BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi dan jaringan komputer berkembang sangat cepat dan sudah menjadi kebutuhan sangat penting apalagi bagi sekolah untuk mempermudah komunikasi serta berbagi atau mencari informasi dalam konteks pembelajaran baik bagi siswa-siswi, karyawan, maupun bagi guru. Banyak keuntungan yang didapat dengan adanya jaringan komputer, salah satunya bisa memudahkan pekerjaan yang dilakukan.

SMA Negeri 1 KOBA adalah sekolah menengah atas yang terletak di Desa Arung Dalam, Kecamatan Koba, Kabupaten Bangka Tengah. Awal mula sekolah ini bernama SMU Negeri 1 Koba yang memulai operasionalnya pada tahun pelajaran 1996/1997. Pada sekolah ini terdapat infrastruktur jaringan yang berfungsi sebagai penunjang proses belajar mengajar.

Banyaknya pengguna jaringan ini dapat menimbulkan terjadinya penyalahgunaan atau kejahatan *cyber*. Salah satu cara yang digunakan untuk melakukan tindak kejahatan ini yaitu melakukan *dns cache poisoning*. *Dns cache poisoning* (juga dikenal sebagai *DNS Spoofing*) adalah jenis serangan yang mengeksploitasi kerentanan dalam sistem nama domain (DNS) untuk mengalihkan lalu lintas dari situs web resmi ke situs web palsu. Prinsip serangan didasarkan pada pemalsuan DNS dengan tujuan pengalihan lalu lintas. Salah satu *DNS Cache Poisoning* yang paling berbahaya adalah karena dapat menyebar dari server DNS ke server DNS[1]. Menurut *Global DNS Threat Report*, pada tahun 2021 serangan *dns hijacking* ini sebanyak 27% dan pada tahun 2022 sebanyak 28%, itu artinya kejahatan *cyber* ini terus meningkat dari tahun ke tahun[2]. Hal ini juga bisa terjadi pada jaringan SMAN 1 KOBA.

Berdasarkan permasalahan tersebut, penulis mengusulkan kemanan jaringan terhadap serangan *dns cache poisoning* menggunakan *firewall* berbasis *routerboard* mikrotik. *Firewall* adalah sebuah sistem atau perangkat keamanan, khususnya dalam jaringan komputer, yang bertanggung jawab untuk menjamin keamanan

transmisi data pada jaringan komputer [3]. *Firewall* ini nantinya diharapkan bisa memberikan keamanan pada jaringan terhadap serangan *dns cache poisoning*. Untuk memperkuat penelitian yang dilakukan, penulis melakukan studi literatur terkait serangan *dns cache poisoning*. Penelitian ini telah dilakukan oleh peneliti terdahulu yang akan penulis gunakan sebagai referensi dan bahan penelitian ini. Penelitian pertama oleh Novianto, Dian dkk pada tahun 2021 mengenai "Implementation of a Network Security System Using the Simple Port Knocking Method on a Mikrotik-Based Router" , penelitian kedua oleh Dissanayake, I. M.M. pada tahun 2018 menegenai "DNS Cache Poisoning: A Review on its Technique and Countermeasures"[4], penelitian ketiga oleh Man, Keyu dkk pada tahun 2020 mengenai "DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels"[5], penelitian keempat oleh Zheng, Xiaofeng dkk pada tahun 2020 mengenai "Poison over troubles forwarders: A cache poisoning attack targeting DNS forwarding devices"[6], penelitian kelima oleh Man, Keyu dkk pada tahun 2021 mengenai "DNS Cache Poisoning Attack: Resurrections with Side Channels"[7], penelitian keenam oleh Pangestu, Teguh dan Liza, Risko pada tahun 2022 mengenai "Analisis Keamanan Jaringan Pada Jaringan Wireless Dari Serangan Man In The Middle Attack DNS Spoofing"[8].

Berdasarkan permasalahan yang telah diuraikan pada latar belakang sebelumnya, maka penulis mengajukan judul "**Implementasi Keamanan Jaringan Terhadap Serangan *Dns Cache Poisoning* Menggunakan *Firewall* Berbasis *Routerboard Mikrotik* Di SMAN 1 KOBA**".

1.2 Rumusan Masalah

Beberapa permasalahan yang dapat dirumuskan berdasarkan latar belakang yang terjadi di atas adalah sebagai berikut:

1. Bagaimana membuat serangan *dns cache poisoning* dengan ettercap di *KaliLinux*?
2. Bagaimana menggunakan *firewall* di *routerboard mikrotik* RB951Ui-2^{nD} untuk mengatasi serangan *dns cache poisoning*?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini dibatasi agar mengacu pada implementasi keamanan jaringan sebagai berikut:

1. Penulis hanya mengimplementasikan keamanan jaringan terhadap serangan *dns cache poisoning* menggunakan *firewall* berbasis *routerboard* mikrotik
2. Konfigurasi mikrotik menggunakan aplikasi *Winbox* v3.37
3. Dalam melakukan *test* serangan penulis menggunakan *Kali Linux pada VirtualBox*
4. Serangan *dns spoof* menggunakan *Ettercap*
5. *Routerboard mikrotik* yang digunakan versi RB951Ui-2nD
6. *RouterOS* yang digunakan pada mikrotik versi 6.48.7
7. Perancangan topologi jaringan menggunakan *Cisco Packet Tracer 7.3.0*

1.4 Tujuan dan Manfaat Penulisan

1.4.1 Tujuan Penelitian

Adapun tujuan dari penelitian ini sebagai berikut:

1. Agar pembaca mengerti betapa pentingnya kemanan jaringan komputer
2. Agar pembaca bisa memahami cara mengimplementasikan *firewall* keamanan jaringan terhadap serangan *dns cache poisoning* di *routerboard mikrotik*
3. Agar jaringan di SMAN 1 KOBA terhindar dari serangan *dns cache posoning* dengan menerapkan *firewall* berbasis *routerboard mikrotik*

1.4.2 Manfaat Penelitian

Adapun manfaat pada penelitian ini sebagai berikut:

1. Dapat mengerti betapa pentingnya kemanan jaringan komputer
2. Dapat memahami cara mengimplementasikan *firewall* keamanan jaringan terhadap serangan *dns cache poisoning* di *routerboard mikrotik*
3. Dapat meminimalisir dan mencegah terjadinya serangan *dns cache poisoning* pada jaringan SMAN 1 KOBA dengan menerapkan *firewall* berbasis *routerboard mikrotik*

1.5 Sistematika Penulisan

Sistematika penulisan skripsi ini dibuat untuk memudahkan dalam pembahasan, namun merupakan satu kesatuan antara bab yang satu dengan bab yang lainnya. Adapun susunan dari uraian bab-bab tersebut adalah:

BAB I : PENDAHULUAN

Bab ini berisi mengenai latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, dan sistematika penulisan. Yang berfungsi sebagai penghantar bagi para pembaca untuk mengetahui hal apa saja yang akan dibahas secara keseluruhan.

BAB II : LANDASAN TEORI

Bab ini menjelaskan tentang teori-teori yang digunakan dalam penelitian untuk mendukung implementasi keamanan jaringan pada routerboard mikrotik di SMAN 1 KOBA

BAB III : METODOLOGI PENELITIAN

Bab ini berisi tentang jenis metode penelitian yang digunakan, sumber data yang digunakan, teknik pnegumpulan data, dan alat bantu dalam menganalisa masalah yang diteliti.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini berisi profil sekolah, analisis masalah, solusi pemecahan masalah, analisis kebutuhan sistem, perancangan sistem, uji coba serangan sebelum firewall dan DoH diaktifkan, konfigurasi firewall dan DoH, uji coba serangan setelah firewall dan DoH diaktifkan.

BAB V : PENUTUP

Bab ini berisi tentang kesimpulan dan saran dari hasil kegiatan penelitian yang telah dilakukan.