tetap terjaga kerahasiaan datanya.

1.6 Metodologi Penelitian

Metodologi penelitian ini dilakukan agar dalam proses pengujian yang dilakukan dapat lebih terarah, sesuai rencana dan mencapai tujuan yang diharapkan. Adapun metodologi yang diterapkan dalam pembuatan tugas akhir ini adalah sebagai berikut:

1.6.1 Pengecekan alamat IP

Pengecekan alamat *IP* dilakukan sebagai syarat utama melakukan *penetration testing* terhadap domain siakad.esaunggul.ac.id. Dan disini alamat *IP* siakad.esaunggul.ac.id : 182.16.164.230.

1.6.2 Footprinting

Tahap awal dalam melakukan penguasaan suatu *web* yaitu dengan cara mengumpulkan segala bentuk informasi penting mengenai *web yang* ber domain siakad.esaunggul.ac.id yang akan dilakukan *pentest*.

1.6.3 Scanning

Setelah mendapatkan informasi mengenai *web* target, proses selanjutnya adalah melakukan *scanning* yaitu proses dimana mencari *port* atau celah keamanan lain pada *web* yang dapat disusupi.

1.6.4 Uji Penetration

Melakukan pengujian celah kerentanan keamanan pada *web* ber domain siakad.esaunggul.ac.id menggunakan metode *OWASP* 10.

1.6.5 Pembuatan Laporan Pengujian

Proses penjabaran dan penjelasan hasil dari pengujian yang telah dilakukan menggunakan metode *OWASP* 10 disertakan solusi menurut metode pengujian.

1.7 Sistematika Penulisan

Untuk memberikan gambaran secara menyeluruh mengenai masalah yang akan dibahas dalam penulisan laporan tugas akhir ini, maka sistematika laporan ini dibagi menjadi 5 bab. Adapun penjabarannya sebagai berikut:

BAB I PENDAHULUAN

Bab pendahuluan berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan laporan *penetration testing* yang telah dilakukan pada domain *siakad.*esaunggul.ac.id menggunakan metode *OWASP* 10.

BAB II LANDASAN TEORI

Bab ini membahas tentang gambaran umum tentang teori yang diterapkan dalam pengujian *penetration testing*, menggunakan *OWASP* 10. Selain itu dalam bab ini juga terdapat penjelasan tentang metode dan *tools* yang digunakan untuk melakukan *penetration testing*.

BAB III METODOLOGI

Bab ini membahas tentang metode yang dilakukan dalam penelitian. Metode tersebut adalah pengumpulan data, analisis kebutuhan serta perancangan pembangunan *web* dan termasuk didalamnya perancangan pengujian yang dilakukan secara sistematis.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang langkah-langkah proses pengujian yang dilakukan dan hasil yang didapatkan dari proses pengujian yang dilakukan terhadap beberapa target yang ditentukan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi penutup yang meliputi kesimpulan-kesimpulan dari hasil pengujian yang telah dilakukan sebelumnya yang berupa hasil analisis pengujian yang telah dilakukan.