BAB I
PENDAHULUAN

1.1. Latar Belakang

Jaringan komputer berkembang dengan sangat pesat, baik di instansi-instansi komersil, dunia akademik, bahkan rumah-rumah penduduk yang membutuhkan akses internet. Internet merupakan sebuah singkatan dari *Interconnection Networking*, atau yang berarti jaringan yang terhubung secara luas. Internet merupakan keterkaitan jaringan komputer melalui standard yang disebut *global Transmission Control Protocol atau Internet Protocol TCP/IP* yang terdapat sistem pertukaran paket komunikasi yang berasal melalui data. Dengan jaringan inilah semua orang bisa berkomunikasi dengan mudah dan dalam waktu yang singkat dari seluruh dunia tanpa batas.

Internet telah diakses oleh sebagian besar masyarakat yang ada di dunia dan memanfaatkannya untuk kegiatan masing-masing. Namun pemanfaatan jaringan internet tersebut tidak hanya pada kegiatan positif saja namun banyak juga yang memanfaatkannya pada perilaku tindak kejahatan atau sering disebut dengan kejahatan dunia cyber *(cybercrime)*. Pelaku tindakan *cybercrime* ini biasa disebut dengan *hacker* atau *cracker*, dengan alasan tertentu mereka melakukan penyusupan yang dapat merugikan para pemilik *server* dan jaringan komputer. Mereka menggunakan berbagai macam serangan jaringan komputer dengan *tools* yang dibuat secara mandiri ataupun yang telah ada di pasar.

Tindakan *cybercrime* yang memanfaatkan jaringan internet ini merupakan salah satu isu yang sangat penting dalam dunia teknologi dimana isu tersebut dianggap merugikan bagi para pengguna. Menurut berita yang dikeluarkan oleh

Kementerian Komunikasi dan Informatika Republik Indonesia (www.kominfo.go.id) menjelaskan bahwa angka serangan jaringan internet di Indonesia mengalami peningkatan dari tahun 2019 yang masih 1,25 juta kali menjadi 1,5 juta kali pada tahun 2020. Hal tersebut membuktikan bahwa nilai kegentingan dari tindakan *cybercrime* yang memanfaatkan jaringan internet ini sangat serius untuk dilakukan proses pengkajian yang mendalam. Berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor : 16 /Per/M. Kominfo/ 10 /2010 menjelaskan bahwa pengamanan jaringan telekomunikasi berbasis protokol internet bertujuan untuk menjamin keamanan dan menciptakan lingkungan serta pemanfaatan jaringan telekomunikasi berbasis protokol internet yang aman dari berbagai macam potensi ancaman dan gangguan (Pemerintah Indonesia, 2010).

Ketersediaan layanan *(availability)* merupakan salah satu aspek keamanan yang diperlukan dalam membuat sistem keamanan jaringan komputer atau internet. Keamanan jaringan merupakan faktor penting untuk menjamin data dari pencurian atau pengurus data. Dengan meningkatnya pengetahuan tentang *hacking* dan *cracking* (tindakan *cybercrime*) serta di dukung banyak *tool* yang bisa digunakan secara mudah untuk melakukan serangan atau penyusupan. Ketika serangan terjadi, maka perlu dilakukan investigasi. Investigasi jaringan bisa dilakukan dengan menggunakan suatu cabang ilmu digital forensik yaitu forensik jaringan (Dewi et al., 2017).

Mekanisme forensik jaringan dapat digunakan untuk konstruksi sebuah kejadian dengan memanfaatkan sebuah sistem yang menyimpan dan melihat kembali segala aktivitas lalu lintas data sehingga administrator dapat melakukan

investigasi melalui peristiwa ataupun kejadian yang tersimpan pada *log system*. Terdapat beberapa proses pada forensik jaringan seperti, monitoring, koleksi data, analisa data serta *source TRACEBACK* untuk mengetahui apa yang sebenarnya terjadi, untuk mengetahui detail koneksi, serta untuk mengetahui alamat asal dan tujuan, yang mungkin dapat mencegah dari adanya serangan terhadap sistem keamanan jaringan (Ridho et al., 2016).

