BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi dan komunikasi telah berkemabang dengan sangat pesat pada era digital saat ini sehingga memiliki peran yang penting bagi masyarakat. Jaringan Komputer merupakan salah satu teknologi yang berkembang dibidang transmisi data dan jaringan komputer memiliki 2 jenis media transmisi data diantaranya kabel dan nirkabel. Jaringan nirkabel memanfaatkan gelombang radio sebagai media untuk terhubung antara perangkat satu dengan perangkat lainnya. Jaringan nirkabel atau *wireless* ini sangat sering digunakan karena merupakan salah satu sarana yang penting dalam peningkatan jumlah pengguna internet di Indonesia. Wifi menawarkan kemudahan dalam mengakses dan kecepatan tinggi serta harga yang terjangkau, sehingga pengguna internet semakin antusias untuk menggunakan *wireless* walaupun dengan tingakat keamanan yang rendah. Namun penggunaan Jaringan *wireless* tidak luput dari kejahatan *cyber* yang dilakukan oleh orang yang tidak bertanggung jawab sehingga dapat merugikan orang lain.

Serangan MITM (*Man In The Middle Attack*) adalah serangan terhadap jaringan akses terbuka. MITM merupakan bentuk serangan di dalam jaringan komputer, dimana (*attacker*) atau si penyerang berada ditengah-tengah (*Middle*) antara korban dengan tujuan korban. Bentuk dari serangan MITM dapat berupa adanya penyadap komunikasi suara dan teks, perusakan privasi dan hilangnya jaminan keaslian suatu data, seta termasuk pembajakan sesi, pencurian data sensistif, pencurian *login*, dan pencurian informasi pribadi (Ajharie & Sulistiyono. 2022).

Serangan ARP *Poisioning* sangat merugikan bagi *user* karena bersifat aktif, yaitu penyerang dapat melakukan tindakan langsusng pada *user*. Serangan ini dapat digunakan untuk mencuri data sensitif yang dikirimkan melalui jaringan, seperti kata sandi, informasi finansial, dan informasi pribadi. Penyerang juga dapat mengalihkan

lalu lintas sehingga menggangu koneksi internet, membuat layanan tidak tersedia bagi pengguna yang seharusnya menerimanya.

Forensik jaringan merupakan proses mendeteksi, menangkap, mencatat, dan menganalisa aktivitas jaringan guna menemukan bukti digtal dari suatu serangan atau kejahatas yang dilakukan melalui jaringan komputer sehingga pelaku kejahatan dapat dituntut sesuai hukun yang berlaku. Metode *Live Forensics* adalah situasi atau proses analisa forensik yang dilakukan ketika sistem jaringan komputer beroperasi. Hal ini disebabkan oleh informasi bukti digital yang hanya dapat diperoleh saat sistem berfungsi dan informasi tersebut dapat hilang jika sistem jaringan mati. (Jaya, *et.al.,* 2020)

Universitas Dumai merupakan perguruan tinggi yang terletak di kota Dumai, Riau yang juga berpartisipasi dalam menyelenggarakan sistem keamanan. Universitas Dumai perlu menyediakan perlindungan jaringan untuk medukung dan memastikan lancarnya kegiatan ada Universitas Dumai. Jaringan Komputer pada Universitas Dumai menjadi jembatan antara Dosen, pihak Civitas Akademika dan juga Mahasiswa.

Penelitian lain dilakukan oleh Kamajaya *et,al* (Kamajaya et al., 2020) yang melakukan Analisa investigasi *Static Forensic* Serangan *Man In The Middle Attack* berbasis ARP *Poisioning.* Penelitian ini dilakukan dengan menerapkan pendekatan metode Statik Forensik, untuk mendeteksi aktivitas ilegal yang terjadi pada wi-fi. Proses investigasi dibagi menjadi sepuluh tahapan dimulai dari proses *preparation, detection, incident, respon, collection, examination, presevation, examinations, analysism investiation* dan *reporting*. Penelitian ini akan difokuskan pada serangan *Man In The Middle Attcak berbasis* ARP *Poisioning*. Hasil dari penelitian ini dapat menganalisa data dan menenukan barang bukti maupun informasi pelaku yang dapat dipertanggung jawabkan.

Penelitian yang dilakukan oleh Saraun *et,al* (Saraun et al., 2021) yang melakukan Analisis Keamanan Jaringan Nirkabel IEEE 802.11 pada Kantor Dinas Pendidikan Kabupaten Minahasa. Penelitian ini menggunakan metode Penetration test. Pada penelitian ini dilakukan pengujian dengan serangan *cracking the encrtption*, ARP *Poisioning* dan *denial of service* terhadap jaringan nirkabel. Data yang digunakan pada penelitia ini adalah jaringan pada Kantor Dinas Pendidikan Kabupaten Minahasa. Hasil dari pengujian dnegan serangan-serangan yang dilakukan dapat disimpulkan bahwa penerapan sistem keamanan jaringan yang

diterapkan masih belum sepenuhnya dikatakan aman dikarenakan serangan *cracking the encrtption* yang disimulasikan berhasil.

Penelitian lain dilakukan oleh Diansyah *et.al* (Diansyah et al., 2023) yang melakukan Manajemen Pencegahan Serangan Jaringan *Wireless* Dari Serangan *Man In The Middle Attack*. Pada penelitian ini melakukan kemungkinan dalam penyerangan dengan jenis serangan yang dilakukan adalah *Man In The Middle Attack.* Dari percobaan ini dilakukan sebanyak 5 kali dan dilakukan perhitungan QoS (*Quality of Service*) yaitu mengitung berapa banyak paket *loss* dan hasil yang didapatkan dari percobaain penyerangan ini dengan menghitung paket *loss* nya sebanyak *loss* 0.291%, serangan 1 model 2 dengan paket *loss* 0,124%, serangan 2 model 2 dengan paket *loss* yang diartikan pada serangan ini berhasil untuk menyerang komunikasi *wireless*. Untuk mencagah dari penyerangan ini, terlebih dahulu untuk mengetahui teknik cara serangan itu berjalan pada *wireless,* dengan menggunakan *ettercap* pada *kali linux.*

Penelitan lain dilakukan oleh Adriyansa & Panjaitan (Adriyansa & Panjaitan, 2020) yang melakukan Analisis Sistem Keamanan Jaringan Menggunakan *Framework* NIST. Keamanan jaringan merupakan aspek yang sangat penting bagi sebuah jaringan komputer. Jaringan komputer memiliki kelemahan-kelemahan yang jika tidak dilindungi dan dijaga dengan baik maka akan menyebabkan kerugian. Maka sudah sepatutnya keamanan jaringan harus lebih diperhatikan untuk mencegah ancaman menyerang sistem, terlebih lagi saat jaringan LAN sudah tersambung ke internet maka ancaman keamanan jaringan akan semakin signifikan. Universitas Sjakhyakirti merupakan universitas yang terletak di kota Palembang yang juga berpartisipasi dalam menyelenggarakan sistem keamanan tersebut. Pentingnya penelitian ini yaitu agar dapat mengurangi adanya ancaman yang berdampak negatif terhadap sistem keamanan informasi, sehingga mengurangi dampak insiden sistem informasi dan meminimalisir resiko-resiko yang mungkin akan terjadi. Selanjutnya dilakukan analisa sistem keamanan jaringan dengan *Framework* NIST *(National Institute Standard Technology), framework* yang dirancang untuk sesuatu perhitungan kualitatif yang didasarkan pada analisis sistem keamanan.

Penelitian lain dilakukan oleh Pangestu & Liza (Pangestu & Liza, 2022) yang melakukan Analisis Keamanan Jaringan pada Jaringan *Wireless* dari Serangan *Man In The Middle Attack* DNS *Spoofing*. Namun tetapi, dengan adanya *wireless* tidak sepenuhnya aman dalam melakukan aktivitas interaksi sesama manusia dalam

mengirim data dan lain sebagainya, salah satunya kegiatan *illegal man in the middle attack DNS spoofing*. Dengan adanya kegiatan *illegal* tersebut maka dibutuhkan sistem keamanan yang diharapkan dapat mencegah kegiatan *illegal man in the middle attack DNS spoofing*. Hasil dari penyerangan yang di dapatkan berdasarkan 7 kali pengujian dengan menghitung *quality of service (QOS)* yaitu *packet loss* dengan hasil serangan 1 model 1 dengan *packet loss* 0,154%, serangan 2 model 1 dengan *packet loss* 0,234%, serangan 3 model 1 dengan *packet loss* 0.291%, serangan 1 model 2 dengan *packet loss* 0,173%, serangan 2 model 2 dengan *packet loss* 0,128%, serangan 3 model 2 dengan *packet loss* 0,028%, serangan 4 model 2 dengan *packet loss* 0,231%, yang dapat diartikan serangan ini dapat berjalan dengan baik. Dan hasil dengan memanfaatkan sistem keamanan *firewall* hanya dapat mencegah dengan memutus interaksi komunikasi antar penyerang dengan korban dan korban dengan penyerang.

