Bab I PENDAHULUAN

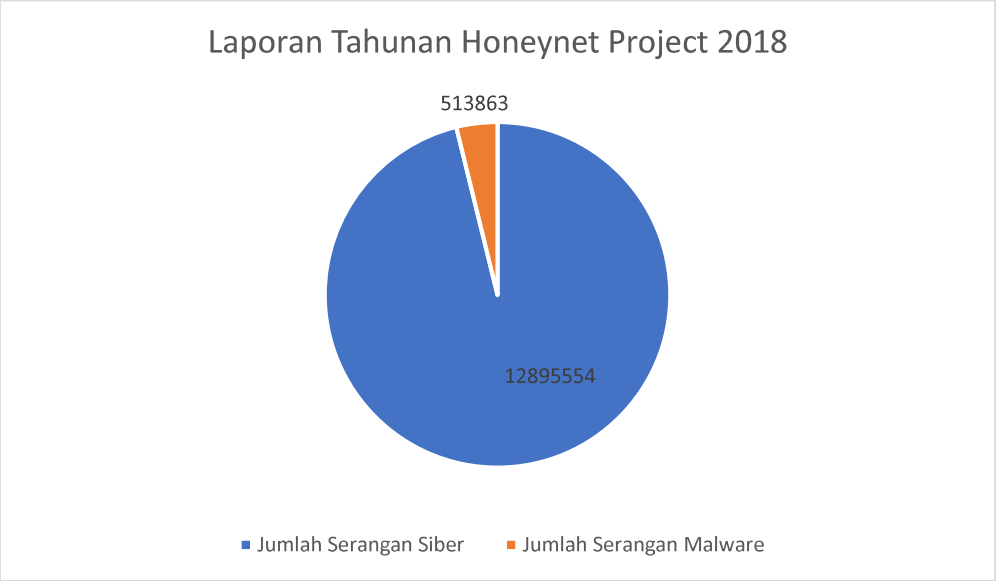
I.1 Latar Belakang

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Seringkali urutan keamanan berada diurutan kedua, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performa sistem, seringkali keamanan dikurangi atau bahkan ditiadakan. Terhubungnya komputer ke internet membuka potensi adanya celah keamanan informasi. (Hartiwati, 2014). Keamanan informasi yang tidak dirancang dengan baik dapat menyebabkan kebocoran data, pelanggaran privasi, hingga kerugian finansial. Oleh karena itu, dibutuhkan rekomendasi keamanan yang dapat memberikan informasi tentang cara meminimalisir celah kerentanan yang ada (Prabowo, 2015). Peran situs web dalam hal ini dapat digunakan untuk mendapat keuntungan secara finansial karena situs web dapat dijadikan sebagai media jual beli secara *online* atau digunakan untuk mengolah data yang dapat menghasilkan suatu informasi bagi pengguna. Hal ini membuat suatu instansi atau perusahaan bersaing untuk menyediakan layanan keamanan informasi yang terbaik.

Sistem yang dapat di retas oleh orang-orang yang tidak bertanggung jawab menandakan bahwa sistem tersebut memiliki celah. Hal ini dapat mengurangi tingkat kepercayaan dari pengguna sistem tersebut (Paryati, 2008). Sistem yang umumnya menjadi sasaran para hacker maupun *cracker* adalah aplikasi berbasis *website*. *Hacker* adalah orang yang mempelajari, menganalisis, memodifikasi, serta menerobos masuk ke dalam sistem jaringan atau aplikasi, baik untuk keuntungan secara pribadi atau kepentingan suatu organisasi. Tidak semua *hacker* bersifat negatif, ada beberapa pengelompokan *hacker* memiliki etika serta mengetahui dan menyadari seluruh akibat dari apa yang dilakukannya, dan bertanggung jawab atas apa yang dilakukannya. Cracker adalah seseorang yang menganalisa kelemahan suatu sistem yang bertujuan untuk, merusak atau mengacak-acak untuk keuntungan atau kepentingan sendiri yang bisa merugikan pihak lain. *Website* menjadi salah satu sasaran utama untuk diretas karena banyak digunakan dalam segala aspek

