Penerapan Metode Network Forensik Untuk Analisis Serangan DOS Pada Perangkat Router

Singgih Mitro S[1*)], Dadan Sukma[2]
[1,2]Program Studi Informatika, Universitas Insan Cita Indonesia, Jakarta
[1,2]Jln. H,R Rasuna Said, Kota Jakarta Selatan, 12940, Indonesia
email:singgihmitro@uici.ac.id, [2]dadansukma@uici.ac.id

Abstract **−− Denial of Service (DoS) attacks on router devices can cause damage to the network and hinder connectivity. The application of the Network Forensic method can be used to analyze DoS attacks on router devices. This method includes stages such as preparation, incident handling, data collection, preservation, data analysis, investigation and presentation of results. From the attack process, it is analyzed that the DoS attack uses the LOIC application by sending messages repeatedly so that the router network goes down. The application of the Network Forensic method can be used to analyze DoS attacks on router devices and assist in taking action to prevent further attacks. However, this method requires special experience and expertise in networking and forensics.**

Kata Kunci **– Denial of Services (DoS), Network Forensics, Router.**

Abstrak **− Serangan Denial of Service (DoS) pada perangkat router dapat menyebabkan kerusakan pada jaringan dan menghambat konektivitas. Penerapan metode Network Forensik dapat digunakan untuk menganalisis serangan DoS pada perangkat router. Metode ini meliputi tahap-tahap seperti persiapan, penanganan insiden, pengumpulan data,pemeriksaan, analisis data, investigasi dan presentasi hasil. Dari proses penyerangan yang di analisa bahwa serangan DoS menggunakan aplikasi LOIC dengan cara mengirim pesan secara bertubi-tubi sehingga membuat jaringan Router menjadi Down. Penerapan metode Network Forensik dapat digunakan untuk menganalisis serangan DoS pada perangkat router dan membantu dalam mengambil tindakan untuk mencegah serangan selanjutnya. Namun, metode ini memerlukan pengalaman dan keahlian khusus dalam bidang jaringan dan forensik.**

Kata Kunci **– Denial of Services (DoS), Network Forensics, Router.**

I.PENDAHULUAN

Investigasi forensik digital adalah pada kejahatan yang dilakukan melalui komputer. [1] Namun, selama beberapa tahun terakhir tahun, bidang telah diperluas untuk memasukkan berbagai perangkat digital lainnya di mana informasi yang disimpan secara digital dapat diproses dan digunakan untuk berbagai jenis kejahatan.[2]

Investigasi digital forensic disebut sebagai Digital forensics Investigations (DFI). DFI adalah fase terhubungnya informasi yang diekstraksi dan bukti digital untuk membuat informasi faktual untuk ditinjau oleh lembaga peradilan [1], [2]. [3] dalam penelitianya menyoroti kebutuhan untuk menetapkan informasi faktual sebagai hasil dari penyelidikan semacam itu. DFI melakukan investigasi setelah terjadinya insiden. Oleh karena itu jenis penyelidikan yang berbeda "di mana prosedur ilmiah dan teknik yang digunakan akan memungkinkan hasil, dengan kata lain bukti digital, dapat diterima di pengadilan. [4]. Bukti digital atau elektronik terdiri dari informasi dan data nilai yang disimpan atau ditransmisikan oleh perangkat digital[2]. Dengan demikian, bukti elektronik adalah bukti laten dalam arti yang sama bahwa sidik jari atau bukti DNA adalah laten.

Penggunaan teknologi komputer yang berbasis jaringan telah memberikan kontribusi kemudahan bagi para pengguna. Namun, di balik kecanggihan teknologi jaringan komputer, muncul masalah tentang forensik jaringan. Penyebab utama dari masalah forensik jaringan adalah tindak penyalahgunaan teknologi oleh orang-orang yang tidak bertanggung jawab dengan tujuan memanfaatkan fasilitas jaringan pihak lain untuk kepentingan pribadi maupun kelompok,Serangan DoS (Denial of Service) salah satu serangan yang paling sering terjadi di jaringan komputer adalah jenis serangan jaringan Router yang tidak dapat melayani permintaan pengguna, dan akhirnya menyebabkan jaringan komputer menjadi down. [5]

