BAB I
PENDAHULUAN

1.1 Latar Belakang

Semakin berkembangnya dunia teknologi informasi saat ini memudahkan pengguna dalam memberikan dan memperoleh informasi. Dunia teknologi informasi tidak terlepas dari kemajuan dunia jaringan komputer, yang memberikan banyak kemudahan dalam mengakses dan mendapatkan informasi. Pengguna dibuat terhipnotis dengan banyak fasilitas yang diberikan, sehingga tidak menyadari bahwa banyak kejahatan yang dapat terjadi dalam dunia jaringan komputer.

Cyber crime merupakan aktivitas teknologi yang melakukan kejahatan, seperti menghapus informasi, meretas jaringan, mengambil data pengguna jaringan, dan menyembunyikan informasi, dalam suatu jaringan komputer. Beberapa kejahatan pada suatu jaringan komputer, seperti Distributed Denial of Service (DDoS), Sniffing, Spoofing, dan Man In The Middle Attack, sangat berbahaya apabila terjadi pada sebuah jaringan komputer. Kejahatan-kejahatan yang terjadi dapat mengakibatkan pencurian data, rusaknya alat komunikasi, dan terputusnya konektifitas pada jaringan. Hal tersebut sangat merugikan pengguna jaringan, karena pelaku bisa saja mendapatkan informasi-informasi targetnya secara ilegal. Adapun informasi-informasi penting yang biasanya didapat oleh pelaku, seperti informasi kartu kredit, username dan password, baik email atau layanan perbankan, dan data-data penting lainnya.

Terdapat alat untuk melakukan serangan Man in the Middle (MITM) dengan melakukan sniffing, sehingga bagi client yang berada pada jaringan tersebut menjadi tidak secure. Ketika client berada pada jaringan yang tidak secure saat terjadinya pertukaran data antara client dan server memungkinkan datapada client tersebut menjadi tidak aman, Oleh karena itu pada sisi client bisa menambahkan pengamanan tambahan. Namun pada server yang di akses oleh client masih harus di tinjau kembali, dikarenakan sebagian server masih ada yang tidak menggunakan pengamanan yaitu berupa koneksi Hypertext Transfer Protocol (HTTP) dan Hypertext Transfer Protocol Secure (HTTPS) only. Dengan

menggunakan pengamanan ini sudah bisa menjamin bahwa ketika pertukaran data antara client dan server pada jaringan tersebut sudah aman dengan adanya serangan sniffing.

Man in the Middle (MitM), dimana posisi si attacker berada ditengah-tengah koneksi korban yang sedang melakukan koneksi, attacker ini mempunyai kemampuan untuk menyadap, mencegat, mengubah, bahkan mengontrol data/pesan di antara korban yang sedang melakukan konektivitas tersebut. Serangan MitM dilakukan dengan menyusup ke dalam sebuah session yang aktif diantara dua sistem dan kemudian mencegat atau menghadang data-data yang dikirimkan oleh kedua sistem tersebut untuk kemudian menginjeksi atau penyuntikan informasi yang bersifat menipu keduanya.

Berdasarkan dari permasalahan tersebut maka penelitian ini bertujuan untuk menganalisis dan menginvestigasi serangan MitM, peneliti akan memaparkan bagaimana investigasi serangan tersebut dilakukan, dengan mengungkap penyerang, waktu serangan, dan tipe serangan yang dilakukan.

1.2 Rumusan Masalah

Menurut pembahasan latar belakang diatas maka dapat di rumuskan bagaimana Menganilisis Serangan Man In The Middle Attack (ARP Spoofing) Menggunakan Metode Live Forensic antara lain yaitu :

Bagaimana mekanisme akuisisi investigasi network forensic dan live forensicuntuk mendapatkan bukti digital dan mengungkap aktivitas hacking ARP Spoofing (MITMA) ?

