Buletin Ilmiah Sarjana Teknik Elektro
Vol. 3, No. 1, April 2021, pp. 21-30
ISSN: 2685-9572, DOI: 10.12928/biste.v3i1.1752

Intruder Detection Systems on Computer Networks Using Host Based Intrusion Detection System Techniques

Sistem Deteksi Penyusup Pada Jaringan Komputer Menggunakan Teknik *Host Based Intrusion Detection System*

Rio Widodo[1], Imam Riadi[2]
[1] Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Indonesia
[2] Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Indonesia

INFORMASI ARTIKEL

Riwayat Artikel:

Dikirimkan 14 Februari 2020,
Direvisi 02 Juni 2020,
Diterima 03 Januari 2021.

Kata Kunci:

IDS,
Snort,
HIDS,
DOS,
DDOS,
Keamanan Jaringan Komputer.

Penulis Korespondensi:

Rio Widodo, Imam Riadi
Universitas Ahmad Dahlan,
Kampus 4 UAD, Jln. Ring Road Selatan, Tamanan, Banguntapan, Bantul, D.I Yogyakarta, Indonesia.

Surel/Email:
rio1300022033@webmail.uad.ac.id
imam.riadi@mti.uad.ac.id

***ABSTRACT* / ABSTRAK**

The openness of access to information raises various problems, including maintaining the validity and integrity of data, so a network security system is needed that can deal with potential threats that can occur quickly and accurately by utilizing an IDS (intrusion detection system). One of the IDS tools that are often used is Snort which works in real-time to monitor and detect the ongoing network by providing warnings and information on potential threats in the form of DoS attacks. DoS attacks run to exhaust the packet path by requesting packets to a target in large and continuous ways which results in increased usage of CPU (central processing unit), memory, and ethernet or WiFi networks. The snort IDS implementation can help provide accurate information on network security that you want to monitor because every communication that takes place in a network, every event that occurs and potential attacks that can paralyze the internet network are monitored by snort.

Keterbukaan akses informasi memunculkan berbagai masalah antara lain pemeliharaan validitas dan integritas data sehingga diperlukan suatu sistem keamanan jaringan yang dapat menanggulangi potensi ancaman yang dapat terjadi secara cepat dan akurat dengan memanfaatkan IDS (*intrusion detection system*). Salah satu perangkat IDS yang sering digunakan adalah *Snort* yang bekerja secara *real-time* memonitor dan mendeteksi jaringan yang sedang berlangsung dengan memberikan peringatan dan informasi terhadap potensi ancaman berupa serangan DoS. Serangan DoS berjalan untuk menghabiskan jalur paket dengan meminta paket kepada suatu target secara besar dan secara terus menerus yang berdampak pada meningkatnya penggunaan CPU (*central processing unit)*, *memory*, dan jaringan *ethernet* ataupun *WiFi*. Pengimplementasikan IDS *snort* dapat membantu memberikan informasi akurat terhadap keamanan jaringan yang ingin dipantau karena setiap komunikasi yang berlangsung dalam suatu jaringan, setiap event yang terjadi dan potensi serangan yang dapat melumpuhkan jaringan internet terpantau oleh *snort*.

Sitasi Dokumen ini:

R. Widodo and I. Riadi, "Intruder Detection Systems on Computer Networks Using Host Based Intrusion Detection System Techniques," *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 3, no. 1, pp. 21-30, 2021. DOI: 10.12928/biste.v3i1.1752

1. PENDAHULUAN

Seiring dengan keterbukaan akses informasi memunculkan berbagai masalah pada keamanan jaringan, di antaranya menyangkut validitas dan integritas data [1]. Penggunaan internet yang terus meningkat tentu harus di imbangi pula dengan membuat sistem keamanan jaringan yang bagus dengan kecepatan yang lebih baik. Hal tersebut tentu tidak lain karena keterbatasan kemampuan manusia yang sudah tidak memungkinkan lagi melakukan pemantauan terhadap kemanan jaringan komputer secara manual oleh manusia. Sistem yang dapat digunakan untuk menjawab kebutuhan tersebut sangat diperlukan, terlebih untuk menaggulangi ancaman-ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat [2]. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan. Keamanan jaringan yang diharapkan dapat membantu meringankan kerja manusia dalam melakukan pengawasan terhadap jaringan komputer secara *real time* dengan cepat dan tepat, juga diharapkan mampu bertugas memberikan peringatan apabila terjadi upaya penyusupan yang bisa merugikan dan melemahkan keamanan jaringan.

Sistem keamanan jaringan menjadi faktor penting untuk menjamin stabilitas, integritas dan validitas data maka perlu adanya fungsi pengamanan, salah satu cara yang dapat digunakan adalah dengan memanfatkan IDS (*intrusion detection system*) yang dibuat dan dikembangkan oleh Martin Roesch [3]. IDS mampu mendeteksi adanya tindakan ancaman yang memaksa masuk pada suatu jaringan atau melakukan sabotase data dan infromasi, selanjutnya IDS akan mengirimkan informasi yang terjadi pada *administrator* jaringan [4]. Dilihat dari kemampuannya, IDS dibagi menjadi dua yaitu NIDS atau *network-based intrusion detection system* dan HIDS atau *host-based intrusion detection system* [5]. NIDS dapat melakukan pengawasan dan menganalisa trafik pada keseluruhan sub jaringan dan melakukan proses *capturing* pada semua trafik, sedangkan HIDS pada fungsinya melakukan pengawasan dan menganalisa trafik jaringan yang berasal dan keluar dari sbuah *host* dimana perangkat IDS diimplementasikan. Secara garis besar HIDS hanya melakukan pengawasan spesifik *host* saja sedangkan NIDS seluruh *subnet*.

