BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dinas Komunikasi dan Informatika Provinsi Jawa Barat (Diskominfo Provinsi Jabar) bertempat di Jalan Tamansari no. 55 Kota Bandung, merupakan instansi milik pemerintahan yang mempunyai tugas dan fungsi pokok melaksanakan pengelolaan *web hosting* dan *colocation server* serta pengolaan nama *subdomain* go.id untuk *website* di lingkungan Pemerintahan Provinsi Jawa Barat dengan nama *top level domain* yaitu jabarprov.go.id[1]. Untuk menjaga keamanan data informasi yang dikelola oleh Diskominfo serta mengantisipasi gangguan dari berbagai pihak yang tidak bertanggungjawab berupa *cyber attack* yang berasal dari lingkungan internal maupun eksternal, maka Diskominfo harus benar-benar memantau dan mengantisipasi semua serangan *cyber* yang berasal dari *attacker* yang ingin mencoba masuk kedalam sistem keamanan pada *web server*, langkah ini dilakukan untuk menjaga keamanan data informasi dan demi terwujudnya Jabar *Cyber Province*.

Website adalah media informasi yang efektif, efisien serta mudah diakses untuk saat ini, dengan menerapkan teknologi *internet* di instansi pemerintahan, tidak lain bertujuan agar memudahkan semua informasi yang berhubungan dengan kegiatan instansi dan sebagainya ada didalamnya. Data *website* disimpan pada *webserver* sedangkan media yang digunakan untuk mengaksesnya adalah *internet.* Demikian juga halnya dengan instansi pemerintahan di Provinsi Jawa Barat salah satunya Diskominfo untuk mempermudah masyarakat memperoleh berbagai informasi tentang instansi pemerintahan di Provinsi Jawa Barat, maka Diskominfo membuat *website* resmi milik Pemerintah Provinsi Jawa Barat yang dapat diakses melalui alamat *subdomain* diskominfo.jabarprov.go.id. Namun dibalik semua sisi positif yang ada, *internet* juga memiliki sisi negatif diantaranya terdapat berbagai kejahatan *cyber* yang berasal dari pihak internal dan eksternal yang tidak bertanggungjawab. Menurut *website zone-h.org* dari April 2009

sampai April 2014 *website* resmi milik pemerintahan di lingkungan Provinsi Jawa Barat telah diretas sebanyak 145 kali, dua diantaranya berasal dari *website* resmi milik Diskominfo[2] yang berakibat perubahan pada tampilan dan tidak bisa mengakses *website* karena serangan dari *attacker* tersebut. Hal ini disebabkan masih adanya *vulnerability* (kerentanan) keamanan pada *website* yang ada pada diskominfo, sehingga *attacker* dapat dengan leluasa masuk kedalam sistem dan merubah data yang ada pada *webserver*.

Penetration Testing (Pentest) adalah kegiatan untuk mengevaluasi dan mengidentifikasi kerentanan dalam keamanan jaringan komputer untuk memastikan bahwa kerentanan itu benar-benar ada. Ada tiga tipe metode dalam kegiatan *penetration testing* yaitu *whitebox penetration testing*, *blackbox penetration testing* dan *graybox penetration testing* yang merupakan kombinasi dari metode *whitebox* dan *blackbox penetration testing*[7].

Berdasarkan permasalahan yang ada pada latarbelakang, maka Dinas Komunikasi dan Informatika Provinsi Jawa Barat perlu mengadakan kegiatan evaluasi kemananan terhadap *web server* terutama pada *website* yang berfungsi untuk mengetahui adanya *vulnerability* (kerentanan) pada sistem keamanan *website* di lingkungan Pemerintahan Provinsi Jawa Barat dan mencegah terulang kembalinya serangan *cyber* dari *attacker* pada sistem keamanan *webserver* yang sewaktu-waktu bisa terjadi, dan memberikan solusi pengamanan pada *website* agar meminimalisir kejadian serangan *cyber* dari *attacker* serupa terulang kembali .

