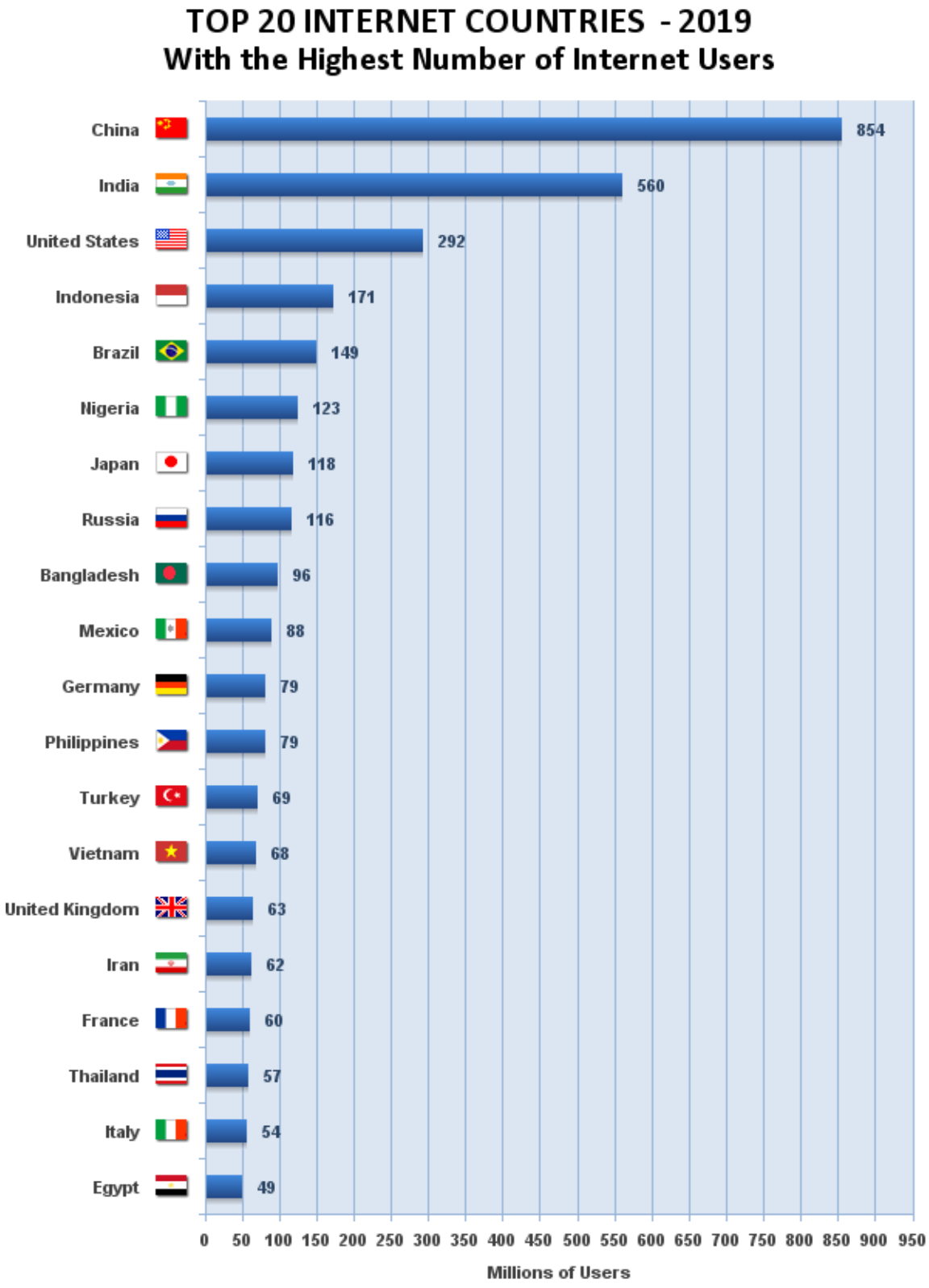
BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi yang sangat pesat dari tahun ke tahun membuat kesadaran bahwa pentingnya pengolahan data dan informasi sangat dibutuhkan untuk menjadi *input* dari semua aspek kehidupan terutama aspek yang bergantung dengan teknologi. Dengan pengolahan data yang akan ditransformasikan menjadi informasi mampu membawa perubahan dalam cara berpikir dan belajar seseorang sehingga digunakan untuk membantu dalam menyelesaikan suatu permasalahan maupun menyebarkan bantuan dengan cepat. Oleh karena itu dapat dikatakan bahwa pada zaman modern ini, kebutuhan informasi sudah sangat umum digunakan demi perubahan dan keberlangsungan hidup pada lingkungan hidup manusia (Wu & Yun, 2010).

Salah satu bentuk penggunaan teknologi informasi adalah internet yang dapat membantu manusia saling terkoneksi dan menjalin hubungan yang membuat pertukaran informasi terjadi. Dengan melihat tren abad ke-20 dan ke-21 tentunya internet akan mengalami kemajuan yang sangat masif. Internet telah memberikan bukti dengan menciptakan dunia virtual yang memberikan semua pengguna kesempatan dalam berekspresi dan menggambarkan tentang kehidupan mereka (Witono, 2017).

Dengan melihat sistem komunikasi global yang dapat menghubungkan semua pengguna berhubungan diseluruh dunia maka negara-negara di dunia ikut serta dalam mengukur penggunaan pengguna internet di masing-masing negara. Dengan melihat dari Gambar I.1 berdasarkan data statistik dari InternetWorldStats negara pengguna internet tertinggi saat ini dipegang oleh China dengan 854 juta pengguna terakhir tercatat pada 30 Juni 2019 (InternetWorldStats, 2019).



Gambar I.1 Negara Dengan Pengguna Internet Tertinggi Tahun 2019

(InternetWorldStats, 2019)

Berdasarkan data statistik dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2019-2020, negara Indonesia memiliki pengguna internet sebesar 196.71 juta jiwa dari total populasi penduduk Indonesia yang berjumlah 266.91 juta jiwa atau dapat dikatakan sebesar 73,7% dari total penduduk Indonesia sehingga dapat dikatakan bahwa terjadi kenaikan dari data tahun lalu sebesar 8.9% (Irawan dkk., 2020). Data dapat dilihat pada Gambar I.2.

Gambar I.2 Penetrasi Pengguna Internet Tahun 2019-2020 Di Indonesia (Irawan dkk., 2020)

Salah satu penggunaan informasi yang telah diolah untuk membantu dan memiliki kegunaan adalah *website*. Penggunaan *website* untuk dijadikan penyedia layananan dibantu dengan ketersediaan teknologi informasi dan komunikasi mampu membantu pekerjaan manusia dalam mendukung keberlangsungan beragam aktivitas. Sebagai contoh penggunaan *website* untuk mendukung bisnis dalam menyediakan layanan kepada pengguna dalam bentuk produk maupun layanan. Tidak hanya mendukung bisnis, *website* memiliki kepribadian masing-masing yang berfungsi sebagai nilai dalam meningkatkan *brand website* itu sendiri (Ho dkk., 2016).

Penggunaan *website* tentunya juga harus diperhatikan dalam pengimplementasian sehingga *website* dapat berjalan sebagaimana yang telah ditentukan dan

dimaksudkan oleh pihak penyedia. Dengan cara menganalisa kerentantan sebuah *website* dengan *tools* yang mampu mendeteksi kerentanan pada keamanan yang diimplementasikan. Pendeteksian kerentanan biasanya dilakukan dengan melakukan *vulnerability assessment* yang bertujuan untuk mengetahui kelemahan pada sistem karena terdapat proses identifikasi, mengukur, dan memprioritaskan kerentanan pada sistem. Untuk membuktikan celah keamanan dapat melakukan pengujian berupa *penetration testing* atau dapat dikenal dengan istilah *ethical hacking*. Pengujian biasanya dilakukan dengan mengikuti sebuah standar atau panduan yang dibuat oleh mereka yang ahli pada bidang keamanan seperti Penetration Testing Execution Standard (PTES). Contoh lainnya dari suatu organisasi *non-profit* yaitu *Open Web Application Security Project* (OWASP) berupa *The Web Security Testing Guide* (WSTG) (Anantharaman & Wukkadada, 2020).