Berdasarkan uraian yang telah di jabarkan maka peneliti mengangkat penelitian yang ditulis dalam bentuk tesis yang berjudul **"Perancangan ARP Poisioning dalam Menganalisa Keamanan Jaringan Wireless dari Serangan Man In The Middle Attack."**

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah tersebut diatas, maka rumusan masalah yang diajukan pada penelitian ini yaitu sebagai berikut :

1. Bagaimana perancangan ARP *Poisoning* dapat menganalisa Keamanan Jaringan *Wireless* dari Serangan *Man In the Middle Attack* ?
2. Bagaimana cara pencegahan dari serangan *Man In The Middle Attack* pada jaringan *Wireless*?
3. Bagaimana menguji rancangan ARP *Poisoning* dapat menganalisa Keamanan Jaringan *Wireless* dari Serangan *Man In the Middle Attack* ?

1.3 Batasan Masalah

Adapun beberapa batasan masalah dalam penelitian ini untuk lebih terarah sesuai dengan tema yang diankat, maka peneliti mencantumkan batasan masalah sebagai berikut:

1. Penelitian ini melakukan analisa dan perancangan pengujian keamanan jaringan wireless pada Universitas Dumai.
2. Penelitian ini menggunakan *tools* Wireshark untuk menganalisa kemanan jaringan wireless di Universitas Dumai.
3. Penelitian ini menggunakan *tools Ettercap* untuk melakukan Perancangan Serangan ARP Poisioning.
4. Penelitian ini dilakukan untuk mengetahui apakah jaringan *wireless* di Universitas Dumai tidak rentan dan sudah aman dari serangan ARP *Poisioning* dan *Man In The Middle Attack*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang diangkat pada penelitian ini, maka tujuan dari penelitian ini adalah:

1. Merancang ARP *Poisoning* dalam menganalisa Keamanan Jaringan *Wireless* dari Serangan *Man In the Middle Attack*.
2. Melakukan analisa keamanan jaringan dari ARP *Poisioning.*
3. Menguji rancangan ARP *Poisoning* dalam menganalisa Keamanan Jaringan *Wireless* dari Serangan *Man In the Middle Attack* menggunakan metode *Live Forensic*.

1.5 Manfaat Penelitian

Sesuai dengan tujuan penelitian ini dilakukan, maka manfaat yang yang diharapkan pada penelitian ini diantaranya sebagai berikut:

1. Untuk menerapkan metode *Live Forensic* pada Perancangan ARP *Poisioning* dalam menganalisa Keamanan Jaringan *Wireless* dari Serangan *Man In The Middle Attack.*
2. Mengetahui cara-cara pencegahan dari serangan *Man In The Middle Attack.*
3. Untuk mengetahui apakah Serangan ARP *Poisioning* yang dilakukan berhasil atau tidak.

1.6 Sistematika Penulisan

Penulisan yang sistematis digunakan untuk memudahkan pembacaan dan pemahaman, oleh karena itu penulis dalam menyusun tesus memuat beberapa bab tergantung bagaimana permasalahan yang disajikan sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian dan manfaat penelitian yang dilakukan serta sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini berisi teori-teori yang berkaitan dengan permasalah yang ada pada penelitian ini, diantarnya tentang ARP *Poisioning,* Keamanan Jaringan, *Man In The Middle Attack*, Wireshark dan *Live Forensic*.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan tentang penelitian yang akan dilakukan, objek penelitian, sumber data, metode dan analisa pengumpulan data yang dilakukan secara sistematis dan tepat sasaran.

BAB IV ANALISA DAN PERANCANGAN

Pada bab ini membahas tentang Analisa Keamanan Jaringan dan Perancangan ARP *Poisioning* dari serangan *Man In The Middle Attack*.

BAB V IMPLEMENTASI DAN HASIL

Pada bab ini menjelaskan tentang implementasi dan perancangan yang telah dilakukan secara detail dan hasil dari pengujian yang telah dilakukan.

BAB VI KESIMPULAN DAN SARAN

Bab ini berisi tentang simpulan hasil penelitian yang diperoleh sesuai dengan tujuan penelitian serta memuat saran mengenai masalah dan kemungkinan pemecahannya untuk penelitian selanjutnya.