1.3 Batasan Masalah

Agar penelitian lebih terarah dan sesuai dengan rumusan masalah yang telah dipaparkan sebelumnya, maka peneliti membuat batasan masalah. Adapun batasan masalah yang ditetapkan adalah sebagai berikut :

a. Data trafik yang digunakan peneliti adalah real time traffic, karena pada kasusini trafik jaringan tidak tersimpan pada local database ataupun Network TAP.

b. Penelitian menggunakan skenario serangan ARP Poisoning (MITMA) pada area LAN yang digunakan sebagai acuan investigasi dan terbatas pada pembuktian serangan.
c. Analisis pada penelitian ini Terbatas pada skenario sederhana dengan tujuan mengenalkan tahapan forensik dan metode analisis yang bisa diterapkan pada live network forensic.
d. Sistem operasi yang digunakan pelaku adalah Kali Linux 2023 dan korban menggunakan Windows 7, dalam hal ini dijadikan sebagai instance victim atau target serangan.
e. Ekosistem environment penelitian ini terbatas pada penggunaan Virtual Machine dengan konektivitas antar virtual machine menggunakan adapterhost only adapter.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah sebelumnya maka tujuan yang ingin dicapaidari penelitian adalah :

a. Mengimplementasikan teknik live forensic dan network forensic untuk melakukan investigasi skenario serangan Man in the middle attack. Penelitian ini memperlihatkan secara rinci proses investigasi mulai dari akuisisi barang bukti.
b. Mencari dan menemukan artefak yang bisa dijadikan bukti pada network traffic.
c. Mengetahui karakteristik bukti digital pada artefak tiap-tiap teknik forensik.

1.5 Manfaat Penelitian

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

a. Memberikan gambaran bagaimana melakukan investigasi secara live forensic pada studi kasus network forensic.
b. Menjadi referensi implementasi teknik live forensic dan network forensic untuk investigasi skenario serangan Man in The Middle Attack.

c. Memberikan gambaran karakteristik bukti digital pada artefak hasil penerapan teknik-teknik digital forensic untuk kegiatan live dan network forensic.
d. Menjadi referensi akademisi dan melengkapi penelitian sebelumnya terkait proses live network forensic investigation dengan tujuan mengembangkan penelitian forensika digital di Indonesia.

1.6 Sistematika Penulisan

Tujuan sistematika penulisan berisikan garis besar atau gambaran secara umum laporan penelitian ini sehingga mempermudah pemahaman alur isi.

Adapun garis besar isi laporan skripsi sebagai berikut:

Bab I Pendahuluan, tahapan ini merupakan bab awal yang menjelaskan tentang latar belakang masalah penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

Bab II Landasan Teori, bab ini menjelaskan tinjauan pustaka dari penelitian terkait dan membahas beberapa teori terkait forensika digital, standar operasional prosedur, bukti digital, network forensic, live forensic, Man in The Middle Attack,ARP Poisoning dan tool yang digunakan dalam proses investigasi.

Bab III Metodologi Penelitian, bab ini berisikan gambaran umum tentang alur proses penelitian, prosedur dan mekanisme metode analisis yang diterapkan pada skenario kasus penelitian dan skenario kasus yang diterapkan pada penelitian.

Bab IV Pembahasan, pada tahapan ini membahas implementasi skenario kasus, implementasi investigasi dan hasil analisis berbagai artefak yang dapat ditemukan menggunakan beberapa metode analisis. Bab ini juga menyampaikan rangkuman pembahasan secara teknis dari hasil analisis.

Bab V Penutup, bab ini menjelaskan tahapan terakhir yang dilakukan peneliti dan memuat kesimpulan dari keseluruhan uraian dari bab-bab sebelumnya. Tahapan ini juga memaparkan kekurangan serta saran untuk pengembangan penelitian berikutnya.

Daftar Pustaka, berisi referensi terkait dengan penelitian ini, baik melalui ebook, publikasi jurnal, dan artikel situs yang dapat menunjang proses penelitian.