ANALISIS SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDoS) PADA ROUTER MENGGUNAKAN METODE *LIVE FORENSIC*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

MUHAMMAD FAJAR PUTRA

09011181520009

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN

ANALISIS SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDoS) PADA ROUTER MENGGUNAKAN METODE *LIVE FORENSIC*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

MUHAMMAD FAJAR PUTRA
09011181520009

Indralaya, Agustus 2020

Pembimbing Tugas Akhir 1	Pembimbing Tugas Akhir 2
Deris Stiawan, P.hD	**Ahmad Heryanto,S.Kom.,M.T**
NIP. 197806172006041002	**NIP. 198701222015041002**

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :
Hari : Kamis
Tanggal : 30 Juli 2020

Tim Penguji :

1. Ketua : Rahmat Fadli Isnanto, M.Sc

2. Pembimbing I : Dr. Deris Stiawan, M.T.

3. Pembimbing II : Ahmad Heryanto, M.T.

4. Penguji I : Ahmad Zarkasi, M.T

5. Penguji II : Aditya Putra Perdana P, M.T

Mengetahui
Ketua Jurusan Sistem Komputer

Dr.Ir.H.Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Muhammad Fajar Putra

NIM : 09011181520009

Judul : Analisis Serangan Distributed Denial of Service (DDoS) Pada Router Menggunakan Metode Live Forensic

Hasil pengecekan *Software iThenticate/Turnitin* : 19%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, 25 Agustus 2020

Muhammad Fajar Putra

09011181520009

KATA PENGANTAR

Bismillahirrahmanirrahim. Assalamu'alaikum Warahmatullahi Wabarakatuh. Puji dan syukur penulis panjatkan kehadirat Allah SWT, karena berkat rahmat-Nya dan karunia sehingga penulis sampai pada saat ini dapat menyelesaikan penyusunan proposal tugas akhir ini dengan judul "Analisis Serangan Distributed Denial of Service (DDoS) Pada Router Menggunakan Metode Live Forensic".

Pada penyusunan proposal tugas akhir ini, tidak terlepas dari bantuan, bimbingan, ajaran serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan terima kasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga penulisan proposal tugas akhir ini dapat berjalan dengan lancar.
2. Orang tua, Adik dan Kakakku yang selalu memberikan semangat dan do'a.
3. Bapak Jaidan Jauhari, S.Pd. M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
4. Dr.Ir.H.Sukemi, M.T..selaku Ketua Jurusan Sistem Kompuer Fakutas Ilmu Komputer Universitas Sriwijaya
5. Bapak Deris Stiawan, M.T.,Ph.D. dan Ahmad Heryanto,S.Kom.,M.T selaku Pembimbing Tugas Akhir Penulis.
6. Ibu Prof. Dr. Ir. Siti Nurmaini, M.T. selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer.
7. Jurusan Sistem Komputer Reguler kelas A angkatan 2015 yang tidak dapat saya sebutkan satu persatu.

Penulis juga berterima kasih kepada semua pihak yang terlibat, baik secara langsung ataupun tidak langsung dalam penyelesaian proposal tugas akhir ini.

Tentunya dalam pembuatan proposal tugas akhir ini, masih terdapat beberapa kekurangan dan kesalahan yang mungkin terjadi. Oleh karena itu sebagai bahan perbaikan kedepan penulis tentunya mengharapkan koreksi, saran, serta Inputan terhadap isi dari proposal tugas akhir ini.

Akhir kata, semoga dengan pembuatan proposal tugas akhir ini, akan menjadi tambahan ilmu dan pengembangan wawasan kita terhadap pengolahan citra digital dan dapat menjadi bahan referensi terhadap mahasiswa yang membutuhkan.

Indralaya, 25 Agustus 2020

Penulis

Muhammad Fajar Putra

09011181520009

HALAMAN PERSEMBAHAN

Dengan rasa syukur Alhamdu lillahi rabbil 'alamin, sebuah karya yang dapat kupersembahkan kepada :

- Kedua orang tuaku yang telah mengajari, mendidik, membesarkanku, memberi kasih sayang, mendukung, memberi motivasi, dan semangat.
- Saudara-saudara kandungku yang kusayangi.
- Sahabat-sahabat perjuangan.
- Teman-teman perjuangan di Fakultas Ilmu Komputer Jurusan Sistem Komputer 2015

