BAB I
PENDAHULUAN

1.1. Latar Belakang

Berdasarkan definisi dalam modul *EC-Council Certified Ethical Hacker* (EC|CEH), *Penetration Testing* (*pentest*) merupakan metode evaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan bagian dari *security audit* [1]. Simulasi serangan yang dilakukan dibuat seperti kasus yang bisa dibuat oleh *black hat hacker*, *cracker*, dan sebagainya. *Penetration Testing Life Cycle* merupakan salah satu metode yang dapat digunakan bertujuan untuk menentukan dan mengetahui macam-macam serangan yang mungkin dilakukan pada sistem beserta akibat yang bisa terjadi karena kelemahan sistem.

SMA Negeri 1 Kalasan memiliki 2 *website*, yaitu http://sman1kalasan.sch.id dan http://sman1kalasan.org. *Website* http://sman1kalasan.sch.id digunakan sebagia media informasi sekolah, data guru, data alumni, kegiatan sekolah, artikel, dan lain sebagainya, *website* ini pernah mengalami penyerangan oleh *hacker* sekitar 2-3 tahun yang lalu mengakibatkan fasilitas forum pada *website* tidak dapat digunakan sampai saat ini. *Website* http://sman1kalasan.org merupakan *website* yang menggunakan *dedicated server*, *website* ini digunakan sebagai media proses belajar mengajar, mulai dari pengumpulan tugas siswa, pembagian materi, penilaian/raport, dan lain sebagainya. Untuk dapat masuk ke fasilitas *website* hanya dapat diakses oleh *adminisrator*, guru dan siswa/siswi yang terdaftar pada sistem dengan izin akses yang berbeda. Menyadarkan pentingnya keamanan dalam menajaga fungsi pada

web server, maka diperlukan pengujian dalam bentuk *pentest* guna mengidentifikasi adanya kelemahan keamanan pada website sebelum terjadi penyerangan oleh pihak yang tidak bertanggung jawab.

Ada 3 tujuan keamanan, yaitu *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan). Untuk mencapai tercapainya tujuan keamanan maka diperlukan suatu mekanisme yang dapat bekerja bersama-sama untuk tujuan tersebut, maka diperlukan mekanisme *access control* (kendali akses), *authentication* (autentikasi), dan *auditing* (audit) [2]. Berdasarkan hasil studi pustaka dan observasi, penelitian lebih memfokuskan pada segi tujuan keamanan *confidentiality - access control*. Dimana *confidentiality* berarti perlindungan terhadap informasi rahasia dan sensitif dari user yang tidak berhak. Sedangkan *access control* merupakan sebuah kebijakan dalam membatasi hak akses seorang user ke dalam sistem untuk mengerjakan tugas-tugas tertentu.

Berdasarkan uraian permasalahan di atas maka dilakukan penelitian dengan judul "Analisis Keamanan Jaringan Web Server pada SMA Negeri 1 Kalasan Menggunakan Metode *Penetration Testing Life Cycle*". Jika kelemahan dapat diidentifikasi dan dapat dibuktikan beserta dengan analisis resikonya, maka harapannya akan memiliki kemampuan dan waktu untuk memperbaikinya sebelum seseorang yang tidak berkepentingan mengambil keuntungan dari kelemahan tersebut.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana mengidentifikasi kelemahan web

server dengan metode *Penetration Testing Life Cycle* pada jaringan web server pada SMA Negeri 1 Kalasan?

1.3. Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini dilaksanakan di SMA Negeri 1 Kalasan.
2. *Penetration testing* dilakukan pada web server yang digunakan *website* http://sman1kalasan.org.
3. Metode pengujian yang digunakan adalah metode *Penetration Testing Life Cycle*.
4. Dalam melakukan *pentest*, sistem operasi yang digunakan adalah BackBox 4.4.
5. Melakukan *reconnaissance* pada web server menggunakan *tools* whois 7.01, NSLookup, tracepath, dan Web Browser Mozilla Firefox 50.1.0.
6. Melakukan *scanning* pada web server menggunakan *tools* Nmap 7.01 dan msfconsole 4.15.
7. Melakukan *exploitation* pada web server menggunakan *tools* msfvenome 4.15 dan msfconsole 4.15.
8. Melakukan *maintaining access* pada web server menggunakan *tools* msfconsole 4.15.
9. *Reporting* berupa dokumentasi dan presentasi dalam bentuk hasil penelitian (skripsi).

