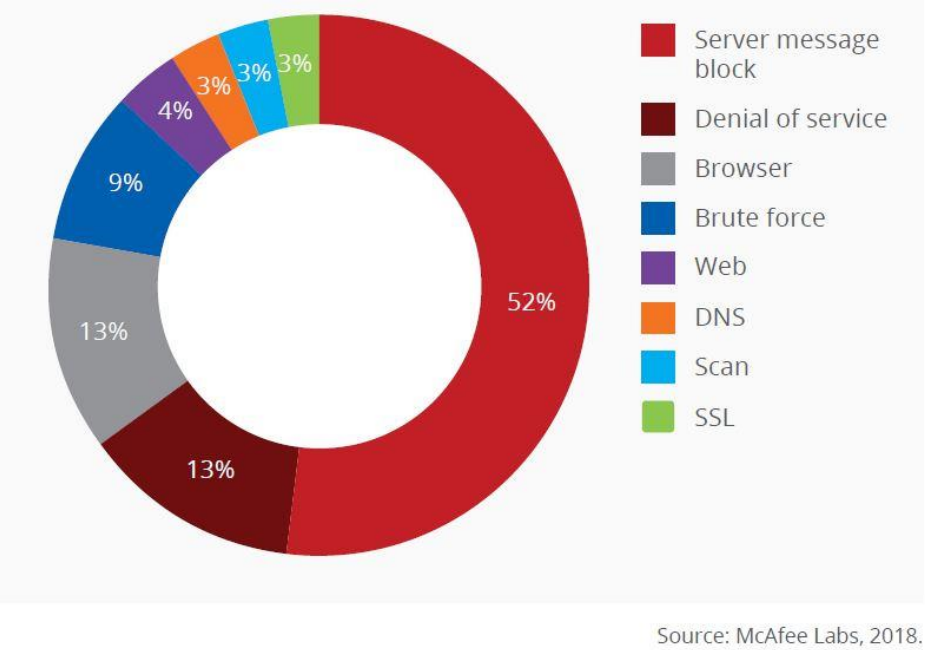
BAB 1
Pendahuluan

1.1 Latar belakang

Pesatnya perkembangan teknologi informasi dan komunikasi di era saat ini terutama dibidang komputer berbasis jaringan memberi kemudahan bagi para penggunanya dalam proses penyampaian maupun memperoleh informasi. Namun, dibalik semua itu masih terdapat oknum-oknum yang menyalahgunakan teknologi tersebut untuk mengambil data tanpa izin ataupun merusaknya dengan melakukan serangan pada jaringan komputer.

Serangan pada jaringan komputer atau yang biasa disebut network attack ini, dapat dilakukan oleh orang dalam maupun orang luar. Tujuannya pun berbeda-beda, beberapa diantaranya melakukan serangan hanya sekedar untuk mencoba tools yang ditemukan di internet namun ada beberapa juga melakukan serangan dengan tujuan saling menjatuhkan satu sama lain dalam konteks persaingan bisnis. Teknik serangan yang dilakukan pun bermacam-macam beberapa diantaranya seperti *DoS (Denial of Service)*, *Server Message Block, Browser, Brute Force*, *Web*, *DNS, Scan* dan *SSL*. ("McAfee Labs Threats Report." 2018).

