BAB I

PENDAHULUAN

I.I Latar Belakang

Perkembangan teknologi dibidang informasi saat ini tealah merambat kepelosok bagian di tanah air Indonesia, baik desa, kecamatan, kabupaten dan kota sudah mulai memiliki divisi yang menerapkan sistem penyebaran informasi kepada masyarakat dengan menggunakan *website* dan salah satu pihak yang bertanggung jawab atas pelayanan penyebaran informasi. Penting untuk menjamin kerahasiaan dan keamanan informasi harus tetap terjaga dari ancaman dan bahaya yang berpotensi menimbulkan banyaknya serangan yang terjadi juga menimbulkan kerugian bagi siapapun pihak yang terkait.

Hal ini mengalami peningkatan pada tahun sebelumnya. Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat 88.414.296 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020. Pada bulan Januari terpantau 25.224.811 serangan dan kemudian pada bulan Februari terekam 29.188.645 serangan lalu kemudian pada bulan Maret terjadi 26.423.989 serangan dan sampai dengan 12 April 2020 telah tercatat 7.576.851 serangan.

Data yang dihimpun oleh Pusopskamsinas BSSN, hingga 12 April 2020 telah terjadi 25 serangan siber menggunakan latar belakang isu pandemi Covid-19, dimana terdapat 17 serangan dengan target secara global dan 8 serangan yang menargetkan suatu negara. Jenis serangan yang paling banyak adalah *trojan activity*sebanyak 56% dan kemudian disusul dengan aktifitas *information gathering* (pengumpulan informasi) sebanyak 43% dari total keseluruhan serangan, sedangkan1% sisanya merupakan *web application attack*.(Saputra et al., 2023)

Salah satu kunci penting dalam perkembangan digital dewasa ini baik untuk organisasi, bisnis maupun individu adalah informasi. Informasi pribadi

tersebar di internet dengan sangat mudah menandakan semakin menipisnya privasi yang dimiliki oleh seseorang.

Hasil pengolahan data akan menjadi sumberdaya yang berperan penting dalam perkembangan teknologi dan informasi. Salah satu hal tindakan yang dapat diambil adalah melakukan pendekatan yang tepat dan terstruktur sebagai upaya perlindungan terhadap risiko keamanan data.

Keamanan jaringan sendiri memiliki 3 dasar untuk menentukan jaringan tersebut aman yang biasa disebut CIA TRIAD. Confidentiality (kerahasiaan) kerahasiaan yang dijamin dari pihak luar yang tidak memiliki hak, Integrity (integritas) menjaga agar informasi tidak berubah dari pihak luar dan Availability (ketersediaan) menjaga agar informasi selalu tersedia untuk diakses. Jika melihat dari konsep tersebut, nampak bahwa ketiga bertujuan sebagai keamanan mendasar untuk kedua data dan informasi serta layanan komputasi, sehingga konsep tersebut dapat menjadi acuan untuk terhindar dari serangan yang ada

Salah satu cara untuk menghindari terjadinya peretasan adalah dengan menutup celah-celah keamanan yang mungkin dimiliki sistem. Sebelum menutup celah keamanan, kita harus mengetahui celah keamanan tersebut dengan melakukan pengujian seperti yang dilakukan oleh peretas, namun dengan prosedur yang telah disetujui.

CKAN adalah sebuah sistem manajemen data yang membuat data dapat diakses dengan menyediakan alat untuk penerbitan, berbagi, menemukan dan menggunakan data (CKAN, 2020). Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi seperti sistem manajemen data terbuka seperti CKAN yang diakses oleh banyak pihak dari organisasi hingga pemerintah. Oleh karena itu, untuk mengatasi masalah tersebut dapat dilakukan analisis terhadap keamanan sistem manajemen data terbuka CKAN. Penelitian ini berfokus pada pengujian penetrasi pada aplikasi CKAN berdasarkan metode *National Institute of Standards and Technology* (NIST SP 800-115).

I.II Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam melakukan penelitian pengujian keamanan ini adalah sebagai berikut:

1. Untuk mengetahui celah kerentanan pada sistem manajemen data sumber terbuka *CKAN* melalui salah satu *website* open data satudata.bandung.go.id berdasarkan pengujian *penetration testing* menggunakan metode NIST SP (800 – 115) .
2. Mengetahui hasil analisis pengujian keamanan terhadap sistem manajemen data sumber terbuka *CKAN*.
3. Membuat laporan atau *reporting* hasil analisis *penetration testing* yang telah dilakukan sebagai bentuk dokumentasi.

I.III Rumusan Masalah

Adapun rumusan masalah pada penelitian ini berdasarkan penjelasan latar belakang diatas sebagai berikut:

1. Bagaimana mengidentifikasi kerentanan pada sistem manajemen data sumber terbuka CKAN melalui *website* satudata.bandung.go.id dengan melakukan *Penetration Testing* ?
2. Bagaimana hasil pengujian keamanan dengan *Penetration Testing* menggunakan metode *National Institute of Standards and Technology* (NIST SP 800-115) pada *website* satudata.bandung.go.id?