إِنَّ اللَّهَ لَا يُغَيِّرُ مَا بِقَوْمٍ حَتَّىٰ يُغَيِّرُوا مَا بِأَنْفُسِهِمْ

"Sesungguhnya Allah tidak akan mengubah keadaan suatu kaum sebelum mereka mengubah keadaan diri mereka sendiri." (QS.ar-Ra'd:11)

"*Tubuh seseorang tidak akan lemah jika ia memiliki niat yang kuat."* (Imam Ja'far As-Shodiq)

"*Sesungguhnya keutamaan seorang yang berilmu dibanding ahli ibadah, seperti keutamaan bulan di malam purnama dibanding seluruh bintang- bintang."* (HR. Abu Dawud dan Ibnu Majah)

ANALYSIS OF DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS ON ROUTER USING LIVE FORENSIC METHOD

Muhammad Fajar Putra (09011181520009)

Computer Engineering Department, Computer Science Faculty,
Sriwijaya University
Email : fajarmuhammad29@gmail.com

Abstract

Distributed Denial of Service (DDoS) attacks on a network continue to grow in the society. Especially the DDoS DNS Flooding attack carried out by irresponsible people and aimed at someone else's Router network to paralyze the Router network. Therefore network forensics is needed to obtain forensic evidence so that the perpetrators of crimes can be prosecuted according to the applicable law. The purpose of this research is to identify DNS Flooding attack patterns, perform data acquisition and analizing the attacks on Router networks, and search for attack traffic information on Router networks that can be used as digital evidence through the Live Forensics method. The dataset used in this study is a dataset created by utilizing Hping3's tools to create DNS Flooding attack data traffic with three dataset creation scenarios, then the dataset will be extracted to get the attack pattern . The process of analyzing and data acquisition using the Wireshark tool aims to process data or information retrieval regarding the activity log and the attacker's IP address. In this study, it was successful in retrieving DDoS attack information data related to attack patterns, the state of the victim's computer before and after being attacked, activity log data and the attacker's IP address.

Keywords: DDoS (Distibuted Denial of Service) Attacks , DNS Flooding, Router, Live Forensics

ANALISIS SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDoS) PADA ROUTER MENGGUNAKAN METODE *LIVE FORENSIC*

Muhammad Fajar Putra (09011181520009)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : fajarmuhammad29@gmail.com

Abstrak

Serangan *Distributed Denial of Service* (DDoS) pada suatu jaringan terus berkembang dilingkungan masyarakat. Khususnya serangan DDoS *DNS Flooding* yang dilakukan oleh orang yang tidak bertanggung jawab dan ditujukkan pada jaringan Router orang lain untuk melumpuhkan jaringan Routernya. Maka dari itu Forensik jaringan sangat dibutuhkan untuk mendapatkan bukti-bukti forensik sehingga pelaku kejahatan dapat dituntut sesuai hukum yang berlaku . Tujuan dari penelitian ini adalah untuk mengenali pola serangan *DNS Flooding*, melakukan akuisisi data dan menganalisa serangan pada jaringan Router, serta mencari informasi lalu-lintas serangan pada jaringan Router yang bisa digunakan sebagai bukti digital melalui metode *Live Forensics*. *Dataset* yang digunakan dalam penelitian merupakan dataset yang dibuat dengan memanfaatkan *tools Hping3* untuk membuat lalu lintas data serangan *DNS Flooding* dengan tiga skenario pembuatan *dataset*, kemudian *dataset* akan diekstraksi untuk mendapatkan pola serangan. Proses analisa dan akuisisi data menggunakan *tools Wireshark* bertujuan untuk keperluan proses penarikan data atau informasi mengenai *Log Activity* dan *IP Address* penyerang. Pada Penelitian ini berhasil menarik data informasi serangan DDoS terkait Pola serangan, keadaan komputer korban saat sebelum dan sesudah diserang,data log aktivitas dan alamat IP penyerang.

Kata Kunci: Serangan DDoS (Distibuted Denial of Service), DNS Flooding, Router, Live Forensics

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1. Latar Belakang

Menurut [1] mengatakan bahwa Internet merupakan suatu hubungan antara berbagai jenis komputer dan juga dengan jaringan di dunia yang memiliki sistem operasi dan juga aplikasi yang berbeda maupun, dimana hubungan tersebut memanfaatkan kemajuan perangkat kompunikasi seperti telepon dan satelit yang menggunakan protokol standar dalam melakukan hubungan komunikasi, yaitu protokol TCP/IP (Transmission Control/Internet Protocol). Namun dibalik kecangihan teknologi jaringan komputer, telah banyak juga memunculkan permasalahan Forensik Jaringan.

