Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 21, No. 3, July 2022, pp. 567∼582
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v21i3.1732

Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi *Proprietary*

Network Forensics DDoS Attack using ADDIE and HIDS Method on Proprietary Operating System

Sri Suharti[1], **Anton Yudhana**[2], **Imam Riadi**[3]
Universitas Ahmad Dahlan, Indonesia

Informasi Artikel

Genesis Artikel:

Diterima, 29 Januari 2022
Direvisi, 29 April 2022
Disetujui, 30 Mei 2022

Kata Kunci:

DDoS
Firewall
HIDS
Sistem Operasi
Snort

ABSTRAK

Forensik jaringan sangat dibutuhkan dalam mempertahankan kinerja jaringan komputer dari serangan *Distributed Denial of Service* (DDoS). Penelitian ini bertujuan untuk mendapatkan bukti *digital* keakurasian tool DDoS, keberhasilan metode HIDS dan implementasi *firewall* pada *Network layer* dalam menghentikan DDoS. Metode penelitian ini menerapkan ADDIE (*Analyze*, *Design, Develop, Implement and Evaluate*) dan *Host-Based Intrusion Detection System* (HIDS) *Snort* pada simulasi jaringan berbasis lokal dan luas. Hasil pengujian menyatakan Slowloris merupakan DDoS paling melumpuhkan *web server* IIS pada sistem operasi *proprietary* dengan penurunan performa *server* sebesar 78%, akurasi peningkatan trafik jaringan sebesar 92,84% *alert* 150 kali. Implementasi *firewall* pada *network layer* dalam menghentikan DDoS memiliki keberhasilan sebesar 98.91%. Hal ini menunjukkan metode ADDIE berhasil diterapkan dalam penelitian dan menyatakan DDoS pelumpuh *server* berhasil dideteksi pada metode HIDS dan berhasil dihentikan oleh *firewall* pada sistem operasi *proprietary*.

Keywords:

DDoS
Firewall
HIDS
Operating System
Snort

ABSTRACT

Network forensics is needed in defending computer networks from Distributed Denial of Service (DDoS) attacks. This study aims to obtain digital evidence of the accuracy of the DDoS tool, the success of the HIDS method and the implementation of the firewall at the Network layer in successful DDoS. This research method applies ADDIE (Analyze, Design, Develop, Implement and Evaluate) and Host-Based Intrusion Detection System (HIDS) Snort on local and wide-based network simulations. The test results state that Slowloris is the deadliest DDoS for the IIS web server on the proprietary operating system with a 78% decrease in server performance, an increase in network traffic accuracy of 92.84%, 150 warnings. Firewall implementation at the network layer in the success of DDoS has a success of 98.91%. This shows that the ADDIE method was successfully applied in the study and stated that the DDoS disabler server successfully detected the HIDS method and was successfully stopped by the firewall on the proprietary operating system.

Penulis Korespondensi:

Sri Suharti,
Program Studi Informatika,
Universitas Ahmad Dahlan,
Email: sri2007048006@webmail.uad

1. PENDAHULUAN

Kebutuhan akan jaringan komputer menjadi prioritas bagi suatu instansi-instansi seperti perguruan tinggi, perbankan, rumah sakit, dan perusahaan, keberlangsungan jaringan komputer sangat bergantung pada *server* dan proses transmisi data. Transmisi data membutuhkan infrastruktur yang stabil akan tetapi infrastruktur jaringan juga berisiko terhadap serangan berbahaya [1]. Salah satu serangan yang paling berbahaya dan sangat menantang adalah DDoS yang melancarkan serangan dalam jumlah sangat besar dan terus meningkat mencapai *terabyte* [2–5]. Motif utama serangan DDoS adalah menurunkan kinerja server secara drastis karena kewalahan melayani banyak permintaan palsu untuk menguras server sehingga mengalami kemacetan total [6–8]. Kerugian dan kerusakan yang ditimbulkan DDoS cukup besar sfehingga menjadi ancaman serius bagi web server karena tidak hanya pada lapisan aplikasi tetapi juga menembus lapisan jaringan pada jaringan komputer [9–11]. Menurut Kaspersky DDoS Intelligence pada kuartal kedua menyatakan terjadi peningkatan sebesar 30% dari kuartal satu dengan rata-rata serangan sebanyak 300 per hari pada tanggal 9 April 2020. Pada tahun yang sama menurut Akmai serangan DDoS meningkat secara signifikan dengan jumlah paket 809 juta paket [12]. Menurut NETSCOUT Arbor pada bulan Maret 2018 terjadi serangan pada Github sebesar 1.3 Tbps dilakukan pada Domain Name Sistem (DNS) sebesar 81% dan dilakukan pada HTTP dan HTTPS sebesar 19% [13]. Beberapa perusahaan yang telah menjadi sasaran DDoS seperti *Amazon Web Service*, Github, CloudFlare, dan Bank of America. Saat ini *user* masih banyak yang menggunakan sistem operasi *proprietary* berlisensi seperti Windows mencapai 90,42%. Pada tahun 2020 serangan siber terjadi pada 10 industri besar yang meliputi sektor keuangan sebesar 23%, manufaktur 17,7% dan energi 10,2%. Pada tahun berikutnya yaitu tahun 2021 menurut data IBM *Security X-Force* terjadi *server access attack* sebesar 28% pada sektor keuangan dengan kerugian mencapai US $123 juta. Peningkatan DDoS menyebabkan kerugian besar sehingga membutuhkan riset-riset untuk mendeteksi terjadinya DDoS beserta cara menghentikannya.

Pada penelitian sebelumnya menyatakan bahwa dalam menjaga kinerja *server* harus memperhatikan keamanan *hardware* dan *software* serta keamanan jaringan. Penerapan *firewall* terintegrasi pada perangkat router memiliki keterbasan konfigurasi sehingga dibutuhkan aplikasi *firewall* yang terintegrasi pada router pada program terintegrasi metode Network Development Life Cycle (NDLC) [14]. Pada penelitian lain penerapan *Intrusion Detection System* (IDS) dan *Intrusion Prevetention System* (IPS) untuk penanganan DDoS untuk menemukan sumber serangan dengan metode penelitian laboratorium jaringan real pada sebuah perusahaan dan organisasi [15]. Pada penelitian lainnya menyatakan simulasi dilakukan dengan beberapa *tool* DDoS untuk mendapatkan hasil identifikasi, *log* dan analisis trafik sehingga ditemukan sumber serangan [16, 17]. Penghentian DDoS pada *tool* yang paling mematikan pada riset dapat menerapkan sistem keamanan jaringan berupa *firewall* untuk menyaring lalu lintas berbahaya [18].

Pada penelitian ini menerapkan dua variabel utama terdiri dari variabel tetap dan bebas, variabel tetap pada *firewall* pada router mikrotik dan variabel bebas pada tiga *tools* DDOS yang disimulasikan pada jaringan komputer area lokal dan luas. Penelitian ini tidak hanya menerapkan tool DDoS tetapi menganalisa keakurasian beberapa tool DDoS, metode yang digunakan dengan mengintegrasikan dua metode yaitu ADDIE dalam alur penelitian dan HIDS dalam simulasi deteksi serangan.

Forensik jaringan *Denial Distributed of Service* (DDoS) pada sistem operasi *proprietary Windows* mengimplementasikan *firewall network layer* untuk menghentikan serangan DDoS pada jaringan berbasis lokal dan luas. Metode penelitian ini menggunakan tahapan *Analyze, Design, Develop, Implement and Evaluate* (ADDIE) yang meliputi analisa kesenjangan trafik normal dan DDoS, perancangan desain *Host-Based Intrusion Detection System* (HIDS), pembangunan *web server* dalam jaringan lokal dan luas, selanjutnya melakukan proses penyerangan *web server* menggunakan *tool* DDoS yaitu LOIC UDP, LOIC TCP, PoD dan *Slowloris* serta implementasi *firewall* pada jaringan lokal dan luas. Alur metode ini diakhiri dengan pengukuran hasil pantauan trafik pada jaringan lokal dan luas. Analisa data pada penelitian ini dengan membandingkan hasil pemantauan secara menyeluruh baik dari jumlah paket dan jumlah *byte* paket sah dan paket tidak sah yang ter-*capture* pada aplikasi *Wireshark* serta banyak *allert snort* pada trafik normal dan DDoS. Hasil penelitian menunjukkan *Slowloris* merupakan *tool* paling melumpuhkan dengan menurunkan performa *server* sebesar 78% sehingga mengalami *down*. Berdasarkan hal tersebut maka penelitian ini memberikan solusi implementasi *firewall network layer* dan dinyatakan berhasil menghentikan DDoS dengan keefektifan rata-rata sebesar 98.91%. Untuk menjaga performa *server* diharapkan penelitian selanjutnya menerapkan *firewall application layer* dan *network layer* dengan metode *Host Intrusion Detection System* (HIDS) dan *Network Intrusion Detection System* (NIDS).