*) **penulis korespondensi**: Singgih Mitro S
Email: singgihmitro@uici.ac.id

II.PENELITIAN YANG TERKAIT

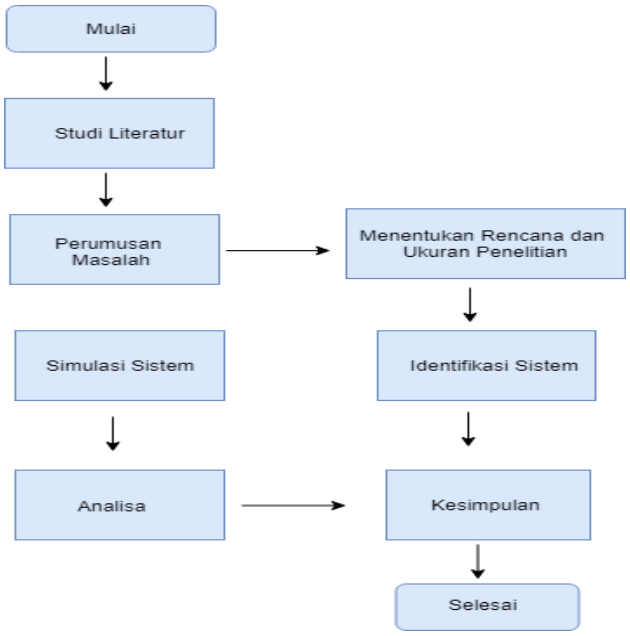
Beberapa penelitian dahulu berkaitann dengan Netwok forensic yang dilakukan oleh A. R. Caesarano and I. Riadi dengan judul " Network Forensics for Detecting SQL Injection Attacks using NIST Method yang bertujuan untuk mendeteksi serangan SQL Injection dan notifikasi serangan real time menggunakan email dengan pengembangan system web server menggunakan Snort untuk system deteksi dan menggunakan NIST untuk mendapatkan bukti digital. [6]

Penelitian lainya dilakukan oleh M. Alim, I. Riadi, and Y. Prayudi dengan judul Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard bertujuan untuk explorasi terhadap bukti digital yang bisa didapatkan dari Sistem Operasi Router untuk memperoleh informasi yang digunakan dalam penyelidikan forensic. [5]

Berdasarkan referensi diatas, penelitian ini akan difokuskan pada penerapan metode network forensic untuk analisis searangan DoS pada perangkat router yang bertujuan untuk menemukan barang bukti digital.

III. METODE PENELITIAN

Pada penelitian ini menggunakan f*lowchart* metodologi penelitian yang dapat dilihat pada Gambar 1.



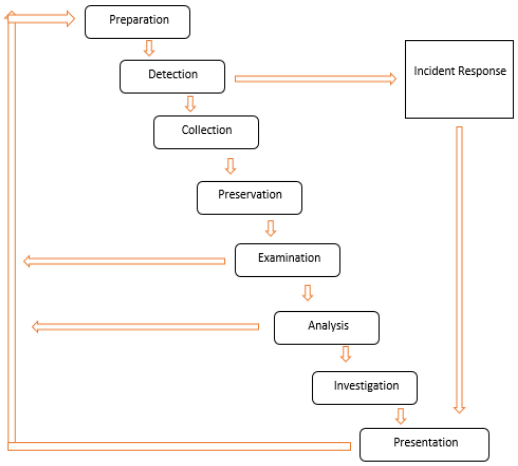
Gambar 1 *Flowchart* Metodologi Penelitian

1. Network Forensik

Maraknya tindakan kejahatan dalam dunia komputer, membutuhkan proses pembuktian yang tidaklah mudah, oleh karena itu, kajian bidang komputer forensik ini masih tergolong baru dan masih terus dikembangkan, sehingga nantinya, semua kasus-kasus kejahatan komputer mampu dibuktikan secara sah di pengadilan. *Digital forensic* mempunyai banyak cabang salah salah satunya adalah *network forensics*. *F*orensic jaringan memfokuskan pada data yang diperoleh berdasarkan pengamatan pada jaringan.[7]. Dalam kegiatan *forensics* mempunyai tujuan yaitu salah satunya untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat bukti yang sah di pengadilan.