Penyebab utama masalah forensik jaringan yaitu penggunaan teknologi yang disalahgunakan oleh orang-orang yang tidak bertanggung jawab dengan tujuan memanfaatkan fasilitas jaringan orang lain untuk kepentingan pribadi maupun kelompok. Diantara banyaknya serangan yang sering terjadi di Internet adalah serangan DDoS (Distributed Denial of Service). DDoS adalah jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan. Umumnya serangan ini dilakukan menggunakan beberapa komputer host penyerang sampai dengan komputer target tidak bisa diakses.

RouterOS adalah sistem operasi yang Linux Based berfungsi layaknya jaringan Router yang dirancang untuk memudahkan *user*. Untuk pengaturan dan cara administrasi dapat dilakukan pada aplikasi WinBox. Proses instalasi juga dapat dijalankan pada komputer. Komputer yang akan dijadikan Router server untuk keperluan standar sebagai Gateway tidak memerlukan resource yang cukup besar. Sedangkan penggunaan yang lebih berat disarankan menggunakan komputer dengan spesifikasi yang mumpuni.

Pengendalian penuh terhadap Router yang berarti pengendalian penuh terhadap jaringan ada pada hak akses administrator pada perangkat Router. Sedangkan fungsi utama dari sistem operasi Router meliputi Firewall dan NAT, Bandwidth Limiter, Routing, Hospot, Akses Point to Point Tunneling Protocol,

DNS Server, Hotspot dan lain sebagainya. Hal ini dapat menjadi alasan mengapa hacker/penyerang menjadikan Router sebagai target serangan karena Router merupakan salah satu perangkat penting pada sebuah jaringan.

Serangan pada Router dilakukan dalam bentuk penyusupan dengan menggunakan berbagai macam jenis serangan jaringan komputer melalui *Tools* yang dibuat sendiri maupun Tools yang beredar di internet. Dari uraian tersebut dapat dipahami bahwa pentingnya melakukan analisis serangan pada Router karena keamanan data menjadi hal penting dalam komunikasi data pada suatu sistem jaringan komputer.

Network Forensic adalah suatu proses, menangkap,mendeteksi, mencatat dan menganalisa aktivitas pada suatu jaringan untuk menemukan bukti digital dari suatu serangan yang dilakukan melalui jaringan komputer sehingga pelaku kejahatan dapat dituntut sesuai hukum yang ada [2]. Bukti digital dapat diidentifikasi dari pola serangan yang dikenali melalui metode Live Forensics.

Dari beberapa rujukan diatas, penulis bermaksud untuk melakukan analisis serangan DDoS menggunakan metode Live Forensic pada jaringan Router untuk dapat mengenali pola serangan *DNS Flooding* dan membedakannya dengan pola data normal kemudian menemukan bukti-bukti digital yang diperlukan untuk keperluan forensik .

1.2 TUJUAN

Penelitian ini bertujuan untuk:

1. Mengenali pola serangan DNS Flooding
2. Melakukan akuisisi data dan analisis serangan pada jaringan Router.
3. Mencari informasi lalu-lintas serangan pada jaringan Router yang bisa digunakan sebagai bukti digital melalui metode Live Forensics.

1.3 MANFAAT

Adapun manfaat yang dapat diambil dari penelitian ini adalah:

1. Memberikan kemudahan dalam mengenali serangan *DNS Flood.*
2. Dapat membedakan paket serangan *DNS Flood* dengan paket normal.

3. Sebagai pendalaman materi dalam bidang Network Forensics terutama pada sub bidang Router melalui metode Live Forensics.
4. Memberikan panduan dalam proses investigasi Forensik pada jaringan Router.

1.4 Rumusan Masalah

1. Bagaimana melakukan analisis serangan DDoS (Distributed Denial of Service) pada Router.
2. Bagaimana melakukan akuisisi data pada Router menggunakan metode Live Forensics.
3. Bagaimana karakteristik bukti digital yang didapatkan.

1.5 Batasan Masalah

1. Kegiatan akuisisi data penelitian ini bersifat Live Forensics (dilakukan pada saat sistem operasi jaringan sedang beroperasi)
2. Data akan dikelompokan dalam 3 bagian, yaitu paket data normal, paket serangan, dan paket gabungan.
3. Tidak membahas bagaimana cara pencegahan serangan tersebut
4. Skenario untuk analisis serangan pada Router menggunakan aplikasi Wireshark.
5. Tidak diujikan pada lalu lintas jaringan yang terenskripsi.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam tugas akhir ini akan melewati beberapa tahapan sebagai berikut :

1. Mengumpulkan Data

   Proses mengumpulkan data yang dilakukan adalah studi pustaka atau literature. Studi *literature* dilakukan dengan cara mempelajari dan mengumpulkan informasi mengenai penelitian yang akan diujikan. *Literature* didapatkan dari jurnal, buku dan lain sebagainya agar dapat membantu metodologi dan pendekatan yang diterapkan pada penelitian**.**

2. Pengolahan Data

Pada tahapan ini membahas mengenai proses yang sudah dilakukan dalam penelitian kedalam bentuk tulisan. Pengolahan data bertujuan untuk melihat apakah hasil penelitian sudah sesuai serta mengevaluasi jalannya sistem berdasarkan batasan masalah dari penelitian

3. Pengujian

   Tahap ini adalah tahap pengujian metodologi penelitian dan penelitian sebelumnya sehingga didapatkan data hasil uji yang sesuai dan tepat.

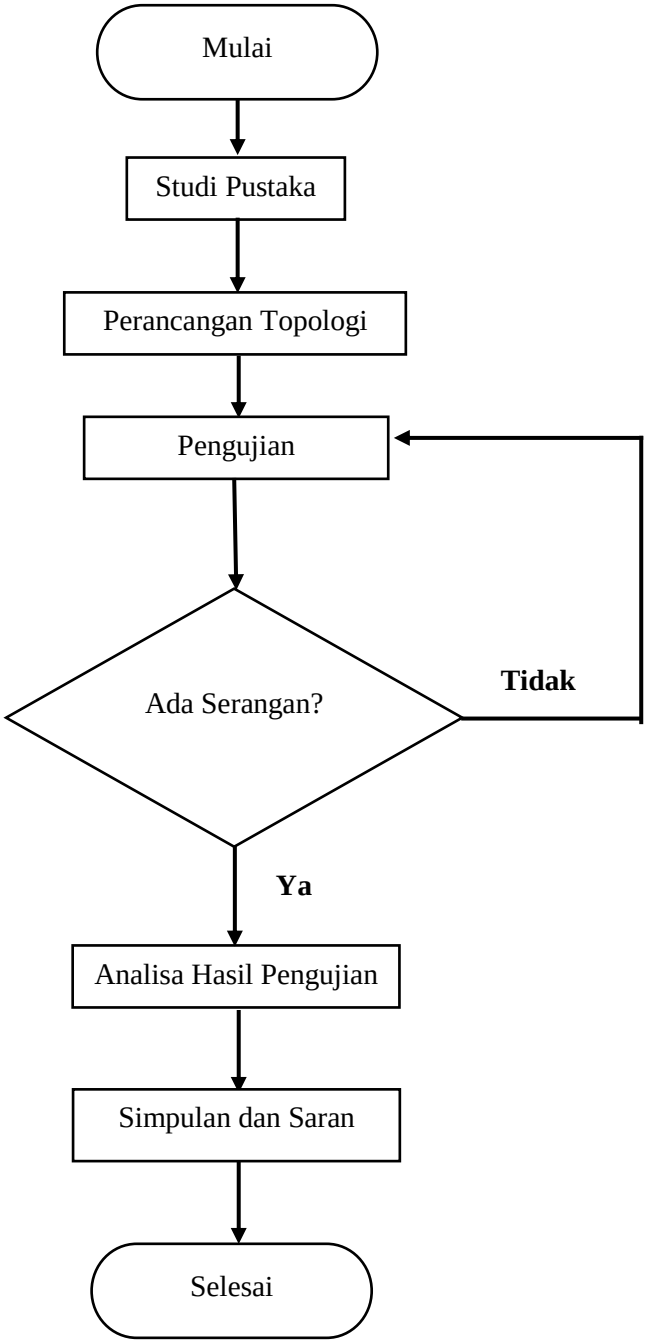
4. Analisa

   Tahapan ini menganalisa hasil yang telah didapatkan pada tahapan sebelumnya. Tujuan dari tahapan ini yaitu mendapatkan data-data yang bersifat objektif dari analisa hasil pengolahan data agar dapat dilakukannya pengembangan pada penelitian sebelumnya.

5. Kesimpulan dan Saran

   Tahapan terakhir yang akan merumuskan kesimpulan pada penelitian yang sudah dilakukan dan saran yang dapat menjadi landasan pada penelitian selanjutnya

Pada Gambar 1.1 berikut ini metodologi penelitian dalam bentuk diagram air yang merepresentasikan proses pelaksanaan penelitian :



Gambar 1.1 Diagram Alir Metodologi Penelitian

1.7 Sistematika Penulisan

Penyusunan laporan tugas akhir ini, penulis membuat sistematika penulisan agar mempermudah mengetahui isi dari setiap bab yang dibuat pada laporan tugas akhir ini. Adapun seitematika penulisan laporan tugas akhir sebagai berikut :

BAB I. PENDAHULUAN

Bab yang menjelaskan tentang latar belakang masalah, tujuan dan manfaat, masalah yang dirumuskan, batasan masalah, metodologi penelitian, dan juga sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Bab 2 terdiri dari dasar teori dari penelitian terkait dengan *Dns Flooding Attack*, *Live Forensic*, dan yang berkaitan langsung dengan penelitian

BAB III. METODOLOGI

Bab 3 berisi penjelasan langkah-langkah (metodologi) penelitian dan perancangan sistem pada tugas akhir ini.

BAB IV. HASIL DAN ANALISIS

Bab ini menjelaskan hasil dari penelitian yang telah dilakukan, hasil tersebut dapat dilakukan analisis dari data yang telah didapatkan.

BAB V. KESIMPULAN DAN SARAN

Bab ini akan menjelaskan tentang kesimpulan yang didapat dari data penelitian yang sudah dilakukan. Kemudian saran yang diharapkan bias membuat penelitian ini dikembangkan lebih baik.

DAFTAR PUSTAKA

[1] B. Arps, “Special report JAVANESE ON THE INTERNET,” vol. 38, no. December 2002, pp. 1–10, 2003.

[2] S. Mukkamala, G. Janoski, and A. Sung, “Intrusion detection using neural networks and support vector machines,” *Proc. Int. Jt. Conf. Neural Networks*, vol. 2, pp. 1702–1707, 2002

.

[3] D. R. N. TAHIR and E. By, “International Journal of Computer Science and Security (Ijcss),” pp. 60–65, 2008.

[4] J. Gao, Y. Xiao, S. Rao, and F. Shalini, “Security tests and attack experimentations of ProtoGENI,” *Int. J. Secur. Networks*, vol. 10, no. 3, pp. 151–169, 2015.

[5] C. Liu and P. Albitz, DNS and BIND (5th Edition). O’Reilly Media, Inc., 2006.

[6] K. Nguyen, D. Tran, W. Ma, and D. Sharma, “An approach to detect network attacks applied for network forensics,” *2014 11th Int. Conf. Fuzzy Syst. Knowl. Discov. FSKD 2014*, pp. 655–660, 2014.

[7] A. M. Saliu, “Internet Authentication and Billing (Hotspot) System Using MikroTik Router Operating System,” *Int. J. Wirel. Commun. Mob. Comput.*, vol. 1, no. 1, p. 51, 2013.

[8] A. R. Arasteh, M. Debbabi, A. Sakha, and M. Saleh, “Analyzing multiple logs for forensic evidence,” *Digit. Investig.*, vol. 4, no. SUPPL., pp. 82–91, 2007.

[9] P. Parningotan, “Analisis Network Security Snort Menggunakan Metode Intrusion Detection System (Ids) Untuk Optimasi Keamanan Jaringan Komputer,” *JURSIMA J.*, vol. 6, no. 1, 2018.

[10] S. Niccolini, R. G. Garroppo, S. Giordano, G. Risi, and S. Ventura, “SIP intrusion detection and prevention: Recommendations and prototype implementation,” *1st IEEE Work. VoIP Manag. Secur. VoIP MaSe 2006*, pp. 45–50, 2006.

[11] J. Gómez, C. Gil, N. Padilla, R. Baños, and C. Jiménez, “Design of a snort-based hybrid intrusion detection system,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5518 LNCS, no. PART 2, pp. 515–522, 2009.

[12] D. V. Sandi and M. Arrofiq, “Implementasi Analisis NIDS Berbasis Snort Dengan Metode Fuzy Untuk Mengatasi Serangan LoRaWAN,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 3, pp. 685–696, 2018.

[13] E. A. Winanto, A. Heryanto, and D. Stiawan, “Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means,” *Annu. Res. Semin. 2016*, vol. 2, no. 1, pp. 359–362, 2016.

[14] M. I. Mazdadi, I. Riadi, and A. Luthfi, “Live Forensics on RouterOS using API Services to Investigate Network Attacks,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 2, pp. 406–410, 2017.