Snort adalah perangkat lunak berbasis IDS yang *open source* dan dapat diimplementasikan sebagai alat pendeteksi intrusi atau serangan pada jaringan komputer. *Snort* dirancang beroperasi dalam *command line* dan diintegrasikan ke beberapa aplikasi pihak ketiga dan sudah mendukung *cross platform* seperti Linux dan Windows [6]. *Snort* banyak digunakan untuk mengamankan sebuah jaringan dari aktifitas yang berbahaya. Cara kerja *snort* mirip dengan TcpDump, tetapi fokus sebagai *security packet sniffing*. Fitur utama *snort* yang membedakan dengan TcpDump adalah *payload inspection*, dimana *snort* melakukan analisis *payload rule set* yang disediakan [7]. Kehandalan *snort* sebagai alat pendeteksi intrusi sangat bergantung pada pengaturan jaringan dan *rules* yang di buat dan diintegrasikan pada *host* maupun target serangan yang akan dilindungi. *Rule snort* sangat berdampak pada kehandalan *snort* itu sendiri dalam kemampuanya mengamankan jaringan dari ancaman yang terjadi. *Rules* membuat *snort* mampu mendeteksi serangan dengan mengenali *signature* yang telah di atur untuk fokus bekerja mendeteksi *ip*, *port*, protokol maupun jenis serangan yang digunakan dengan menutup akses paket data yang berasal dari penyusup dengan *signature* yang telah ditentukan.

Firewall adalah sebuah sistem keaamanan yang sudah diberikan dan ditanam dalam sistem operasi dalam hal ini adalah sistem operasi Windows untuk membantu dalam pengamanan jaringan, akan tetapi sekarang ini hanya dengan *firewall* keamanan belum sepenuhnya terjamin. Karena telah berkembang teknologi IDS untuk membantu pengamanan data dan jaringan [8]. Oleh karena itu, penerapan IDS *snort* merupakan salah satu solusi yang dapat digunakan untuk membantu pengaturan jaringan dalam memantau kondisi jaringan dan menganalisa paket-paket berbahaya yang terdapat dalam jaringan tersebut, hal tersebut bertujuan untuk mencegah adanya penyusup tanpa adanya hak akses [1].

Serangan DoS sudah berkembang menjadi serangan yang terdistribusi yang biasa disebut DDoS (*Distributed Denial of Services*) [9]. Adapun macam-macam serangan *DoS attack* yang sering digunakan yaitu *SYN-Flooding, SMURF attack, UDP-Flooding, ICMP-Flooding, dan DNS-Flooding*. Pengujian pada sistem IDS dilakukan dengan beberapa pola serangan untuk menguji kehandalan *snort* dalam mendeteksi serangan DoS. Berdasarkan pada hasil pengujian sistem *snort* IDS dengan menggunakan metode *ping* dan LOIC, *snort* bekerja dengan baik sehingga mampu memberikan peringatan serangan. Berdasarkan pada pembahasan permasalahan yang telah dijabarkan diatas, maka pada penelitian ini peneliti memilih judul "Sistem Deteksi Penyusup Pada jaringan Komputer Menggunakan Teknik *Host Based Intrussion Detection System* (HIDS)".

2. METODE PENELITIAN

Perangkat lunak yang digunakan pada penelitian ini adalah *snort* yang berfungsi sebagai IDS dan berjalan di atas sistem operasi Windows 10. Perangkat lunak pendukung lainnya seperti WinPcap, Notepad++ untuk mengedit *snort rules*, dan *softawre* LOIC (*Low Orbit Ion Cannon*) yang digunakan untuk melakukan serangan kepada *client* atau komputer target. Adapun perangkat keras yang diperlukan berupa tiga komputer laptop, satu komputer laptop *host* yang diinstal dengan *snort* IDS difungsikan sebagai *bridge* atau jembatan antar dua komputer lain agar saling terhubung. Komputer *host* memiliki spesifikasi yang cukup

untuk dapat menjalankan sistem operasi Windows 10 v1903. Dua komputer laptop lainnya difungsikan sebagai penyerang dan komputer target. Selain menggunakan tiga komputer laptop untuk pengujian digunakan juga perangkat jaringan lain.

Penelitian ini diawali dengan melakukan analisis sistem berupa analisis kebutuhan, tahap selanjutnya adalah melakukan perancangan sistem kemudian dilakukan tahap instalasi sistem. Setelah proses instalasi selesai, selanjutnya adalah mengkonfigurasi sistem sengan perangkat jaringan lainnya agar memastikan bahwa semua komponen dapat saling terhubung dan bekerja dengan baik. Proses pengujian dilakukan dengan cara melakukan serangan terhadap komputer target yang dimonitor dan dilindungi oleh sistem IDS.

