BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan dalam teknologi jaringan telah melahirkan berbagai jenis jaringan komputer, seperti LAN (*Local Area Network*), MAN (*Metropolitan Area Network*), dan WAN (*Wide Area Network*). LAN biasanya digunakan untuk menghubungkan perangkat dalam area yang terbatas seperti rumah atau kantor, sedangkan WAN mencakup area yang lebih luas, bahkan antar negara [1].Ancaman yang biasa terjadi pada jaringan LAN khususnya adalah serangan *malware*, implementasi pembatasan sumber daya diperlukan sebelum *malware* tersebut dideteksi oleh *antivirus*.

Pemahaman mendalam terhadap masalah-masalah ini akan menjadi dasar untuk merumuskan solusi yang sesuai dan berkelanjutan. Penelitian ini akan menggali lebih dalam tentang aspek-aspek spesifik, dengan fokus pada upaya identifikasi masalah dan tantangan yang dihadapi oleh SMK Muhammadiyah 3 Yogyakarta dalam membatasi celah keamanan jaringan. Untuk itu penilis mengajukan penelitian ini untuk mengukur konfigurasi yang dapat mengurangi kerentanan pada laboratorium komputer.

Penulis akan melakukan studi pustaka untuk menelusuri referensi penelitian terdahulu, identifikasi rumusan masalah untuk mengetahui *poin point* yang dihadapai laboratorium SMK Muhammadiyah 3 Yogyakarta, penentuan tujuan penelitian agar cakupan masalah dapat difokuskan. Setelah itu peneliti akan menggunakan metode NDLC (*Network Development Life Cycle*) dimana metode tersebut adalah kerangka kerja untuk mengevaluasi jaringan komputer di sebuah instansi, metode ini meliputi analisis, desain, simulasi prototipe, pengujian, dan monitoring.

Pada penelitian ini penulis akan melakukan implementasi *Port Security* pada jaringan non manageable *switch* yang menggunakan *web proxy* pada suatu ekosistem jaringan yang menerapkan *non manageable switch* untuk memblokir sumber daya tertentu dalam rangka mengurangi vektor penyerangan menggunakan

kerangka kerja NDLC dengan harapan memperkuat landasan pengetahuan yang telah ada dan menjadi bahan evaluasi pada laboratorium komputer SMK Muhammadiyah 3 Yogyakarta.

1.2. Rumusan Masalah

1. Bagaimana penggunaan *Keamanan jaringan* dapat membatasi celah keamanan jaringan di SMK Muhammadiyah Yogyakarta?
2. Bagaimana hasil penggunaan *Keamanan jaringan* dapat membatasi celah keamanan jaringan di SMK Muhammadiyah Yogyakarta?

1.3. Batasan Masalah

1. Penelitian ini akan membatasi fokus pada analisis dan solusi terhadap masalah keamanan jaringan dengan menggunakan *Keamanan jaringan* melalui pendekatan *Network Development Life Cycle* (NDLC).
2. Evaluasi efektivitas akan difokuskan pada keamanan jaringan dengan metrik jumlah kerentanan, dan tidak mencakup aspek-aspek lain terkait dengan manajemen jaringan.
3. Menggunakan *web proxy* pada *router* utama dimana beberapa *switch* terkoneksi dengan seperangkat PC laboratorium.
4. Hasil penelitian terbatas pada jumlah kerentanan yang ada sebelum dan sesudah dilakukan konfigurasi jaringan sebagai metrik utama.
5. Penelitian hanya terbatas pada konfigurasi *web proxy* dan konfigurasi pendukung lain seperti *routing* dan DHCP.
6. Penelitian ini tidak menyertakan *log* konfigurasi jaringan.
7. Penelitian ini hanya menjadi bahan pertimbangan bagi pihak manajemen jaringan, kesalahan dalam eksekusi konfigurasi menjadi hal yang dapat diabaikan.

1.4. Tujuan Penelitian

1. Mengetahui penggunaan *Keamanan jaringan* dapat membatasi celah keamanan jaringan di SMK Muhammadiyah Yogyakarta?
2. Mengetahui hasil penggunaan *Keamanan jaringan* dapat membatasi celah keamanan jaringan di SMK Muhammadiyah Yogyakarta?

1.5. Manfaat Penelitian

1. Penelitian ini diharapkan dapat menjadi tambahan kepustakaan dalam bidang *web proxy* dan keamanan jaringan, serta mengadopsi fakta-fakta dari penelitian sebelumnya untuk implementasi keamanan di instansi pendidikan.
2. Penelitian ini memberikan solusi praktis untuk meningkatkan keamanan jaringan di SMK Muhammadiyah 3 Yogyakarta melalui penggunaan *Keamanan jaringan* dan metode *Network Development Life Cycle* (NDLC).
3. Hasil penelitian ini dapat menjadi bahan pertimbangan dalam implementasi keamanan jaringan di dunia nyata, khususnya di lingkungan pendidikan yang menggunakan *non-manageable switch* dan *web proxy*.
4. Penelitian ini memberikan langkah-langkah implementasi praktis dan monitoring yang dapat membantu dalam evaluasi efektivitas keamanan jaringan.
5. Penelitian ini diharapkan dapat memberikan solusi yang berkelanjutan untuk mengatasi celah keamanan jaringan, membantu dalam perumusan kebijakan keamanan yang lebih baik di institusi pendidikan.

1.6. Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab I akan membahas latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, dan manfaat penelitian dan sistematika penulisan yang digunakan dalam penyusunan skripsi.

BAB II TINJAUAN PUSTAKA

Menyajikan studi literatur yang relevan, keaslian penelitian dibandingkan dengan penelitian sebelumnya, serta dasar teori yang digunakan dalam penelitian ini.

BAB III METODE PENELITIAN

Menjelaskan objek penelitian, alur penelitian, dan metode penelitian yang digunakan, serta kebutuhan alat dan bahan yang digunakan selama penelitian.

BAB IV HASIL DAN PEMBAHASAN

Berisi hasil-hasil yang diperoleh dari penelitian, termasuk lingkungan konfigurasi *web proxy*, langkah-langkah konfigurasi *web proxy* pada mikrotik yang

akan membatasi akses pada *non-managable switch*, serta hasil implementasi konfigurasi dan hasil analisis kerentanan keamanan jaringan.

BAB V PENUTUP

Menyajikan kesimpulan dari penelitian serta saran-saran untuk penelitian lebih lanjut atau implementasi praktis.