Susunan penulisan pada artikel ini yaitu bagian Pendahuluan yang berisi tentang perbedaan dari rujukan artikel terdahulu yang digunakan sebagai pembanding pada artikel ini, bagian ke 2. Metode Penelitian yang membahas tentang Metode ADDIE dan HIDS untuk mendapatkan hasil penelitian yang akurat, bagian ke 3. Hasil dan Analisis yang menjelaskan tentang hasil Analisa penelitian yang menggunakan metode ADDIE dan HIDS menggunakan *Wireshark* dan *Snort* saat terjadinya serangan DDoS pada *web server*, Bagian ke 4. Kesimpulan yang menjelaskan kesimpulan dari penelitian ini dan saran untuk peneitian berikutnya.

2. METODE PENELITIAN

Penelitian dan pengembangan pada Forensik DDoS ini mengadopsi teori Robert Maribe Branch (2009) yang memiliki lima urutan yaitu metode ADDIE yang terdiri dari tahapan *Analyze, Design, Develop, Implement and Evaluate*. Kelima urutan ini dintegrasikan dalam simulasi metode *Host-based Intrusion Detection System* (HIDS) tergambar pada langkah *Design* dalam jaringan berbasis lokal dan luas. Adapun lima urutan tersebut mengikuti dalam tahapan yang harus dilakukan guna mendapatkan hasil penelitian yang akurat terangkum pada Gambar 1.

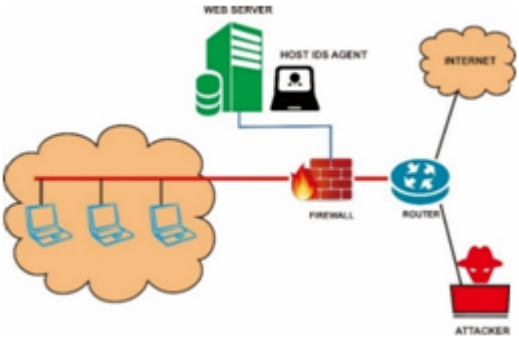
Gambar 1. Alur Metode ADDIE

2.1. *Analyze*

Analyze meliputi kegiatan pengenalan situasi dan kondisi trafik dan sistem keamanan jaringan *real time*, menentukan kesenjangan antara harapan dan kenyataan sebuah jaringan saat ini. Kesenjangan yang muncul dan teknik-teknik yang harus dilakukan untuk menentukan solusi tersebut. Saat ini kesejangan jaringan yang terjadi banyak disebabkan oleh serangan-serangan jaringan komputer atau dunia siber sehingga menimbulkan kerugian sangat besar dikarenakan *server* tidak dapat melayani permintaan klien dan serangan yang paling mematikan dan beresiko fatal yaitu DDoS.

2.2. *Design*

Design meliputi kegiatan merancang *design* penelitian yang akan dikerjakan yaitu melakukan simulasi pada jaringan komputer area lokal dan area luas dengan serangan DDoS pada *application layer* [19]. Serangan-serangan DDoS yang terjadi pada jaringan dipantau berdasarkan metode *Host-based Intrusion Detection System* (HIDS) *Snort* aktivitas yang mencurigakan percobaan penyerangan pada *web server* yang dibangun menggunakan *Internet Information Services* (IIS) di *application layer*. Metode ini diharapkan dapat menemukan sumber serangan sehingga dapat menentukan sebuah solusi yang tepat, pada penelitian menguji sebuah sistem keamanan jaringan berupa *firewall* dengan Mikrotik yang berbiaya rendah yang dibangun pada *network layer* [20–22]. Teknik analisa hasil penelitian menggunakan deteksi yang dinyatakan efektif dengan proses membandingkan saat tidak ada serangan dan ada serangan DDoS pada *application layer*, kondisi serangan DDoS tanpa *firewall* dan kondisi saat ada serangan DDoS dengan *firewall* pada *network layer* [23–25]. Metode HIDS Deteksi Serangan DDoS ditunjukkan Gambar 2.

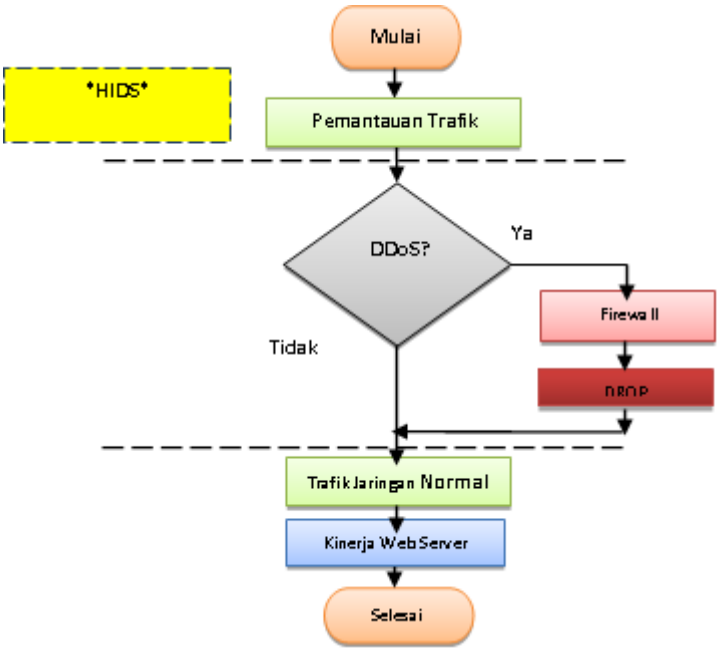


Gambar 2. Metode HIDS Deteksi Serangan DDoS

2.3. *Develop*

Develop meliputi pekerjaan simulasi DDoS pada jaringan berbasis lokal dan luas menggunakan tiga *tool* yaitu LOIC, *Slowloris* dan *Ping of Death* (PoD). Terjadinya DDoS ke *server* di pantau menggunakan metode *Host Intrusion Detection System* (HIDS) dengan

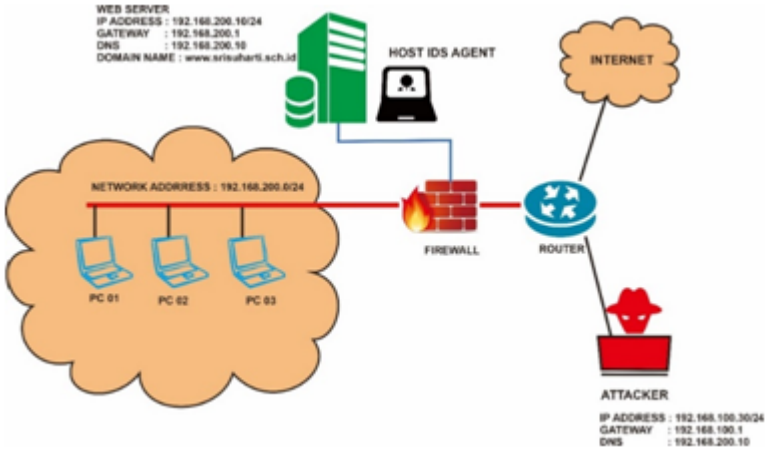
memasang *tool Wireshark* dan *Snort* pada *web server* lokal www.srisuharti1212.sch.id dan luas pada www.smknxxxx.sch.id. Apabila tidak ada alert atau tidak ada serangan maka trafik permintaan diteruskan dan dilayani oleh web server www.srisuharti1212.sch.id, apabila ada *alert* atau ada serangan maka akan di drop oleh *firewall*. Pengembangan alur dalam simulasi pada Gambar 3.