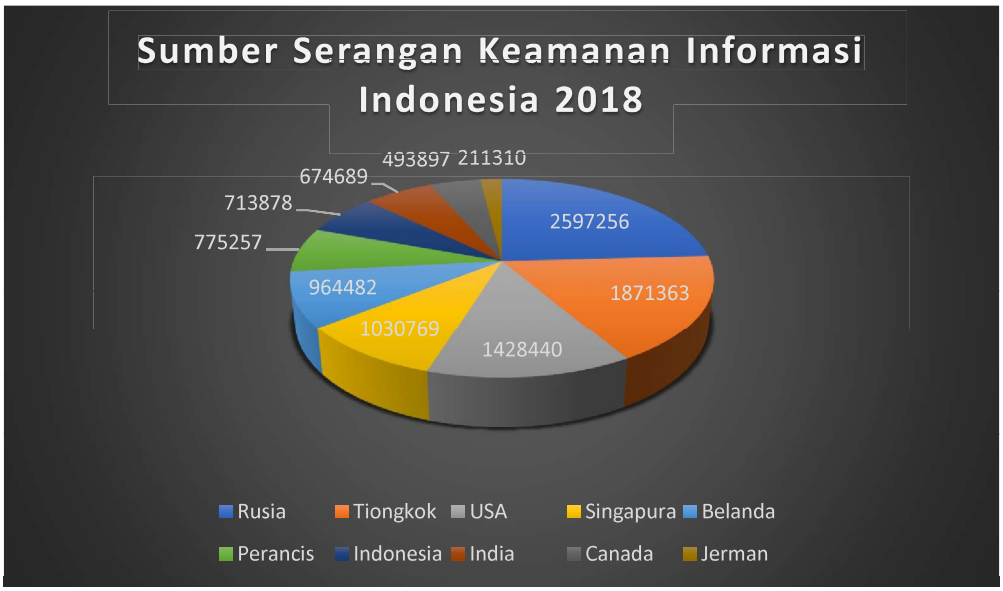
kehidupan, seperti *online shop*, perbankan, atau bahkan sebagai media untuk menyebarkan informasi baik secara visual maupun tertulis.

Dalam mencari celah dari *website* dapat digunakan dengan berbagai cara. Beberapa kemungkinan jenis serangan yang sering terjadi adalah *Structured Query Language* (SQL) *Injection*, *Denial of Service* (DoS), maupun memasukkan *malware* terhadap *website* tersebut. SQL *Injection* adalah jenis aksi *hacking* pada keamanan komputer di mana seorang penyerang bisa mendapatkan akses dan dapat merusak atau mengubah data yang ada didalam basis data di dalam sistem. SQL *Injection* dan *Cross Site Scripting* (XSS) mempunyai kesamaan dalam hal injeksi, yaitu dapat dilakukan *manual testing* dengan cara menginputkan kode injeksi. *Denial of Service* (DoS) adalah jenis kejahatan *cyber* yang dilakukan dengan cara mencegah pengguna mendapatkan akses ke suatu situs yang ingin dikunjungi dengan cara menganggu *server* situs tersebut. Untuk menyerang suatu *server*, para *attacker* akan membanjiri situs tersebut dengan *request* dari banyak sekali komputer sehingga *server* tidak mampu menampung *request* baru lagi. *Malware* adalah suatu program berbahaya yang dirancang untuk merusak suatu sistem. *Malware* mencakup virus, *worm, trojan horse, spyware,* dan *ransomware*. Ketika *malware* dimasukkan kedalam suatu *website*, *malware* ini dapat melakukan berbagai hal seperti mengambil alih sistem pada perangkat kita, membaca aktivitas dan bahkan mencuri data serta privasi dalam sistem *website* yang kita miliki.



Gambar I. 1 Data Serangan Siber dan Malware 2018

Berdasarkan penelitian yang dilakukan oleh Honeynet Project yang bekerja sama dengan Badan Siber dan Sandi Negara (BSSN) pada tahun 2018 dapat dilihat pada Gambar I.1 jumlah total serangan di Indonesia melalui internet berjumlah 13.409.417. Jumlah serangan tersebut terdiri dari 12.895.554 serangan siber dan 513.863 serangan *malware*. Data pada Gambar I.1 menunjukkan bahwa ancaman keamanan informasi di Indonesia harus diberikan perhatian lebih karena jumlah serangan siber dan *malware* mempunyai angka yang cukup besar.



Gambar I. 2 Sumber Serangan Keamanan Informasi Indonesia 2018 (BSSN, 2018)

Menurut hasil analisis yang dilakukan oleh Honeynet Project yang bekerja sama dengan Badan Siber dan Sandi Negara (BSSN) pada tahun 2018 yang dapat dilihat pada Gambar I.2 bahwa serangan keamanan informasi ke Negara Indoensia berasal dari berbagai Negara di dunia. Data pada Gambar I.2 menunjukkan bahwa sangat banyak para *hacker* dari berbagai Negara maupun dari Negara Indonesia yang ingin mencuri informasi atau merusak sistem pada situs web atau sistem operasi.

Pada situs web, penyerang dapat mengeksploitasi data dengan menyerang situs web target yang dapat menyebabkan kerusakan atau mencuri informasi sensitif yang ada pada situs web tersebut (Mohammadi, 2016). Berdasarkan penelitian yang telah dilakukan oleh *White Hat Security* dihasilkan informasi bahwa 86% dari 30.000 situs web diuji memiliki setidaknya satu kerentanan dengan level kerentanan *high*, dan sebagian besar memiliki lebih dari satu kerentanan dengan *risk level high* (Alsadoon, 2016). Situs web sulit untuk diamankan karena situs web terbuka untuk umum dan dapat diakses oleh semua orang, termasuk *hacker*. Kerentanan aplikasi web telah secara luas diakui sebagai masalah serius karena data pelanggaran karena kerentanan ini telah berulang dalam beberapa tahun terakhir dan kemungkinan akan terus menjadi utama masalah di masa depan (Bau, 2013).
Objek target dalam penelitian ini adalah Situs web Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Pada Pemerintah Daerah XYZ. Situs web tersebut disediakan oleh pemerintah daerah dalam memberikan layanan kepada masyarakat. Situs web ini menyediakan layanan *online* dalam bentuk aplikasi web untuk memfasilitasi masyarakat dalam mengakses informasi dan untuk mengurus hal-hal yang berkaitan dengan investasi dan proses pemenuhan perizinan bisnis pada Pemerintah Daerah XYZ. Situs web ini menyimpan banyak data publik dan pemerintah yang sensitif. Karena itu, dibutuhkan sistem keamanan informasi yang baik pada situs web ini untuk meminimalkan para peretas yang ingin mengambil data.

Pada penelitian ini, untuk melakukan pengujian kerentanan menggunakan sistem operasi Kali Linux. Alasan penggunaan sistem operasi Kali Linux dalam penelitian ini dikarenakan sistem operasi ini mempunyai keunggulan pada bagian *digital*

forensik, *penetration testing* dan audit keamanan sistem informasi. Sistem operasi Kali Linux secara *default* sudah menyediakan banyak *tools* yang bersifat *free* sehingga pengguna dapat memiliki banyak referensi dalam melakukan pengujian keamanan. Metode yang digunakan pada penelitian ini adalah *Black Box Testing*. *Black Box Testing* merupakan suatu metode pengujian yang dilakukan pada aplikasi yang menguji fungsionalitas tanpa mengetahui struktur aplikasi secara detail dan bagaimana proses yang terjadi dalam aplikasi tersebut (Larrea, 2017).

Tugas Akhir ini dilakukan untuk melakukan analisis kemananan terhadap Situs web Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Pada Pemerintah Daerah XYZ. Setelah analisis selesai dilakukan, maka akan diberikan rekomendasi untuk meminimalisir kerentanan yang ada pada situs web tersebut.

I.2 Rumusan Masalah

Rumusan masalah berfungsi sebagai fokus dari suatu permasalahan dalam tugas akhir. Berdasarkan latar belakang permasalahan, masalah yang dirumuskan pada tugas akhir ini adalah sebagai berikut:

1. Bagaimana kondisi keamanan situs web Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu?
2. Bagaimana rekomendasi untuk menutupi kerentanan pada situs web Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu?

I.3 Tujuan Penelitian

Tujuan tugas akhir ini adalah mendapat informasi atau hasil yang ingin diusulkan didalam penelitian ini. Tujuan diadakannya penelitian ini adalah sebagai berikut:

1. Memperoleh kondisi kemanan situs web Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu
2. Memberikan rekomendasi keamanan situs web sesuai dengan hasil analisis dalam penelitian ini.

I.4 Manfaat Penelitian

Manfaat yang didapat didapat dari penelitian ini adalah sebagai berikut:

1. Memberikan usulan rekomendasi, atau usulan dalam hal pengembangan keamanan dari situs web tersebut.
2. Meminimalisir segala kemungkinan kejahatan pada website tersebut baik dari segi internal maupun eksternal sistem.
3. Memberikan referensi kepada *public* tentang kemampuan *tools* yang digunakan dalam penelitian ini.

I.5 Batasan Penelitian

Batasan dalam penelitian ini dilakukan agar penelitian atau pengamatan yang sedang kita lakukan tidak keluar dari pokok inti permasalahan objek penelitian. Berikut ini adalah beberapa batasan penelitian:

1. Penelitian ini hanya dilakukan untuk mencari kerentanan suatu website kemudian memberikan solusi atas kerentanan tersebut
2. *Tools* yang digunakan pada penelitian ini adalah Paros, Nmap, dan Vega
3. Penelitian ini dilakukan secara *remote* melalui *Tools* yang digunakan dalam penelitian ini.
4. Metode yang digunakan pada penelitian ini adalah *Black Box Testing*
5. Penelitian ini hanya memberikan usulan atau rekomendasi dalam keamanan website tersebut. Untuk keputusan implementasi atau tidaknya diserahkan sepenuhnya kepada pihak yang bersangkutan.

I.6 Sistematika Penulisan

1. Bab I Pendahuluan

   Bab ini berisi mengenai uraian latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan penelitian dan sistematika penelitian

2. Bab II Kajian Teori

   Bab ini berisi penjelasan tentang teori-teori pendukung yang digunakan dalam penelitian ini.

3. Bab III Metodologi Penelitian

   Bab ini berisi penjelasan serta model konseptual yang digunakan dalam mengerjakan tugas akhir.

4. Bab IV Skenario dan Hasil Pengujian

   Bab ini berisikan penjelasan mengenai spesifikasi *hardware,* spesifikasi *software*, skenario deteksi kelemahan situs web*,* dan hasil pengujian praktik yang dilakukan saat penelitian.

5. Analisis

   Bab ini berisikan penjelasan mengenai analisis celah kerentanan dan solusi untuk meminimalisir celah kerentanan tersebut.

6. Kesimpulan dan Saran

   Bab ini memuat rincian kesimpulan dari penelitian yang telah dilakukan. Saran untuk penelitian lanjutan juga dituliskan pada bab ini.