PENGEMBANGAN SISTEM PENGAMAN JARINGAN KOMPUTER BERDASARKAN ANALISIS FORENSIK JARINGAN

Abdul Fadlil, Imam Riadi, Sukma Aji
Program Studi S2 Magister Teknik Informatika
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
fadlil@mti.uad.ac.id, files.riadi@gmail.com, sukma.aji@staff.uad.ac.id

Abstract

Network forensics is a computer security investigation to find sources of the attacks on the network by examining data log evidence, identifying, analyzing, and reconstructing the incidents. Types of attacks againist a computer or server on the network by spending resources that are owned by the computer until computer is not able to function properly, thus indirectly preventing other users to obtain access to network services that were attacked is Distributed Denial of Service attack (DDoS). Network Forensics Research conducted in Research Laboratory of Information Engineering Master of Ahmad Dahlan University Yogyakarta. Detection of attacks carried out by Winbox RouterOS v3,6 where the software shows resources, attacker(IP Address), data packets, and when attack doing. Simulated attacks carried out by LOIC software to determine performance of safety system in computer network. To anticipate DDoS attacks,then developed a computer network security system.

Keywords: *DdoS; router; safety system of security network*

Abstrak

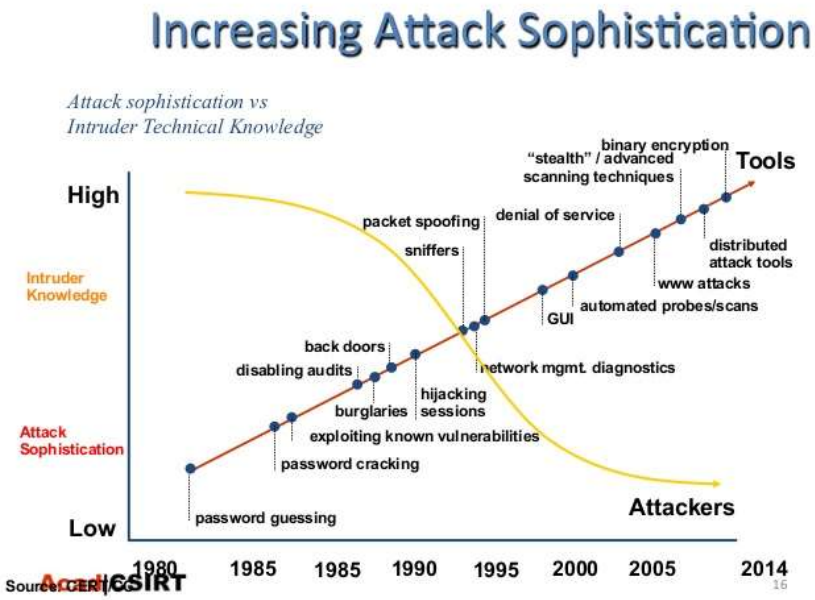
Ilmu pengetahuan tentang keamanan komputer yang terkait dengan penyelidikan untuk menentukan sumber serangan jaringan berdasarkan data log bukti, identifikasi, analisis, dan rekonstruksi kejadian adalah Forensik Jaringan yang merupakan cabang dari Forensik Digital. Jenis serangan terhadap suatu komputer atau server di dalam jaringan dengan cara menghabiskan sumber daya (resources) yang dimiliki oleh komputer sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses dari layanan jaringan yang diserang disebut dengan serangan Distributed Denial of Service (DDoS). Riset Forensik Jaringan dilakukan dalam Laboratorium Riset Magister Teknik Informatika Universitas Ahmad Dahlan Yogyakarta. Deteksi serangan dilakukan oleh Winbox RouterOS v3,6 dimana software tersebut menunjukan resources, data penyerang (IP Address), jumlah paket data, dan kapan terjadi serangan. Simulasi serangan dilakukan dengan software LOIC untuk mengetahui kinerja sistem pengaman jaringan komputer, sedangkan sistem pengaman jaringan komputer berupa antisipasi terhadap bentuk serangan DDoS.

Kata Kunci: DDoS*;* router*;* pengaman jaringan komputer.