1.2 Perumusan Masalah

Berdasarkan permasalahan yang telah dikemukakan pada latar belakang dapat dirumuskan, sebagai berikut :

1. Bagaimana mengetahui *vulnerability* (kerentanan) yang terdapat pada *website*?
2. Bagaimana mengamankan *vulnerability* (kerentanan) yang terdapat pada *website*?

1.3 Maksud dan Tujuan

Maksud dari penulisan tugas akhir ini adalah untuk mengevaluasi sistem keamanan jaringan komputer pada *web server* di Dinas Komunikasi dan Informatika Provinsi Jawa Barat.

Tujuan dari penelitian ini adalah :

1. Dapat mengetahui faktor-faktor penyebab *vulnerability* (kerentanan) yang terdapat pada *website*.
2. Dapat mengamankan *vulnerability* (kerentanan) yang terdapat pada *website*.

1.4 Batasan Masalah

Batasan masalah yang ditentukan pada Evaluasi Sistem Keamanan Jaringan Komputer pada *Web Server* di Dinas Komunikasi dan Informatika Provinsi Jawa Barat, meliputi:

1. Jenis metode yang digunakan dalam evaluasi sistem keamanan ini menggunakan jenis metode *black box penetration testing* dimana *pentester* (*tester*) harus terlebih dahulu menggali informasi dari luar terkait dengan target sistem berdasarkan informasi yang *pentester* temukan.
2. Pengujian keamanan hanya pada *website* diskominfo yang menggunakan *Content Management System* (CMS) berupa WordPress sebagai *engine website*.
3. Pengujian keamanan ini dilakukan pada *website* resmi milik Diskominfo dengan alamat http://diskominfo.jabarprov.go.id.
4. Pengujian menggunakan sistem operasi berupa Kali Linux 1.0.7 64 bit.
5. Pengujian menggunakan aplikasi *tools :*
   a. *Reconnaissance* berupa *google dork, exploit-db, nslookup, whois,* dan *dnsenum*.
   b. *Scanning* menggunakan *whatweb, wpscan, nmap dan sqlmap*.

1.5 Metodologi Penelitian

Metodologi penelitian yang akan digunakan dalam menyusun tugas akhir ini adalah metode analisis deskriptif, yaitu suatu metode yang bertujuan untuk mendapatkan gambaran yang jelas tentang hal-hal yang

diperlukan, melalui metode pengumpulan data dan metode *black box penetration testing,* diantaranya :

1.5.1 Studi Pustaka

Metode pengumpulan dan mempelajari buku dan *ebook* yang berhubungan dengan penelitian yang dilakukan. Untuk melihat referensi selengkapnya terdapat pada halaman daftar pustaka.

1.5.2 Studi Lapangan

Studi Lapangan dalam penelitian tugas akhir ini dibagi menjadi 3 bagian, yaitu :

1. **Observasi**

   Teknik pengumpulan data dengan mengadakan penelitian dan peninjauan langsung terhadap permasalahan yang diambil. Observasi dilaksanakan di Dinas Komunikasi dan Informatika Provinsi Jawa Barat, Jalan Taman Sari no. 55 Telp. : 022-2502898 Fax : 022-2511505 Kota Bandung 40132.

2. **Wawancara**

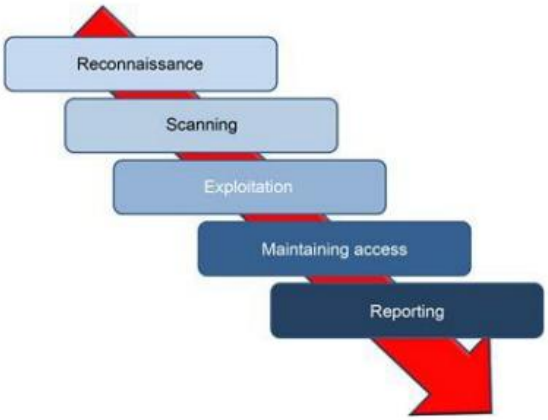
   Teknik pengumpulan data dengan mengadakan tanya jawab secara langsung yang ada kaitannya dengan topik yang diambil. wancara dilakukan pada Bapak Buddhi Sudrajat, ST selaku Seksi Penyajian Data Informasi di Bidang Pusat Data Elektonik (PDE) Dinas Komunikasi dan Informatika Provinsi Jawa Barat.

