# BAB 1
# PENDAHULUAN

## 1.1 LATAR BELAKANG

Pemanfaatan teknologi berbasis jaringan telah berkembang dengan seiring berjalannya kemajuan teknologi. Kemudahan dalam pengguna mengakses sebuah jaringan komputer telah memberikan manfaat yang berdampak besar terhadap kebutuhan masyarakat di era modern. Kemudahan yang dapat dirasakan oleh para pengguna adalah mempermudah untuk melakukan aktivitas pengiriman data dari pengirim ke tujuan secara online dan mengakses media online yang lainnya. Hal ini dapat terlihat dari survey yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2020, survey tersebut membuktikan bahwa pada tahun 2020 jumlah pengguna internet mengalami kenaikan sebesar 10,12 % yaitu menjadi 17,17 juta jiwa pengguna yang mengakses internet [1].

Semakin berkembang dan meningkatnya pengguna dalam mengakses jaringan komputer, maka semakin rentan pula jaringan komputer mengalami suatu penyerangan atau peretasan dari pihak-pihak yang tidak bertanggung jawab. Salah satu serangan yang dapat dilakukan adalah ARP poisoning. Serangan ARP poisoning dapat mengancam untuk jaringan komputer, karena penyerang dapat memanfaatkan mekanisme ARP untuk menyadap dan memodifikasi alur lalu lintas jaringan dengan cara memalsukan alamat IP dan MAC [2]. Pada perancangan sistem jaringan komputer dibutuhkan server untuk menyediakan layanan-layanan yang dapat diakses oleh *client* layanan ini hanya dapat diakses oleh pihak *client* akan tetapi hal ini dapat menyebabkan penyerang menjadikan server sebagai target serangan ARP poisoning karena seluruh akses layanan data terletak pada server.

Upaya yang dilakukan dalam pencegahan tindakan-tindakan peretasan pada suatu jaringan komputer, *network forensic* dapat dijadikan sebagai salah satu langkah untuk mencatat bukti-bukti, menangkap, merekam serta menganalisa aktivitas mencurigakan pada jaringan komputer [3]. Pada proses mengumpulkan bukti-bukti dalam menganalisis aktivitas lalu lintas jaringan, dibutuhkan sebuah

aplikasi atau *tools* yang dapat memberikan informasi terkait informasi-informasi untuk forensik jaringan. *Tools* yang dapat digunakan adalah *wireshark*, karena didalam *tools wireshark* dapat merekam serta memunculkan berbagai informasi dalam proses keluar masuknya data pada jaringan komputer. Informasi forensik yang dapat direkam oleh *tools wireshark* adalah IP *address list* yang berusaha masuk dan tindakan-tindakan apa saja yang dilakukan oleh masing-masing IP *address* tersebut.

Pada penelitian ini forensik jaringan digunakan dalam upaya pendeteksian serangan pada jaringan komputer, terdapat beberapa metode yang dapat dilakukan, salah satu metode dari *network forensic* adalah *live forensic*. Metode *live forensic* dilakukan ketika sistem jaringan komputer sedang beroperasi dan dilakukan secara *real time* ketika komputer atau *router* sedang beroperasi.

Berdasarkan penjelasan latar belakang diatas, maka penulis melakukan penelitian yang berjudul "**ANALISIS PENDETEKSIAN SERANGAN ARP *POISONING* DENGAN MENGGUNAKAN METODE *LIVE FORENSIC*"**.

## 1.2 RUMUSAN MASALAH

Rumusan masalah dalam penelitian ini adalah :

1. Bagaimana cara kerja dari serangan ARP *Poisoning* pada suatu jaringan komputer?
2. Bagaimana langkah-langkah yang dilakukan untuk mengumpulkan bukti-bukti forensik pada jaringan komputer menggunakan *wireshark*?
3. Bagaimana cara untuk melakukan pendeteksian serangan ARP *Poisoning* dengan menggunakan metode *live forensic*?

## 1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1. Uji coba serangan dalam penelitian ini dilakukan pada perangkat komputer server pada jaringan LAN (*Local Area Network*).
2. Dalam membangun web server penlitian ini menggunakan PHP My Admin dan Filezilla.

3. Layanan yang disediakan pada web server mencakup layanan *login* (*Username* dan *Password*).
4. Serangan yang dilakukan adalah ARP *poisoning*
5. *Tools* yang digunakan untuk *monitoring* trafik jaringan yaitu *wireshark* dan *tools* yang digunakan untuk mendeteksi serangan ARP *poisoning* adalah XARP.
6. *Tools* yang digunakan untuk melakukan serangan ARP *poisoning* adalah *Ettercap*.
7. IP *address* yang digunakan adalah IPv4 (IP *Private*).
8. Metode untuk pengumpulan bukti-bukti forensik adalah menggunakan metode *live forensic*.
9. Skenario pengujian dilakukan pada saat perangkat komputer dan switch sedang beroperasi.

## 1.4 TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah:

1. Mampu menjelaskan terkait cara kerja dari serangan ARP *Poisoning* pada suatu jaringan komputer.
2. Mampu menjelaskan terkait langkah-langkah yang dilakukan untuk mengumpulkan bukti-bukti forensik pada jaringan komputer menggunakan *wireshark* dan XARP.
3. Mampu menjelaskan terkait cara untuk melakukan pendeteksian serangan ARP *Poisoning* dengan menggunakan metode *live forensic*.

## 1.5 MANFAAT PENELITIAN

Penelitian ini diharapkan memberikan manfaat, yaitu :

1. Sebagai panduan terkait langkah-langkah yang perlu dilakukan dalam melakukan forensik jaringan pada sebuah jaringan komputer.
2. Sebagai bentuk implementasi dalam melakukan pencatatan dan perekaman aktivitas lalu lintas jaringan yang dijadikan sebagai barang bukti dalam melakukan proses investigasi forensik jaringan menggunakan *tools* wireshark.

3. Sebagai pengujian dalam melakukan penyelidikan suatu serangan pada jaringan komputer dengan menggunakan metode *Live Forensic.*

## 1.6 SISTEMATIKA PENULISAN

Penelitian ini terbagi menjadi beberapa bab. Bab 1 berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan pada penelitian ini. Bab 2 membahas tentang tinjauan pustaka terkait dengan penelitian-penelitian yang telah dilakukan sebelumnya serta teori-teori dari berbagai sumber yang berkaitan dengan implementasi penelitian ini. Teori-teori tersebut terdiri dari *network protocol analyzer*, *network attack*, pengertian dan cara kerja dari ARP poisoning, wireshark, pengertian mengenai *network forensic* dan *live forensic*. Pada Bab 3 membahas tentang alur pada penelitian ini dan topologi jaringan yang digunakan. Bab 4 berisi tentang analisa dan pembahasan dari implementasi penelitian ini. Selanjutnya, bab 5 membahas mengenai kesimpulan dan saran untuk penelitian yang akan dilakukan selanjutnya.