Gambar 3. Alur Metode HIDS pada DDoS

2.4. *Implement*

Implement meliputi kegiatan penggelaran kabel seperti yang terlihat pada topologi jaringan beserta sebaran pengalamatan *Internet Protocol* (IP) yang digunakan. Komputer penyerang memiliki pengalamatan IP 192.168.100.20/24 dengan *server* target 192.168.100.20/24. Simulasi sesuai topologi dan sebaran IP menerapkan penyerangan DDoS *tools* yaitu LOIC bekerja pada *Transmission Control Protocol/ Internet Protocol* (TCP/ IP) dan *User Datagram Protocol* (UDP), *Slowloris* bekerja pada *Hypertext Transfer Protocol* (HTTP) dan *Ping of Death* bekerja pada *Internet Control Message Protocol* (ICMP). Adapun topologi dengan sebaran Pengalamatan IP seperti pada Gambar 4.



Gambar 4. Topologi Jaringan dan pengalamatan IP

2.5. *Evaluate*

Evaluate meliputi kegiatan pengukuran pantaun trafik jaringan berbasis lokal dan luas berdasarkan metode *Host based Intrusion Detection System* (HIDS) menghasilkan data berupa banyak paket dan jumlah *byte* yang ter*capture* pada *Wireshark*. Hasil pantauan ini dianalisa membandingkan hasil pemantauan secara menyeluruh baik dari jumlah paket dan jumlah *byte* pada paket sah dan paket tidak sah. Adapun variabel dalam menghasilkan sebuah akurasi dengan persamaan (1).

$$Akurasi : (DD + NN)/(DD + NN + ND + DN) \quad (1)$$

Keterangan:
DD : Paket serangan DDos dan benar serangan DDoS
NN : Paket normal dan berupa paket normal
ND : Paket yang teridentifikasi paket normal tetapi serangan DDoS
DN : Paket yang teridentifikasi serangan DDoS tetapi paket normal

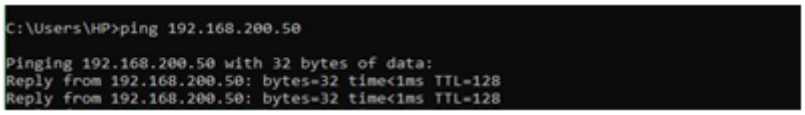
3. HASIL DAN ANALISIS

Pengujian dan analisa hasil informasi dari metode HIDS menggunakan *Wireshark* dan *Snort* saat terjadinya serangan DDoS pada *web server* terjadi pada tanggal 11 Juli 2021. Spesifikasi komputer *server* i3 dengan sistem operasi *proprietary Windows Server* 2019 dengan IP address 192.168.200.10/24, penyerang melakukan serangan dari PC3 dengan IP 192.168.100.20/24 dengan spesifikasi komputer i3 dengan OS Windows 10. Serangan dilakukan dengan tiga *tool* DDoS yaitu LOIC, *Slowloris* dan *Ping of Death* (PoD).

3.1. Uji Konektivitas Jaringan melalui *Command Prompt* saat Kondisi Normal

Persamaan harus ditempatkan di tengah baris dan diberikan secara berurutan dengan nomor persamaan dalam tanda kurung yang diluruskan ke *margin* kanan, seperti dalam (1). Penggunaan *Microsoft Equation Editor* atau *MathType* lebih disukai.

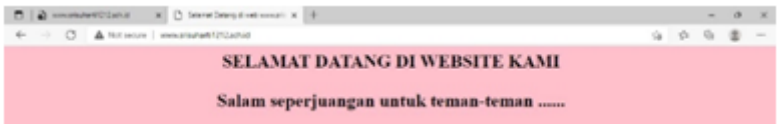
Sampling monitoring saat melalui *command prompt* saat trafik normal dengan uji konektivitas melalui *command prompt* CMD menunjukkan hasil *sampling* konektivitas antar perangkat dalam kondisi berjalan dengan baik ditunjukkan dengan hasil Reply form 192.168.200.10; bytes=32 time=2ms TTL=128 seperti pada Gambar 5.



Gambar 5. Uji Konektivitas Jaringan melalui CMD

3.2. Uji Koneksi ke *Web Server* Saat Kondisi Normal

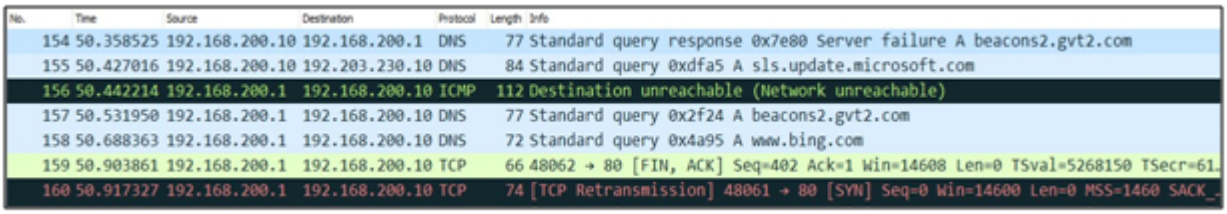
Sampling monitoring saat melalui halaman *web* dari domain www.srisuharti1212.sch.id dengan trafik normal menunjukkan hasil konektivitas ke *web server* www.srisuharti1212.sch.id dapat dilakukan dengan baik dengan tertampilnya halaman web dalam wakut kurang dari 50 detik , hal ini menunjukkan *server* dan trafik lancar tanpa ada gangguan, adapun tampilan halaman web www.srisuharti1212.sch.id. pada Gambar 6.



Gambar 6. Hasil Uji Koneksi melalui web www.srisuharti1212.sch.id

3.3. Hasil *Sampling Monitoring* pada *Wireshark*

Sampling monitoring trafik pada *Wireshark* menunjukkan pengambilan data lalu lintas jaringan menggunakan *Wireshark* dalam kondisi normal, ada serangan, ada serangan dengan tanpa *firewall* dan ada serangan dengan *firewall* dengan beberapa informasi antara lain waktu yang dibutuhkan, Alamat IP sumber, Alamat IP tujuan , Protokol , *Length of packet data* dan trafik terlihat pada sampling hasil *capture monitoring* trafik dari *Wireshark* seperti Gambar 7.



Gambar 7. *Sampling* Hasil *Capture Monitoring* Trafik dari *Wireshark*

3.4. *Sampling* serangan *Tool* DDoS

Serangan DDoS merupakan serangan yang sangat mematikan dan berbahaya melumpuhkan *webserver*, pada penelitian ini menggunakan DDoS yang bertipe *protocol* DDoS *Attack* dengan *tool* LOIC, *Slowloris* dan *Ping of Death*. LOIC dalam penelitian ini bekerja pada protokol TCP dan UDP, *Slowloris* bekerja pada protokol HTTP dan PoD bekerja pada protokol ICMP yang terakurasi pada jaringan berbasis lokal dan luas.

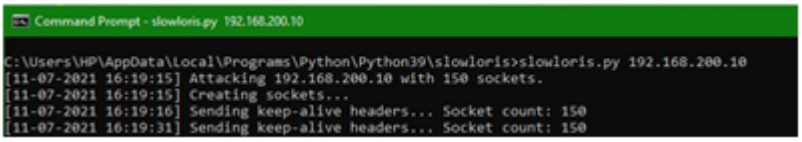
1. *Sampling* serangan *Tool* DDoS LOIC melalui protokol TCP dan UDP

Tool DDoS LOIC (*Low Orbit Ion Canon*), *tool* ini umumnya digunakan oleh *group hacker anonymous* dalam melakukan penyerangannya bekerja dengan memanfaatkan pelontar. Pada *tool* ini dengan cara memasukkan url atau IP *address web server* www.srisuharti1212.sch.id atau pada IP *address* 192.168.200.10, Serangan yang dikirim sebanyak 99 *threat* dan pada *Port* 80. Tipe serangan yang digunakan TCP dan UDP, serta melakukan *Imma Charging Mah Laser* untuk memulai penyerangan, pada LOIC ini tidak dapat menyembunyikan IP sumber sehingga IP dapat dapat terlacak. Adapun sampling serangan DDoS LOIC seperti pada Gambar 8.

Gambar 8. Sampling Tampilan Serangan DDoS melalui Tool LOIC

2. Sampling Serangan Tool DDoS Slowloris

DDoS dengan tool Slowloris ini merupakan serangan DDoS pada layer application, serangan DDoS pada Slowloris ini merupakan serangan DDoS dengan bandwith rendah sehingga pada filtering tidak terlalu kelihatan dalam volume jumlah paket dan bekerja pada protokol HTTP sehingga serangan Slowloris dari sebuah komputer diduga sangat dapat melumpuhkan web server. Slowloris membuka koneksi secara pada berulang melalui header HTTP dengan socket count 150. Adapun tampilan serangan DDoS Slowloris terlihat seperti Gambar 9.

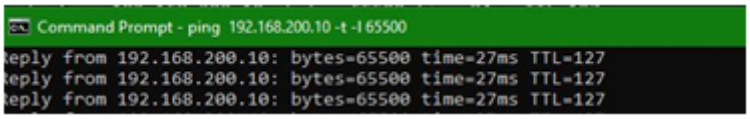


Gambar 9. *Sampling* Tampilan Serangan DDoS melalui *Tool Slowloris*

3. Serangan *Ping of Death* (PoD) pada *Internet Control Message Protocol* (ICMP)

Serangan DDoS PoD merupakan serangan DDoS yang bekerja pada *Internet Control Message Protocol* (ICMP) atau *Ping* yang sebenarnya merupakan sarana untuk menguji konektivitas jaringan dengan *Ping* paket yang biasa dikerjakan dalam ukuran sangat kecil.

Pada PoD ini menggunakan *ping* paket sebesar 65. 535 *Byte* pada batas maksimal yang diperbolehkan hal ini seperti pada Gambar 10.



Gambar 10. Tampilan Proses Penyerangan DDoS melalui PoD

3.5. Akurasi Serangan *Tool* DDoS pada Sistem Operasi *Proprietary*

Nilai akurasi yang didapat dari simulasi saat tidak ada serangan atau jaringan normal dan saat ada serangan DDoS, hal ini untuk mengetahui terjadinya kesenjangan saat kedua kondisi tersebut. Simulasi ini selain untuk nilai akurasi mendapatkan hasil kesenjangan kondisi juga untuk banyaknya paket dan banyak *byte* serta sumber serangan dari masing-masing *tool* DDoS yang digunakan.

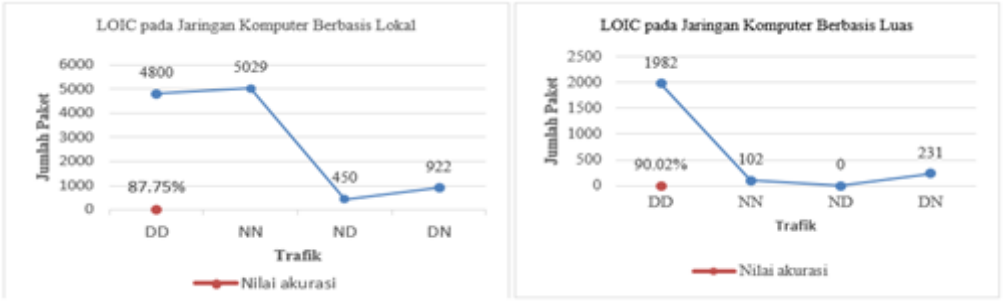
1. Nilai Akurasi Serangan Menggunakan LOIC

Hasil uji coba serangan DDoS menggunakan LOIC tool pada jaringan komputer berbasis lokal dan luas. Pada percobaan ini menghasilkan DD, NN, ND dan DN sangat signifikan. Hal ini menunjukkan bahwa LOIC DDoS adalah sebuah penyerang yang kuat atau mematikan baik saat simulasi DDoS pada jaringan berbasis lokal dan luas. Hal ini terlihat pada Tabel 1. Perbandingan Nilai Akurasi Serangan LOIC pada jaringan berbasis lokal dan luas.

Tabel 1. Perbandingan Nilai Akurasi Serangan LOIC di Jaringan Berbasis Lokal dan Luas

Jaringan Berbasis Lokal					**Jaringan Berbasis Luas**				
LOIC	DD	NN	ND	DN	LOIC	DD	NN	ND	DN
Jaringan Area Lokal	4800	5029	450	922	Jaringan Luas	1982	102	0	231
Nilai akurasi		87.75%			Nilai akurasi		90.02%		

Hasil Akurasi serangan LOIC pada jaringan berbasis lokal dan luas. LOIC ini bekerja pada protokol TCP dan UDP pada Jaringan komputer berbasis lokal dan luas menunjukkan nilai akurasi serangan DDoS hampir sama yaitu 87.75% pada jaringan berbasis lokal dan 90.02% pada jaringan berbasis luas. Perbandingan Nilai Akurasi Serangan LOIC di jaringan komputer berbasis lokal dan luas juga terlihat pada Gambar 11.



Gambar 11. Hasil Akurasi Serangan LOIC di Jaringan Komputer Berbasis Lokal dan Luas

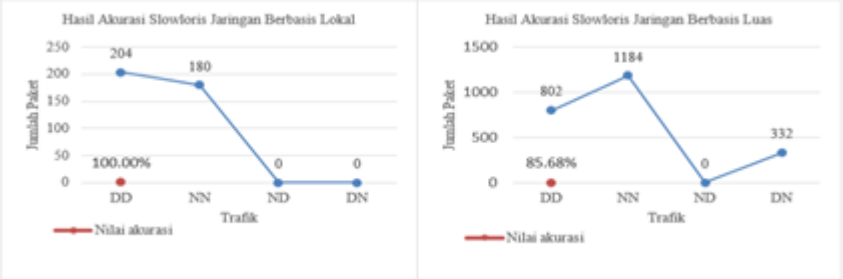
2. Nilai Akurasi Serangan menggunakan Slowloris

Hasil uji coba serangan DDoS menggunakan *Slowloris tool* pada jaringan komputer berbasis area lokal dan luas. Pada percobaan ini menghasilkan DD, NN, ND dan DN signifikan. Hal ini menunjukkan bahwa DDoS *Slowloris* adalah sebuah penyerang yang perlu diwaspadai baik pada jaringan komputer area berbasis lokal dan luas Hal ini terlihat pada Tabel 1. Perbandingan Nilai Akurasi Serangan *Slowloris* di jaringan komputer area berbasis lokal dan luas.

Tabel 2. Perbandingan Nilai Akurasi Serangan *Slowloris* di Jaringan Berbasis Lokal dan Luas

Jaringan Berbasis Berbasis Lokal					**Jaringan Komputer Berbasis Luas**				
SLOWLORIS	DD	NN	ND	DN	SLOWLORIS	DD	NN	ND	DN
	204	180	0	0		802	1184	0	332
Nilai akurasi	100.00%				Nilai akurasi	85.68%			

Hasil Akurasi serangan *Slowloris* pada jaringan berbasis lokal dan luas, pada Jaringan jaringan berbasis lokal dan luas menunjukkan nilai akurasi serangan DDoS berselisih sebesar 100% pada jaringan berbasis lokal dan 85.68% pada area luas. Perbandingan Nilai Akurasi Serangan *Slowloris* di jaringan berbasis lokal dan luas juga terlihat secara jelas pada Gambar 12.



Gambar 12. Hasil Akurasi Serangan *Slowloris* di Jaringan Berbasis Lokal dan Luas

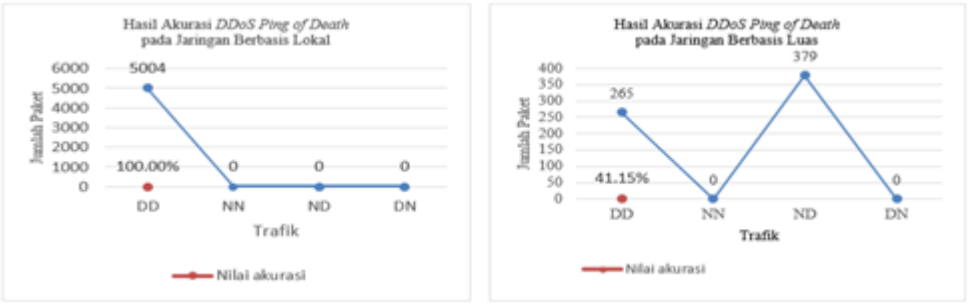
3. Nilai Akurasi Serangan menggunakan PoD

Hasil uji coba serangan DDoS menggunakan PoD tool jaringan komputer berbasis area lokal dan luas. Pada percobaan dengan variabel DD, NN, ND dan DN kurang signifikan. Hal ini menunjukkan bahwa DDoS PoD adalah perlu diwaspadai baik pada jaringan berbasis lokal dan luas. Hal ini terlihat pada Tabel 3. Perbandingan Nilai Akurasi Serangan PoD di jaringan komputer area lokal dan luas.

Tabel 3. Perbandingan Nilai Akurasi Serangan PoD pada Jaringan Komputer Berbasis Lokal dan Luas

Jaringan Berbasis Lokal					**Jaringan Berbasis Luas**				
Ping of Death	DD	NN	ND	DN	Ping of Death	DD	NN	ND	DN
	5004	0	0	0		265	0	379	0
Nilai akurasi	100.00%				Nilai akurasi	41.15%			

Pada jaringan berbasis lokal dan luas menunjukkan nilai akurasi serangan DDoS berselisih sangat besar yaitu 100% pada jaringan berbasis area lokal dan 41,45% pada jaringan berbasis luas sehingga PoD sebuah *tool* yang kurang handal. Perbandingan Nilai Akurasi Serangan PoD jaringan berbasis lokal dan luas juga terlihat secara jelas pada Gambar 13.



Gambar 13. Hasil Akurasi Serangan PoD di Jaringan Berbasis Lokal dan Luas

3.6. Performa *Server* pada Sistem Operasi *Proprietary Windows Server* 2019

Performa *server* meliputi penggunaan CPU saat tidak ada serangan dan saat ada serangan. Hasil simulasi sebelum dan sesudah penyerangan menunjukkan penurunan performa *server* karena hampir semua *resource* dari *server* digunakan melayani permintaan dari penyerang DDoS pada PC I3 *memory* 6 GB sistem operasi *Windows Server* 2019 seperti pada Tabel 4. *Performa Server* sebelum dan sesudah ada serangan pada jaringan berbasis lokal dan luas.

Tabel 4. Performa *Server* sebelum dan sesudah ada Serangan pada Jaringan Berbasis Lokal dan Luas

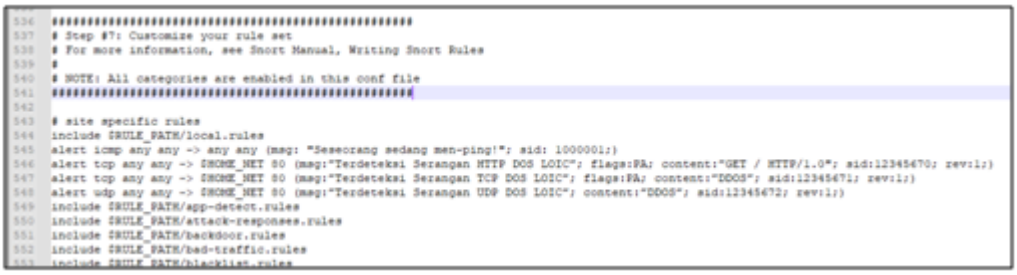
DDoS Tools	Tanpa Serangan DDoS		Ada Serangan DDoS	
	CPU	Memory	CPU	Memory
LOIC	6%	46%	83%	43%
Slowloris	7%	40%	85%	54%
Ping of Death	6%	46%	52%	54%

Kenaikan penggunaan CPU dari sebelum dan sesudah ada serangan DDoS LOIC naik sebesar 77%, Penggunaan CPU dari sebelum ada serangan menjadi ada serangan DDoS *Slowloris* naik sebesar 78%, dan Penggunaan CPU dari sebelum ada serangan menjadi ada serangan DDoS *Ping of Death* naik sebesar 46%, sedangkan perubahan dari sebelum ada serangan menjadi ada serangan pada penggunaan *memory* yaitu DDoS LOIC sebesar 3%, pada *Slowloris* sebesar 14% dan pada PoD sebesar 8%. Penurunan performa dan kinerja *server* DDoS saat menggunakan *tool Slowloris* dengan protokol HTTP mengalami *down* hanya dalam waktu 3 menit dibandingkan LOIC dan PoD. Performa *server* saat serangan DDoS menggunakan *Slowloris* mengalami peningkatan yang sangat signifikan baik pada kinerja CPU maupun pada *memory*. Serangan DDoS yang paling mematikan pada penelitian ini adalah LOIC yang bekerja pada protokol UDP dan TCP, yang terakhir adalah *Ping of Death* yang bekerja pada protokol ICMP. kemudian Perbandingan Performa *Server* pada beberapa tool DDoS pada Sistem Operasi *proprietary Windows Server* 2019 yang ditampilkan pada Gambar 14.

Gambar 14. Performa *Web Server* dengan Beberapa *tool* DDos Saat Terjadi Serangan

3.7. Analisa *HIDS Snort*

Analisa penggunaan metode *Host Intrusion Detection System* (*HIDS*) dengan menerapkan pendeteksi serangan jaringan yang ditempatkan pada host dinyatakan berhasil mendeteksi terjadinya serangan dari beberapa *tool* DDoS secara *real time*. *HIDS* ini berbantuan *Snort* yang ditempakan pada sisi *server*. HIDS diincludekan dalam sebuah konfigurasi deteksi sehingga apabila terjadi serangan maka akan dapat mengirimkan peringatan adanya aktivitas mencurigakan beserta sumber aktivitas. Adapun *rule* pada *snort* yang diterapkan seperti pada Gambar 15.

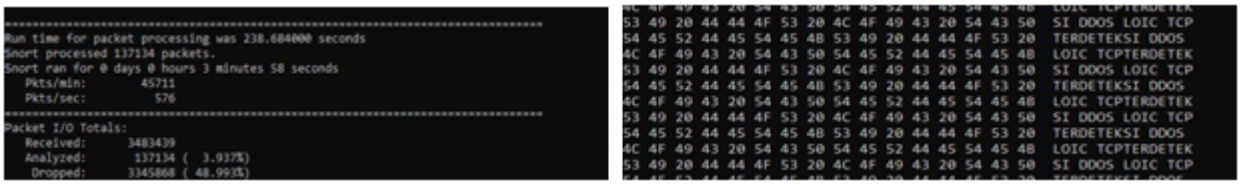


```
##################################################
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
##################################################

# site specific rules
include $RULE_PATH/local.rules
alert icmp any any -> any any (msg: "Seseorang sedang men-ping!"; sid: 1000001;)
alert tcp any any -> $HOME_NET 80 (msg:"Terdeteksi Serangan HTTP DOS LOIC"; flags:PA; content:"GET / HTTP/1.0"; sid:12345670; rev:1;)
alert tcp any any -> $HOME_NET 80 (msg:"Terdeteksi Serangan TCP DOS LOIC"; flags:PA; content:"DDOS"; sid:12345671; rev:1;)
alert udp any any -> $HOME_NET 80 (msg:"Terdeteksi Serangan UDP DOS LOIC"; content:"DDOS"; sid:12345672; rev:1;)
include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/blacklist.rules
```

Gambar 15. *Script Rule Snort* pada *HIDS*

1. Hasil Deteksi *HIDS Snort* pada *DDoS LOIC TCP*

Deteksi *HIDS Snort* pada *DDoS LOIC* yang berjalan pada protokol *TCP* yang dideteksi dalam waktu 3 menit 58 detik mengirimkan total paket 137.134 dengan paket per menit sebanyak 45.711 paket per menit, dan paket 576 per detik dengan mengirimkan peringatan sebanyak 62 kali. yang berisi pesan TERDETEKSI *DDOS LOIC TCP* yang bersumber dari IP 192.168.20.40 menuju 192. 168. 200. 10 sampai dalam waktu 5 menit tidak mengalami *down*. Adapun waktu deteksi dan banyak paket serta peringatan yang dikirimkan oleh *HIDS Snort* seperti pada Gambar 16.



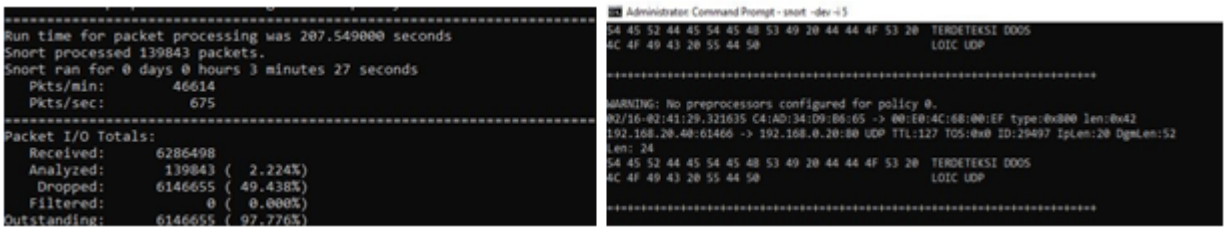
```
===============================================================================
Run time for packet processing was 238.684000 seconds
Snort processed 137134 packets.
Snort ran for 0 days 0 hours 3 minutes 58 seconds
   Pkts/min:        45711
   Pkts/sec:          576
===============================================================================
Packet I/O Totals:
   Received:      3483439
   Analyzed:       137134 (  3.937%)
    Dropped:      3345868 ( 48.993%)
```

```
53 49 20 44 44 4F 53 20 4C 4F 49 43 20 54 43 50  SI DDOS LOIC TCP
54 45 52 44 45 54 45 4B 53 49 20 44 44 4F 53 20  TERDETEKSI DDOS
4C 4F 49 43 20 54 43 50 54 45 52 44 45 54 45 4B  LOIC TCPTERDETEK
53 49 20 44 44 4F 53 20 4C 4F 49 43 20 54 43 50  SI DDOS LOIC TCP
54 45 52 44 45 54 45 4B 53 49 20 44 44 4F 53 20  TERDETEKSI DDOS
4C 4F 49 43 20 54 43 50 54 45 52 44 45 54 45 4B  LOIC TCPTERDETEK
53 49 20 44 44 4F 53 20 4C 4F 49 43 20 54 43 50  SI DDOS LOIC TCP
54 45 52 44 45 54 45 4B 53 49 20 44 44 4F 53 20  TERDETEKSI DDOS
4C 4F 49 43 20 54 43 50 54 45 52 44 45 54 45 4B  LOIC TCPTERDETEK
53 49 20 44 44 4F 53 20 4C 4F 49 43 20 54 43 50  SI DDOS LOIC TCP
```

Gambar 16. Hasil Deteksi HIDS Snort pada DDoS LOIC TCP

2. Analisa Deteksi *HIDS Snort* pada *DDoS LOIC UDP*

Deteksi *HIDS Snort* pada *DDoS LOIC* yang berjalan pada protokol *UDP* yang dideteksi dalam waktu 3 menit 27 detik mengirimkan total paket 139.843 dengan paket per menit sebanyak 46.614 paket per menit, dan paket 675 per detik dengan mengirimkan peringatan sebanyak 84 kali yang berisi pesan TERDETEKSI *DDOS LOIC UDP* yang bersumber dari IP 192.168.20.40 menuju 192.168.200.10 Hal ini menunjukkan bahwa *DDoS LOIC UDP* membutuhkan paket yang banyak sehingga *server* mengalami *down*, Adapun waktu deteksi dan banyak paket serta peringatan yang dikirimkan oleh *HIDS Snort* seperti pada Gambar 17.



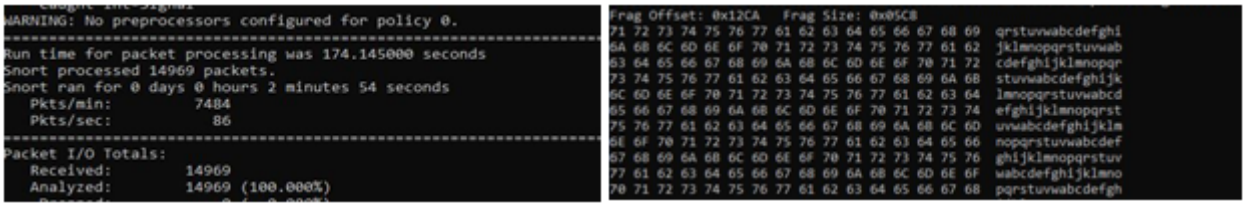
```
===============================================================================
Run time for packet processing was 207.549000 seconds
Snort processed 139843 packets.
Snort ran for 0 days 0 hours 3 minutes 27 seconds
   Pkts/min:        46614
   Pkts/sec:          675
===============================================================================
Packet I/O Totals:
   Received:      6286498
   Analyzed:       139843 (  2.224%)
    Dropped:      6146655 ( 49.438%)
   Filtered:            0 (  0.000%)
Outstanding:      6146655 ( 97.776%)
```

```
54 45 52 44 45 54 45 4B 53 49 20 44 44 4F 53 20  TERDETEKSI DDOS
4C 4F 49 43 20 55 44 50                          LOIC UDP

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
02/16-02:41:29.321635 C4:AD:34:D9:B6:65 -> 00:E0:4C:68:00:EF type:0x800 len:0x42
192.168.20.40:61466 -> 192.168.0.20:80 UDP TTL:127 TOS:0x0 ID:29497 IpLen:20 DgmLen:52
Len: 24
54 45 52 44 45 54 45 4B 53 49 20 44 44 4F 53 20  TERDETEKSI DDOS
4C 4F 49 43 20 55 44 50                          LOIC UDP

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Gambar 17. Hasil Deteksi *HIDS Snort* pada *DDoS LOIC UDP*

3. Analisa Deteksi *HIDS Snort* pada *DDoS PoD*

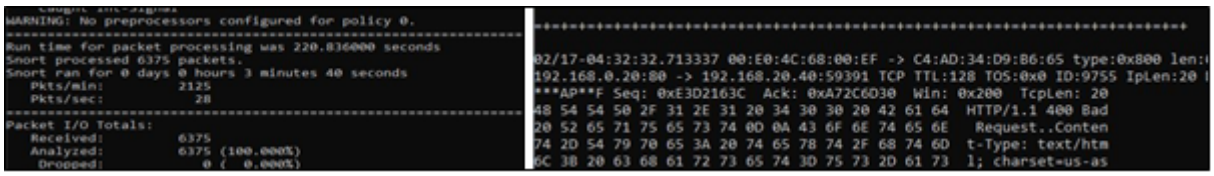
Deteksi *HIDS Snort* pada *DDoS PoD* yang berjalan pada protokol ICMP yang dideteksi dalam waktu 2 menit 54 detik mengirimkan total paket 14969 dengan paket per menit sebanyak 7484 paket per menit, dan paket 86 per detik dengan mengirimkan peringatan sebanyak 90 kali yang bersumber dari IP 192.168.20.40 menuju IP target 192.168.200.10 . Adapun waktu deteksi dan banyak paket serta peringatan yang dikirimkan oleh *HIDS Snort* seperti pada Gambar 18.



Gambar 18. Hasil Deteksi HIDS Snort pada DDoS PoD

4. Hasil deteksi *HIDS Snort* pada *Slowloris*

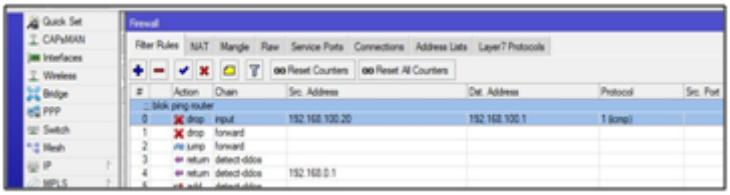
Deteksi *HIDS Snort* pada *DDoS SLowloris* yang berjalan pada protokol HTTP yang dideteksi dalam waktu 3 menit 40 detik mengirimkan total paket 6375 dengan paket per menit sebanyak 2125 paket per menit, dan paket 28 per detik dengan mengirimkan peringatan sebanyak 150 kali yang bersumber dari IP 192.168.20.40 menuju IP target 192.168.100.20. Hal ini menunjukkan bahwa *Slowloris* mengirimkan paket yang tidak membutuhkan banyak paket tetapi peringatan serangan sangat banyak dan *server* mengalami *down*. Adapun waktu deteksi dan banyak paket serta peringatan yang dikirimkan oleh *HIDS Snort* seperti pada Gambar 19.



Gambar 19. Hasil Deteksi *HIDS Snort* pada *DDoS Slowloris*

3.8. Analisa Penggunaan *Firewall*

Analisa penggunaan *firewall* pada *router* mikrotik seri 951ui-2hnd untuk cara menyaring jumlah paket yang dikirim dari dengan memantau, mengidentifikasi dan penyaringan koneksi. Analisa meliputi pemantauan saat terjadinya serangan dengan mengaktifkan konfigurasi *firewall* dan saat tidak mengaktifkannya baik dalam jumlah paket maupun jumlah *byte*, adapun tampilan dari proses blokir IP pada *firewall* tertampil pada Gambar 20.



Gambar 20. Tampilan Proses *Dropping* IP pada *firewall* pada *Layer Netwok*

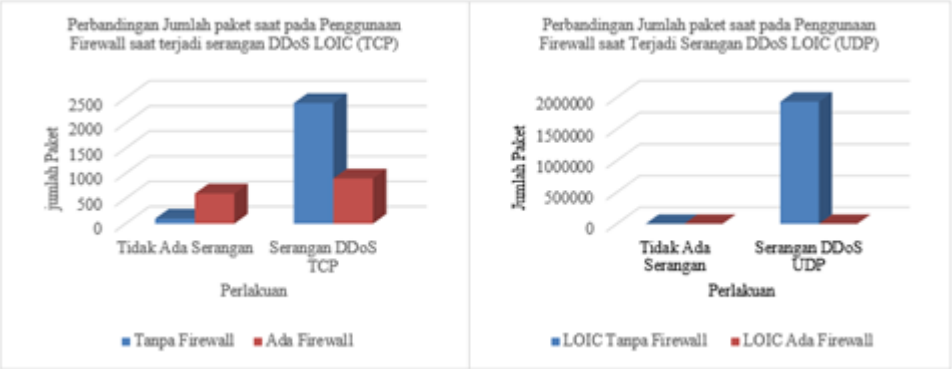
1. Analisa Penggunaan *Firewall* pada Jumlah Paket Trafik Jaringan

Hasil uji keamanan jaringan pada *layer network* yaitu pemasangan *firewall* menghasilkan perubahan jumlah paket sebelum ada serangan dan setelah ada serangan yang sangat signifikan. Perbandingan uji keamanan jaringan ini diuji cobakan terhadap serangan *DDoS* menggunakan tiga *tool* yaitu *LOIC*, *Slowloris* dan *PoD*, masing-masing jumlah paket sebelum ada *firewall* dan setelah ada *firewall* menurun secara drastis. Hal ini seperti terlihat pada Tabel 5. Perbandingan Jumlah Paket Data Sebelum Dan Sesudah Ada *Firewall*.

Tabel 5. Perbandingan Jumlah *Byte* sebelum dan sesudah Ada Serangan

Jumlah Bytes (MB)				
Perlakuan		**Tanpa Serangan DDoS**	**Serangan DDoS (TCP, ICMP)**	**Serangan DDoS HTTP & UDP**
LOIC	Tanpa firewall	60	6433	11600000
	Ada firewall	516	1388	120
SLOWLORIS	Tanpa firewall	60	-	6433
	Ada firewall	156	-	148
PoD	Tanpa firewall	60	1474000	-
	Ada firewall	516	78	-

Hasil uji keamanan jaringan pada *layer network* yaitu pemasangan *firewall* menghasilkan perubahan jumlah paket sebelum ada serangan dan setelah ada serangan yang sangat signifikan. Setelah dipasang *firewall* pada *LOIC* dengan serangan *TCP* menurun sebesar 33,33% , *firewall* pada serangan *DDoS UDP* menurun sebesar 99,90% seperti terlihat pada Gambar 21.



Gambar 21. Perbandingan sebelum dan setelah ada *firewall* pada *DDoS LOIC* pada *TCP* dan *UDP*

Hasil uji keamanan jaringan pada *network layer* yaitu pemasangan *firewall* menghasilkan perubahan jumlah paket sebelum ada serangan dan setelah ada serangan yang sangat signifikan. Setelah dipasang *firewall* serangan *DDoS Slowloris* mengalami penurunan sebesar 97.67%., *firewall* pada serangan DDoS PoD menurun sebesar 91,67%. Perbandingan sebelum dan setelah penerapan keamanan jaringan pada *network layer* menggunakan *firewall* pada *DDoS, Slowloris* dan *PoD* seperti terlihat pada Gambar 22.

Gambar 22. Perbandingan Jumlah Paket Tanpa dan Ada *Firewall* dengan *DDoS Slowloris* (HTTP) dan *PoD* (ICMP)

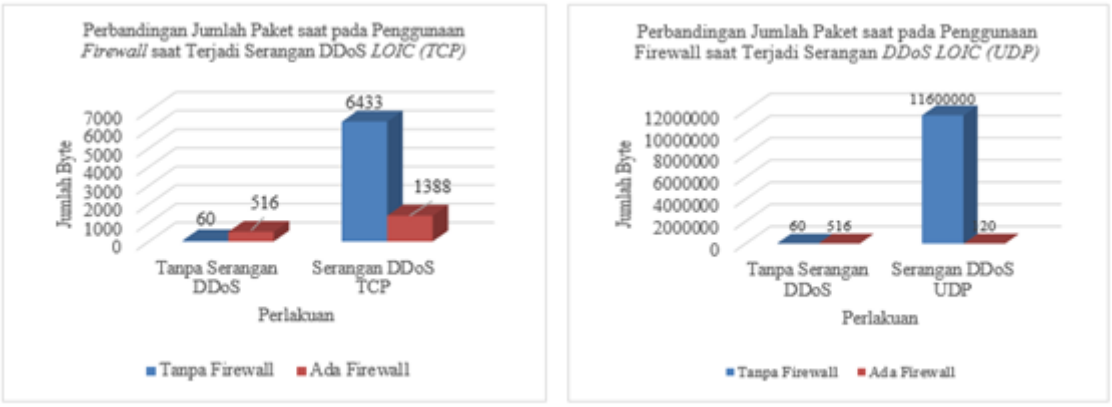
2. Analisa Penggunaan *Firewall* pada Jumlah *Byte* pada Trafik Jaringan

Jumlah *Byte* pada trafik dengan keamanan jaringan pada *firewall network layer* menghasilkan perubahan jumlah *byte* sebelum ada serangan dan setelah ada serangan yang sangat signifikan. Perbandingan uji keamanan jaringan terhadap serangan *DDoS* menggunakan tiga *tool* yaitu *LOIC*, *Slowloris* dan *PoD*, masing-masing jumlah *byte* sebelum ada *firewall* dan setelah ada *firewall* menurun secara drastis. Hal ini seperti terlihat pada Tabel 6. Perbandingan Jumlah Paket Data sebelum dan sesudah Ada *Firewall*.

Tabel 6. Perbandingan Jumlah *Byte* sebelum dan sesudah Ada Serangan

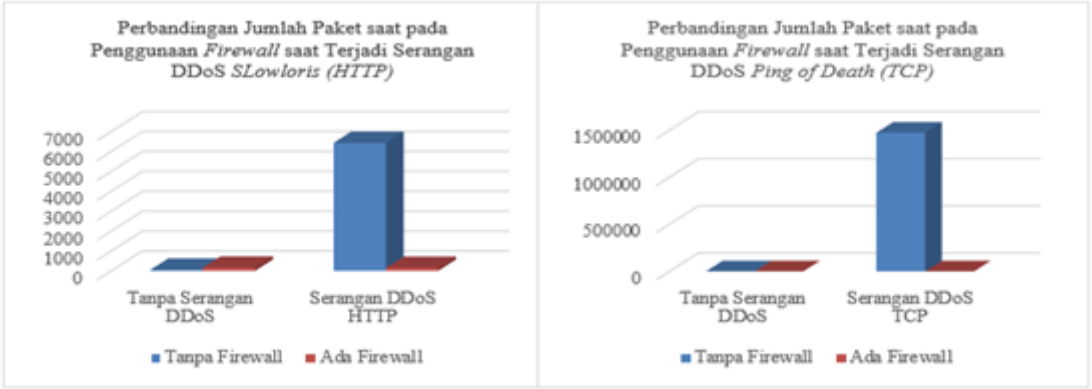
		Jumlah Bytes (MB)		
Perlakuan		Tanpa Serangan DDoS	Serangan DDoS (TCP, ICMP)	Serangan DDoS HTTP & UDP
LOIC	Tanpa firewall	60	6433	11600000
	Ada firewall	516	1388	120
SLOWLORIS	Tanpa firewall	60	-	6433
	Ada firewall	156	-	148
PoD	Tanpa firewall	60	1474000	-
	Ada firewall	516	78	-

Hasil uji keamanan jaringan pada *layer network* yaitu pemasangan *firewall* menghasilkan perubahan jumlah *byte* sebelum ada serangan dan setelah ada serangan yang sangat signifikan. Setelah dipasang *firewall* pada *LOIC* dengan serangan *TCP* menurun sebesar 99.07% , *firewall* pada serangan DDoS UDP menurun sebesar 99,99%. Perbandingan jumlah *byte* sebelum dan setelah ada *firewall* pada *DDoS LOIC* pada TCP dan UDP seperti terlihat pada Gambar 23.



Gambar 23. Perbandingan Jumlah *Byte* sebelum dan setelah ada *firewall* pada *DDoS LOIC* pada TCP dan UDP

Hasil uji keamanan jaringan pada *layer network* yaitu pemasangan *firewall* menghasilkan perubahan jumlah *byte* sebelum ada dan setelah ada serangan yang sangat signifikan. Setelah dipasang *firewall* serangan *DDoS Slowloris* mengalami penurunan sebesar 97.67%. *Firewall* pada serangan *DDoS PoD* menurun sebesar sebesar 99.96% . Perbandingan jumlah *byte* sebelum dan setelah ada *firewall* pada *DDoS Slowloris* dan *PoD* seperti terlihat pada Gambar 24.



Gambar 24. Perbandingan Jumlah *Byte* Sebelum dan Setelah ada *firewall* pada *DDoS Slowloris* dan *PoD*

4. KESIMPULAN

Penelitian ini memberikan nilai akurasi *tool DDoS Slowloris* yang bekerja pada HTTP merupakan *tool DDoS* yang paling merusak dengan keakurasian peningkatan trafik sebesar 92,84%, penurunan performa *server* sebesar 78% yang mengakibatkan *server down* dibandingkan dengan *LOIC UDP, LOIC TCP* dan *PoD*. Pada *Slowloris* membutuhkan paket data yang sedikit dibandingkan *LOIC UDP* dan yang lainnya dalam melakukan serangan, hal ini membuat serangan tidak mudah diketahui sehingga harus menerapkan *HIDS* untuk peringatan sebuah serangan, peringatan terbanyak oleh *HIDS Snort* terdeteksi pada *DDoS Slowloris*. Berdasarkan hal tersebut maka untuk menghentikan *DDoS* dengan *firewall* pada *layer network* dengan keefektifan rata-rata sebesar 98.91%. Implikasi dari penelitian ini adalah keakurasian beberapa *tool DDoS* pada jaringan berbasis lokal dan luas, pendeteksian dengan metode *HIDS Snort* dan penghentian *DDoS* dengan *firewall* mikrotik pada *network layer*. Untuk penelitian selanjutnya diharapkan dapat menggabungkan antara *Host Intrusion Detection System* (*HIDS*) dan *Network Intrusion Detection System (NIDS)*, serta penerapan *firewall* pada *hardware* dan *software* yang terintegrasi.

UCAPAN TERIMA KASIH

Bagian ucapan terimakasih adalah opsional. Sumber dana penelitian dapat diletakkan di sini.

REFERENSI

[1] L. Tan, K. Huang, G. Peng, and G. Chen, "Stability of TCP/AQM Networks Under DDoS Attacks with Design," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 3042–3056, 2020.

[2] W. M. A, "Securing Vehicular Ad-Hoc Networks: A DDoS Case Study," *2nd International Conference on Computation, Automation And Knowledgee Management Amity University*, pp. 1–6, 2021.

[3] H. Huang, L. Hu, J. Chu, and X. Cheng, "An Authentication Scheme to Defend Against UDP DrDoS Attacks in 5G Networks," *IEEE Access*, vol. 7, pp. 175 970–175 979, 2019.

[4] P. Bhale, S. Biswas, and S. Nandi, "LORD: Low Rate DDoS Attack Detection and Mitigation Using Lightweight Distributed Packet Inspection Agent in IoT Ecosystem," *International Symposium on Advanced Networks and Telecommunication Systems, ANTS*, vol. 2019-December, pp. 2–7, 2019.

[5] X. Liang and T. Znati, "An Empirical Study of Intelligent Approaches to DDoS Detection in Large Scale Networks," *2019 International Conference on Computing, Networking and Communications, ICNC 2019*, pp. 821–827, 2019.

[6] rajorshi Biswas and J. Wu, "Optimal Filter Assignment Policy Against Distributed Denial-of-Service Attack," *IEEE Transactions on Dependable and Secure Computing*, vol. 5971, no. c, pp. 1–1, 2020.

[7] R. Sanjeetha, "Mitigating HTTP GET FLOOD DDoS Attack Using an SDN Controller," *International Conference on Recent Trends on Electronic, Information, Communictioan & Technology*, pp. 6–10, 2020.

[8] S. Bagheri and A. Shameli-Sendi, "Dynamic Firewall Decomposition and Composition in The Cloud," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 2, pp. 3526–3539, 2020.

[9] F. Antony and R. Gustriansyah, "Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 1, pp. 43–52, 2021.

[10] S. M. Xia, S. Z. Guo, W. Bai, J. Y. Qiu, H. Wei, and Z. S. Pan, "A New Smart Router-Throttling Method to Mitigate DDoS Attacks," *IEEE Access*, vol. 7, pp. 107 952–107 963, 2019.

[11] T. Hirakawa, K. Ogura, B. B. Bista, and T. Takata, "An Analysis of A Defence Method Against Slow HTTP DoS Attack," *Proceedings of 2018 International Symposium on Information Theory and its Applications, ISITA 2018*, no. C, pp. 316–320, 2019.

[12] A. Yudhana, I. Riadi, and S. Suharti, "Distributed Denial of Service (DDoS) Analysis on Virtual Network and Real Network Traffic," *Journal of Informatics and Telecommunication Engineering-Jite*, vol. 5, no. 1, pp. 112–121, 2021.

[13] Netscout System, "Application-Layer DDoS Attacks : Bad Things Come In Small Pacages," *NETSCOUT*, p. 1, 2018.

[14] A. Anggrawan, R. Azhar, B. K. Triwijoyo, and M. Mayadi, "Developing Application in Anticipating DDoS Attacks on Server Computer Machines," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 2, pp. 427–434, 2021.

[15] S. Sivanantham, R. Abirami, and R. Gowsalya, "Comparing The Performance of Adaptive Boosted Classifiers in Anomaly Based Intrusion Detection System for Networks," *Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019*, pp. 1–5, 2019.

[16] N. Jaswal, *Hands-on Network Forensics : Investigate Network Attacks and Find Evidence Using Common Network Forensic Tools*, 2019.

[17] C. Y. Tseung and K. P. Chow, "Forensic-Aware Anti-DDoS Device," *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*, pp. 148–159, 2018.

[18] P. Senthilkumar and M. Muthukumar, "A Study on Firewall System, Scheduling and Routing Using Pfsense Scheme," *Proceedings of IEEE International Conference on Intelligent Computing and Communication for Smart World, I2C2SW 2018*, pp. 14–17, 2018.

[19] A. Praseed and P. Santhi Thilagam, "DDoS Attacks at The Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 661–685, 2019.

[20] B. Rashidi, C. Fung, and M. Rahman, "A Scalable and Flexible DDoS Mitigation System Using Network Function Virtualization," *IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018*, pp. 1–6, 2018.

[21] J. M. Ceron, C. Scholten, A. Pras, and J. Santanna, "MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification," *Proceedings of IEEE/IFIP Network Operations and Management Symposium 2020: Management in the Age of Softwarization and Artificial Intelligence, NOMS 2020*, 2020.

[22] A. Yudhana, I. Riadi, and F. Ridho, "DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, pp. 177–183, 2018.

[23] Y. Fu, M. H. Au, R. Du, H. Hu, and D. Li, "Cloud Password Shield: A Secure Cloud-Based Firewall Against DDoS on Authentication Servers," *Proceedings - International Conference on Distributed Computing Systems*, vol. 2020-November, pp. 1209–1210, 2020.

[24] S. Alam, Y. Alam, S. Cui, C. Akujuobi, and M. Chouikha, "Toward Developing A Realistic DDoS Dataset for Anomaly-Based Intrusion Detection," *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, vol. 2021-Janua, 2021.

[25] L. Z. A. Mardedi and K. Marzuki, "Network Rancang Bangun Jaringan Komputer LAN Berdasarkan Perbandingan Kinerja Routing Protokol EIGRP dan Routing Protokol OSPF," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 18, no. 2, pp. 202–210, 2019.