BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam perkembangan teknologi sekarang ini memungkinkan segala hal menjadi jauh lebih praktis, seperti sekarang ini di Indonesia sudah menerapkan revolusi industri 4.0. Revolusi industri 4.0 sendiri adalah penggabungan antara teknologi otomatisasi dan pertukaran data dalam teknologi manufaktur. Istilah revolusi industri 4.0 juga di kenal sebagai "*internet of things*" (IoT), yang mulai menyentuh dunia virtual, bentuk konektifitas manusia, mesin dan data. Dengan adanya revolusi industri 4.0 tersebut, tentunya membuat para pelaku usaha bisa melakukan bisnis produk menggunakan platform digital. Dan dengan beralihnya para pelaku usaha ke *platform* digital maka penggunan server akan semakin banyak pula. Saat ini penggunaan server menjadi sangat penting untuk membantu kebutuhan bisnis dalam mengelola berbagai dokumen atau produk aplikasi di sebuah perusahaan.

Server adalah sebuah sistem komputer yang menyediakan jenis layanan (*service*) tertentu dalam sebuah jarngan komputer. Server didukung dengan proses yang bersifat *scalable* dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang di sebut sebagai sistem operasi jaringan (*network operating system*). Dengan banyaknya penggunaan server maka tidak menutup kemungkinan akan adanya *trafik* illegal yang dapat mengganggu sehingga saat pengguna ingin mengakses layanan dari server akan terjadi gangguan. Untuk itu salah satu cara terbaik untuk menghindari hal tersebut adalah dengan melakukan hardening.

Hardening merupakan salah satu teknik yang digunakan untuk kebutuhan dalam penguatan keamanan pada lapisan server dan network sehingga lapisan tersebut menjadi lebih kuat dan lebih tahan terhadap suatu serangan yang dapat menyebabkan kerusakan, baik terhadap hardware maupun software. Tujuan di lakukannya hardening adalah untuk menurunkan tingkat risiko keamanan dan menghilangkan bagian-bagian yang rentan terhadap sebuah serangan. Langkah pengamanan tersebut dapat di lakukan dengan mengurangi bagian-bagian yang tidak diperlukan oleh sistem utama, dapat berupa software, akun, port, permission,

akses, dan lain-lain. Dengan dilakukannya hal tersebut, tentunya dapat meminimalisir serangan terhadap sistem dari ancaman-ancaman seperti malware.

Untuk metode hardening server sendiri ada beberapa metode yang dapat di jadikan sebagai acuan untuk melakukan proses hardening server, yang tentunya sudah di akui keamanan dari metode tersebut. Yaitu dengan menggunakan metode NIST (*NATIONAL INSTITUTE of STANDARD and TECHNOLOGY*) dan EC-Council. Namun dengan perkembangan teknologi yang terus menerus tentunya akan ada masalah masalah yang tentunya dapat mengganggu.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, dapat dirumuskan sebuah permasalahan yaitu cara menigkatkan keamanan sebuah server dari serangan yang tidak di inginkan. Salah satu caranya adalah dengan meningkatkan keamananan pada server tersebut, di penelitian ini hardening server akan dijadikan acuan untuk analisis di bab selanjutnya..

1.3 Batasan Masalah

Untuk batasan masalah dalam proses penelitian ini dapat di uraikan sebagai berikut :

a. Penelitian dilakukan dengan menggunakan metode Eksperimental.
b. Proses implementasi dilakukan di *virtual box*.
c. Malakukan *hardening server*.
d. Penelitian ini hanya membandingkan antara NIST dan *EC Council*.
e. Melakukan pentesting brute force.

1.4 Tujuan Penelitian

Tujuan yang ingin penulis raih dalam pembuatan laporan penelitian ini adalah untuk membuat perbandingan tingkat keamanan pada sebuah server dengan mengikuti kaidah-kaidah yang terdapat pada metode hardening di *NIST* dan *EC Council*. Dalam penelitian ini penulis akan melakukan perbandingan keamanan pada server yang menggunakan *framework* NIST dan server yang menggunakan *framework* EC Council.