2.1. Alat Penelitian

Alat penelitian yang digunakan terdiri dari perangkat keras yang digunakan untuk pengambilan data serangan berupa tiga komputer yang terhubung menggunakan metode komunikasi sambungan tiga arah atau disebut juga (*three-way handshake*) [10]. Komputer *host* akan berfungsi sebagai *bridge* untuk menjembatani komunikasi antara komputer *client* dan komputer penyerang, artinya semua aktivitas komunikasi akan melalui komputer *host*. Selain menjembatani sambungan komputer *host* juga berfungsi membagi layanan jaringan internet untuk kedua komputer lain yang sedang tersambung. Alat lain yang digunakan; kabel UTP (*Unshielded twisted-pair*) RJ-45 bertipe *cross-over*, dan perangkat *adaptor* LAN *to* USB. Sedangkan perangkat lunak yang digunakan adalah *snort* dan *snort rules*, WinPcap, Notepad++ untuk mengedit *snort rules*, dan *softawre* LOIC (*Low Orbit Ion Cannon*).

2.2. IDS

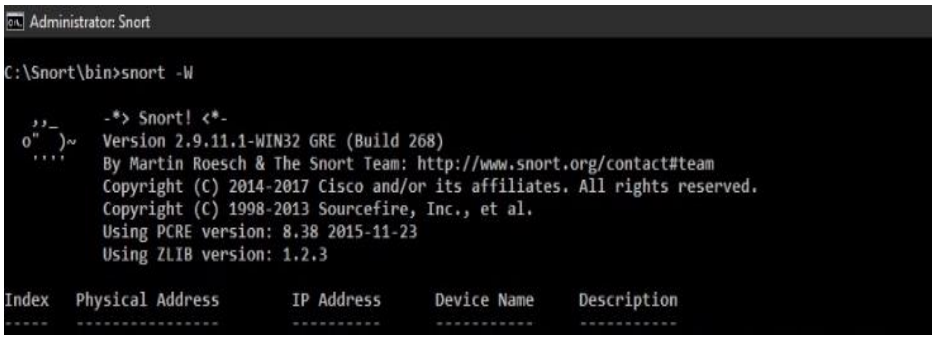
IDS (*Intrusion Detection System*) adalah suatu sistem keamanan yang berguna mendeteksi intrusi yang dilakukan oleh penyusup dalam jaringan komputer. Pada dasarnya IDS mirip seperti *alarm*, apabila IDS mencatat adanya serangan atau gangguan dalam suatu jaringan, maka IDS akan memperingati *administrator* jaringan dengan mengirimkan *alert* ataupun notifikasi.

2.3. HIDS

HIDS (*Host-based Intrusion Detection System*) adalah salah satu kemampuan dari IDS. HIDS adalah sistem yang hanya melakukan pemantauan pada *host* tempat *Intrusion Detection System* diimplementasikan. Aktivitas sebuah *host* jaringan individu akan dipantau apakah terjadi percobaan serangan atau penyusupan ke dalamnya atau tidak. Pengaplikasian *Host-based Intrusion Detection System* biasanya sering diletakkan pada *server* jaringan yang kritis seperti halnya *firewall*, *web server*, atau *server* yang terkoneksi ke internet [5].

2.4. SNORT

Snort adalah sebuah perangkat lunak *open source* bersifat *intrusion detection system* (IDS). *Snort* digunakan untuk pemantauan sistem keamanan jaringan. *Snort* akan mendeteksi serangan atau paket data yang masuk ke dalam jaringan dan memperingatkan *administrator* jaringan untuk mengambil tindakan pencegahan. Tampilan awal *Snort* ditunjukkan pada Gambar 1**.**



Gambar 1. Tampilan Awal *Snort*

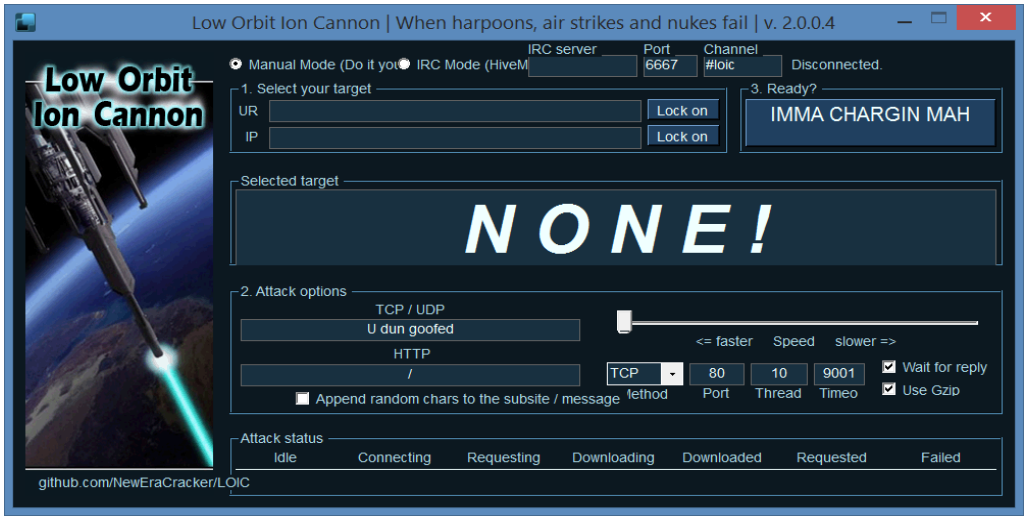
2.5. DOS

DoS (*Denial of Service*) adalah jenis serangan yang bekerja dengan cara menghabiskan sumber daya yang dimiliki oleh komputer target hingga komputer tidak dapat menjalankan fungsinya dengan benar.

