BAB I
PENDAHULUAN

A. Latar Belakang Masalah

Dalam era teknologi yang semakin berkembang dan semakin maju pada beberapa dekade terakhir, telah memunculkan pengaruh yang begitu penting terhadap aspek kehidupan, termasuk pada bidang keamanan siber. Dengan semakin banyaknya data yang tersimpan secara digital, ancaman juga semakin meningkat terhadap keamanan informasi tersebut. Salah satu metode serangan yang umum terjadi adalah serangan *brute force*, di mana nantinya penyerang akan mencoba bermacam-macam kombinasi kata sandi untuk mendapatkan akses login yang tidak sah ke dalam sistem. Serangan ini dapat mengakibatkan kerugian besar, baik dari segi finansial maupun reputasi dan juga bagi individu maupun organisasi seperti adanya kebocoran data, perubahan sistem tanpa persetujuan, serta gangguan terhadap operasional suatu sistem (Aji, 2022).

Sebagai bentuk persiapan dalam memahami dan menangani pasca serangan tersebut, forensik digital menjadi salah satu disiplin ilmu yang sangat pasti dalam bidang investigasi insiden keamanan teknologi. Forensik digital adalah sebuah metode pengumpulan data, analisis, dan penyajian hasil analisis secara lengkap dan detail pada laporan forensik digital tersebut, laporan dapat digunakan dalam pertanggungjawaban terhadap kejahatan yang diarahkan pada target serangan tersebut. Dengan menggunakan sebuah *tools* maupun Teknik, forensik digital dapat sangat berguna dalam membantu mengidentifikasi jejak digital terutama pada kasus kasus kejahatan, menganalisis pola aktivitas mencurigakan, dan memulihkan data yang mungkin telah diubah atau terhapus oleh penyerang (Hariyadi *et al.* 2023; Sudyana *et al.* 2023).

Penelitian ini bertujuan untuk melakukan simulasi forensik digital dalam investigasi serangan brute force pada lingkungan virtual. Proses penelitian dilakukan dengan membangun simulasi serangan brute force terhadap server yang dijalankan di dalam VirtualBox, dan kemudian melakukan analisis serangan tersebut menggunakan perangkat lunak forensik Autopsy. Autopsy

dipilih sebagai tools penelitian karena termasuk salah satu tools yang paling sering digunakan dalam tahapan awal belajar forensik digital, kemampuannya dalam menampilkan, mengekstraksi, dan menganalisis data log sistem pun tergolong cukup baik. Fokus penelitian ini tidak hanya pada proses simulasi serangan, tetapi terutama pada bagaimana penggunaan Autopsy dapat membantu dalam mengungkap serangan, menemukan jejak digital yang ditinggalkan, dan memberikan informasi penting untuk upaya mitigasi.

Urgensi dari penelitian ini terletak pada kebutuhan yang semakin meningkat untuk mengembangkan keterampilan serta memperdalam pemahaman dalam forensik digital, terutama dalam konteks penggunaan tools forensik autopsy sebagai tools analisis insiden serangan *brute force*. Serangan semacam ini dapat menyebabkan akses tidak sah ke sistem, sehingga diperlukan pendekatan yang tepat dalam investigasi forensik guna mengidentifikasi jejak digital yang ditinggalkan oleh penyerang. Penelitian ini menggunakan metode kualitatif dengan fokus utama pada investigasi forensik digital, di mana analisis data forensik dilakukan untuk memahami serta mendeteksi keberadaan serangan *Brute Force* secara digital.

Secara keseluruhan pada penelitian yang dibuat saat ini, memiliki upaya untuk mengimplementasikan ilmu forensik digital pada tools autopsy yang telah dipelajari, serta memberikan Gambaran yang jelas mengenai pentingnya forensik digital untuk menghadapi ancaman dan bahaya dari serangan siber, khususnya terhadap serangan brute force. Dengan adanya penelitian ini diharapkan tidak hanya bermanfaat bagi penelitian selanjutnya, tetapi juga memberikan sumbangsih penting dalam pengembangan ilmu forensik digital di Indonesia.

B. Perumusan Masalah

Berdasarkan latar belakang masalah yang sudah dijelaskan di atas, penelitian ini memiliki rumusan masalah yaitu:

1. Bagaimana analisis log server menggunakan autopsy untuk mendeteksi serangan brute force?

2. Apakah hasil analisis pada autopsy sudah memberikan informasi mengenai serangan *Brute Force* secara informatif?

C. Batasan Masalah

Berdasarkan penjelasan latar belakang di atas, Batasan masalah penelitian ini di jelaskan juga untuk memberikan Batasan pada ruang lingkup penelitian sehingga tidak keluar dari masalah yang diteliti, adapun berikut Batasan masalah yang ada:

1. Simulasi serangan dilakukan pada VirtualBox menggunakan sistem operasi kali linux.
2. Server menggunakan sistem operasi ubuntu di VirtualBox dan dipasangkan protokol keamanan SSH.
3. Akuisisi hanya tertuju pada file yang berhubungan dengan *brute force.*
4. Analisis dilakukan menggunakan tools autopsy.

D. Tujuan Penelitian

Tujuan dari dilakukannya penelitian ini adalah sebagai berikut:

1. Mengimplementasikan penggunaan autopsy dalam analisis forensik digital terhadap log server pasca serangan brute force.
2. Mengevaluasi efektivitas penggunaan autopsy sebagai alat bantu dalam investigasi forensik digital, khususnya dalam kasus serangan log server.

E. Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini adalah sebagai berikut:

1. Menyediakan panduan dasar dalam penggunaan autopsy untuk analisis log server pasca serangan.
2. Menjadi referensi bagi peneliti lain yang tertarik pada topik yang sama.
3. Menambah literatur tentang forensik digital dan analisis log server.