1. Pendahuluan

Jaringan Komputer berkembang dengan sangat pesat, baik di instansi-instansi komersil, dunia akademik, bahkan rumah-rumah penduduk yang membutuhkan akses internet. Internet diakses oleh banyak orang tanpa terkecuali hacker dan 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. Kecanggihan serangan dan tools pada jaringan komputer berbanding terbalik dengan pengetahuan tentang penyusupan pada jaringan komputer. Hal ini dikarenakan serangan yang terjadi menjadi lebih otomatis dan menyebabkan jumlah yang besar. Gambar 1 [1] menunjukan , dari tahun 1980an hingga tahun 1990an dimulainya penebakan *password*, mengetahui *password*, eksploitasi pengetahuan kerentanan, menonaktifkan audit, pencurian, sampai pada sesi pembajakan. Tahun 2000an diawali dengan serangan *Denial of Service* hingga tahun 2014an berkembang menjadi serangan *Distributed Denial of Service* dan enkripsi biner. Sementara pengetahuan tentang cara-cara penyusupan semakin menurun, hal ini dikarenakan investigasi dilakukan setelah tindakan-tindakan penyusupan terjadi.



Gambar 1. Kecanggihan serangan vs pengetahuan tentang cara penyusupan [1].

Efek utama dari serangan jaringan komputer berupa lambatnya akses internet. Selain itu untuk jenis serangan jaringan yang sangat berbahaya dapat mengakibatkan rusaknya data pada server, sehingga hal ini sangat merugikan pengguna ataupun *end user* yang sedang mengakses. Kegiatan merusak, mengganggu, mencuri data, dan segala hal yang merugikan pemilik server pada jaringan komputer adalah suatu tindak ilegal dan dapat dijatuhkan sangsi secara hukum di pengadilan. Memerangi kejahatan internet telah menjadi porsi utama bagi agen-agen penegak hukum dan intelejen, baik nasional maupun internasional, tanpa kecuali para praktisi bisnis, sampai kepada para pelanggan, dan *end user*. Umumnya kejahatan internet dimulai dengan mengeksploitasi host-host dan jaringan komputer sehingga para penyusup datang melintasi jaringan, terutama jaringan yang berbasis TCP/IP. Forensik jaringan yang lebih spesifik adalah kegiatan menangkap, mencatat, dan menganalisa kejadian pada jaringan komputer untuk menemukan sumber serangan keamanan atau masalah kejadian lainya. Kekuatan dari Forensik adalah memungkinkan analisis dan mendapatkan kembali fakta dan kejadian dari lingkungan, karena fakta mungkin saja tersembunyi.

Forensik Jaringan merupakan bagian dari forensik digital, dimana bukti ditangkap dari jaringan dan diinterpretasikan berdasarkan pengetahuan dari serangan jaringan. Hal ini bertujuan untuk menemukan penyerang dan merekonstruksi tindakan serangan melalui analisis bukti penyusupan [2]. Kasus SQL Injection terjadi ketika seorang penyerang dapat memasukan serangkaian pernyataan SQL ke query dengan memanipulasi data input ke aplikasi [3]. SQL Injection adalah sebuah metodologi serangan yang menargetkan data yang berada dalam data base melalui firewall yang melindungi data tersebut. Forensik jaringan berakar dari keamanan jaringan dan deteksi penyusupan. Forensik jaringan berkaitan dengan perubahan data dari mili detik ke mili detik. Investigasi serangan cyber atau penyusupan adalah investigasi forensik

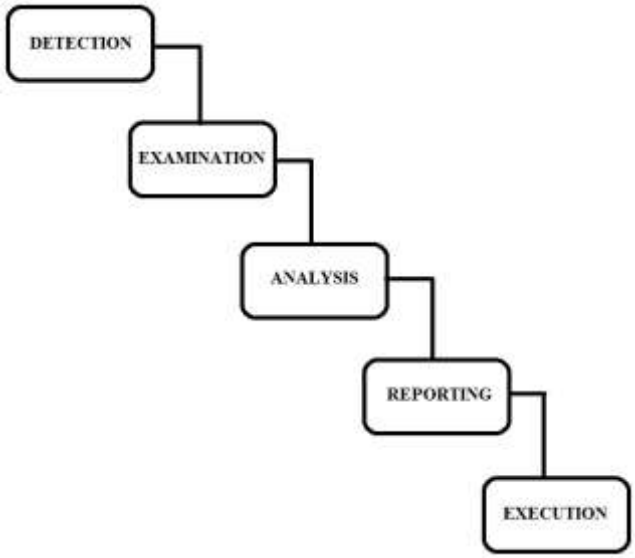
jaringan. Tantangan utama yang dihadapi dari forensik jaringan adalah bagaimana cara untuk mempertahankan bukti, kemudian digunakan dalam proses di pengadilan [4].

Mikrotik Router adalah salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan. Selain itu Mikrotik dapat juga berfungsi sebagai investigator untuk penyusupan pada jaringan komputer dan firewall bagi komputer lain dan memberikan prioritas kepada komputer lainya agar dapat mengakses data internet maupun data lokal. Mikrotik bertujuan untuk mengatur bandwidth serta melakukan manajemen jaringan komputer. Router Mikrotik ditempatkan pada sebuah komputer yang dijadikan sebagai gateway suatu jaringan. Komputer gateway tersebut berfungsi untuk mendistribusikan data keluar masuknya dari dan ke komputer lainya, sehingga seluruh komputer dapat mengakses data bersama-sama seperti internet sharing. Pengelolaan jaringan lokal (Local Area Network) merupakan salah satu alternatif penyelesaian masalah supaya didapatkan layanan yang maksimal. Mikrotik router diimplementasikan untuk mengatur lalu lintas data internet serta melakukan filter beberapa jenis serangan jaringan yang dapat mengganggu konektifitas jaringan komputer sesuai dengan aturan yang telah ditetapkan dan disepakati bersama [5].

Serangan Distributed Denial of Service (DDoS) ditujukan tidak untuk memperoleh informasi melainkan untuk mengganggu pengguna yang sah dari sistem atau fasilitas dalam mengakses layanan jaringan komputer. Serangan ini dilakukan dari beberapa komputer sekaligus menuju target yang disebut sebagai zombie [6]. Serangan DDoS adalah salah satu ancaman paling serius untuk keamanan jaringan, dan jumlah korban serangan DDoS meningkat setiap hari [7]. Deteksi anomali dari sekumpulan data selalu menjadi isu yang sangat penting pada semua jenis solusi pendekatan [8]. Semua teknik mitigasi memerlukan tindakan tertentu, seperti *blackholing* untuk penyedian *upstreams* atau pemberitahuan perubahan rute. Jika proses ini ditangani oleh manusia kemungkinanya akan sangat lama. Sebagai contoh ketika terjadi serangan hal ini mustahil dilakukan oleh manusia [9]. Serangan DDoS dapat dilakukan ditingkat manapun. Ada beberapa solusi untuk mengurangi serangan DDoS pada router menggunakan firewall pada Mikrotik [10]. Dalam Jaringan dimana lapisan 3 dan lapisan 4 layanan keamanan berada, penggunaan *rate shaping* untuk mencegah dari banjir TCP. Batas koneksi dapat menjadi teknik mitigasi yang efektif [11]. Pengubahan *data size* menuju target serangan DDoS dapat meningkatkan level serangan serta menyebabkan router yang dilewati data tersebut mengalami konsumsi daya listrik meningkat begitu pula dengan beban CPU [12].

2. Metodologi Penelitian

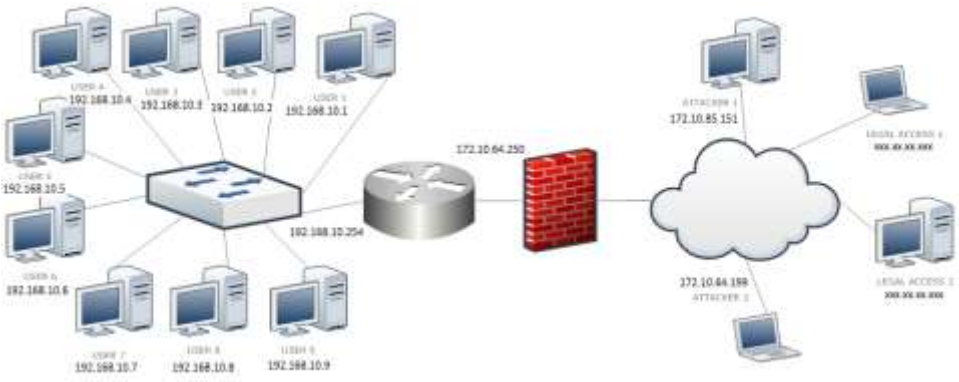
Metodologi yang digunakan dalam penelitian ini adalah model proses forensik *(The Forensic Process Model)* yang dilukiskan oleh Gambar 2 [13]



Gambar 2. Model proses forensik [13]

Tahap penelitian:

1. Deteksi (Detection). Pada tahap ini yang dilakukan adalah mendeteksi dan mencari bukti-bukti, pengenalan terhadap bukti-bukti penyusupan, dan pengumpulan bukti. Winbox RouterOS digunakan untuk mendeteksi serangan
2. Pemeriksaan (Examination), pada tahap ini pencarian informasi yang tersembunyi dan mengungkapkan dokumentasi yang relevan. Pemeriksaan menggunakan software Winbox RouterOS semisal memeriksa urutan paket, jumlah paket data, dan lain-lain.
3. Analisis (Analysis), yaitu tahap yang akan menjawab pertanyaan forensik yaitu **apa** yang terjadi, IP Address **siapa** yang melakukan serangan, **kapan** serangan tersebut terjadi, **dimana** serangan tersebut terjadi, dan **bagaimana** serangan tersebut terjadi.
4. Laporan (Reporting), yaitu menuliskan laporan mengenai proses pemeriksaan dan data yang diperoleh dari semua penyelidikan.
5. Tindakan (Execution), hasil forensik jaringan yang sudah didapat kemudian menjadi rujukan untuk membuat sistem Pengaman Jaringan Komputer menggunakan Mikrotik.



Gambar 3. Topologi Jaringan Komputer Laboratorium Riset MTI UAD

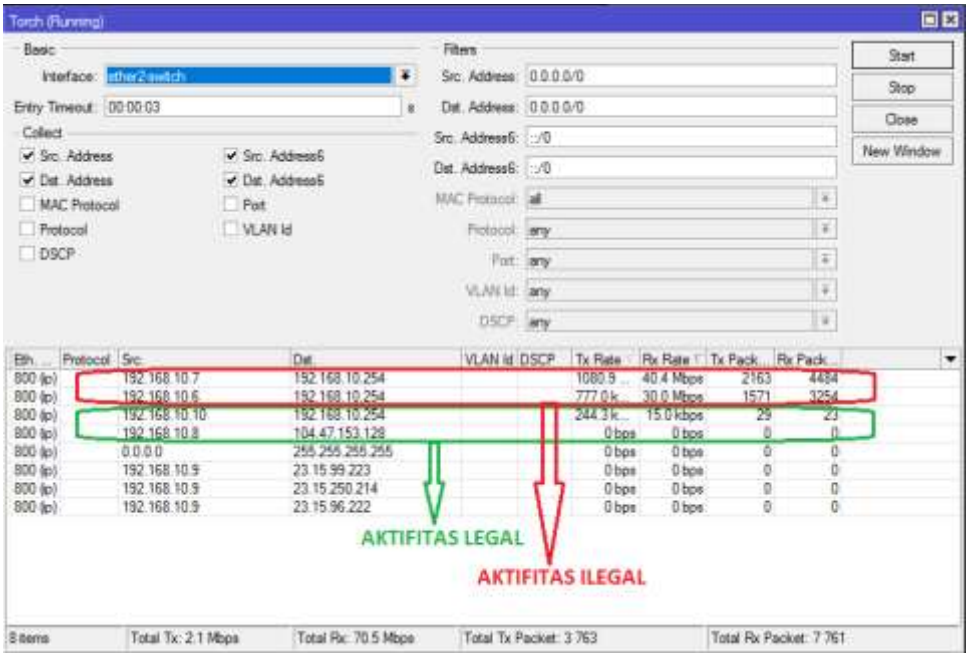
Skenario penelitian ditunjukan pada Gambar 3. Dimana komputer pengguna dihubungkan model bintang (star) dengan switch kemudian berturut-turut dihubungkan dengan router kemudian dibuat firewall sebagai sistem pengaman dan yang terakhir dihubungkan dengan internet. Jaringan tersebut dapat diakses baik dari dalam maupun dari luar jaringan komputer Laboratorium Riset MTI UAD. Untuk simulasi serangan jaringan komputer, Laboratorium Riset MTI UAD diserang menggunakan serangan DDoS dengan software LOIC yang ditunjukan pada Gambar 4. Serangan dilakukan dengan memasukan IP Address target pada baris “IP” dan menekan tombol “Lock on”, kemudian memilih menu “methode” ada 3 pilihan yaitu “TCP”, “UDP”, dan “HTTP”. LOIC siap untuk melakukan serangan menuju target yaitu layanan jaringan Lab Riset MTI UAD.

Gambar 4. Software LOIC yang digunakan untuk melakukan simulasi serangan jaringan komputer

3. Hasil dan Pembahasan

3.1. Deteksi

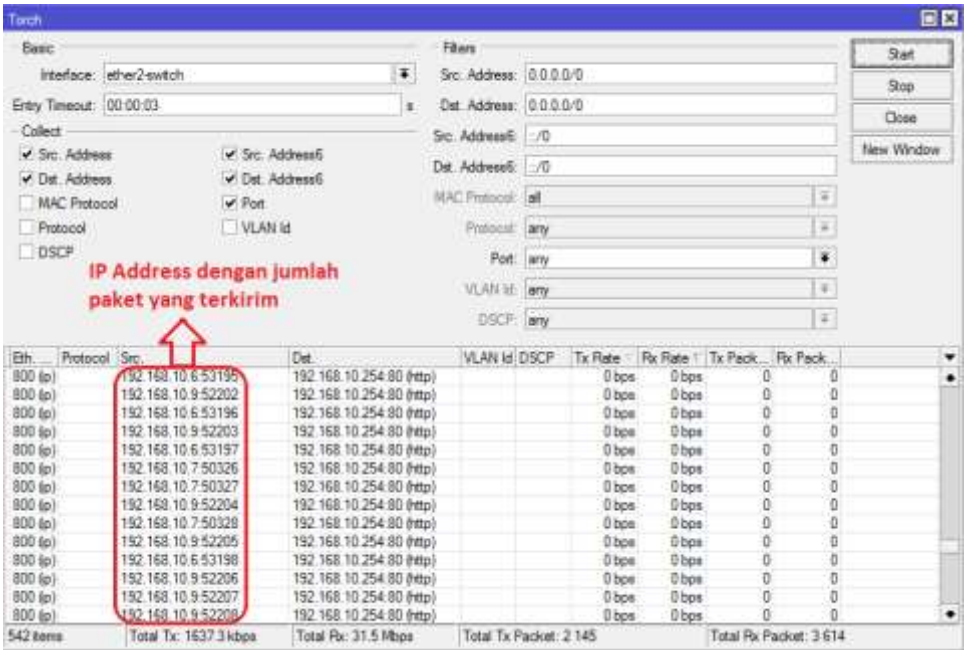
Deteksi serangan DDoS dalam hal ini menggunakan software Winbox RouterOS yang menunjukan identitas dari penyerang. Warna hijau menunjukan akses legal, sedangkan warna merah menunjukan akses ilegal dalam jaringan komputer Laboratorium Riset MTI UAD pada Gambar 5.



Gambar 5. Akses legal dan akses ilegal

3.2. Pemeriksaan

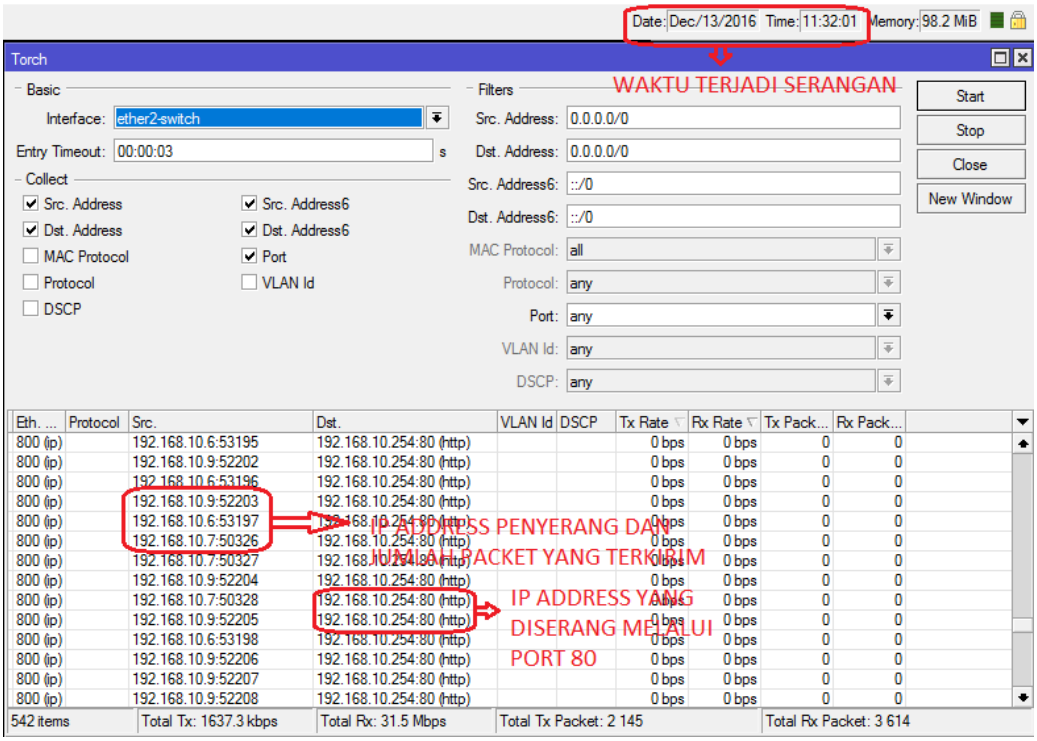
Jumlah paket data yang dikirimkan oleh penyerang yang masuk kedalam layanan jaringan komputer ditunjukan pada Gambar 6.



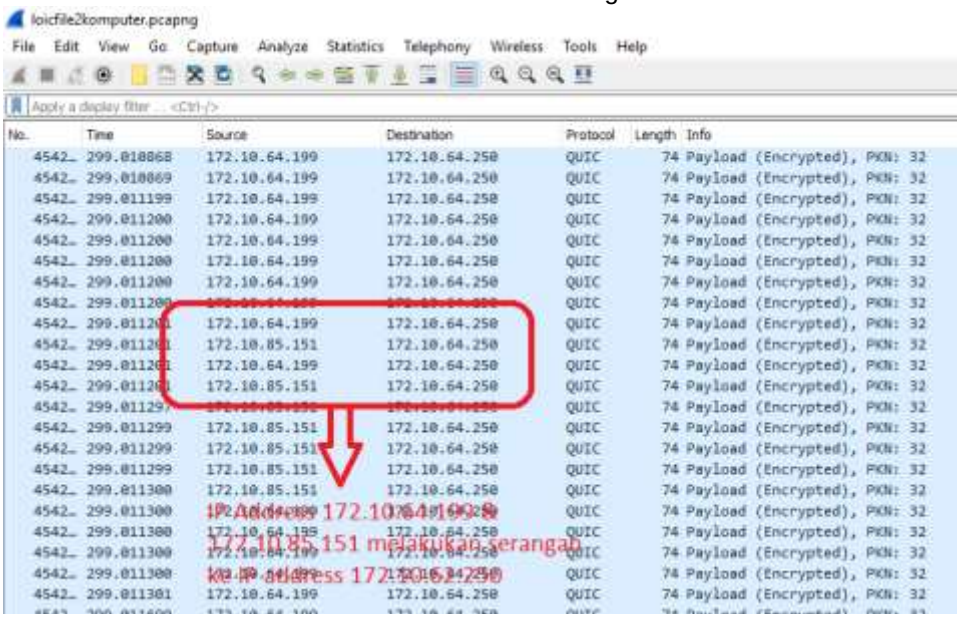
Gambar 6. Pemeriksaan jumlah paket data

3.3. Analisis Forensik Jaringan

Software Winbox RouterOS setelah mendeteksi adanya akses ilegal kemudian memberikan informasi yang lebih detil dalam menu Tourch yaitu menunjukan adanya **serangan DDoS**, IP Address yang melakukan serangan **(192.168.10.9, 192.168.10.7, 192.168.10.6)**, kapan serangan tersebut terjadi yaitu **pada tanggal 13 Desember 2016 pukul 11:32:01**, sedangkan simana serangan tersebut terjadi yaitu pada **port 80**, dan mengapa itu terjadi yaitu dikarenakan **port 80 terbuka**. Gambar 7 menunjukan relevansinya. Barang bukti lain berupa *Traffic Network* ditunjukan pada Gambar 8 menggunakan *tools investigation wireshark*.



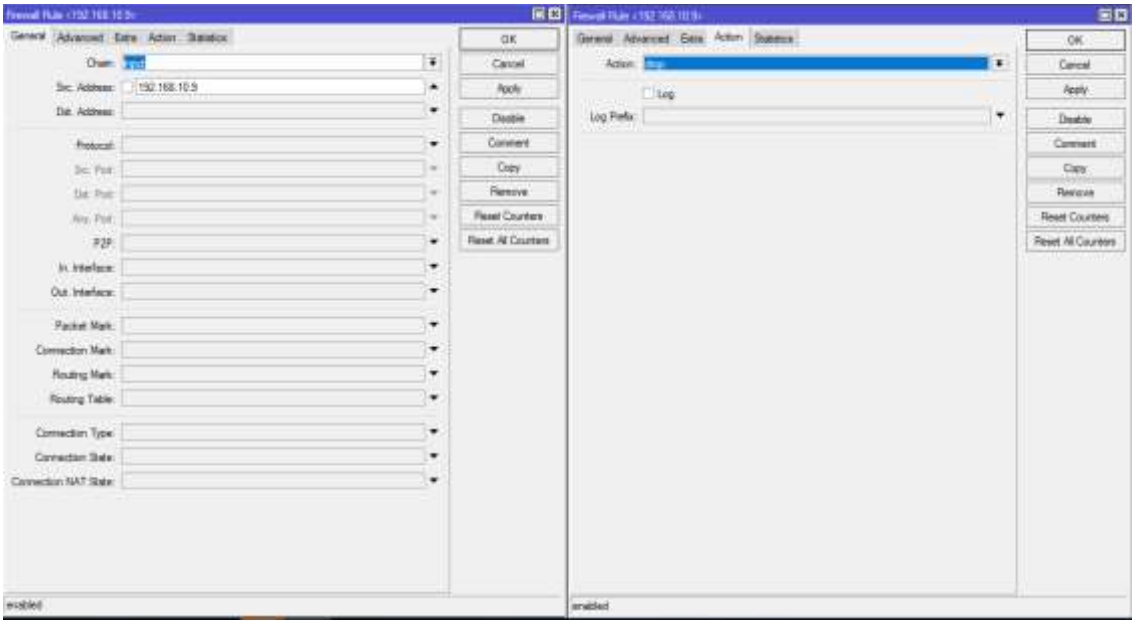
Gambar 7. Analisis serangan



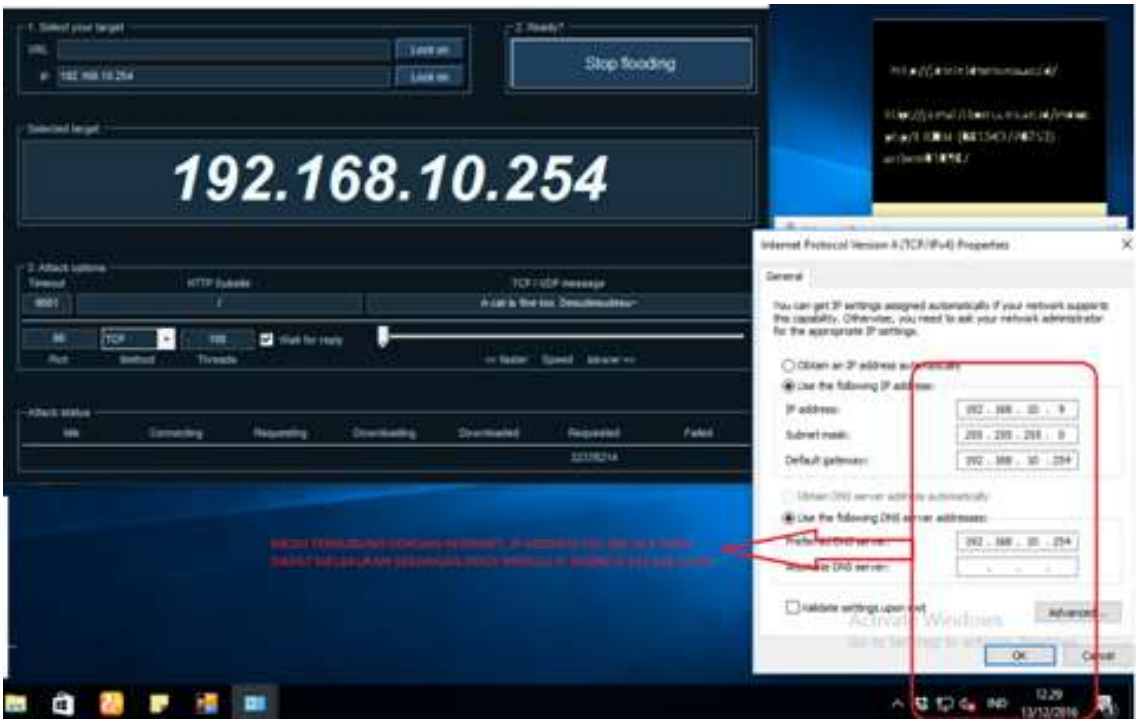
Gambar 8. *Traffic network capture* menggunakan *wireshark*