2.6. LOIC

LOIC (*Low Orbit Ion Cannon*) adalah sebuah perangkat lunak yang dibuat dan dikembangkan secara terbuka dan digunakan untuk melakukan serangan DoS. Cara kerja LOIC adalah membanjiri *url* atau alamat

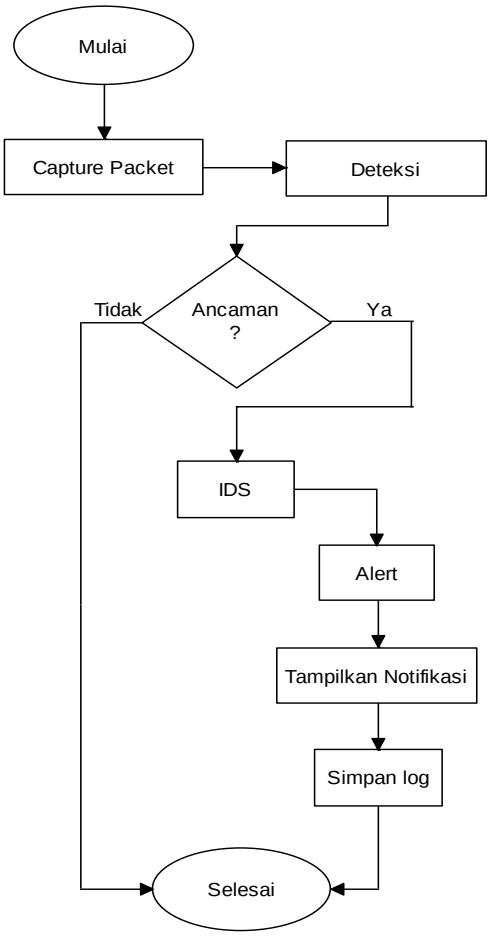
jaringan target dengan paket TCP-*flooding* dan UDP-*flooding* secara terus menerus dan berskala besar. Tampilan awal LOIC ditunjukkan oleh Gambar 2.



Gambar 2. Tampilan Awal LOIC

2.7. Diagram Alir

Diagram alir atau *flowchart* menjelaskan proses kerja sistem hingga dapat melakukan tugasnya sebagai alat pendeteksi serangan. *Snort* akan melakukan *capture packet* dan memindai paket yang masuk dan keluar melaluinya. Pada penelitian ini *snort* diintegrasikan pada komputer *host* sehingga *snort* akan menjembatani komunikasi kedua komputer target dan komputer penyerang. Proses pendeteksian serangan ditunjukkan Gambar 3.



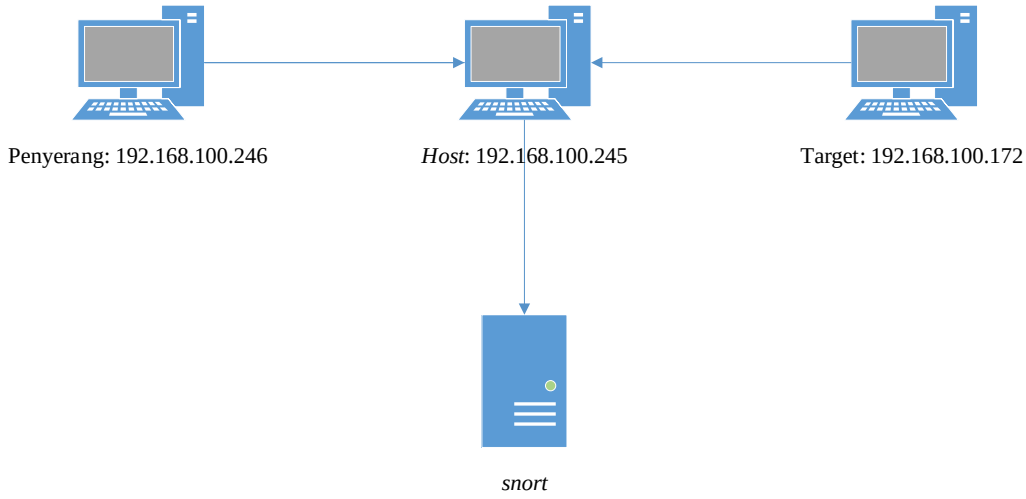
Gambar 3. Diagram Alir Sistem Pendeteksian Serangan dan *Alert*

Snort IDS memulai proses pendeteksian serangan dengan mengambil data paket dari komunikasi yang berlangsung antar komputer *client* atau target dengan komputer penyerang, selanjutnya *snort* akan memilah data paket menjadi potensi ancaman dan bukan ancaman. Jika *Snort* IDS menemukan paket yang berbahaya maka *Snort* akan mengirimkan *alert* atau peringatan kepada *administrator* jaringan dengan menampilkan notifikasi pada layar *command line*, kemudian *Snort* secara otomatis akan menyimpan hasil pendeteksian dalam *log* serangan yang dapat ditampilkan oleh *administrator* jaringan untuk proses mitigasi.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Simulasi Serangan

Snort ditempatkan dalam jaringan yang berfungsi mendeteksi serangan pada komputer yang akan dipantau. Dalam hal ini, *snort* akan menyadap semua lalu lintas data yang masuk dan keluar melalui sistem *snort*. *Snort* yang diinstal pada komputer yang berfungsi sebagai *bridge*, ditunjukkan Gambar 4.