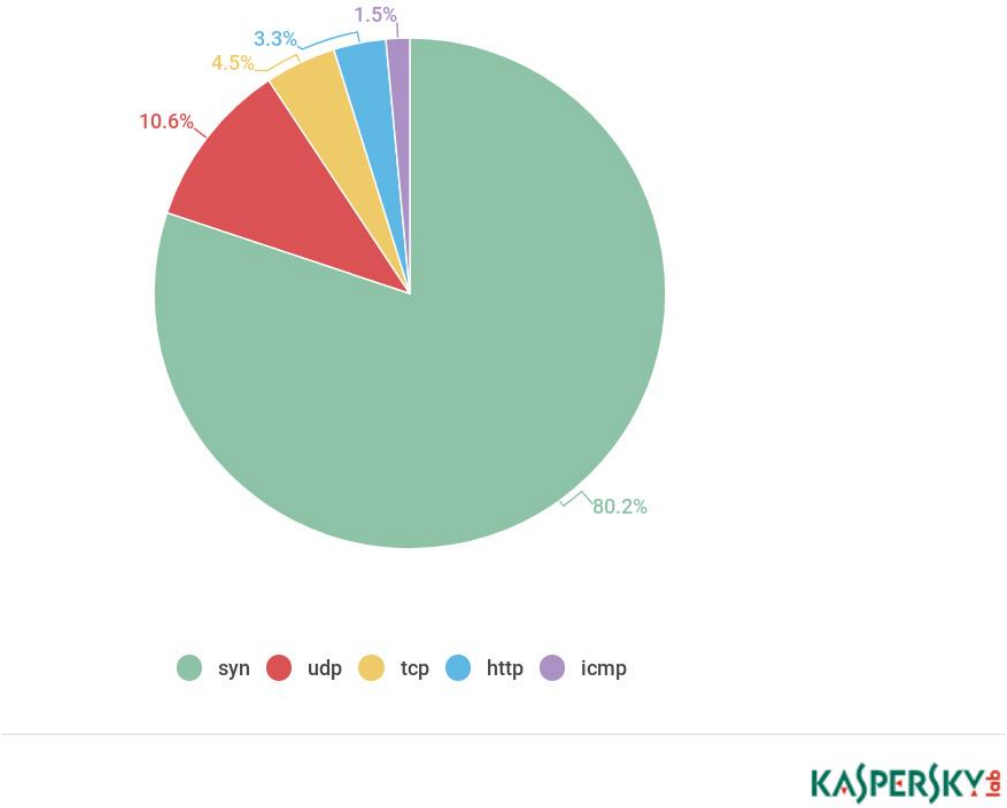


Gambar 1.1 Top Network Attack.

Sumber: Laboratory McAfee ("McAfee Labs Threats Report." 2018)

Pada gambar 1.1 diatas menunjukkan bahwa teknologi informasi dan komunikasi dibagian jaringan komputer masih rentan terhadap serangan. Serangan dilakukan dengan memanfaatkan celah yang ada pada perangkat jaringan yang digunakan. Dari serangan

yang dilakukan dapat mengakibatkan akses pada website menjadi lambat, terjadinya *flooding* data serta pencurian informasi dan data melalui jaringan internet. Salah satu akibat yang ditimbulkan dapat membuat perangkat jaringan yang digunakan menjadi down. Hal ini bisa terjadi karena adanya *flooding* data yang disebabkan serangan *DoS (Denial of Service)*.



Gambar 1.2 Top DoS Attack type.

Sumber: KasperskyLab

Berdasarkan gambar 1.2 diatas dalam serang *DoS (Denial of Service)* tipe syn atau yang biasa disebut *Syn Flood* merupakan yang paling sering dilakukan. Router merupakan perangkat jaringan yang sering diserang. Hal ini dikarenakan router merupakan perangkat yang mengatur lalu lintas pengiriman paket data ke perangkat lain melalui jaringan internet. Router merupakan sebuah system operasi berbasis linux yang dapat digunakan sebagai pengatur jaringan. Router memiliki hak akses penuh dalam mengatur pengendalian lalu lintas pada jaringan. Hal ini dikarenakan router memiliki banyak fungsi didalamnya sehingga menjadikan router sebagai target utama karena perannya yang sangat penting dalam jaringan.

Dalam perkembangan teknologi saat ini, terdapat studi ilmu yang mempelajari hal tersebut. Network forensic merupakan salah satu cabang ilmu yang mempelajari keamanan jaringan termasuk menyelidiki serangan yang terjadi pada sebuah jaringan berdasarkan bukti digital yang ditemukan di lokasi kejadian. Bukti digital yang ditemukan kemudian akan diidentifikasi untuk mengetahui serangan yang dilakukan oleh penyerang. Salah satu metode yang bisa dilakukan untuk melakukan identifikasi yaitu metode Live Forensics.

Live Forensics merupakan keadaan atau proses analisis forensik yang dilakukan disaat system yang dianalisis sementara dalam keadaan sedang berjalan atau beroperasi, (Artformatics, 2013). Metode ini dilakukan karena informasi yang dapat menjadi sebuah bukti digital memiliki kemungkinan bisa hilang apabila sistem yang di analisis berada dalam keadaan mati. Salah satu cara dalam melakukan analisis serangan pada router berdasarkan metode diatas, dapat dilakukan menggunakan aplikasi yang tersedia salah satunya adalah *Wireshark.*

Wireshark adalah sebuah aplikasi analisis paket jaringan. Aplikasi ini akan mencoba untuk menangkap paket jaringan dan mencoba menampilkan dalam bentuk data sedetail mungkin. Aplikasi ini dapat digunakan sebagai alat pengukur untuk memeriksa apa yang terjadi didalam suatu jaringan. Untuk keperluan analisis forensik jaringan terkait serangan terhadap router, maka dalam penelitian yang akan dilakukan ini akan dilakukan simulasi serangan pada router menggunakan aplikasi metasploit.

Serangan yang akan dilakukan pada simulasi tersebut yaitu DoS *(Denial of Service).* Adapun tipe serangan DoS yang akan diterapkan adalah Syn Flood, dimana serangan ini akan membanjiri paket-paket request yang dikirim ke router melalui protocol yang terdapat pada jaringan computer. Hal ini dapat menyebabkan Router akan menampung banyak paket request sehingga membuat jaringan down.

Penelitian terdahulu yang dilakukan oleh Mohammad Alim Zulkifli (2018) dengan menggunakan metode Live Forensic dalam menganalisis serangan DoS *(Denial of Service)* pada router mengungkapkan bahwa serangan DoS dengan tipe serangan DNS Flooding memiliki karakteristik yang mana dapat melakukan Ping atau mengirimkan pesan secara terus menerus dan mampu membuat jaringan Router menjadi down dikarenakan beban yang masuk tidak dapat ditampung atau berlebihan. Serta adanya aktivitas yang tidak wajar dalam proses komunikasi dara pada protocol DNS dengan IP tertentu terhadap Router dalam rentan waktu tertentu.

Mazdadi (2017) dalam penelitian menggunakan metode Live Forensic untuk menganalisis serangan pada router melalui API Service mengungkapkan bahwa ada cara

lain dalam menganalisis serangan yang terjadi pada router yaitu dengan mengembangkan media API *(Application Programming Interface) service* untuk menggali informasi dari perangkat router. Proses kerja aplikasi ini yaitu berkomunikasi secara remote dengan memanfaatkan port 8726 yang terdapat pada router. Dalam penelitian ini, serangan yang terjadi pada router adalah brute force dan mengambil alih hak akses penggunaan router tersebut.

Berdasarkan pemaparan dari hasil kedua peneliti di atas terkait serangan pada router, dapat diketahui bahwa masih ada tipe serangan pada router yang perlu diamati dan dianalisis karena kedua penelitian diatas terfokus pada serangan tertentu yang masuk dalam jaringan. Oleh sebab itu penulis berasumsi bahwa untuk mendeteksi tipe serangan pada router perlu dilakukan analisis serta akuisisi data terhadap router sehingga mendapatkan informasi yang dapat menjadi barang bukti digital dan dapat menentukan karakteristik serangan melalui metode Live Forensics.

1.2 Rumusan masalah

Berdasarkan latar belakang diatas, dirumuskan permasalahan penelitian ini yaitu :

1. Bagaimana melakukan forensik router untuk mendeteksi serangan flooding pada jaringan komputer?
2. Bagaimana hasil forensik router dimanfaatkan dalam menemukan barang bukti digital forensik?

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Penelitian ini terfokus pada perangkat router mikrotik RB750.
2. Metode yang digunakan dalam proses akuisisi data bersifat live forensic.
3. Penelitian ini terfokuskan pada ruang lingkup dimana router sebagai pengendali utama dalam jaringan namun tanpa adanya konfigurasi tambahan.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah

1. Melakukan forensik router untuk mendeteksi serangan flooding pada jaringan computer.
2. Mendapatkan barang bukti digital dari hasil forensic router

1.5 Manfaat Penelitan

Berdasarkan tujuan dari penelitian, diharapkan dapat membantu dalam mendeteksi serangan flooding pada jaringan serta hasil analisis bisa digunakan sebagai barang bukti digital untuk dimanfaatkan dalam proses investigasi forensik.

1.6 Metode Penelitian

Dalam menyelesaikan penelitian ini perlu disusun langkah-langkah penyelesaian penelitian secara sistematika yang disebut dengan metodologi penelitian. Metodologi yang digunakan pada penelitian ini adalah sebagai berikut:

1. Studi literatur

   Penelitian ini dilandaskan pada studi kepustakaan dengan mengumpulkan teori atau referensi yang relevan untuk menunjang tujuan penelitian ini melalui buku-buku, jurnal ilmiah, artikel, paper, makalah, dan akses beberapa situs website yang membahas tentang masalah yang akan menjadi titik fokus pada penelitian yang akan dilakukan.
2. Pemeriksaan (examination)

   Pada tahapan ini dilakukan pencarian data pada Router menggunakan aplikasi *Wireshark.*
3. Simulasi Serangan dan Pengujian

   Simulasi serangan dalam penelitian ini menggunakan *Metasploit* sebagai tools penyerang Router. Simulasi dan pengujian ini bertujuan untuk mengetahui keberhasilan dalam penarikan data serta informasi yang ada pada Router dan untuk menguji data yang telah berhasil ditarik menggunakan aplikasi *Wireshark.*
4. Analisis

   Tahapan analisis ini dilakukan untuk menemukan bukti digital yang terdapat pada hasil penarikan data serta informasi dari Router untuk digunakan dalam proses forensik.
5. Kesimpulan dan Saran

   Tahapan ini merupakan tahapan akhir untuk menyampaikan kesimpulan dari temuan-temuan yang diperoleh selama penelitian.

1.7 Sistematika Penulisan

Tahapan ini memberikan gambaran secara umum tentang penyusunan penelitian yang dilakukan, dalam sistematika penulisan terbagi dalam beberapa BAB yaitu :

Bab I Pendahuluan

Pendahuluan, merupakan pengantar terhadap permasalahan yang akan diteliti. Di dalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

Bab II Landasan Teori

Pada Bab ini menjelaskan teori-teori yang terkait untuk memecahkan masalah dalam penelitian yang dilakukan.

Bab III Metodologi Penelitian

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat keras dan perangkat lunak yang akan digunakan, proses dan mekanisme forensik pada router mikrotik serta implementasi terhadap penerapan metode Live Forensic untuk proses akuisisi data pada router.

Bab IV Hasil dan Pembahasan

Hasil dan Pembahasan, berisi tentang pembahasan penyelesaian masalah yang dianalisis dan cara pengujian yang dilakukan untuk menjawab permasalahan yang di usulkan.

Bab V Kesimpulan dan Saran

Kesimpulan dan Saran, memuat kesimpulan-kesimpulan dari hasil penelitian dan saran-saran yang perlu diperhatikan berdasar keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.