

1 PENDAHULUAN

1.1 Latar Belakang

Diskominfo Kota Bogor merupakan instansi pemerintah yang bertugas untuk mengelola data dan juga menyediakan ruangan *data center* yang didalamnya berisikan *server – server* instansi pemerintah di Kota Bogor. Tugas *server* yaitu melayani seluruh yang terhubung ke jaringannya dan merupakan perangkat utama dalam sistem komunikasi jaringan berfungsi sebagai penyedia layanan dan memiliki log yang sangat banyak (Sholihah *et al.* 2020). Instansi ini juga bertugas untuk mengelola jaringan pada kelurahan, kecamatan, dan dinas – dinas terkait yang masih di bawah pemerintahan Kota Bogor. Kebutuhan akan internet dan jaringan komputer pada saat ini semakin bertambah banyak, baik dalam hal pendidikan, pekerjaan maupun dalam sebuah permainan. Salah satu hal yang paling penting ketika memelihara atau merawat jaringan internet yaitu keamanan dari jaringan itu sendiri, dengan banyaknya pengguna yang masuk atau mengakses ke jaringan internet itu maka akan semakin besar pula peluang tindak kejahatan yang bisa terjadi di dalam jaringan tersebut, salah satu diantaranya yaitu pencurian data yang mengakibatkan kerugian, ataupun adanya *hacker* yang menonaktifkan sumber daya jaringan tersebut, dsb (Lukman dan Bahtia 2016).

Dengan demikian yang harus diwaspadai oleh para pengelola jaringan (administrator) komputer yaitu banyaknya serangan yang bisa dilakukan di internet. Jangan sampai ada celah (*Vulnerability*) yang dapat dimanfaatkan oleh para peretas. Salah satu jenis serangan yang dapat dilakukan pada jaringan komputer adalah *port scanning*. Serangan ini masuk dalam kategori *Reconnaissance Attack* yakni melakukan pemantauan terhadap jaringan serta mengumpulkan informasi yang ada di dalamnya. *Port Scanning* adalah tahapan awal untuk mendeteksi *port-port* yang terbuka dan mendapatkan informasi dari *port* yang terbuka pada target, servis apa yang sedang dijalankan, versi dari server dan lain sebagainya (Valianta *et al.* 2016). Dengan sistem ini memungkinkan menjadi awal mula terjadinya serangan terhadap sumber daya yang terdapat pada jaringan. Ketika informasi mengenai *protocol / port* sudah didapatkan maka '*Hacker*' langsung bisa memanfaatkannya untuk melakukan eksploitasi dari *protocol / port* tersebut.

Keamanan jaringan pada saat ini menjadi suatu kebutuhan yang penting bagi semua instansi. Untuk mengamankan jaringan internet dari serangan pihak luar yang tidak bertanggung jawab, maka diperlukan sebuah sistem keamanan yang handal, agar tetap terjaganya keutuhan jaringan internet di wilayah Kota Bogor. PSD (*Port Scan Detection*) diharapkan mampu menjadi solusi untuk mengamankan sistem jaringan internet Diskominfo Kota Bogor. Sistem ini akan dapat mendeteksi setiap serangan berupa *port scanning* yaitu kegiatan untuk mengetahui *port – port* apa saja yang terbuka dan servis apa saja yang sedang dijalankan.

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

- a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
- b. Pengutipan tidak merugikan kepentingan yang wajar IPB.

2. Dilarang mengemukakan atau memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.

1.2 Rumusan Masalah

Rumusan masalah dari pembuatan tugas akhir mengenai sistem keamanan jaringan menggunakan *Port Scan Detection* ini yaitu:

1. Bagaimana cara mendeteksi *port scanning* pada suatu jaringan?
2. Tindakan apa yang harus dilakukan ketika terjadi *port scanning*?
3. Bagaimana seorang administrator mengetahui ketika terjadi *port scanning*?

1.3 Tujuan

Tujuan dari pembuatan tugas akhir mengenai sistem keamanan jaringan menggunakan *Port Scan Detection* ini yaitu:

1. Mendeteksi setiap perangkat yang melakukan *port scanning*.
2. Memblokir *IP Address* pelaku *port scanning* dalam waktu yang sudah ditentukan.
3. Mendapatkan pemberitahuan berupa pesan bot telegram ketika terjadi serangan.

1.4 Manfaat

Manfaat dari pembuatan tugas akhir mengenai sistem keamanan jaringan menggunakan *Port Scan Detection* ini yaitu:

1. Melindungi jaringan dari serangan pihak luar
2. Memudahkan seorang administrator mengetahui bahwa telah terjadi serangan berupa *port scanner*.
3. Membuat jaringan menjadi lebih kebal terhadap serangan yang bersifat mengetahui port apa yang terbuka dan servis apa yang sedang dijalankan.

1.5 Ruang Lingkup

Ruang lingkup dari pembuatan laporan tugas akhir mengenai sistem keamanan jaringan menggunakan *Port Scan Detection* ini yaitu:

1. Percobaan *port scanning* hanya menggunakan Nmap.
2. Pengiriman notifikasi hanya melalui Telegram.
3. Hanya menampilkan pesan bahwa telah terjadi serangan.
4. Hanya dapat diterapkan pada jaringan lokal.
5. Mendeteksi *port scanning* yang menggunakan protocol TCP saja.