Gambar 4. Rancangan Sistem *Snort*

Proses instalasi *snort* pada Windows dapat dilakukan dengan *offline*. Setelah proses instalasi, tahap konfigurasi dilakukan agar *snort* dapat memantau jaringan dari sistem yang akan dilindungi oleh *administrator*. Pada penelitian ini alamat jaringan yang ingin dilindungi adalah 192.168.100.172. Langkah konfigurasi dilakukan terhadap file *snort.conf* yang terletak di direktori *\snort\etc* dengan mengeksekusi perintah:

snort -i 1 -c c:\snort\etc\snort.conf -T

Alamat jaringan yang akan dilindungi telah sebelumnya di tentukan dan di set di file *snort.conf* pada proses konfigurasi, yang ditulis di bagian:

 # Setup the network addresses you are protecting
ipvar HOME_NET 192.168.100.172/24

Alert yang ditampilkan oleh *snort* di tentukan pada file *local.rules* yang berisi *rules* yang akan dibuat, diuji dan disertifikasi oleh *snort*. *Rules* ini berisi *alert* serangan dari TCP-*flooding*, UDP-*flooding*, dan ICMP-*flooding*. Skema serangan pada penelitian ini menggunakan tiga metode serangan yaitu TCP-*flooding*, UDP-*flooding*, dan ICMP-*flooding*. Serangan TCP-*flooding* dan UDP-flooding memanfaatkan *software* LOIC dengan menyerang komputer target dengan alamat jaringan 192.168.100.172.

3.1.1 Serangan Pertama

Skema serangan pertama menggunakan metode serangan TCP-*flooding*. Serangan ini akan melakukan pengiriman banyak paket sehingga akan membanjiri sesi koneksi ke alamat jaringan target menggunakan *software* LOIC. Skema serangan TCP-*flooding* ditunjukkan Gambar 5.

Gambar 5. Serangan TCP-*flooding*

Serangan menggunakan metode serangan TCP-*flooding* ke alamat jaringan target 192.168.100.172 dengan jumlah paket sebanyak 100 *thread*, artinya dalam satu detik alamat jaringan tujuan mendapatkan permintaan paket sebanyak 100 paket dengan set kecepatan serangan pada posisi tercepat melalui *port* 80. Serangan akan otomatis berhenti ketika telah menempuh waktu selama 9001 detik. Hasil serangan ditunjukkan Gambar 6.

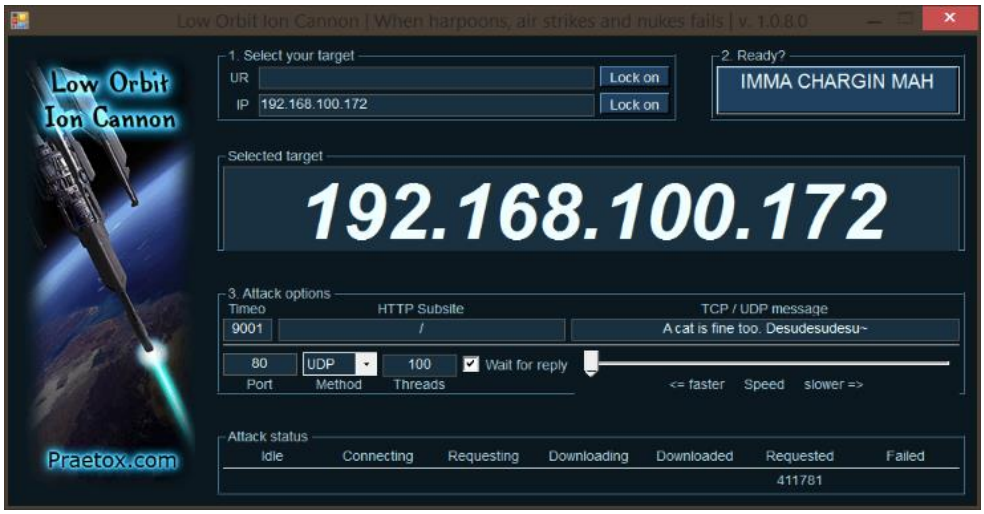
```
Commencing packet processing (pid=216)
01/27-16:01:20.481962  [**] [122:3:1] (portscan) TCP Portsweep [**] [Classification: Attempted Information Leak] [Priority: 2] {
0.172
01/27-16:01:25.972446  [**] [1:10001:1] Terdeteksi TCP DoS [**] [Priority: 0] {TCP} 192.168.100.246:53384 -> 192.168.100.172:80
01/27-16:01:32.810276  [**] [1:10001:1] Terdeteksi TCP DoS [**] [Priority: 0] {TCP} 192.168.100.246:53427 -> 192.168.100.172:80
```

Gambar 6. *Alert* Serangan TCP

Alert menunjukkan bahwa alamat jaringan 192.168.100.246 melalui *port* 53384 dan *port* 53427 melakukan dua serangan DoS berupa TCP-*flooding* tehadap komputer dengan alamat jaringan 192.168.100.172.