10. Penelitian lebih memfokuskan pada segi tujuan keamanan *confidentiality-access control*.
11. Untuk menjaga keamanan privasi dari pihak sekolah, pada tahapan *exploitation* dan *maintaining access* dilakukan dengan virtualisasi dengan skema topologi jaringan yang sama dengan milik sekolah.
12. Pengujian tidak menggunakan *penetration testing development* atau tidak membuat aplikasi untuk pengujian.
13. *Pentest* ini tidak melakukan serangan terhadap konfigurasi dan algoritma sistem keamanan yang diuji.
14. *Pentest* akan memanfaatkan kelemahan yang ada dari kondisi jaringan komputer pada lokasi.
15. Penelitian ini tidak membahas algoritma dari enkripsi sistem keamanan web server yang digunakan.
16. Penelitian ini tidak membahas *Sistem Manajemen Course* (CMS) yang digunakan pada web server target.
17. Penelitian ini tidak melakukan pengujian keamanan pada wifi SMA Negeri 1 Kalasan.
18. Jika tidak didapatkan celah kerentanan pada tahap analisis sistem menggunakan metode *Penetration Testing Life Cycle*; *Scanning*, pengujian kembali akan langsung menuju tahap pengujian sistem menggunakan metode *Penetration Testing Life Cycle*; *Exploitation* dan *Maintaining Access*.

1.4. Maksud dan Tujuan Penelitian

Adapun maksud dari penelitian ini adalah melakukan *penetration testing* terhadap keamanan jaringan website SMA Negeri 1 Kalasan dan mendokumentasikan keamanan *website* tersebut, dan sebagai syarat untuk menyelesaikan pendidikan program Strata 1 (S1) di Program Studi Informatika Fakultas Ilmu Komputer Universitas Amikom Yogyakarta

Adapun tujuan dari penelitian ini adalah mengevaluasi kelemahan keamanan jaringan dan memberikan saran berupa rekomendasi dari kelemahan sistem pada web server yang ada pada SMA Negeri 1 Kalasan.

1.5. Metode Penelitian

Berikut ini penjabaran cara-cara memperoleh data-data yang digunakan untuk kebutuhan penelitian.

1.5.1. Metode Pengumpulan Data

Agar mendapatkan data dan hasil yang benar, relevan tentang penelitian yang dilakukan, maka dari itu diperlukan metode untuk mencapai tujuan penelitian. Berikut metode penelitian yang digunakan:

1.5.1.1. Observasi

Yaitu teknik pengumpulan data yang di peroleh dengan cara melakukan pengamatan secara langsung terhadap objek yang akan diteliti serta secara cermat dan sistematik.

1.5.1.2. Wawancara

Merupakan teknik pengumpulan data dengan menanyakan langsung kepada seorang informan atau autoritas sorang ahli yang berwenang dalam masalah yang diteliti.

1.5.1.3. Pengumpulan bahan dokumen/data sekunder

Merupakan teknik pengumpulan data dengan memanfaatkan data atau dokumen yang di hasilkan oleh pihak lain Misalnya media massa, lembaga penelitian, tempat penelitian. Data yang di hasilkan berupa bukti, catatan atau laporan historis yang telah tersusun dalam sebuah arsip.

1.5.2. Metode Analisis dan Implemenstasi

Analisis dan implementasi yang akan dilakukan melalui beberapa tahapan yaitu:

1. Melakukan observasi jaringan yang ada pada objek melalui pengamatan maupun wawancara terhadap admin IT SMA Negeri 1 Kalasan.
2. Menganalisis hasil survei dan mengidentifikasi kebutuhan informasi.
3. Menganalisis kerentanan pada sistem dan mengimplementasikan *pentest* pada kerentanan yang didapatkan dengan menggunakan metode *Penetration Testing life Cicle*, dengan langkah-langkah sebagai berikut:
    a. *Reconnaissance*; mengumpulkan data informasi mengenai target.
    b. *Scanning*; mengumpulkan informasi kerentanan.
    c. *Exploitation* (*Gaining Access*); memasuki kedalam sistem.
    d. *Maintaining Access*; mengamankan jalur yang sudah digunakan untuk masuk kembali kedalam sistem.
    e. *Reporting*; dokumentasi dan presentasi.

1.6. Sistematika Penulisan

Sistematika penulisan yang digunakan untuk menyusun dan menyelesaikan skripsi adalah sebagai berikut :

BAB I. PENDAHULUAN

Bab ini akan membahasa latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian, dan sistematika penulisan laporan penelitian.

BAB II. LANDASAN TEORI

Bab ini diuraikan teori-teori yang mendukung untuk penelitian ini yang menjadi landasan dan mendukung pelaksanaan penulisan penelitian.

BAB III. METODOLOGI PENELITIAN

Bab ini membahas mengenai dasar metode apa yang digunakan dalam melakukan penelitian berserta analisis informasi yang diperoleh.

BAB IV. IMPLEMENTASI DAN PEMBAHASAN

Bab ini akan mengimplementasikan dan membahas hasil analisis penelitian pengujian keamanan jaringan webserver yang telah dilakukan, untuk mengetahui seberapa aman web server yang digunakan.

BAB V. PENUTUP

Bab ini berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian berlangsung.

DAFTAR PUSTAKA

Daftar pustaka memuat keterangan buku-buku dan literatur yang menjadi acuan dalam penulisan laporan skripsi ini.