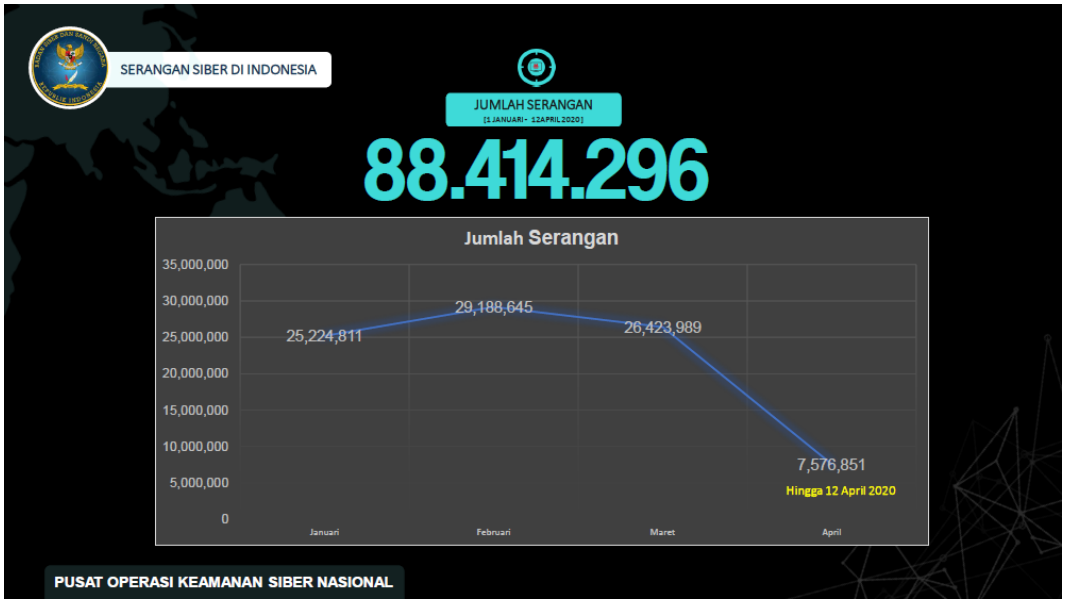
BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi berjalan sangat pesat di masa ini, beragam kemudahan yang ditawarkan oleh teknologi menjadi hal yang amat menguntungkan bagi kehidupan. Pengelolaan data yang diotomatisasi serta kemudahan dalam bertukar informasi menjadi salah satu keuntungan yang dihasilkan dari adanya perkembangan teknologi informasi. Namun demikian, sejalan dengan berbagai keuntungan yang dihasilkan, perkembangan teknologi juga tidak luput dari ancaman kerugian. Serangan siber adalah kejahatan yang memanfaatkan perkembangan teknologi informasi dan dapat mengakibatkan kerugian yang besar.

Tercatat dalam pembukuan Badan Siber dan Sandi Negara (BSSN), telah terjadi 88.414.296 serangan siber dalam rentang waktu 1 Januari hingga 12 April 2020 dengan sebaran 25.224.811 serangan pada bulan Januari, 29.188.645 serangan pada bulan Februari, 26.423.989 serangan terekam pada bulan Maret, dan 7.576.851 serangan pada rentang 1 sampai dengan 12 April 2020. (BSSN, 2020) Hal ini tentunya menjadi salah satu ancaman eksternal keamanan bagi setiap sistem.



Gambar 1.1 Serangan Siber Di Indonesia Januari-April 2020 (BSSN, 2020)

Universitas PQR sebagai salah satu perguruan tinggi memiliki web Pembelajaran Daring untuk mengelola kegiatan belajar para mahasiswanya. Web pembelajaran daring menjadi satu wadah utama dalam menunjang kegiatan belajar mahasiswa PQR agar tetap dapat berlangsung secara semestinya terutama di era pandemi ini. Di dalam web tersebut tentunya terdapat banyak data yang disimpan dan diolah dalam kesehariannya, seperti halnya materi pembelajaran, nilai tugas dari pelajar, dan lain sebagainya. Data-data yang tersimpan dalam web tersebut bersifat rahasia sehingga keamanan data perlu dijamin untuk menghidari kebocoran maupun manipulasi data yang tersimpan pada sistem tersebut. Web Pembelajaran Daring yang menyimpan banyak data mahasiswa Universitas PQR juga memiliki potensi terkena serangan siber yang dapat mengakibatkan kerugian bagi banyak pihak. Dengan demikian diperlukan langkah yang dapat mengurangi potensi penyerangan terhadap setiap sistem.

Penetration Testing atau dengan Uji Penetrasi adalah metode pengujian suatu sistem yang dilakukan dengan mengeksploitasi kerentanan yang ditemukan pada sistem tersebut. Dengan melakukan uji penetrasi, kita akan melihat sistem dari sudut pandang penyerang sehingga kita dapat meminimalisir potensi masuknya serangan. Terdapat banyak metodologi uji penetrasi, salah satunya adalah OSSTMM. OSSTMM adalah metode atau lebih tepatnya merupakan standar dalam melakukan uji penetrasi yang bersifat *open source* yang memungkinkan siapapun dapat memberikan ide untuk melakukan pengujian keamanan yang lebih akurat, dapat ditindaklanjuti, dan efisien. OSSTMM dikembangkan oleh komunitas bernama Institute for Security and Open Methodologies (ISECOM) dan terus ditinjau serta dimodifikasi secara berkala oleh pakar-pakar industri.

