BAB I. PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi memungkinkan manusia untuk berkomunikasi serta bertukar data dengan lebih mudah dan cepat. Hal tersebut tentunya diperlukan suatu sistem serta aplikasi untuk menyimpan informasi yang akan diolah menjadi sebuah data. Dalam sistem informasi komputer, keamanan *server* sangat diperlukan untuk mengatur *traffic* dari jaringan, mengelola autentifikasi dari *user* dan menghindari pencurian informasi/data pada *server* suatu instansi atau perusahaan. Seiring dengan perkembangan teknologi tersebut, keamanan terhadap aset/data sangat perlu diperhatikan oleh semua pihak. Mengingat banyaknya serangan yang dilakukan *hacker* belakangan ini yang bertujuan mengambil data-data yang sensitif untuk kepentingan pribadi ataupun komersil.

Berdasarkan informasi yang dilansir BSSN oleh Kepala Subdirektorat Penanggulangan dan Pemulihan Infrastruktur Informasi Kritikal Nasional I Badan Siber dan Sandi Negara (BSSN) Teguh Wahyono, kewaspadaan dan kesiapsiagaan merespon potensi ancaman atau serangan siber pada berbagai sistem layanan elektronik harus senantiasa dilatih dan diperkuat. Bahkan pada era pandemi *Covid-19* saat ini pun dapat dijadikan ajang bagi penyerang untuk menguji sistem keamanan jaringan dari berbagai perusahaan diantaranya berupa *Distributed Denial of Service* (DDoS) sebesar rata-rata tiga kali lipat setiap tahunnya. Khusus dalam masa pandemi Covid-19, lonjakan penyerangan terjadi lima kali lipat lebih banyak dari biasanya (BSSN, 2020). Hal ini dibuktikan pula oleh Sigit Kurniawan, Kepala Sub Direktorat Identifikasi Kerentanan dan Penilaian Risiko Infrastruktur Informasi Kritikal Nasional III BSSN berdasarkan informasi dari portal berita CNN bahwa *Cyber Attack* pada bulan Januari hingga Agustus 2019 terdapat 39.330.231, dan pada periode yang sama di tahun 2020, serangan yang terhitung mencapai 189.937.542 atau hampir lima kali lipat lebih banyak dari tahun berikutnya.

Pada kasus *data breach* periode Januari hingga Agustus 2020, terdapat sekitar 36.771 akun data yang tercuri di sejumlah sektor, termasuk sektor keuangan. Data BSSN 2020, memperlihatkan kerentanan dari sektor bank bahwa kerentanan siber terbesar ada pada minimnya *security awareness* dengan persentase 49 persen (Ikhsan, 2020). Terdapat aduan *cyber* pada periode Januari-September 2020, paling banyak terkait konten negatif dengan jumlah 1.048 aduan, diikuti kasus penipuan *online* sebanyak 649 aduan. Terhubungnya komputer dengan dunia luar tidak luput dari peran internet, dimana peningkatan sistem diperluas dan pertumbuhannya pun begitu cepat. Pesatnya perkembangan dunia komputasi telah membuka masalah keamanan perangkat lunak seperti aplikasi-aplikasi yang berjalan maupun perangkat keras.

Selain itu, perlunya untuk melindungi informasi dengan mengikuti pendekatan yang baik dan terstruktur untuk menghindari adanya resiko yang mungkin terjadi. Alasan pemilihan analisis keamanan terhadap *server* adalah karena banyaknya instansi khususnya pada perguruan tinggi yang mengabaikan keamanan *server* dan menganggap kondisi keamanan sistem informasi yang salah satunya yaitu aplikasi yang dimiliki sudah aman dengan memasang *antivirus* pada *server*. Padahal kenyataannya, banyak data-data yang sangat penting yang memang sangat perlu dijaga keamanannya yang juga melibatkan tiga alasan pentingnya keamanan sistem informasi yang dikenal sebagai *CIA Triad* yaitu *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), *Availability* (Ketersediaan).

Untuk menghindari kerugian yang diakibatkan oleh serangan penyerang, maka perlu dilakukan langkah awal yang harus dilakukan yaitu dengan melakukan semacam evaluasi terhadap keamanan *server* yang ada. Oleh karena itu, pada penelitian ini akan dilakukan analisis keamanan sistem informasi yang meliputi aplikasi yang berada di server untuk mengetahui kerentanan *server* serta membantu meminimalisir dan mengantisipasi *server* yang ada dari kejahatan *hacking*.

Salah satu hal yang dapat dilakukan adalah dengan melakukan *monitoring* rutin pada *server* dan melakukan *penetration testing* yang pada penelitian ini menggunakan metode *Penetration Testing Execution Standard* (PTES) dengan studi kasus pada Universitas VWX yang merupakan salah satu perguruan tinggi yang akan dijadikan target dalam melakukan analisis keamanan *server* karena Universitas VWX juga banyak menggunakan teknologi informasi dalam kegiatan proses belajar mengajar dan dalam proses mengelola data-data yang berkaitan dengan Universitas VWX dalam penelitian ini mengacu pada *server* yang berisi data pegawai. Pengujian yang dilakukan yaitu terhadap aplikasi yang terdapat pada *server* Universitas VWX melalui *port-port* yang terbuka dan *service* yang berjalan pada *port* tersebut.

Pemilihan metode PTES ini dikarenakan memiliki tahapan, alat, dan teknik yang jelas dan mudah untuk dipahami karena mencakup pengujian penetrasi yang sering digunakan pada umumnya. Penilaian dalam metode ini menggunakan *level-level* yang dapat dimengerti oleh *user* yang bukan hanya orang yang berpengalaman dengan *penetration testing*, tetapi dapat juga dimengerti oleh *user* yang juga tidak memiliki pengalaman di bidang *penetration testing.* Metode PTES dalam penelitian ini memiliki tahap-tahap diantaranya yaitu *pre-engagement*, *intelligence gathering*, *threat modelling*, *vulnerability analysis*, *exploitation testing*, *post exploitation*, dan *reporting*.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan, maka yang menjadi pokok permasalahan adalah:

1. Apa saja jenis kerentanan keamanan yang dapat mengakibatkan kegagalan dalam mempertahankan keamanan sistem informasi pada *server* Universitas VWX?
2. Bagaimana cara untuk menguji kerentanan *server* yang berisi data pegawai dengan menggunakan metode *Penetration Testing Execution Standard* (PTES)?

3. Apa saja rekomendasi untuk memperbaiki celah keamanan yang ditemukan pada *server* Universitas VWX?

1.3 Tujuan Penelitian

Tujuan dari analisis keamanan ini adalah:

1. Mengurangi kemungkinan-kemungkinan yang dapat terjadi akibat penyalahgunaan terhadap aset/data yang ada di Universitas VWX.
2. Melakukan analisis terhadap keamanan sistem informasi untuk mengetahui kerentanan *server* Universitas VWX.
3. Menemukan celah keamanan *server* Universitas VWX dan penanganan celah kemanan tersebut agar *server* tersebut dapat dioptimalkan dalam pemeliharaannya.

1.4 Manfaat Penelitian

Bagi Penulis

1. Memenuhi salah satu kelulusan Strata Satu (S1) Informatika Fakultas Ilmu Komputer UPN Veteran Jakarta.
2. Memperoleh pengetahuan dan pemahaman mengenai ilmu keamanan sistem informasi dalam menganalisis keamanan *server* UPN Veteran Jakarta.

Bagi Instansi Terkait

1. Sebagai acuan untuk bahan evaluasi keamanan *server* sistem informasi yang ada.
2. Mencegah terjadinya serangan dalam dunia maya yang dapat merusak jaringan *server*.
3. Sebagai tolak ukur dalam meningkatkan keamanan sistem informasi yang ada baik berupa web maupun *serve*r.

Bagi Universitas

1. Sebagai bentuk kontribusi karya ilmiah dalam studi Informatika mengenai keamanan sistem informasi.
2. Sebagai tambahan bahan referensi untuk penelitian keamanan sistem informasi selanjutnya.
3. Memberikan gambaran mengenai kesiapan mahasiswa dalam menghadapi dunia kerja yang sebenarnya.

Bagi Masyarakat

1. Menambah informasi dan wawasan mengenai keamanan sistem informasi.

1.5 Ruang Lingkup

Ruang lingkup dari penelitian ini adalah sebagai berikut:

1. Terdapat satu *server* yang akan diuji yaitu *server* yang berisi data pegawai.
2. Firewall pada server diaktifkan.
3. *Server* yang akan diuji yaitu *server running/existing* yang diakses di luar jam kerja untuk meminimalisir *traffic* jaringan.
4. Menggunakan Sistem Operasi *Kali Linux* dan *Windows* 10.
5. Pengujian kerentanan hanya bertujuan mencari celah kelemahan *server* yang meliputi aplikasi yang terdapat di *server* dan tidak menyerang serta mengganggu sistem jaringan *server*.

1.6 Luaran Yang Diharapkan

Luaran yang diharapkan dari penelitian ini adalah mengetahui celah dan tingkat kerentanan keamanan *server* yang dimiliki Universitas VWX yang dapat membahayakan dan menghambat kinerja sistem yang ada.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penyusunan proposal ini sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan tentang Latar Belakang, Rumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, Ruang Lingkup, Luaran yang Diharapkan, dan Sistematika Penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi dasar-dasar teori yang menjadi acuan dalam penyusunan laporan penelitian yang mendukung judul dari kegiatan yang penulis lakukan.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang tahapan penelitian dan segala metode pengujian sistem yang terkait dengan penelitian yang dilakukan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang penjelasan mengenai proses pengumpulan data dan pembuatan model *penetration testing*, serta pembahasan analisis hasil pengujian kerentanan dari *server* data yang telah diuji.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran dari hasil penelitian yang telah dilakukan yang dapat digunakan sebagai acuan agar sistem *server* data dapat diperbaiki dan diperbaharui lebih baik lagi.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN