

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Menurut Tanenbaum “Jaringan komputer merupakan kumpulan dari perangkat keras dan perangkat lunak di dalam suatu sistem yang memiliki aturan tertentu untuk mengatur seluruh anggotanya dalam melakukan aktivitas komunikasi satu komputer yang terkoneksi ke jaringan menjadi satu node dari jaringan tersebut. Sedangkan *host* secara umum diartikan sebagai komputer yang terkoneksi ke jaringan yang dapat memberikan layanan jaringan (*network service*)”.

Menurut Ikhwan “Keamanan jaringan sangat vital bagi sebuah jaringan komputer kelemahan-kelemahan yang terdapat pada jaringan komputer jika tidak dilindungi dan dijaga dengan baik akan menyebabkan kerugian berupa kehilangan data, kerusakan sistem *server*, tidak maksimal dalam melayani *user* atau bahkan kehilangan aset-aset berharga institusi”.

Pengukuran tingkat keamanan komputer yang sering dilupakan keamanannya baik dikantor, sekolah, dan tempat umum lainnya yang menggunakan jaringan LAN adalah celah *port* terbuka. Padahal disitulah langkah awal atau pintu pertama penyusup bisa menyerang masuk kedalam jaringan, tentu jika itu terjadi penyusup dapat mengambil data-data dan mengganggu kinerja pada jaringan komputer. Mulai dari bug, worm atau virus dan jenis kejahatan lainnya sering ditemukan di *WEB* yang sering tersambung dengan *host/client* di jaringan internet. Semakin celah tertutup maka tingkat kejahatan pun semakin sedikit.

Tidak ada satu pun sistem keamanan yang sempurna, *scanning port* digunakan untuk meminimalisasi celah keamanan pada *port* komputer dan memeriksa *port* yang terbuka adalah *port* yang sedang digunakan atau *port* yang tidak diketahui kegunaannya. Adapun judul yang diangkat oleh penulis adalah **RANCANG BANGUN SISTEM PENGUKURAN TINGKAT KEAMANAN KOMPUTER PADA JARINGAN LAN.**

## 1.2 Rumusan Masalah

Dari latar belakang di atas penelitian dapat dirumuskan beberapa masalah yaitu:

1. Bagaimana membuat sistem pengukuran keamanan komputer pada jaringan LAN?
2. Apakah dengan menggunakan jenis keamanan *scanning port* dapat meminimalisasi terjadinya ancaman pada komputer?
3. Bagaimana solusi pada saat terdeteksi ancaman pada *port* yang terbuka?

## 1.3 Batasan Masalah

Berdasarkan latar belakang di atas, maka batasan masalah sebagai berikut:

1. Hanya *administrator* yang memiliki hak untuk melakukan *scanning port* tersebut.
2. Penggunaan perangkat *Raspberry Pi* sebagai *server proxy* untuk *scanning port* menggunakan konfigurasi *tools* pada OS *Linux* diantaranya *scanning port*.
3. Melakukan *scanning port* pada jaringan LAN kampus Akademi Telkom Jakarta dan apabila terdeteksi masalah *port* terbuka yang tidak diketahui kegunaannya, maka diberikan solusi memblok atau menutup *port*, agar *port* cepat kembali pulih dari ancaman tersebut.

## 1.4 Tujuan Penelitian

Adapun tujuan dari proyek akhir ini adalah sebagai berikut:

1. Sistem pengukuran keamanan komputer pada jaringan LAN, dibuat untuk memudahkan *administrator* dalam mengecek tingkat keamanan komputer dari serangan *public* khususnya *local* dari serangan *port scanning*.
2. Tambahan *tool nmap* melakukan *scanning port* bertujuan untuk meminimalisasi terjadinya ancaman pada *port* komputer yang aktif sedang digunakan dan tersambung dengan jaringan.
3. Memberikan solusi dengan memblok atau menutup *port* tersebut sehingga komputer menjadi aman kembali digunakan.

## 1.5 Manfaat Penelitian

Manfaat yang diharapkan oleh penulis proyek akhir sebagai berikut:

1. Meningkatkan sistem untuk mengukur keamanan komputer pada jaringan LAN dari pihak yang tidak bertanggung jawab atau yang tidak memiliki akses izin.
2. Mengidentifikasi masalah *port* terbuka yang tidak diketahui kegunaannya, ditampilkan melalui data monitoring tingkat keamanan komputer pada *web* dan notifikasi *via telegram* sehingga memudahkan untuk memonitoring tingkat keamanan pada komputer.

## 1.6 Metodologi Penelitian

Pada pembuatan proyek akhir ini, penulis melakukan metodologi penelitian dengan menggunakan metode sebagai berikut:

1. Studi literatur  
Metode ini dilakukan dengan membaca beberapa *referensi-referensi* yang ada dari berbagai sumber, baik berupa buku, proyek akhir, skripsi, jurnal dan karya ilmiah yang berhubungan dengan rancang bangun sistem keamanan ini.
2. Studi Bimbingan  
Meliputi masukan, pengarahan dan saran dari dosen yang memiliki keahlian pada bidang ini.
3. Pembuatan dan Implementasi  
Metode ini dilakukan untuk merancang sistem keamanan komputer dengan *hardware* dan *software* serta bahasa pemrograman yang sudah ditentukan. Maka dilakukan untuk tahap mengimplementasikan rancang bangun sistem keamanan komputer yang sudah dibuat.
4. Uji coba sistem dan pengukuran  
Pada tahap ini merupakan uji coba sistem keamanan *scanning port* untuk mengukur tingkat keamanan komputer standar ISO 27001. Dilakukan sekali pengujian untuk satu komputer atau lebih yang sudah tersambung dengan jaringan bersama *raspberry*, namun untuk mendapatkan hasil yang akurat dilakukan secara berulang-ulang setiap 15 menit sekali dalam sehari, dengan bentuk tabel data monitoring pada *web* dan

*notifikasi via telegram* khusus untuk komputer tidak aman beresiko tinggi.

## 1.7 Sistematika Penulisan

Secara umum sistematika penulisan proyek akhir ini terdiri dari bab-bab dengan metode penyampaian berikut:

### **BAB I PENDAHULUAN**

Bab ini berisi latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

### **BAB II LANDASAN TEORI**

Bab ini dibahas mengenai teori-teori yang dipakai sebagai landasan dasar yang mendukung penelitian dan penelitian sebelumnya dengan topik terkait mengenai keamanan komputer.

### **BAB III PERANCANGAN DAN ANALISA**

Penulis menyajikan tentang data langkah kerja dan informasi yang dilakukan dalam rancang bangun sistem pengukuran tingkat keamanan komputer pada jaringan LAN.

### **BAB IV HASIL DAN PEMBAHASAN**

Bab ini penulis menguji hasil dari rancang bangun sistem pengukuran keamanan komputer pada jaringan LAN menggunakan data *scanning port* tersebut.

### **BAB V PENUTUP**

Bab ini berisi mengenai kesimpulan dari hasil pembuatan serta pengujian perancangan sistem yang di buat, dan saran agar pengembangannya dimasa yang akan datang dapat lebih baik.