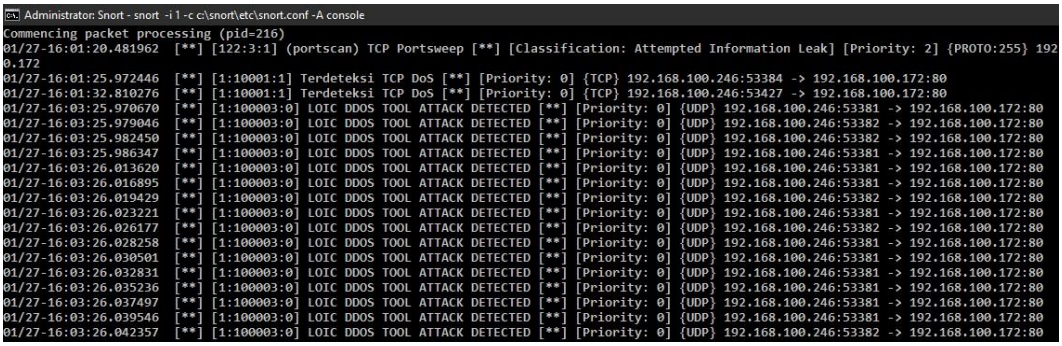
3.1.2. Serangan Kedua

Skema serangan kedua menggunakan metode serangan UDP-*flooding*. Serangan ini akan melakukan pengiriman sejumlah besar paket ke alamat jaringan target dengan tujuan membanjiri kemampuan perangkat target untuk memproses dan merespon tiap *event*. Serangan ini sama dengan serangan Pertama menggunakan *software* LOIC. Skema serangan TCP-*flooding* ditunjukkan Gambar 5.



Gambar 7. Serangan UDP-*flooding*

Tujuan serangan adalah komputer dengan alamat jaringan 172.168.100.172 dengan metode serangan UDP-*flooding* secara terus menerus dengan jumlah *thread* 100 per detik melalui *port* 80, dan serangan akan otomatis berhenti ketika telah melalui waktu selama 9001 detik. Hasil dari serangan ini ditunjukkan oleh Gambar 8.

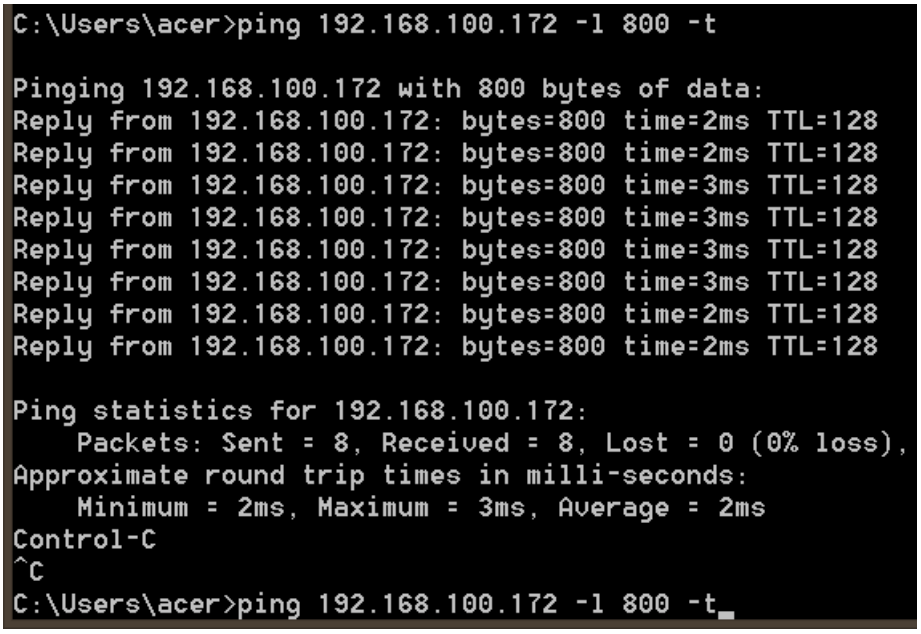


Gambar 8. *Alert* Serangan UDP

Alert menampilkan bahwa terjadi serangan DOS berupa UDP-*flooding* dari alamat jaringan 192.168.100.246 tehadap komputer dengan alamat jaringan 192.168.100.172. Serangan tersebut terkirim dengan sangat cepat dengan meminta paket yang besar secara bersamaan dan terus-menerus terhadap komputer target.

3.1.3. Serangan Ketiga

Tidak seperti pada kedua serangan yang telah dilakukan sebelumnya, pada serangan ketiga ini dilakukan melalui jendela *command line*. Serangan ketiga ini menjalankan permintaan paket *ping* secara terus-menerus atau sering disebut dengan istilah *ping-flood attack*, menggunakan perintah *-T* yang ditunjukkan oleh Gambar 9.



Gambar 9. Perintah Serangan Melalui *Command Line*

Penyerang meminta paket sebesar 800 *bytes* terhadap alamat jaringan 192.168.100.172. Paket yang terkirim adalah sebanyak 8 paket dengan waktu *delay* minimum selama 2 ms dan *delay* maksimum selama 3 ms, maka rata-rata *delay* dari paket sebesar 8 paket adalah selama 2 ms. Sistem *snort* kemudian menampilkan *alert* yang ditunjukkan Gambar 10.

Gambar 10. *Alert* Serangan

Alert yang ditunjukkan Gambar 10, menampilkan metode serangan ICMP, dan reaksi *snort* terhadap serangan ditandai dengan menampilkan pesan "terdeteksi PING BESAR". Pesan tersebut di buat dengan memodifikasi *rule alert*. Penentuan besar atau kecilnya paket serangan PING oleh *snort* dibedakan dari besaran jumlah paket yang diminta oleh penyerang. Jika paket yang diminta >600 *bytes* maka *snort* akan menampilkan *alert* dengan kode BESAR, dan paket serangan <600 akan diidentifikasi sebagai permintaan serangan paket KECIL.