Bercermin dari permasalahan tersebut perlu dilakukan uji keamanan terhadap web Pembelajaran Daring Universitas PQR untuk melihat kerentanan pada sistem sehingga dapat diperbaiki untuk menghindari serangan tak terduga terhadap sistem tersebut. Hasil uji penetrasi akan dapat membantu instansi terkait dalam memperbaiki celah keamanan sistem.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang diuraikan oleh penulis, maka didapatkan rumusan masalah sebagai berikut.

1. Bagaimana cara melakukan pengujian keamanan pada web Pembelajaran Daring Universitas PQR dengan menggunakan metode OSSTMM?
2. Jenis *Vulnerability* apa saja yang ditemukan pada Web Pembelajaran Daring Universitas PQR berdasarkan metode OSSTMM?
3. Apakah hasil yang akan didapatkan dari pengujian yang dilakukan

1.3 Pembatasan Masalah

Dari perumusan masalah yang telah dibuat, maka batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Identitas universitas disamarkan sebagai upaya melindungi privasi Universitas tersebut.
2. Uji penetrasi hanya dilakukan terhadap web Pembelajaran Daring Universitas PQR.
3. Pengujian akan dilakukan dengan menggunakan metode OSSTMM.
4. Channel yang dibahas pada penelitian ini adalah Physical dan Data Network Channel.
5. Waktu pengujian dilakukan dalam rentang waktu minggu kedua bulan Mei hingga akhir Juni tahun 2021.

1.4 Ruang Lingkup Penelitian

Supaya penelitian menjadi terarah dan tidak ada penyimpangan, diperlukan ruang lingkup penelitian. Ruang lingkup pada penelitian ini yaitu:

1. Penelitian ini dilakukan untuk mengetahui kerentanan pada web Pembelajaran Daring Universitas PQR dengan menggunakan beberapa *vulnerability tools* seperti Nessus, Nikto dan Nmap.
2. Sistem yang akan diuji hanya web Pembelajaran Daring dari Universitas PQR.
3. Pengujian akan dilakukan mengikuti standar dari OSSTMM.

1.5 Tujuan dan Manfaat Penelitian

Tujuan penelitian ini adalah untuk mengetahui celah dari Web Pembelajaran Daring Universitas PQR yang berpotensi membahayakan kerahasiaan data melalui *penetration testing* dan memberikan rekomendasi atas celah keamanan yang ditemukan sehingga dapat membantu mempertahankan keamanan Web Pembelajaran Daring Universitas PQR.

Adapun manfaat dari penelitian ini antara lain:

1. Bagi Universitas PQR

   Diharapkan dapat digunakan sebagai bahan evaluasi terhadap keamanan Web Pembelajaran Daring Universitas PQR.

2. Bagi Program S1 Informatika

   Diharapkan dapat digunakan sebagai referensi informasi khususnya bagi mahasiswa S1 Informatika dalam menyusun tugas akhir.

3. Bagi Penulis

   Hasil penulisan digunakan sebagai sarana untuk mengembangkan kemampuan penulis dalam menerapkan ilmu yang diperoleh selama di bangku perkuliahan untuk menemukan celah keamanan dari Web Pembelajaran Daring Universitas PQR.

4. Bagi Pembaca

   Diharapkan dapat memberikan informasi kepada pembaca khususnya dalam hal penetration testing atau uji penetrasi, juga supaya pembaca dapat mengetahui standar keamanan pada aplikasi Web Pembelajaran Daring yang diterapkan oleh Universitas PQR.

1.6 Sistematika Penulisan

Dalam penyusunan skripsi ini, sistematika pembahasan diatur dan disusun dalam lima bab dimana tiap-tiap bab terdiri dari beberapa sub bab. Untuk memberikan gambaran yang lebih jelas, maka diuraikan secara singkat mengenai materi dari tiap bab dalam penulisan skripsi ini sebagai berikut.

BAB I : PENDAHULUAN

Bab ini menjelaskan secara singkat dan jelas mengenai latar belakang permasalahan, rumusan dan pembatasan masalah, maksud dan tujuan, manfaat, serta sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini berisi dasar-dasar teori yang menjadi acuan dalam penyusunan proposal tugas akhir yang mendukung judul dari kegiatan yang penulis lakukan.

BAB III : METODOLOGI PENELITIAN

Bab ini berisikan tentang uraian dan penjabaran dari pemecahan masalah ke dalam suatu bentuk yang diperlukan dalam mencapai penyelesaian masalah tersebut.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini menjelaskan tentang proses pengujian keamanan yang dilakukan, tahapan-tahapan, serta pembahasan tentang hasil yang didapatkan dari pengujian tersebut.

BAB V : PENUTUP

Bab ini berisi tentang kesimpulan dan saran dari hasil penelitian yang telah dilakukan serta saran untuk penelitian selanjutnya

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN