BAB I
PENDAHULUAN

I.1 Latar Belakang

Perkembangan Internet dalam teknologi informasi berkembang dengan pesat seiring dengan pertumbuhan penggunanya. Demikian pula, tingkat kejahatan dalam teknologi informasi berbahaya baik bagi pengguna individu maupun organisasi. Keamanan teknologi informasi diperlukan untuk meningkatkan efisiensi keamanan *cyber-crime*, pemantauan, analisis ancaman, dan insiden dalam keamanan teknologi informasi.

Berdasarkan data dari Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri menerima 2.259 laporan kasus kejahatan siber sepanjang Januari hingga September 2020. Tercatat, laporan soal penyebaran konten provokatif merupakan yang paling banyak dilaporkan yakni sebanyak 1.048 kasus. Selain itu, masyarakat juga melaporkan kejahatan siber lainnya sepert penipuan online, pornografi, akses ilegal, manipulasi data, pencurian data/identitas, dan sebagainya. Melalui situs patrolisiber.id, hingga saat ini terdapat total 7.535 aduan masyarakat terkait kejahatan siber. Ribuan kasus ini diprediksi telah menimbulkan kerugian sebesar Rp 27,19 miliar. (Annur, 2020)

PT. XYZ merupakan salah satu produsen es krim yang ternama di Indonesia, dengan rangkaian produk yang selalu menjadi pilihan konsumen di Indonesia. PT. XYZ selalu berinovasi untuk menciptakan produk produk unggul dengan standar perusahaan yang sudah ditetapkan. PT. XYZ sendiri melakukan penjualan tidak hanya pada *offline store*, PT XYZ juga melakukan penjualan secara *online* dengan memanfaatkan *website* untuk melakukan penjualan.

Berdasarkan hasil wawancara dengan pihak perusahaan, *website* XYZ sendiri pernah mengalami percobaan peretasan oleh beberapa akun *spam* yang berdampak baik itu bagi pengguna maupun *website* XYZ, selain itu website XYZ sendiri mengalami insiden berulang 1 sampai 2 *case* dalam rentang waktu 1 sampai 2 bulan. Oleh karena itu diperlukan sebuah *walkthrough* berdasarkan *performance indicator* agar kinerja dari *website* ataupun kinerja dari divisi it dapat

meningkat dan mengantisipasi peretasan, sehinga keamanan informasi tetap terjaga. Selain itu ntuk mengantisipasi ancaman tersebut dilakukan *Vulnerability Assessment* merupakan proses mengidentifikasi, menilai, dan mengklasifikasikan tingkat kerentanan keamanan di jaringan komputer, sistem, aplikasi, atau bagian lain dari ekosistem IT berdasarkan kerentanan yang mungkin dapat ditimbulkan ke perusahaan. *Vulnerability assessment* pada aplikasi *web* bertindak sebagai pelengkap dan menguji kinerja serangan pada target sehingga kita bisa melihat ancaman apa saja yang terdapat pada *web* tersebut. Terdapat beberapa tools untuk melakukan *vulnerability assessment* diantaranya Nessus.

I.2 Perumusan Masalah

Berdasarkan latar belakang, adapun perumusan masalah yang terdapat pada penelitian ini, yaitu:

1. Bagaimana melakukan *vulnerability assessment* pada suatu *website*?
2. Bagaimana melakukan identifikasi *performance indicator* berdasarkan data perusahaan?
3. Bagaimana melakukan analisis *walkthrough* menggunakan *framework* VAPT?

I.3 Tujuan Penelitian

Berdasarkan perumusan masalah, maka tujuan dari penelitian ini adalah:

1. Melakukan pengujian *vulnerability assessment* menggunakan *tools* Nessus.
2. Melakukan identifikasi *performance indicator* berdasarkan data perusahaan menggunakan Key Performance Indicator berdasarkan ITIL *Incident Management*
3. Melakukan analisis jenis ancaman yang terjadi menggunakan Nessus berdasarkan *framework* VAPT.

I.4 Batasan Penelitian

Adapun Batasan masalah pada tugas akhir ini adalah:

1. Penelitian ini menggunakan *framework* VAPT sebagai acuan untuk melakukan pengujian.
2. *Key Performance Indicator* (KPI) pada penelitian ini berdasarkan referensi dari KPI *Information Technology Infrastructure Library* (ITIL) *Incident Management.*
3. Penelitian ini tidak melakukan *penetration testing*.

I.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah:

1. Memberikan laporan mengenai kerentanan suatu *website* yang dapat digunakan sebagai acuan dan pertimbangan dalam melakukan perbaikan maupun pengembangan untuk meningkatkan kinerja suatu *website*, juga dapat meminimalisir terjadinya ancaman dari peretas yang dapat merugikan pengguna *website*.
2. Penelitian ini dapat memberikan informasi terkait implementasi *framework* VAPT sebagai referensi untuk penelitian selanjutnya yang berhubungan dengan *Vulnerability Assessment* serta menjadi bahan kajian lebih lanjut.