Berdasarkan pada hasil pengujian serangan satu, serangan dua, dan serangan tiga terlihat bahwa IDS *snort* dapat mengenali paket data yang masuk dan keluar melaluinya. *Snort* berhasil mananpilkan pesan peringatan sesuai dengan *rule* yang sudah ditentukan pada saat proses konfigurasi. Agar kemampuan *snort* dapat terus optimal dan dapat bekerja dengan baik maka *rule snort* harus selalu diperbarui, hal ini agar *snort* dapat mengenali intrusi jenis baru. Pada sistem dengan *snort* lebih banyak menghasilkan *alert yang* berupa *false positive* atau paket yang sebetulnya belum tentu paket berbahya namun dianggap sebagai paket berbahya oleh *snort*. Akibatnya *log alert* yang dihasilkan lebih banyak.

3.2. Analisis Hasil Serangan

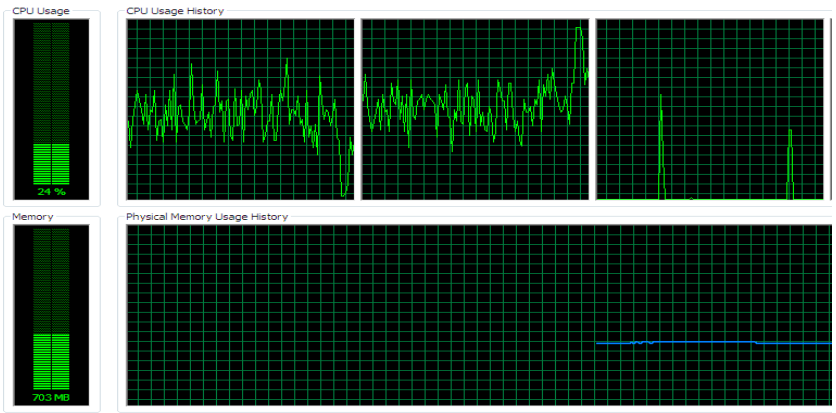
Berdasarkan pada hasil dari ketiga serangan yang telah dilakukan, kemudian di dapat data serangan berbeda yang ditunjukkan pada Tabel 1.

Tabel 1. Jumlah *Alert* Serangan Terdeteksi

Jenis serangan	Jumlah serangan yang ditangkap	Waktu
TCP	966 serangan	10 menit 55 detik
UDP	179.049 serangan	10 menit 55 detik
ICMP	283 serangan	10 menit 55 detik

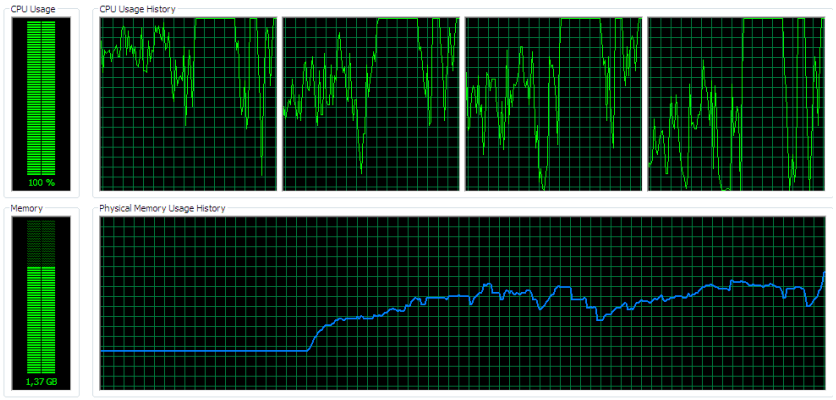
Berdasarkan pada Tabel 1, didapatkan hasil serangan dari ketiga metode serangan yang telah dilakukan dengan jumlah serangan TCP mencapai 966 serangan, UDP sebanyak 179.049 serangan, dan metode serangan ICMP sebanyak 283 serangan, selama 10 menit 55 detik secara bersamaan.

Dampak serangan yang dapat dirasakan secara langsung oleh komputer target adalah meningkatnya penggunaan CPU, memori, dan *bandwidth* yang terpakai saat komputer target menerima serangan. Hal ini ditunjukkan pada Gambar 11. Gambar 11 menunjukkan persentase penggunaan CPU sebelum komputer target di serang dengan metode LOIC dan melalui jendela *command line*. Berdasarkan pada Gambar 11 terlihat bahwa penggunaan CPU berkisar antara 24-25% saja.



Gambar 11. Penggunaan CPU Sebelum Serangan Dilakukan

Berdasarkan pada Gambar 12, menunjukkan penggunaan CPU pada komputer target setelah menerima serangan naik menjadi berkisar 90-100%.