Dengan perkembangan teknologi yang makin canggih maka penggunaan teknologi menjadi umum untuk digunakan. Sehingga penggunaan teknologi secara umum membuat berkembangnya cara-cara penyerangan terhadap teknologi semakin marak juga. Orang yang melakukan penyerangan dengan tujuan untuk membahayakan, mengeksploitasi, dan mencuri demi keuntungan pribadi atau tertentu disebut dengan *hacker* atau *black hat hacker*. Ternyata ada juga *hacker* yang melakukan kebaikan demi memperkuat pertahanan teknologi yang digunakan disebut dengan *white hat hackers.* Yang membedakan adalah *white hat hackers* melakukan metode penyerangan seperti *hacker* namun dengan menggunakan *ethical hacking* atau disebut juga *penetration testing*. Bekerja dengan berpikir seperti *hacker* yaitu menggunakan cara atau metode yang sama serta dengan *tools*, *tricks*, dan *technique* yang sama juga. Penyerangan yang dilakukan oleh *white hat hackers* dapat dikatakan legal karena *ethical hacking* dilakukan dengan sepengetahuan korban yang diserang (Patil dkk., 2018).

Penelitian ini dilakukan untuk dapat menganalisis kerentantan pada *website* dengan melakukan *vulnerability assessment* dan pengujian berupa *penetration testing* atau disebut *ethical hacking* beserta penggunaan dari *tools* yang mendukung fase-fase dalam *penetration testing*. Umumnya fase dimulai dengan fase *reconnaissance* yaitu pengintaian terhadap target yang akan diserang dengan

mengumpulkan informasi untuk memberikan petunjuk penyerangan. Dilanjutkan ke fase *vulnerability scanning* yaitu pendeteksian kerentanan dengan menggunakan *tools*. Kemudian masuk ke fase *exploitation* yaitu percobaan untuk menyerang dengan hasil dari pendeteksian kerentanan yang telah dilakukan. Setelah melakukan semua fase maka dapat membuat laporan terhadap hasil dari *penetration testing* dan melaporkan kepada subjek yang menjadi target sehingga mampu menangani kerentanan dengan memperkuat jaringan keamanan pada teknologi yang digunakan (Yevdokymenko dkk., 2017).

Perubahan dari penyedia layanan luar jaringan menjadi dalam jaringan atau layanan elektronik dapat membantu masyarakat menggunakan layanan yang disediakan oleh suatu instansi pemerintahan. Namun karena perubahan itu maka muncul juga tingkat penyerangan siber yang terutama sering menyerang penyedia layanan dari instansi pemerintahan. Penyerangan dilakukan dengan mengeksploitasi kerentanan pada sistem operasi, protokol jaringan, enkripsi data, dan aplikasi web yang menyebabkan hilang atau bocornya data pribadi suatu daerah yang merupakan sebuah aset penting tiap pribadi. Ini dikarenakan kurangnya ahli keamanan atau kurangnya kesadaran dalam memperkuat keamanan aplikasi web yang disediakan (Ali & Zamri Murah, 2019). Oleh karena itu pemilihan penelitian terhadap *website* ABC milik pemerintah daerah ABC dilakukan.

Pada penelitian ini dilakukan pengujian keamanan menggunakan PTES karena menyediakan metodologi yang terstuktur terhadap *penetration assessment* dan langkah-langkah yang terlibat (Dinis & Serrao, 2015). Pengujian dilakukan terhadap *website* ABC dengan bantuan dari empat *tools* yaitu Zenmap, OWASP ZAP, Arachni, dan Vega yang diharapkan membantu menemukan kerentanan pada sisi keamanan yang dapat dijadikan peluang terjadinya penyerangan oleh pihak tertentu demi keuntungan suatu pihak. Setelah dilakukan pengujian keamanan terhadap *website* maka kerentanan keamanan dapat menjadi masukan untuk dilakukan perbaikan dan pengamanan bagi penyedia *website*. Sehingga kemungkinan penyerangan yang terjadi kedepannya dapat dicegah.

I.2 Perumusan Masalah

Pada bagian ini diuraikan pertanyaan berdasarkan latar belakang sebagai sebagai rumusan masalah dengan uraian berikut:

1. Bagaimana hasil pemindaian kerentanan dan pengujian keamanan *website* ABC menggunakan standar PTES dan *tools* Zenmap, OWASP ZAP, Arachni, dan Vega?
2. Bagaimana analisis celah keamanan dan usulan keamanan dari hasil pengujian yang dilakukan pada *website* ABC menggunakan standar PTES?

I.3 Tujuan Penelitian

Pada bagian ini diuraikan tujuan penelitian yang dilakukan berdasarkan rumusan masalah pada penelitian dengan tujuan sebagai berikut:

1. Mengetahui hasil pemindaian kerentanan dan pengujian keamanan *website* ABC menggunakan standar PTES dan *tools* Zenmap, OWASP ZAP, Arachni, dan Vega.
2. Mengetahui analisis celah keamanan dari hasil pengujian yang dilakukan pada *website* ABC menggunakan standar PTES serta memberikan usulan keamanan.

I.4 Batasan Penelitian

Batasan masalah untuk tugas akhir ini adalah sebagai berikut:

1. Tugas akhir ini melakukan pengujian celah keamanan dengan target *website* ABC.
2. Penggunaan standar PTES dijadikan sebagai panduan dalam melakukan penemuan kerentanan *website* ABC.
3. Tahapan standar PTES yang hanya digunakan adalah *Pre-engagement Interactions, Intelligence Gathering, Vulnerability Analysis, Exploitation, Post Exploitation,* dan *Reporting*.
4. Pada tahapan *Post Exploitation* hanya memberikan rekomendasi untuk menutupi celah keamanan terhadap kerentanan yang ditemukan.

5. *Tools* yang digunakan dalam pengujian adalah Zenmap, OWASP ZAP, Arachni, dan Vega.
6. Pengujian kerentanan hanya dilakukan dengan *tools vulnerability assessment* dari Vega yang berkategori resiko *high*.
7. Memberikan usulan terhadap kerentanan keamanan pada *website* ABC.

I.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan untuk memberikan manfaat dan solusi secara teoritis maupun praktis, yaitu:

1. Secara teoritis, hasil dari penelitian yang dilakukan dapat menjadi referensi dan untuk dijadikan bahan edukasi dalam meningkatkan keamanan pada teknologi yang digunakan dalam kasus ini adalah *website* ABC.
2. Secara praktis, hasil dari penelitian ini dapat menjadi pertimbangan untuk meningkatkan keamanan pada sisi *website* ABC.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Pada bab ini berisi mengenai urairan latar belakang masalah, perumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, dan sistematika penulisan.

Bab II Tinjauan Pustaka

Bab ini berisi literatur yang relevan dengan permasalahan yang dihadapi penelitian terdahulu yang memiliki keterkaitan dengan penelitian yang sedang dilakukan, dan menjelaskan metode yang digunakan.

Bab III Metodologi Penelitian

Bab ini berisi literatur yang relevan dengan permasalahan yang dihadapi serta penelitian terdahulu yang memiliki keterkaitan dengan penelitian yang sedang dilakukan.

Bab IV Perancangan Pengujian

Bab ini menguraikan detail dari perancangan pengujian dan skenario pemindaian dan penyerangan yang akan dilakukan.

Bab V Analisis Pengujian Sistem

Bab ini menguraikan langkah-langkah pengujian yang terjadi pada saat penelitian serta hasil yang berupa analisis dari penelitian tersebut.

Bab VI Kesimpulan dan Saran

Bab ini berisi tentang kesimpulan dan saran yang dapat diambil berdasarkan data yang didapatkan dari hasil penelitian.