BAB I

PENDAHULUAN

1.1 Latar Belakang

Akses internet seluler dan *WIFI* pada saat ini semakin menyeluruh dan dapat di akses dimanapun. Berdasarkan laporan terbaru *We Are Social*, pada tahun 2020 disebutkan bahwa ada 175,4 juta pengguna internet di Indonesia. Dibandingkan tahun sebelumnya, ada kenaikan 17% atau 25 juta pengguna internet di negeri ini. Berdasarkan total populasi Indonesia yang berjumlah 272,1 juta jiwa, maka itu artinya 64% setengah penduduk RI telah merasakan akses ke dunia maya (Haryanto, 2020).

Seiring perkembangan internet dan banyaknya pengguna layanan internet, akan menimbulkan permasalahan yang dihadapi dikala pemanfaatan teknologi jaringan komputer dan komunikasi semakin tinggi, akan semakin banyak pengguna jaringan yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil maksimal baik dari segi efisiensi maupun peningkatan keamanan jaringan itu sendiri, maka dibutuhkan suatu infrastruktur jaringan yang bagus yang dapat menjawab kebutuhan itu.

Filtering MAC addres adalah keamanan jaringan *wireless LAN* yang penggunaannya bertujuan untuk mengamankan akses internet dengan mengizinkan *MAC address* yang sudah terdaftar untuk dapat mengakses jaringan internet, dalam pengimplementasian *filtering MAC address* memiliki celah keamanan yang mampu diretas menggunakan *MAC address cloning*.

Penelitian ini, untuk mengatasi permasalahan yang terdapat pada *filtering MAC address*, dilakukan pendeteksian *MAC address cloning* dengan mendeteksi *packet lost* aktivitas perangkat pada *ARP list* dan pemblokiran menggunakan *firewall* pada mikrotik. Mengacu pada penelitian (Dwi Ratnasari & Safiroh Utsalina, 2017) tentang bagaimana mengatasi peretasan *MAC address cloning* dengan menggunakan *firewall* untuk melakukan pemblokiran terhadap perangkat illegal yang melakukan *cloning* perangkat yang terdaftar pada jaringan internet. Penelitian sebelumnya peretasan *MAC address cloning* menggunakan *PC* dan hanya melakukan pemblokiran *MAC address cloning* dengan *firewall*.

Melihat dari permasalahan tersebut, diusulkan penelitian yang mengintegrasikan *ARP list* dan *firewall* untuk dapat mendeteksi perangkat yang sedang melakukan *cloning* dan melakukan peretasan dengan *smartphone* diusulkan penelitian yang berjudul "INTEGRASI *FIREWALL* DAN *ARP LIST* UNTUK MENGAMANKAN *MAC ADDRESS CLONING* PADA *WIRELESS LAN*". Kelebihan penelitian yang diusulkan yaitu melakukan uji coba peretasan *MAC address cloning* dengan *smartphone* dan pendeteksian perangkat yang melakukan *MAC address cloning* dengan memanfaatkan integrasi *ARP list* dan *firewall*. Yang tidak dilakukan pada penelitian sebelumnya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dirumuskan dalam penelitian ini adalah :

1. Bagaimana cara mendeteksi serangan *MAC address cloning*?
2. Bagaimana cara mengantisipasi dan mengatasi serangan *MAC Address Cloning*?
3. Apakah peretasan *MAC address cloning* hanya bisa dilakukan menggunakan sistem operasi windows?

1.3 Batasan Masalah

Menghindari pembahasan yang terlalu luas, maka penelitian ini membatasi masalah – masalah yang ada, antara lain:

1. Penelitian ini menganalisis keamanan pada mikrotik yang menggunakan keamanan *filtering MAC address*.
2. Hanya menggunakan satu pengujian yaitu *MAC address cloning*.
3. Hanya melakukan pendeteksian terhadap *MAC address* yang dicurigai sedang di *cloning*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, maka dapat ditarik tujuan dari penelitian ini adalah sebagai berikut :

1. Melakukan integrasi *ARP list* dan *firewall* untuk mendeteksi peangkat yang sedang melakukan *cloning* dan melakukan pemblokiran perangkat yang sudah terdeteksi melakukan *cloning.*

2. Melakukan pengujian peretasan pada sistem keamanan *filtering MAC address* dengan *MAC address cloning* untuk menemukan celah keamanan dan memperbaiki celah keamanan yang ditemukan.
3. Melakukan peretasan *MAC address cloning* menggunakan sistem operasi android untuk mengetahui sistem operasi yang dapat menjalankan peretasan MAC address cloning selain windows.

1.4 Manfaat Penelitian

Manfaat yang didapatkan dari penelitian ini adalah menemukan suatu keterbaruan *smartphone* sebagai media peretasan terhadap keamanan jaringan *filtering MAC*. Memperbaiki sistem kemanan yang sudah diketahui kerentanannya.

1.6 Metodologi Penelitian

Metode yang digunakan dalam penelitian terdiri dari langkah-langkah sebagai berikut:

1. Studi Pustaka

   Penelitian yang dilakukan dengan mendapatkan bahan rujukan berupa referensi yang bersifat teoritis dari buku, jurnal, dan sumber bacaan lain yang berkaitan dengan masalah pada penelitian ini.
2. Pengumpulan Data

   Melakukan identifikasi kebutuhan untuk melakukan penelitian pada persiapan awal dan implementasi mencangkup identifikasi kebutuhan *hardware* dan *software*.

3. Pengujian Sistem

   Menguji jaringan wireless yang menggunakan keamanan *filtering MAC address* dengan metode penyerangan *MAC address cloning*.

4. Evaluasi Penelitian

   Hasil penelitian melakukan pengetesan terhadap jaringan keamanan *filltering mac address* dengan metode penyerangan *MAC address cloning* menggunakan *smartphone* dan mengatasi *MAC address cloning* menggunakan *ARP list*.

1.7 Sistematika Penelitian

Sistematika penulisan dalam penelitian dengan judul "INTEGRASI *FIREWALL* DAN *ARP LIST* UNTUK MENGAMANKAN *MAC ADDRESS CLONING* PADA *WIRELESS LAN*" adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisikan tentang laporan secara garis besar dengan meliputi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Landasan teori berisikan tentang kajian dari penelitian terdahulu dan teori yang berupa pengertian dan definisi yang diambil dari kutipan jurnal, web, atupun buku serta beberapa literature review yang berkaitan dengan penyusunan laporan skripsi ini.

BAB III METODOLOGI

Bab ini berisi mengenai metode yang digunakan dalam pembahasan dalam penelitian, baik pada proses pengumpulan data maupun penyelesaian masalah. Tahapan yang digunakan terdiri dari Planning, Discovery, Attack Dan Reporting.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi mengenai hasil analisa dan pembahasan penelitin yang disusulkan dan pembahasan secara detail terhadap bagaimana menganalisis keamanan jaringan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi mengenai kesimpulan yang didapat dari pembahasan yang telah dilakukan, kesimpulan dari penelitian berupa proses perancangan yang diterapkan, apakah metode yang digunakan telah sesuai dengan kondisi yang dibutuhkan, apakah penelitian yang dilakukan akan membuahkan hasil yang baik dan bermanfaat bagi pengguna. Saran yang berisi perbaikan yang harus dilakukan pada keterbatasan dalam penelitian, dan diakhiri dengan daftar pustaka serta lampiran.