I.IV Batasan Masalah

Fungsi batasan masalah ini berperan untuk membuat fokus pada satu pokok persoalan, dan juga untuk membantu dalam mengidentifikasi permasalahan yang dibahas. Dalam penelitian ini penulis membatasi masalah yang akan dianalisis yaitu:

1. Penelitian yang dilakukan terbatas pada pengujian keamanan sistem manajemen data sumber terbuka *CKAN*.
2. Menggunakan uji coba non-destruktif, yaitu uji coba yang tidak membuat kerusakan pada sistem *website* tersbeut.

3. *Penetration testing* yang dilakukan mengacu pada dokumentasi metode *National Institute of Standards and Technology Special Publication* 800 – 115.

I.V Ruang Lingkup

Agar penelitian ini menjadi lebih terarah serta mengurangi adanya penyimpangan, perlu dilakukan ruang lingkup penelitian. Ruang lingkup pada penelitian ini yaitu:

1. Target pengujian dalam penelitian ini merupakan salah satu *website* sistem manajemen data portal yang menggunakan arsitektur *CKAN* yaitu *website* milik diskominfo kota Bandung.
2. Uji penetrasi pada penelitian ini mengacu pada dokumentasi *Penetration Testing* dalam dokumentasi *National Institute of Standards and Technology Special Publication* 800-115.
3. Penerapan dari rekomendasi akan diserahkan sepenuhnya kepada pihak terkait.
4. Alamat IP yang digunakan pada penelitian tidak akan dipublikasikan demi keamanan sistem manajemen data sumber terbuka.

I.VI Manfaat Penelitian

Manfaat penelitian ini bagi pengembangan IPTEK dapat menambah pengetahuan dalam bidang teknologi, khususnya bidang keamanan tentang sistem informasis berbasis *website* serta bisa diharapkann menjadi referensi untuk penelitian terkait pada penelitian mendatang.

Manfaat dari penelitian ini yaitu memberi kontribusi untuk Peneliti, Instansi Terkait, dan Masyarakat.

Bagi Peneliti

1. Penelitian ini diharapkan membuat Peneliti memiliki pengalaman tentang ilmu uji penetrasi dengan mengimplementasikan serta mengembangkan lagi ilmu-ilmu yang telah didapat semasa di bangku perkuliahan.

2. Mendapatkan pemahaman tentang penetration testing menggunakan metode NIST SP (800 – 115).

Bagi Instansi Terkait

1. Sebagai acuan untuk bahan evaluasi keamanan sistem manajemen data diskominfo kota bandung.
2. Dapat mencegah dengan baik ketika terjadinya serangan dalam dunia maya yang dapat merusak jaringan server.
3. Sebagai bahan acuan untuk meningkatkan keamanan sistem manajemen data yang ada baik berupa web maupun server.

Bagi Masyarakat

Penelitian ini diharapkan dapat memberikan informasi dan ilmu yang berguna kepada masyarakat mengenai uji penetrasi atau yang biasa disebut dengan *Penetration Testing* sebagai bagian dari ilmu pengetahuan di bidang Ilmu Komputer, kemudian juga dapat menjadi referensi dan bahan acuan untuk melakukan penelitian yang terkait di masa depan.

I.VII Sistematika Penulisan

Sistematika Penelitian ini ditulis untuk memberikan kemudahan informasi bagi pembaca dan memberikan gambaran dalam mempelajari dan memahami dari uji penetrasi pada sistem manajemen data sumber terbuka *CKAN* menggunakan metode *National Institute Of Standards And Technology Special Publication* (NIST SP 800 – 115).

BAB I PENDAHULUAN

Bab ini menjelasakan secara singkat dan jelas mengenai latar belakang masalah, identifikasi masalah, batasan masalah, batasan masalah, tujuan penelitian, dan manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menguraikan tentang teori-teori dasar yang mendasari pembahasan secara detail, yang berupa tinjauan Pustaka, tinjauan studi, tinjauan objek

penelitian, pola pikir, dan keseluruhan dasar teori yang terkait pada topik penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang metode penelitian, metode penelitian yang akan di rancang, mengidentifikasi kebutuhan, Analisa kebutuhan, alat bantu penelitian, serta jadwal penelitian.

BAB IV HASIL DAN PEMBAHASAN

Pada Bab 4 hasil dan pembahasan, menjelaskan mengenai analisis celah kerentanan yang sudah didapat.

BAB V KESIMPULAN DAN SARAN

Pada bab 5 kesimpulan dan saran ini menjelaskan tentang hasil dari uji penetrasi yang sudah dilakukan dan saran yang direkomendasikan kepada pihak *team* IT diskominfo kota bandung.

DAFTAR PUSTAKA

LAMPIRAN