3. **Studi Literatur.**

   Pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan- bacaan yang ada kaitannya dengan sistem keamanan jaringan komputer pada *web server*.

1.5.3 Metode Evaluasi Sistem Keamanan

Evaluasi sistem keamanan untuk aplikasi *web* ini menggunakan sistem operasi kali linux sebagai media *penetration testing* dengan menggunakan metode *blackbox penetration testing*. Tahapan-tahapan dalam *penetration testing* menggunakan kali linux dengan tahapan-tahapan sebagai berikut *reconnaissance, scanning, exploitation, maintaining acces,* dan *reporting*[7], dan tahapan tersebut bisa dilihat seperti pada gambar 1.1.



Gambar 1. 1 ***The Penetration Testing Life-Cycle***

1. ***Reconnaissance***

Tahapan ini dikenal juga dengan *information gathering* atau pengumpulan data-data untuk mendapatkan secara jelas gambaran dari keseluruhan infrastruktur jaringan, sistem operasi yang digunakan dan servis yang berjalan di tiap-tiap sistem.

2. ***Scanning***

Pada tahap ini dimulainya percobaan evaluasi keamanan, dimana dalam kegiatan ini bertujuan untuk mencari berbagai kemungkinan yang dapat digunakan untuk mengambil alih sistem keamanan komputer dari target, pada langkah ini dapat dilakukan apabila pada tahan *reconnaisance* bisa mendapatkan informasi yang cukup, sehingga *pentester* bisa mencari jalan masuk untuk menguasai sistem keamanan komputer tersebut dengan berbagai *tools* yang digunakan.

3. ***Exploitation***

Pada tahap ini *pentester* mulai melakukan proses penyerangan terhadap sistem keamanan komputer pada target, pengujian ini dilakukan setelah mengetahui kelemahan yang terdapat dari proses *scanning* tadi.

4. ***Maintainning Access***

Mengamankan jalur yang sudah digunakan untuk meretas sistem keamanan komputer agar bisa dipergunakan kembali tanpa harus mengulang dari langkah pertama. Biasanya seorang *attacker* akan menghapus jejaknya dan menanamkan

aplikasi berupa *backdoor, rootkit, trojan* dan sejenisnya agar *attacker* dapat kembali lagi tanpa melakukan tahap dari awal.

5. *Reporting*

Pada tahap ini, seluruh temuan pada kerentanan yang didapat dari hasil evaluasi tadi, akan dibuatkan laporan untuk solusi penanganan sistem keamanan komputer agar lebih baik lagi.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini berisi latar belakang penelitian, identifikasi masalah, maksud dan tujuan penelitian, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab ini membahas tentang profil tempat studi kasus di Dinas Komunikasi dan Informatika Provinsi Jawa Barat dan berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian.

BAB 3 ANALISIS DAN PERANCANGAN

Bab ini menguraikan tentang analisis masalah, analisis jaringan, analisis *web server*, analisis serangan *cyber* di Indonesia, analisis metode *penetration testing lifecycle, black box penetration testing,* analisis keamanan, analisis kebutuhan *pentester* dan perancangan sistem yang terdiri dari simulasi jaringan dan perancangan *website* Diskominfo.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab ini merupakan tahap implementasi dan pengujian yang didapat dari hasil analisis dan perancangan tentang keamanan yang terdapat pada *webserver* untuk dijadikan sebagai bahan evaluasi untuk dilaporkan kepada pihak pengelola atau institusi di Pusat Data Elektronik Dinas Komunikasi dan Informatika Provinsi Jawa Barat.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang sudah diperoleh dari hasil penelitian tugas akhir. Berdasarkan hasil dari kegiatan evaluasi keamanan yang dapat dijadikan catatan untuk pengembangan penelitian selanjutnya.