BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dunia IT adalah salah satu tren yang sangat cepat dalam perkembangannya. Semakin banyak sektor kehidupan manusia yang dimasuki oleh teknologi yang sesuai dengan bidangnya. Mulai dari pendidikan, kesehatan, perkantoran semua berbasis komputer. Dalam penerapannya ada komputer yang bertindak sebagai *client* termasuk *gadget* di dalamnya, namun ada juga yang bertindak sebagai server yang berfungsi untuk melayani.

Karena hampir semua sektor mempunyai *server* masing-masing mulai dari *server* dengan skala kecil hingga *server* yang berskala besar atau dikenal dengan istilah super komputer. Baik itu *server* yang ada di pendidikan, perkantoran, maupun perbankan berjalan dengan fungsinya masing-masing. Kebanyakan *server* yang berjalan di dunia saat ini adalah berbasis linux. Linux adalah salah satau sistem operasi yang *open source* sehingga banyak variannya. Salah satu varian yang terkenal dan banyak digunakan adalah Ubuntu Server.

Kenyataan yang terjadi saat ini, yang menjadi kepentingan utama bagi masing-masing Lembaga hanya bagaimana fungsi dari *server* itu bisa berjalan, tanpa memperhatikan dari segi keamanannya. Dalam dunia saat ini keamanan masih

menjadi hal yang dikesampingkan. Padahal seharusnya keamanan diperhatikan mulai dari

sebuah sistem itu dibangun hingga sistem itu berjalan atau dalam istilah yang dikenal dengan *security by design* dan *security by accident*.

Salah satu cara untuk memastikan keamanan dalam sebuah sistem informasi khususnya *server* yang merupakan komponen dari sistem itu sendiri, yaitu dengan cara melakukan audit dari *server* tersebut. Dari banyak cara untuk mengaudit keamanan salah satunya adalah "Exploit Development". Exploit Development adalah salah satu cara untuk mengetahui celah dari sebuah *software* ataupun sistem operasi.

1.2 Rumusan masalah

Berdasarakan dari uraian latar belakang tersebut dapat dirumuskan permasalahannya.

1. Bagaimana mengaudit keamanan dengan metode Exploit Development menggunakan bahasa pemrograman Python dan Assembly.
2. Bagaimana Mengaudit sistem operasi yang berbasis linux dengan arsitektur 64 bit

1.3 Batasan Masalah

Dalam melakukan audit keamanan dengan menggunakan Exploit Development ini akan dibatasi sebagai berikut:

1. Sistem operasi *server* yang diaudit hanya Ubuntu Server 12.04 64 bit. Namun untuk mempermudah proses penelitian akan di-*install desktop environment*-nya yaitu menggunakan Unity.
2. Bahasa pemrograman yang digunakan hanya menggunakan bahasa pemrograman Python dan Assembly sebagai *primary* dan bahasa C sebagai bahasa sekunder.
3. Seperangkat komputer yang digunakan telah terpasang *interpreter* ataupun *compiler* dari masing-masing bahasa pemrograman yang digunakan.
4. Frame Work yang digunakan untuk melakukan proses audit kemanan adalah Metasploit Framework.
5. Dalam penelitian tidak melibatkan perusahaan atau lembaga tertentu tapi hanya menggunakan lab *private* yang penulis bangun sendiri.
6. Dalam penggunaan bahasa Assembly-nya hanya sesuai dengan arsitektur Intel 64 bit.

1.4 Maksud dan Tujuan Penelitian

Melakukan audit keamanan Ubuntu Server 64 bit menggunakan metode Exploit Development dengan bahasa pemrograman Python dan Assembly.

1.5 Manfaat Penelitian

Penelitian audit keamanan Ubuntu Server 64 bit menggunakan metode Exploit Development bertujuan untuk.

1. Melakukan penelitian apakah sistem operasi Ubuntu Server 64 bit mempunyai celah yang vital sehingga perlu diperhatikan lebih.
2. Untuk administrator jaringan mengetahui apakah sistem operasi *server* yang mereka gunakan benar-benar aman atau masih banyak celah yang seharusnya bisa diperbaiki.

1.6 Metode penelitian

Metode penelitan dalam proses audit menggunakan Exploit Development ini adalah metode *security life cycle*, dimana ada empat tahapan:

1. Identifikasi (Identify).
2. Exploitasi (Exploitation).
3. Pembersihan Jejak (Covering track)
4. Mitigasi (Mitigation).

1.7 Sistematika Penulisan

BAB 1: PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang masalah, rumusan masalah, maksud dan tujuan penelitian, manfaat menelitian, metode penelitian dan sistematika penulisan.

BAB 2: LANDASAN TEORI

Bab ini menjelaskan teori dan acuan dalam penulisan skripsi yaitu mengenai tahapan audit *security* yang di peroleh dari beberapa literatur, jurnal maupun buku-buku yang relevan sesuai dengan judul.

BAB 3: METODE PENELITIAN

Bab ini menjelaskan bagaimana metode-metode yang di gunakan dalam penelitian dan tahapan-tahapan yang di uraikan secara terperinci.

BAB 4: IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas tentang implementasi dari penelitan tentang audit *security*. Disini juga di bahas tentang risiko atau ancaman keamanan dari sebuah *server* yang *vurnerable*.

BAB 5: KESIMPULAN DAN SARAN

Bab ini membahas tentang kesimpulan dan saran dari hasil akhir audit *security* yang dilakukan.