BAB I
PENDAHULUAN

A. Latar Belakang

Pada saat ini dunia memasuki era digital, dimana segala informasi ada dalam bentuk digital yang wadahnya bermacam-macam. *Website* merupakan salah satu wadah informasi yang tidak pernah surut kepopulerannya bahkan setiap tahun bertambah banyak, *website* menyajikan informasi yang begitu beragam seperti informasi umum pemerintah, salah satunya pemerintah Kabupaten Banyumas yang juga memiliki *website* tersendiri untuk menyajikan informasi yang dibutuhkan masyarakat banyumas. *Website* pemerintah Kabupaten Banyumas ini dibuat dengan mengikuti perkembangan zaman dimana masyrakat membutuhkan kemudahaan dalam mengakses informasi mengenai hal-hal yang berkaitan dengan pemerintah banyumas ataupun informasi umum yang ada disekitar Kabupaten Banyumas.

Website pemerintah Kabupaten Banyumas memiliki kunjungan dari ratusan hingga puluhan ribu kunjungan atau daiambil rata-rata mencapai seribu kunjungan perbulan. Berdasarkan kunjungan yang cukup banyak, *website* pemerintah kabupaten banyumas dapat dikatakan sangat aktif dalam menggunakan *website* sebagai media penyalur informasi. Oleh karena itu, keamanan *website* harus seimbang dengan aktifitas kunjungan *website*, bukan berarti apabila telah memasang keamanan pada *website* bisa lepas dari serangan hacker atau cracker yang bertujuan khusus untuk mencari celah keamanan pada *website* tersebut. Salah satu cara untuk mengetahui celah

keamanan pada *website* yaitu dengan analisis celah keamanan pada *website* dengan menggunakan metode *port scanning, brute force, dan sql injection*.

Mantra (2015) menyatakan tidak ada standar dalam melindungi perusakan *web* serangan atau antisipasi *web* di Indonesia, Keanekaragaman bentuk dan pemrograman *web* dilakukan oleh setiap programmer dan administrator *web*, Tidak ada deskripsi rinci tentang *web* Indonesia perusakan diserang baik dari luar maupun dalam negeri.

Rusydianto, *et al* (2017) menyatakan *Psrt scanning* merupakan sebuah teknik *hacking* dimana seorang penyerang dapat membobol *website* atau *web server* melalui *port* yang terbuka untuk dieksekusi. Berdasarkan data dari Pemerintah Meksiko, Amerika Serikat dan Rusia pada tahun 1999-2013, yang melakukan survey mengenai ancaman *cybercrime* yang sering terjadi pada *port scanning, carding, hacking website*, dan penyadapan transmisi maka teknik *port scanning* adalah *bug* yang kedua paling banyak ditemukan di pada *website-website* yang berada di internet.

Romagna & Hout (2017) menyatakan peretas mengejar ketenaran, biasanya peretas individu ataupun peretas tim berlomba-lomba untuk memecah identitas dari *server web* dan meletakkannya di halaman *web* (rumah halaman) atau sub-halaman, dengan harapan siapa saja yang membuka *web* sehingga identitas mereka dapat dibaca dengan jelas. Hacker anonymous memiliki cara unik menyampaikan misinya kepada pemerintah tidak seperti biasanya, situs peretasan peserta anonim (*web defacement*) dari pemerintah dan lumpuh layanan di dalamnya selama berhari-hari atau bahkan

berminggu-minggu. Ini pernah terjadi di berbagai situs di negara Malaysia, lebih dari 40 layanan *Web down*.

Dari penelitian–penelitian tentang faktor yang mempengaruhi para pencari celah keamanan *website* yang telah dilakukan di atas, perlu kesadaran untuk meningkatkan keamanan suatu *website*, akan tetapi belum banyaknya kesadaran masyarakat akan hal ini rentan akan pencurian data dan hal yang tidak menguntungkan lainnya.

Dengan adanya permasalahan di atas, diperlukan penelitian yaitu dengan melakukan analisis celah keamanan website pemerintah banyumas dengan metode *port scanning, brute force,* dan *sql injection.*

B. Perumusan Masalah

Berdasarkan latar belakang, perumusan masalah dalam penelitian ini adalah bagaimana dan apa saja jenis celah keamanan pada *website* pemerintah Kabupaten Banyumas jika diuji keamanannya menggunakan metode *port scanning, brute force,* dan *SQL injection*.

C. Batasan Masalah

Penelitian ini dibatasi pada implementasi sebagai berikut:

1. Proses analisis celah keamanan:
   a. *Pre-attack phase, attack phase, post-attack phase*
   b. Target yang dicari adalah *port* yang terbuka pada *website* pemerintah Kabupaten Banyumas.
   c. Pemindaian kerentanan *query* menggunakan *nmap SQL injection* dan acunetix
2. *Penetration testing website* pemerintah Kabupaten Banyumas menggunakan perintah *brute force wordlist* dan *SQL injection* bertujuan mendapatkan *username* dan *password user* berdasarkan hasil *scanning port* yang terbuka, sehingga dapat memperoleh hak akses dan *source code* halaman *website* yang menjadi target *deface*. Adapun *tools* yang digunakan antara lain:
   a. Ubuntu *Operating System.*
   b. Nmap.
   c. Hydra
   d. Acunetix

D. Tujuan Penelitian

Adapun tujuan yang akan dicapai dalam penelitian ini antara lain:

1. Mencari celah keamanan *website* pemerintah Kabupaten Banyumas dengan metode *port scanning*, *brute force wordlist*, dan *SQL injection scanning*.
2. Menganalisis hasil *scanning* dan *penetration testing* untuk mengetahui tingkat keamanan *website* sehingga dapat dijadikan rujukan evaluasi keamanan pada *website* pemerintah Kabupaten Banyumas.

E. Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

1. Menambah pengetahuan tentang proses mencari celah keamanan *website* dengan metode *port scanning*, *brute force wordlist*, dan *SQL injection*.
2. Mengetahui efektivitas analisis celah keamanan *website* metode *port scanning* dan *penetration testing* menggunakan *brute force wordlist*, dan *SQL injection scanning*.