BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin pesat juga mempengaruhi perkembangan serangan-serangan pada dunia jaringan komputer. Dengan berkembangnya serangan-serangan dunia maya, beberapa instansi terutama pemerintahan dan juga pendidikan sering mengalami serangkaian serangan kejahatan dunia siber. Menurut data statistik yang dihimpun oleh *Hot suite and We Are Social* pada bulan Januari 2019, pengguna internet di indonesia sudah menembus angka 150 juta penduduk dibanding dengan tahun sebelumnya yang hanya 143 juta penduduk yang menggunakannya. Bagi pelaku bisnis tingkat penggunaan ini merupakan pasar potensial. Namun berbeda dengan pelaku di dunia *Information Security* atau keamanan informasi. Karena di lapangannya, semakin mudahnya pengguna menyebar informasi, semakin bebasnya pengguna lain menggunakan informasi tersebut.(Letkol Chb Ir. Bagus Artiadi Soewardi, M.Si)

Semakin terbukanya pengguna menyebarkan informasi miliknya, kemungkinan kecil keamanan informasi yang dimiliki sangat rendah. Meskipun pada suatu perusahaan digital memiliki keamanan yang kuat, tidak menutup kemungkinan keamanan tersebut dapat dibobol oleh pihak yang tidak bertanggung jawab. Pembobolan ini tentunya tidak semua orang menginginkannya terutama perusahaan. Karena dapat menjatuhkan nama dari aplikasi atau perusahaan tersebut.

Dalam pembobolan atau mencari kelemahan ini, biasanya memerlukan tahapan-tahapan yang harus dilakukan dan tahapan yang dibahas pada proyek akhir ini adalah tahapan *information gathering*. *information gathering* adalah suatu tahapan yang digunakan untuk mengumpulkan informasi dari suatu target baik sistem atau jaringan, perseorangan atau perusahaan. *Information gathering* (IG) merupakan tahapan awal dan tahapan terpenting dalam melakukan *penetration testing*. Informasi yang didapat pun bisa beraneka ragam bergantung dari sasaran informasi yang ingin didapat.

Informasi yang disasarkan pada sebuah sistem di internet berguna dalam melakukan *penetration testing*, contohnya seperti informasi mengenai alamat *IP*, nama *DNS Server*, teknologi yang digunakan untuk membangun jaringan tersebut, aplikasi apa saja yang terdapat dalam jaringan tersebut, siapa saja yang dapat menggunakan jaringan tersebut dan lain sebagainya. Seperti yang disinggung paragraf sebelumnya bahwa *information gathering* juga dapat menyasar pada perseorangan. Karena dewasa ini para pengguna dunia maya tanpa sadar telah membagikan informasi pribadinya secara cuma-cuma kepada publik. Hal itulah yang sebenarnya berbahaya karena dapat mengancam nyawa seseorang jika tidak bisa menyikapinya dengan baik.

Dalam penelitian ini, dilakukan uji keamanan pada jaringan intra Kampus ITD Adisutjipto Yogyakarta dengan menggunakan metode *Black Box Penetration* sehingga penulis dapat memposisikan diri sebagai orang luar yang tidak mengetahui informasi mendalam terkait jaringan pada kampus ITD Adisutjipto Yogyakarta.

Banyak *tools* yang dapat digunakan untuk *pentesting*. *Tools* tersebut tentunya berbeda fungsi dan *output*-nya. Bergantung dari kebutuhan. Hasil dari IG tersebut dapat dijadikan sebagai *poin* pemetaan dalam melakukan pola serangan yang akan dilakukan pada sistem yang akan diuji saat melakukan *penetration testing*, selain itu juga apabila informasi yang didapat berupa informasi perseorangan yang bersifat data pribadi, dapat digunakan untuk pola serangan yang memanfaatkan celah pada kewaspadaan orang terhadap keamanan informasi atau biasa disebut dengan *social engineering attack*.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka dapat ditarik rumusan masalah penelitian sebagai berikut:

1. Apa saja celah keamanan yang terdapat pada jaringan intra Kampus ITD Adisutjipto Yogyakarta ?
2. Bagaimana tindakan pencegahan atau perbaikan terhadap celah keamanan yang terdapat pada pengujian ini?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah disebutkan, maka didapatkan Batasan Masalah sebagai berikut:

1. *Penetration Testing* dilakukan pada jaringan Intra Kampus ITD Adisutjipto Yogyakarta.
2. Penelitian menggunakan metode *Black Box Penetration* sebagai metode untuk melakukan pengujian pada suatu jaringan intra.
3. Pengujian *Penetration Testing* dilakukan lebih spesifik terhadap jaringan komputer Kampus ITD Adisutjipto Yogyakarta.
4. Pengujian *Penetration Testing* dilakukan menggunakan *Operating System Linux* dengan varian *Kali Linux*
5. Ditujukan untuk para *administrator* baru agar lebih mudah dalam mengambil keputusan.

1.4 Tujuan Penelitian

Penelitian dengan judul "representasi data *network penetration test* pada keamanan jaringan intra kampus ITD Adisutjipto Yogyakarta" ini mempunyai tujuan:

1. Mendapatkan informasi terkait celah keamanan yang bisa menjadi bahan evaluasi bagi *administrator* jaringan Kampus ITD Adisutjipto Yogyakarta sehingga jaringan intra Kampus ITD Adisutjipto Yogyakarta menjadi lebih baik.
2. Memberikan rekomendasi penanganan terhadap ancaman ataupun celah keamanan yang ditemukan guna memberikan tingkat keamanan yang lebih bagi jaringan intra Kampus ITD Adisutjipto Yogyakarta.

1.5 Manfaat Penelitian

Adapun manfaat yang diperoleh dari analisi *network penetration testing* penelitian ini adalah sebagai berikut:

1. Mengetahui kemudahan yang dimiliki oleh Jaringan Intra Kampus ITD Adisutjipto.
2. Membantu memberikan evaluasi terhadap kampus sehingga dapat melakukan perbaikan terhadap celah keamanan Jaringan Intra Kampus.
3. Mencegah terjadinya serangan terhadap sistem informasi dan jaringan komputer Kampus ITD Adisutjipto Yogyakrta.