Implementasi forensik jaringan pada dasarnya menggunakan standar kerangka kerja diantaranya *National Institute of Justice (NIJ), Digital Forensics Research Workshop (DFRWS), National Institute of Standards and Technology* (NIST) dan lainnya (Yudhana et al., 2019). Penelitian dilakukan menggunakan *framework National Institute of Standards and Technology* (NIST). *National Institute of Standards and Technology (NIST)* merupakan metode yang digunakan untuk melakukan forensik analisis. Metode ini sudah banyak digunakan sebagai acuan analisis forensik (Mustafa et al., 2018).

Salah satu perangkat yang paling penting pada suatu jaringan dengan cakupan yang luas adalah *router*. *Router* dapat menyimpan identitas lalu lintas data berdasarkan tabel-tabel yang tersedia melalui *Router* (Firmansyah et al., 2019). Perpindahan sumber informasi antar jaringan pada router menjadi perhatian utama untuk memonitor lalu lintas data yang menjadi sasaran para *intruder* untuk masuk ke dalam sistem utama untuk merusak, menghapus, bahkan mencuri data penting yang tersimpan pada sistem utama, yang dapat merugikan baik bagi perorangan, perusahaan, maupun instansi terkait.

Pentingnya peran *router* dalam suatu jaringan menjadikan perangkat keras tersebut wajib ada dalam suatu topologi jaringan tetapi topologi jaringan

memiliki kebutuhan dan *Access Control Lists* (ACLs) berbeda. ACLs yang banyak dan terpusat dapat menyebabkan *traffic* padat. Pemisahan ACLs berdampak pada penggunaan *router* yang lebih banyak dan menyebabkan biaya berlebih untuk pembelian *router*, pemakaian listrik dan penggunaan ruang penyimpanan. Permasalahan tersebut dapat diatasi dengan virtualisasi *router* sehingga dapat menghemat biaya pembuatan jaringan komputer, pemakaian energi listrik dan penggunaan tempat dibandingkan router non-virtualisasi (Galang DKK, 2017).

Router yang merupakan perangkat penting dalam sebuah jaringan, banyak bukti-bukti yang dapat diambil dari aktivitas jaringan, selain itu router juga secara cerdas mampu mengetahui alur tujuan informasi *(quota)* yang dilaluinya. Bukti-bukti yang dapat diambil dari router antara lain konfigurasi *firewall, mac address, daftar IP address client, logging admin* dan lain-lain. Untuk mendapatkan bukti-bukti dari tindak *cybercrime* tersebut perlu dilakukannya proses investigasi jaringan forensik dengan tujuan untuk mengetahui pelaku serta dari bukti yang telah didapatkan dapat dijadikan sebagai bahan pembuktian di dalam proses persidangan.

Berdasarkan latar belakang yang telah dipaparkan maka ranah dalam penelitian ini adalah melakukan perancangan *virtual router* dan menguji penyerangan terhadap *virtual router* tersebut, kemudian melakukan analisa investigasi forensik untuk mendapatkan aktifitas lalu lintas yang mencurigakan setelah serangan yang dilakukan.

1.2. Rumusan Masalah

Dari paparan latar belakang yang sudah ada, maka dapat saya ambil rumusan masalah sebagai berikut:

1. Bagaimana proses perancangan *virtual router* yang efektif dan efisien!
2. Bagaimana melakukan analisis serangan DOS (*Denial of Service*) pada Virtual Router?
3. Bagaimana mendapatkan bukti adanya penyerangan pada Virtual Router?
4. Bagaimana karakteristik bukti digital pada Virtual Router?

1.3. Batasan Masalah

Dalam rangka mengarahkan penelitian berdasarkan rumusan masalah yang telah dipaparkan maka perlu adanya batasan masalah sebagai berikut:

1. Penelitian menggunakan perangkat router Mikrotik *RB 951Ui-2HND* dengan *routerOS versi6*.
2. Alat analisis serangan dilakukan dengan pemanfaatan aplikasi Wireshark dan Microsoft Network Monitor.
3. Proses mendapatkan bukti penyerangan menggunakan kerangka kerja NIST.
4. Hasil temuan bukti meliputi, jenis serangan yang masuk, protokol, *Sender* IP, *Sender* Mac *Address*, dan Target IP.