3.4. Eksekusi

Selain mendapatkan barang bukti, dibuat sistem antisipasi yaitu dengan memblokir IP Address dari penyerang supaya tidak terjadi serangan yang sama dikemudian waktu. Gambar 9. Menunjukan, IP address 192.168.10.9 diblokir supaya dilain waktu tidak dapat melakukan serangan. Gambar 10. Menunjukan, proses terhentinya *request* serangan setelah diblokir dan paket data yang dikirim oleh penyerang akan terhenti.



Gambar 9. Pemblokiran IP Address 192.168.10.9



Gambar 10. Pengiriman paket data terhenti setelah IP Address 192.168.10.9 diblokir

4. Kesimpulan

Berdasarkan hasil pengujian dan analisis sistem pengaman jaringan komputer dapat dirancang menggunakan bukti forensik jaringan komputer. Dan setelah dibuat sistem pengaman jaringan komputer, penyerang tidak akan mampu melakukan serangan pada waktu yang akan datang menggunakan metode yang sama.

Referensi

[1] I. Mantra, "Peranan CERT/CSIRT Untuk melindungi Data Pribadi dan Institusi. Seminar Cyber Defence Teknik Informatika Universitas Jendral Sudirman Purwokerto 21 September 2014," *Unsoed*, 2014. .
[2] B. Ruchandani, M. Kumar, A. Kumar, K. Kumari, A. K. Sinha, and P. Pawar, "Experimentation in network forensics analysis," *Proc. Term Pap. Ser. under CDAC-CNIE Bangalore,* pp. 1–13, 2006.
[3] C. Anley, *Advanced SQL injection in SQL server applications*. 2002.
[4] L. Volonino and R. Anzaldua, *Computer Forensics FOR DUMMIES*. Indianapolis: Wiley Publishing, 2008.
[5] I. Riadi, "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik Pendahuluan Landasan Teori," *JUSI, Univ. Ahmad Dahlan Yogyakarta*, vol. 1, no. 1, pp. 71–80, 2011.
[6] A. Silberschatz, P. B. Galvin, and G. Gagne, *Operating Systeme Concepts*, vol. ninth edit. wiley, 2013.
[7] K. Kato and V. Klyuev, "Large-scale network packet analysis for intelligent DDoS attack detection development," *2014 9th Int. Conf. Internet Technol. Secur. Trans. ICITST 2014*, pp. 360–365, 2014.
[8] S. Maiti, C. Garai, and R. Dasgupta, "A detection mechanism of DoS attack using adaptive NSA algorithm in cloud environment," *2015 Int. Conf. Comput. Commun. Secur. ICCCS 2015*, 2016.
[9] F. Lau, S. Rubin, and M. Smith, "Distributed denial of service attacks," *Syst. Man, Cybern.*, 2016.
[10] A. Giordano and M. Ciantar, "Reducing the impact of DoS attacks with MikroTik RouterOS," in *MikroTik User Meeting*, 2015, pp. 1–40.
[11] D. Holmes, *The F5 DDoS Playbook : Ten Steps for Combating DDoS in Real Time*. 2015.
[12] R. Adrian and N. Isnianto, "Analisa Pengaruh Variasi Serangan DDoS Pada Performa Router," in *Prosiding Seminar Nasional Teknologi Terapan SV UGM*, 2016, pp. 1257–1259.
[13] R. Utami and J. Istiyanto, Eko, "Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada," vol. 6, no. 2, pp. 101–112, 2012.