2. Framework Generic Network Forensics

Dalam makalah tentang "A Survey About Network Forensics" penulis mengusulkan model investigasi forensik jaringan. Model yang diusulkan terdiri dari beberapa tahap proses penyelidikan forensik jaringan. Gambar 2 menunjukan model dari forensik jaringan yang digambarkan memiliki sembilan tahapan. [8].



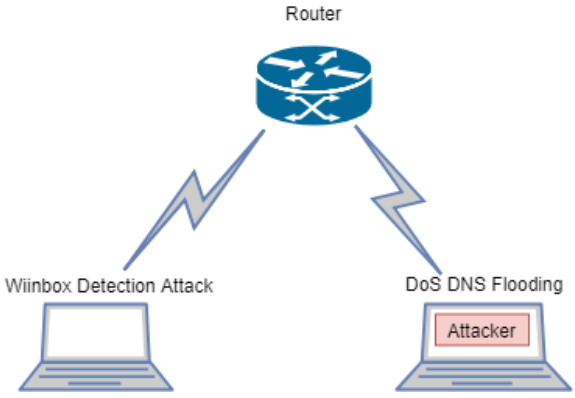
Gambar 2 Network Forensic Process Model

1. Tahap Persiapan : Tujuanya adalah untuk mendapatkan otorisasi yang diperlukan dan jaminan secara hukum.
2. Tahap Penemuan : Menghasilkan peringatan yang menunjukkan pelanggaran keamanan.
3. Tahap Penanganan Insiden : Berlaku ketika penyelidikan dimulai selama serangan berlangsung.
4. Tahap Pengumpulan : Bagian paling sulit karena data mengalir dengan cepat dan tidak mungkin menghasilkan jejak dengan hal yang sama.
5. Tahap Pemeliharaan : Bukti asli tetap aman bersamaan dengan penghitungan hash.
6. Tahap Pemeriksaan : Untuk memeriksa tahap sebelumnya. Semua data yang disembunyikan atau diubah adalah untuk pengungkapan yang dilakukan oleh penyerang.
7. Tahap Analisis : Bukti yang sudah dikumpulkan kemudian dianalisis untuk menemukan sumber serangan.
8. Tahap Investigasi : Penggunaan informasi yang dikumpulkan dalam tahap analisis dan fokus untuk menemukan penyerang.
9. Presentasi : Tahap akhir untuk memproses model, dokumentasi dibuat dan laporan yang dihasilkan dan ditampilkan kepada pihak atau otoritas yang lebih tinggi.

IV. HASIL DAN PEMBAHASAN

1. Simulasi Serangan Dos Pada Router

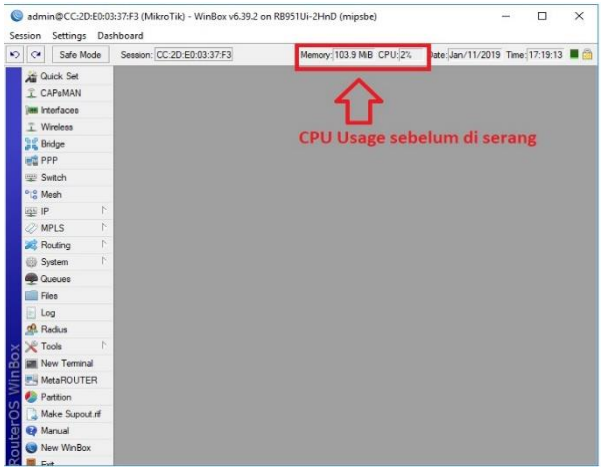
DoS dapat dilakukan dengan menyalahgunakan perangkat, memanipulasi perangkat lunak dan aplikasi, atau mengganggu saluran komunikasi [9]. Salah satu serangan DoS adalah serangan gangguan di mana saluran komunikasi mampu menonaktifkan saluran komunikasi sensor dari membawa sinyal dengan menghasilkan tabrakan. Tabrakan akan menyebabkan pesan komunikasi tergangg [10]. Berikut Rancangan simulasi serangan DoS pada Router menggunakan DNS Flooding, dan analisis serangan pada Router menggunakan aplikasi Winbox.



Gambar 3 Desain Analisis Serangan DoS pada Router

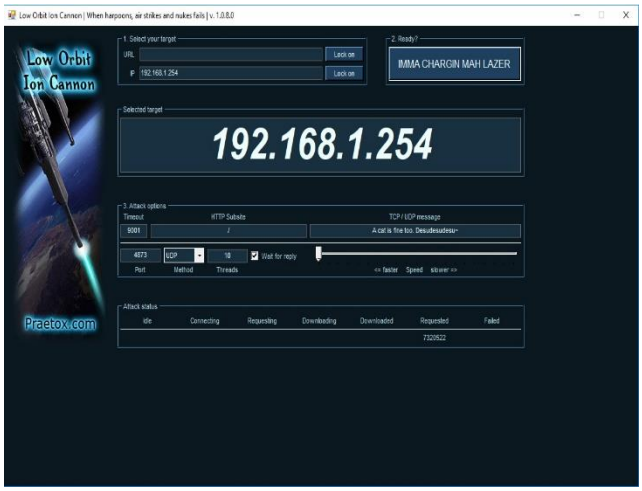
2. Pengujian Menggunakan Aplikasi

Proses awal untuk analisis apakah Router masih dalam keadaan normal atau sudah ada serangan DoS, dapat dilakukan melalui pengecekan pada menu WinBox.



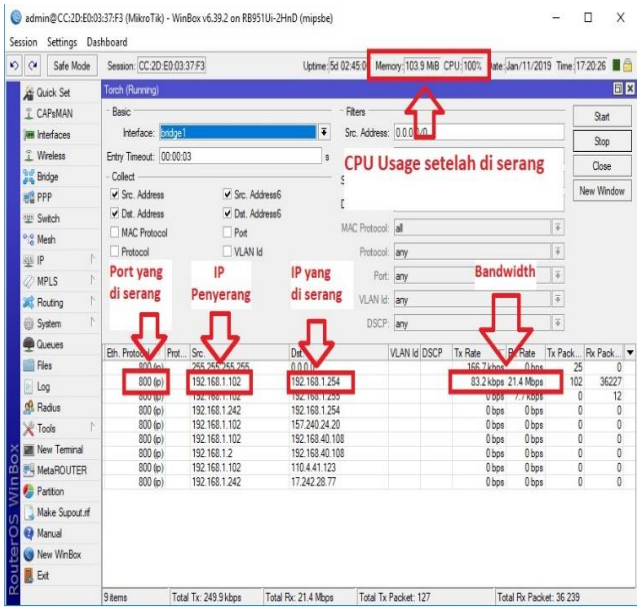
Gambar 4 Tampilan Sebelum Ada Serangan DoS

Berdasarkan tampilan Proses awal pengecekan seperti gambar di atas , dapat disimpulkan belum ada serangan yang masuk dan menganggu lalu-lintas jaringan pada Router. Hal ini dapat dilihat pada kolom merah CPU & Memory masih normal. Langkah berikutnya adalah mulai melakukan simulasi serangan DoS pada Router menggunakan aplikasi LOIC (*Low Orbit Ion Canon*) untuk mengetahui apakah serangan DoS yang diluncurkan berhasil menembus jaringan Router. Setelah melakukan pengujian pengecekan awal terhadap lalu-lintas jaringan Router, maka selanjutnya dilakukan pengujian menggunakan aplikasi. Pada proses ini aplikasi LOIC (*Low Orbit Ion Canon*) dijalankan windows untuk melancarkan serangan.



