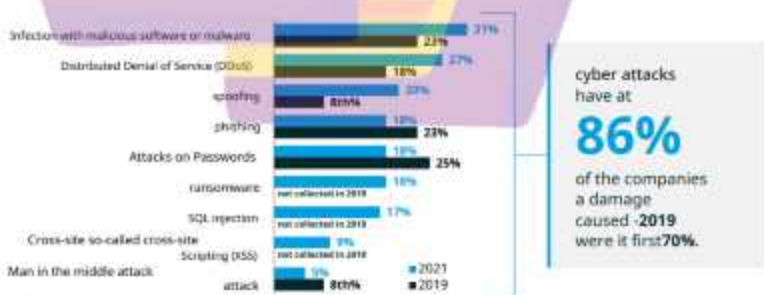
BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan internet memberikan pengaruh besar dalam beberapa dekade terakhir. Pengaruh dari internet itu sendiri telah membantu manusia dalam kehidupan sehari-hari seperti kemampuan untuk mengakses informasi secara instan, memperluas jaringan sosial, dan menemukan peluang bekerja. Menurut hasil survey yang dilakukan oleh [1], pengguna internet seluruh dunia dari 8,01 triliun total populasi dipastikan 64.4% (5,16 triliun) adalah pengguna internet. Sedangkan negara Indonesia hingga bulan Januari 2023 sendiri memiliki pengguna internet sekitar 77% (219,9 juta) dari total populasi [2]. Peningkatan penggunaan internet secara luas tidak terlepas dari pemanfaatan jaringan baik skala kecil sampai skala besar, baik dari individu, perusahaan, dan lembaga pemerintah.

Dalam manfaat internet, *Access Point* (AP) berperan penting sebagai titik akses untuk terhubung ke jaringan internet. *Access Point* merupakan jaringan nirkabel yang menghubungkan kebutuhan manusia pada waktu yang bersamaan. Dampak dari kemudahan ini terdapat dampak negatif dari penggunaan internet yaitu munculnya berbagai model *cyber attack* yang sangat merugikan berbagai pihak [3]. *Cyber attack* merupakan aktivitas kejahatan yang menggunakan teknologi, contohnya peretasan jaringan, pengambilan data milik orang lain, penjualan ilegal di website, dan masih banyak lagi [4].



Gambar 1.1 Data cyber attack 2019-2021

Studi yang dilakukan [5] pada tahun 2021 menunjukkan bahwa, 9 dari 10 perusahaan dalam 12 bulan terakhir mengalami peningkatan *cyber attack* dengan persentase 86% dan menyebabkan kerusakan internal pada perusahaan. Gambar 1.1 menunjukkan bahwa jumlah serangan *spoofing* meningkat sebesar 12% dihitung dari tahun 2019 hingga 2021. *Spoofing* merupakan klasifikasi *cyber attack* yang memanipulasi/mengubah alur lalu lintas jaringan dengan teknik *Man in the Middle Attack* (MITM) [6]. Salah satu jenis dari serangan spoofing yaitu *ARP Spoofing* dengan mengeksploitasi protokol ARP [7]. ARP (*Address Resolution Protocol*) memiliki peranan penting dalam untuk mengidentifikasi atau mencari alamat fisik (MAC) berdasarkan alamat logis (IP) di dalam jaringan lokal [8]. Saat sebuah perangkat ingin berkomunikasi dengan perangkat lain dalam jaringan, perangkat tersebut harus mengirim permintaan ARP untuk mencari tahu alamat fisik dari alamat IP yang dituju. *ARP Spoofing* merupakan serangan yang memanfaatkan kerentanan protokol ARP menggunakan suatu teknik MITM yaitu *ARP Poisoning*.

Serangan ARP Poisoning ini terjadi, ketika sebuah host ingin berkomunikasi maka paket data ARP harus dikirim ke host lain, host tersebut harus mengirimkan permintaan ARP secara *broadcast* untuk mencari tahu alamat fisik dari alamat IP yang dituju [9]. Namun, penyerang dapat memanfaatkan celah dalam metode broadcast ARP ini, dengan mengirimkan permintaan ARP palsu dan menyamarkan alamat MAC palsu kepada host yang dituju. Dalam skenario ini, host yang dituju akan mengirimkan respons balik ke alamat MAC palsu tersebut, yang kemudian dapat digunakan oleh penyerang untuk memantau atau memanipulasi lalu lintas jaringan [10].

Penelitian ini dimulai dari penyusunan skenario dan simulasi kasus dari sisi *attacker* dengan tools Ettercap untuk menemukan informasi host sekaligus alat bantu menyerang jaringan komputer, setelah itu menjalankan tahap simulasi serangan *ARP Poisoning*. *Attacker* menjalankan *port forwarding* pada tools Ettercap dan melancarkan serangan *ARP Poisoning*. Tahap simulasi ini bertujuan untuk mengetahui, bagaimana tahap atau pola dari serangan ini, dan apa saja informasi yang didapat dari si korban.

Tahap penelitian selanjutnya dilakukan pendeteksian serangan menggunakan *tools* XARP dan proses *static forensic* menggunakan framework NIST SP 800-86 untuk menganalisis bukti digital yang diperoleh dari proses *capture* lalu lintas jaringan dengan *tools* Wireshark. Tujuan dari penelitian ini adalah menemukan informasi penting dari hasil analisis dan menyusunnya menjadi bentuk laporan.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang ada diatas, maka rumusan masalah dalam penelitian ini adalah :

1. Bagaimana pola serangan Man In The Middle berbasis ARP Poisoning?
2. Bagaimana penerapan static forensic pada skenario penelitian ini?

1.3 Batasan Masalah

Dalam melakukan penelitian ini adapun batasan masalah yang ditetapkan adalah sebagai berikut :

a. Framework yang digunakan dari NIST SP 800-86 "Guide to Integrating Forensic Techniques into Incident Response".
b. Tools yang digunakan untuk mendeteksi adanya serangan ARP Poisoning adalah Xarp.
c. Tools yang digunakan untuk menangkap dan menganalisis bukti digital adalah Wireshark dan Network Miner.
d. Cakupan area penelitian ini terbatas pada area wlan.
e. Jenis serangan yang digunakan adalah MITM berbasis ARP Poisoning.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah diatas adapun tujuan yang ingin dicapai dari penelitian ini sebagai berikut :

a. Mengimplementasikan teknik *static forensic* dan *network forensic* untuk melakukan investigasi forensik dari skenario serangan *man in the middle*.
b. Penelitian ini memperlihatkan secara detail proses investigasi mulai dari

pengumpulan bukti digital sampai tahap laporan hasil analisis.

c. Penelitian ini juga memperlihatkan proses simulasi serangan *ARP Poisoning*.
d. Mencari atau menemukan informasi penting dari bukti digital dalam bentuk file pcap.
e. Melakukan pemblokiran IP dan MAC Address attacker.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini berdasarkan latar belakang, rumusan masalah, batasan masalah, dan tujuan penelitian adalah sebagai berikut :

a. Memberikan gambaran prosedur melakukan investigasi secara static forensic pada kasus network forensic.
b. Dapat menjadi referensi bagi masyarakat umum khususnya bagi mereka yang ingin belajar mengenai network forensic, dengan belajar menganalisis paket data yang berhasil diambil dari jaringan.
c. Memberikan gambaran cara mengamankan *access point* dari serangan man in the middle.

1.6 Sistematika Penulisan

Tujuan sistematika penulisan berisikan garis besar atau gambaran secara umum laporan penelitian ini sehingga mempermudah alur isi. Adapun beberapa garis besar isi laporan sebagai berikut :

BAB I Pendahuluan, bab ini menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan

BAB II Landasan Teori, bab ini menjelaskan tinjauan pustaka dari penelitian yang terkait dan membahas beberapa teori forensik digital, bukti digital, network forensic, live forensic, static forensic, man in the middle attack, arp poisoning, dan tools forensik seperti snort dan wireshark.

BAB III Metodologi Penelitian, bab ini menjelaskan gambaran tentang alur proses penelitian, alat dan bahan penelitian, instalasi dan konfigurasi, prosedur dan mekanisme metode analisis yang akan diterapkan pada skenario kasus penelitian.

BAB IV Hasil dan Pembahasan, bab ini menjelaskan mengenai implementasi skenario kasus, implementasi investigasi dan hasil analisis berbagai jejak digital yang dapat ditemukan menggunakan beberapa metode analisis. Bab ini juga menyampaikan rangkuman pembahasan secara teknis dari hasil analisis.

BAB V Kesimpulan dan Saran, bab ini menjelaskan mengenai kesimpulan dari hasil penelitian dan saran sebagai bahan evaluasi penelitian selanjutnya.

Daftar Pustaka, berisi referensi terkait dengan penelitian ini, baik melalui e-book, jurnal nasional dan internasional terakreditasi yang dapat menunjang proses penelitian.