1.4. Maksud dan Tujuan Penelitian

Tujuan yang hendak dicapai pada penelitian ini yaitu:

1. Merancang jaringan *virtual router forensic* dengan pemanfaatan *static address*.

2. Meninjau aktifitas jaringan pada setiap *protocol* lalu lintas dengan menyadari berbagai kemungkinan sumber data dapat menjadi bukti.
3. Menerapkan mekanisme jaringan forensik menggunakan *framework National Institute of Standards and Technology* (NIST) dengan tujuan melakukan forensik menggunakan proses yang konsisten.
4. Karakteristik bukti digital pada Virtual Router dapat dijadikan sebagai laporan atau hasil temuan penelitian terkait analisis *forensic*.

1.5. Manfaat Penelitian

Berdasarkan latar belakang, rumusan masalah batasan masalah, dan tujuan dari penelitian yang telah disampaikan pada bagian sebelumnya, adapun manfaat yang ingin dicapai dalam penelitian ini yaitu:

1. Mengetahui bagaimana *setting*, kinerja dan manfaat *virtual router* dalam penerapan *static address*.
2. Mengetahui proses terjadinya serangan pada jaringan *virtual router*.
3. Mengetahui sumber data aktifitas pada *protocol* yang dapat dijadikan sebagai bukti forensik.
4. Mengetahui karakteristik bukti digital pada Virtual Router.

1.6. Metode Penelitian

1.6.1 Metode Pengumpulan Data

1. Studi pustaka

   Tahap ini dilakukan dengan membaca buku, penelitian terdahulu maupun pencarian data melalui internet, artikel, dan informasi dari sumber

terpercaya dan valid untuk mendapatkan pedoman atau bahan tambahan yang berkaitan dengan judul penelitian.

2. Observasi

   Penelitian ini terjun langsung dalam melakukan proses perancangan virtual router sesuai dengan dasar yang telah didapatkan pada proses studi pustaka.

3. Dokumentasi

   Tahap ini dilakukan dengan membuat laporan hasil penelitian dalam bentuk skripsi.

1.6.2 Metode Analisis

Metode Analisis yang digunakan dalam penelitian ini yaitu, metode pengembangan jaringan dengan menggunakan *framework National Institute of Standards and Technology* (NIST) yang merupakan metode yang digunakan pada digital forensik.

1.7. Sistematika Penulisan

Tahapan ini adalah tahapan yang memberikan gambaran secara umum terkait dengan sistematika penulisan, dengan tujuan memberikan penjelasan secara ringkas terhadap kerangka dalam penulisan.

BAB I: PENDAHULUAN

Pendahuluan, merupakan pengantar terhadap permasalahan yang dibahas. Di dalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latarbelakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, serta sistematika penulisan.

BAB II: LANDASAN TEORI

Pada Bab ini menjelaskan teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang dibahas pada bagian ini merupakan teori yang berhubungan dengan network dan routing.

BAB III: ANALISIS DAN PERANCANGAN SISTEM

Bab ini membahas tentang kerangka konsep penelitian dan gambaran umum langkah penyelesaian yang dilakukan. Bagan proses investigasi dibuat berdasarkan referensi yang didapat, untuk menyelesaikan penelitian dilakukan pembuatan rancangan simulasi untuk membuktikan bagan proses investigasi yang dikembangkan.

BAB IV: IMPLEMENTASI DAN PEMBAHASAN

Bab ini simulasi yang sudah dirancang pada sebelumnya di implementasi pada sistem yang sebenarnya. Hasil yang didapat pada tahap simulasi dianalisa kembali dan dilakukan pembahasan terkait dengan penelitian yang dibuat.

BAB V: PENUTUP

Tahapan ini adalah tahapan terakhir yang dilakukan dalam penelitian ini dan memuat tentang kesimpulan dari keseluruhan uraian dari Bab-bab sebelumnya, serta memberikan saran terkait dengan kekurangan yang diperoleh dalam penelitian untuk pengembangan ilmu pengetahuan di kemudian hari.