Gambar 12. Penggunaan CPU Setelah Serangan Dilakukan

Berdasarkan pada Gambar 11 dan Gambar 12 diketahui dampak sebelum dan sesudah dilakukan serangan menunjukkan peningkatan lebih tinggi dalam penggunaan CPU, memori dan *bandwidth*. Kinerja CPU mencapai nilai tertinggi 100%, memori yang terpakai sebesar 1,17 GB dari total jumlah keseluruhan 2 GB. Hal ini membuktikan bahwa sifat serangan DoS menghabiskan jalur paket dengan meminta paket terhadap target secara besar maka dalam jangka waktu yang cukup lama dapat membuat performa komputer menurun bahkan *down*. Namun dengan pemanfaatan sistem *snort* yang terkonfigurasi dengan jaringan komputer, *administrator* akan sedikit terbantu dengan mengetahui apa yang membuat performa komputer dan *bandwidth* turun sehingga dapat dilakukan langkah penanganannya.

4. KESIMPULAN

Berdasarkan hasil penelitian yang berjudul "Sistem Deteksi Penyusup Pada Jaringan Komputer Menggunakan Teknik *Host Based Intrusion Detection* System (HIDS)" ini, di dapatkan data penelitian: *snort* berhasil mendeteksi serangan yang melalui protokol TCP sebanyak 966 paket, UDP sebanyak 179.049 paket, dan ICMP sebanyak 283 paket. Dampak dari serangan DoS menggunakan perangkat lunak LOIC dan dengan menggunakan *command line* dengan metode serangan *ping flood* membuat performa komputer target menurun. Hal ini di buktikan dengan penggunaan CPU yang naik dari 24% menjadi 90% sampai 100%, dan penggunaan memori juga mengalami kenaikan dari 703 MB menjadi sebesar 1,17 GB. Hal ini membuktikan bahwa serangan DoS akan menghabiskan jalur paket dengan meminta paket terhadap target secara besar, apabila waktu serangan kepada target terjadi dalam waktu yang lama tidak hanya dapat membuat performa komputer menurun bahkan bisa menyebabkan komputer target *down*.

UCAPAN TERIMA KASIH

Ucapan terima kasih kepada *editor* dan *reviewer* atas segala saran, masukan dan telah membantu dalam proses penerbitan naskah. Ucapan terima kasih juga ditunjukkan kepada pihak-pihak yang telah mendukung penelitian dan memberikan bantuan moral dan material.

REFERENSI

[1] F. N. R. Muh. Husain, A. I.M Akasara, "Implementasi Keamanan Server Pada Jaringan Wireless Menggunakan Metode Intrusion Detection and Prevention System (Idps) (Studi Kasus : Techno'S Studio)," *semanTIK*, vol. 4, no. 2, pp. 11–20, 2018, DOI: https://doi.org/10.5281/zenodo.1407864

[2] D. A. Nugroho, A. F. Rochim, and E. D. Widianto, "Perancangan dan Implementasi Instrusion Detection System di Jaringan Universitas Diponegoro," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, p. 171, 2015. DOI: https://doi.org/10.14710/jtsiskom.3.2.2015.171-178

[3] M. Affandi and S. Setyowibowo, "Implementasi Snort Sebagai Alat Pendeteksi Intrusi Menggunakan Linux," *J. Teknol. Inf.*, vol. 4, no. 2, 2013. Online

[4] W. Fathoni, Fitriyani, and G. N. Nurkahfi, "Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Ids Snort," *e-Proceeding Eng.*, vol. 3, no. 1, pp. 1169–1172, 2016. Online

[5] I. A. Sobari, "Rancangan Wireless Intrusion Detection System Menggunakan Snort," *J. Techno Nusa Mandiri*, vol. 12, no. 1, pp. 1–9, 2015. Online

[6] A. P. Wicaksono, J. Raya, D. Po, and B. Purwokerto, "Sistem Deteksi Intrusi dengan Snort (Intrusion

Detection System with Snort)," *JUITA - J. Inform.*, vol. 3, no. 1, pp. 31–34, 2014, doi: https://doi.org/10.30595/juita.v3i1.850
[7] E. K. Dewi, "Analisis Log Snort Menggunakan Network Forensic," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 2, no. 2, pp. 72–79, 2017, doi: https://doi.org/10.29100/jipi.v2i2.370
[8] N. Sahrun, R. Roestam, and D. Sarjon, "Pengembangan Sistem Keamanan Jaringan Komputer Melalui Perumusan Aturan (Rule) Snort untuk Mencegah Serangan Synflood," *SATIN - Sains dan Teknol. Inf.*, vol. 1, no. 2, pp. 25–31, 2015. Online
[9] R. Hermawan, "Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)," *Fakt. Exacta*, vol. 5, no. 1, pp. 1–14, 2013. Online
[10] A. Fadlil, I. Riadi, and S. Aji, "Review of detection DDOS attack detection using naive bayes classifier for network forensics," *Bull. Electr. Eng. Informatics*, vol. 6, no. 2, pp. 140–148, 2017, doi: https://doi.org/10.11591/eei.v6i2.605

BIOGRAFI PENULIS

Rio Widodo Lahir di Riau. Menyelesaikan pendidikan S1 Program Studi Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan Yogyakarta.

Imam Riadi Lahir di Kudus. Menyelesaikan pendidikan S1 Pendidikan Teknik Komputer/Teknik Elektro di Universitas Negeri Yogyakarta, S2 dan S3 Ilmu Komputer di Universitas Gajah Mada Yogyakarta dengan judul Disertasi "Framework Untuk Forensik Internet Menggunakan k- means Clustering dan Horizontal Partitioning". Saat ini beliau adalah dosen aktif di Program Studi Sistem Informasi Universitas Ahmad Dahlan Yogyakarta.