BAB I
PENDAHULUAN

1.1 Latar Belakang

Peningkatan pengguna jaringan internet sangat cepat. Dari laporan Metode penelitian apa yang akan digunakan untuk menganalisis serangan hasil *survey* APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) pada tahun 2019 - 2020 Q2, penetrasi internet di Indonesia sendiri pada tahun 2019 sekitar 73,3 % dan pengguna internet hingga 196.714.070 dari total populasi Indonesia di tahun 2019 sebanyak 266.911.900 penduduk [1]. Akses ke jaringan internet, merupakan kebutuhan yang tidak dapat dihindari. Keinginan pengguna jaringan internet untuk mendapatkan hak akses saat ini sangat tinggi, sehingga keamanan sangat dibutuhkan. Sebuah Jaringan Internet area lokal adalah jaringan internet yang menyambungkan setiap perangkat dalam area terbatas seperti tempat tinggal, sekolah, laboratorium, kampus universitas, atau gedung kantor secara nirkabel atau menggunakan kabel [2]. Pada penelitian ini, peneliti menggunakan teknologi jaringan internet nirkabel secara pribadi untuk kepentingan penelitian dan analisis serangan terhadap jaringan nirkabel atau *Wi-Fi*.

Teknologi jaringan nirkabel maupun kabel memiliki celah keamanan yang dapat mengganggu pengguna jaringan. Aktivitas teknologi yang melakukan kejahatan dalam suatu jaringan dengan menghapus informasi, meretas jaringan, mengambil data pengguna jaringan, dan menyembunyikan informasi disebut dengan *Cybercrime*. Beberapa kejahatan jaringan komputer, seperti DDoS (*Distributed Denial of Service*), *Sniffing, Spoofing, Man In The Middle Attack*, serta *Deauther*. Aktivitas Kejahatan pada jaringan internet dapat mengakibatkan pencurian data, kerusakan alat komunikasi, dan hilangnya konektivitas jaringan [2].

Serangan DDoS (*Denial-of-Service*) pada WiFi dapat melumpuhkan komunikasi antar perangkat yang terhubung. Serangan ini terjadi selama

proses otentikasi. Hal ini dilakukan dengan mengirimkan alamat broadcast dan memodifikasi alamat broadcast pada target yang telah diserang. Dalam contoh ini, perangkat ditautkan melalui WiFi. Jenis serangan ini dikenal sebagai deauthentication [3]. Penelitian ini menggunakan modul mikrokontroler ESP8266 Deauther sebagai alat penetration *test jamming*, module mikrokontroler ESP8266 merupakan media alat yang mudah untuk digunakan sebagai serangan terhadap jaringan internet. ESP8266 Deauther dapat digunakan secara *Standalone* dengan menggunakan *source code* yang dapat menimpa sinyal jaringan nirkabel. Dengan menggunakan fitur ARP (*Address Resolution Protocol*) Router Mikrotik. Router dapat membatasi pengguna dan membatasi bandwith dari jaringan yang terhubung, serta memantau lalu lintas paket jaringan melalui log data Router Mikrotik. *Address Resolution Protocol* adalah sistem Mikrotik Router yang memetakan alamat logis (*IP Address)* ke alamat fisik *(Mac Address)* [4].

Pada penelitian ini peneliti menggunakan metode *Live Forensic* yang dapat mendeteksi serta mengidentifikasi serangan berdasarkan tipe serangan. Tipe serangan yang digunakan peneliti adalah Serangan *Jamming* pada jaringan menggunakan *Wifi Deauther* ESP8266. Metode *Live Forensic* telah digunakan pada penelitian terdahulu . Pada penelitian tersebut investigator dapat mendeteksi suatu serangan dan mengidentifikasi penyerang pada jaringan [5].

Skenario *Deauther* pada ES8266 Deauther adalah Deauther mengirimkan paket yang dapat mengganggu kinerja sinyal dari Router serta memutus koneksi semua pengguna yang terhubung pada jaringan internet lokal. ESP8266 Deauther diberikan *source code*. ESP8266 dapat berjalan tanpa harus mengetahui *user* dan *password* dari router Mikrotik. Sedangkan untuk metode *live forensic* yang digunakan dalam penelitian

1.2 Rumusan Masalah

Berdasarkan penjelasan pada latar belakang sebelumnya dapat disimpulkan pokok permasalahan yang angkat peneliti yaitu :

a. Bagaimana mengkonfigurasi ARP Mikrotik untuk skenario serangan Wifi ESP8266 Deauther ?

b. bagaimana menerapkan metode live forensic untuk menganalisis serangan wifi ESP8266 Deauther ?

1.3 Batasan Masalah

a. Metode keamanan jaringan komputer menggunakan fitur ARP pada Mikrotik
b. Analisis serangan *Deauther* pada jaringan internet lokal
c. Penelitian dilakukan pada jaringan internet lokal milik pribadi

1.4 Tujuan Penelitian

a. Menganalisis lalu lintas paket data dengan menggunakan metode *statefull* ARP Mikrotik
b. Melakukan pentesting pada jaringan internet lokal dengan serangan dari WiFi *Deauther* ESP8266 dengan metode *deauther*

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan informasi ilmiah mengenai serangan *deauther* pada Router Mikrotik. Selain itu, juga diharapkan dapat menjadi acuan administrator jaringan dalam menganalisis setiap serangan *deauther* pada jaringan internet lokal.

1.6 Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah *Live* Forensic, metode ini dilakukan untuk mengumpulkan data barang bukti saat sistem sedang berjalan dengan harapan pelaku dapat segera diidentifikasi dan proses penanganan dapat diselesaikan lebih cepat [5]. Sebelum memperoleh bukti dari suatu kejahatan forensik yang dilaporkan, beberapa tahapan dalam *live forensic* perlu diselesaikan, seperti mengumpulkan bukti, memeriksa bukti, dan menganalisis data bukti.

1.7 Sistematika Penelitian

Pada bagian ini dituliskan urut-urutan dan sistematika penelitian yang dilakukan. Berikan ringkasan mengenai isi masing-masing bab.

BAB I : PENDAHULUAN

Bab ini berisi latar belakang masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penelitian.

BAB II : LANDASAN TEORI

Pada bab ini akan dibahas teori dasar yang berkaitan dengan penelitian sebelumnya yang dilakukan dan menjadi dasar dalam pemecahan masalah dalam penelitian.

BAB III : METODOLOGI PENELITIAN

Pada bab ini akan membahas metode penelitian yang digunakan pada penelitian Analisis Keamanan Jaringan Komputer Lokal Dengan Menggunakan fitur ARP (*Address Resolution Protocol*) Pada Mikrotik Untuk Mengatasi Serangan ESP8266 *Deauther*.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini akan membahas perhitungan setiap parameter yang diuji secara matematis untuk kemudian dianalisis berdasarkan standarisasi yang telah ditentukan

BAB V : PENUTUP

Bab ini berisi tentang kesimpulan akhir dan saran untuk pengembangan penelitian.