Gambar 5 Aplikasi LOIC untuk Serangan DoS

Berdasarkan tampilan Gambar di atas, dapat dijelaskan bahwa aplikasi LOIC berhasil dijalankan dan siap melancarkan serangan ke jaringan Router yang menjadi target serangan. Setelah dilakukan serangan, proses selanjutnya melakukan pengecekan serangan yang masuk pada Router melalui aplikasi Winbox. Setelah dicek percobaan simulasi serangan ini sudah berhasil masuk, sehingga dapat dilakukan Monitoring Flooding untuk melakukan serangan pada Router. Penyerangan DoS menggunakan LOIC langsung menuju ke target jaringan Router yang diserang, seperti tampilan pada Gambar berikut:



Gambar 6 Tampilan Sesudah Ada Serangan DoS

HASIL PENGUJIAN SERANGAN DOS PADA ROUTER

Tabel 1 Hasil Analisis Serangan DOS di Router

Analisis	Keterangan
IP Addres Penyerang	192.168.1.102
Kondisi CPU perangkat jaringan yang belum diserang	2 %
Kondisi CPU perangkat jaringan yang sudah diserang	100 %
Serangan DoS pada Router menggunakan aplikasi LOIC	Berhasil melakukan serangan

V. KESIMPULAN DAN SARAN

Setelah melakukan simulasi serangan DoS pada Router, maka dapat ditarik beberapa temuan penelitian sebagai kesimpulan. Berikut kesimpulan penelitian ini:

1. Dari proses penyerangan yang di analisa bahwa serangan DoS menggunakan aplikasi LOIC dengan cara mengirim pesan secara bertubi-tubi sehingga membuat jaringan Router menjadi *Down*.
2. Semua Teknik yang dilakukan berdasarkan metode yang digunakan memiliki keberhasilan 100% untuk mendeteksi serangan DOS di Router.

UCAPAN TERIMA KASIH

Ucapan terima kasih penulis kepada Universitas Insan Cita Indonesia yang membantu ataupun memberikan dukungan terkait dengan penelitian yang dilakukan.

DAFTAR PUSTAKA

[1] E. Casey, "Digital Evidence and Computer Crime, Third Edition," p. 840, 2011.
[2] R. Montasari, "Review and Assessment of the Existing Digital Forensic Investigation Process Models," *Int J Comput Appl*, vol. 147, no. 7, pp. 41–49, 2016, doi: 10.5120/ijca2016911194.
[3] M. N. Faiz, W. A. Prabowo, and M. F. Sidiq, "Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal," *Journal of Informatics, Information System, Software Engineering and Applications (INISTA)*, vol. 1, no. 1, pp. 63–70, 2018, doi: 10.20895/INISTA.V1I1.
[4] G. Notomista and M. Botsch, "Maneuver segmentation for autonomous parking based on ensemble learning," *Proceedings of the International Joint Conference on Neural Networks*, vol. 2015-Septe, no. 5, pp. 118–131, 2015, doi: 10.1109/IJCNN.2015.7280546.
[5] M. Alim, I. Riadi, and Y. Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," *Int J Comput Appl*, vol. 180, no. 35, pp. 23–30, 2018, doi: 10.5120/ijca2018916879.
[6] A. R. Caesarano and I. Riadi, "Network Forensics for Detecting SQL Injection Attacks using NIST Method," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 7, no. 4, pp. 436–443, 2018.
[7] R. Budi, "Sekilas Mengenai Forensik Digital," *Jurnal Sosioteknologi*, vol. Edisi 29, pp. 2–3, 2016, doi: http://dx.doi.org/10.5614%2Fsostek.itbj.2013.12.29.3.
[8] C. S. P. J. Rodrigo, May Lim, "Rodrigo, Optical-feedback Semiconductor Laser.pdf," *Sci Diliman*, vol. 13, no. 2, pp. 88–91, 2010, doi: 10.5120/251-408.
[9] N. H. N. Zulkipli and G. B. Wills, "An event-based access control for IoT," *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing - ICC '17*, no. October 2018, pp. 1–4, 2017, doi: 10.1145/3018896.3025170.
[10] R. Rizal, I. Riadi, and Y. Prayudi, "Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 7, no. 4, pp. 382–390, 2018.