Analisa Keamanaan Jaringan Komputer Menggunakan Sistem Deteksi Intrusi Shorewall

Sugi Aprianti[1*], Riska[2], Hendri Alamsyah[3]

[1]*Program Sstui Rekayasa Sistem Komputer Universitas Dehasen Bengkulu*
E-mail : riska.iskandar@unived.ac.id[2], hendri.alamsyah@unved.ac.id[3]

ABSTRACT

This study aims to build an intrusion detection system on the SMK N 3 Kepahiang computer network by utilizing the Network Intrusion Detection System (NIDS) method using the Shorewall application, as well as knowing how the shorewall works in preventing and overcoming the computer network security system at SMK N 3 Kepahiang. Because based on the observations made, it was found that there were frequent connection failures caused by full ltraffic data on ethernet connected to the internet and also failures to connect to the network caused by invalid mac addresses. In conducting research, the research method used was experimental research methods. In this study, an analysis was carried out which would be used as material for the implementation of an intrusion detection system using the Network Intrusion Detection System (NIDS) method by utilizing shorewall applications. The results of research using experimental methods are then documented, so that appropriate results or recommendations are obtained for building a security system using a shorewall intrusion detection system. The results of this study indicate that Shorewall can be applied to networks using 2 interfaces, 1 interface is used to connect to the internet network and 1 interface for local networks, Shorewall can also be used as an intrusion detection system for Mac clones and DDoS attacks that can be carried out on the network so that it can reject mac clone activities and DDoS attacks. Application of shorewall as an intrusion detection system does not affect service quality, where based on ITU G.114 test results it is still categorized as good with a delay test value of 1.92 ms, a jitter test value of 33.3 ms, a packet loss test value of 0%, and a throughput test value of 548 kb.

Keywords : Shorewall, NIDS, Mac Clone, DDoS

ABSTRAK

Penelitian ini bertujuan untuk membangun sistem deteksi intrusi pada jaringan kompuyer SMK N 3 Kepahiang dengan memanfaatkan metode *Network Intrusion Detection System* (NIDS) menggunakan aplikasi Shorewall, serta mengetahui cara kerja dari shorewall dalam mencegah dan mengatasi sistem keamanan jaringan komputer SMK N 3 Kepahiang. Sebab berdasarkan observasi yang dilakukan ditemukan sering terjadinya kegagalan koneksi yang disebabkan penuhnya *ltraffic* data pada *ethernet* yang terhubung ke internet serta juga pernah terjadi gagal terhubung ke jaringan yang disebabkan oleh *invalid mac address* Dalam melakukan penelitian metode penelitian yang digunakan adalah metode penelitian eksprimen. Pada penelitian ini dilakukan analisa yang akan dijadikan sebagai bahan untuk Implementasi sistem deteksi intrusi menggunaakn metode *Network Intrusion Detection System* (NIDS) dengan memanfaatkan aplikasi shorewall. Hasil dari penelitian dengan metode eksprimen selanjutnya didokumentasikan, sehingga didapatkan hasil ataupun rekomendasi yang tepat untuk membangun sebuah sistem keamanan menggunakan sistem deteksi intrusi shorewall. Hasil penelitian ini menunjukkan Shorewall dapat diterapkan pada jaringan menggunakan 2 *interface*, 1 *interface* digunakan untuk terhubung ke jaringan internet dan 1 interface untuk jaringan lokal, shorewall juga dapat digunakan sebagai sistem deteksi intrusi untuk Mac clone dan DDoS attack yang dapat dilakukan dalam jaringan sehingga dapat melakukan reject terhadap aktifitas mac clone dan DDoS attack. Penerapan shorewall sebagai sistem deteksi intrusi tidak mempengeruhi kualitas layanan, dimana dari hasil pengujian Berdasarkan ITU G.114 masih dikategorikan baik dengan nilai pengujian delay 1.92 ms, nilai pengujian jitter 33.3 ms, nilai pengujian packet loss 0%, dan nilai pengujian throughput 548 kb.

***Kata kunci*: Shorewall, NIDS, Mac Clone, DDoS**

1. PENDAHULUAN

Semakin pesatnya teknologi internet saat ini tidak dapat di pungkiri lagi akan berdampak semakin

meningkatnya kejahatan siber[1]. Kejahatan siber naik signifikan pada 2022 bila dibandingkan dengan periode yang sama di 2021. Bahkan jumlah tindak kejahatan siber meningkat hingga 14 kali[2] Hal ini dapat terjadi baik di perushaan maupun instansi Pendidikan.

SMK Negeri 3 Kepahiang merupakan salah satu Instansi Pendidikan di tingkat menengah kejuruan yang dalam kegiatasn pembelajaran juga sudah menggunakan jaringan komputer. Dimana hasil observasi dan wawancara yang sudah dilakukan SMK Negeri 3 Kepahiang ini memiliki sumber jaringan internet dengan bandwidth sebesar 20 Mbps. Dalam penggunaan jaringan internet ini, SMK Negeri 3 Kepahiang belum menggunakan sistem keamanan jaringan hanya memanfaatkan sistem keamanan yang ada pada Komputer ataupun laptop client saja, yang mana client tersebut langsung terhubung ke Modem yang disediakan oleh ISP atau penyedia layanan internet.

Serangan yang biasa terjadi pada jaringan komputer adalah *MAC Clone* dan *DDos Attack*. *Mac Clone* merupakan duplikasi sebuah alamat perangkat keras pada perangkat jaringan[3]. Sedangkan *DDos Attack* merupakan serangan yang bertujuan untuk membanjiri komputer dengan mengirimkan paket yang melebihi kepasitas dari mesin sumber yang menjadi target untuk menanggapi permintaan.[4].

Berdasarkan observasi yang dilakukan ditemukan sering terjadinya kegagalan koneksi yang disebabkan penuhnya *ltraffic* data pada *ethernet* yang terhubung ke internet serta juga pernah terjadi gagal terhubung ke jaringan yang disebabkan oleh *invalid mac address.* Untuk mengatasi masalah ini, dapat diterapkan suatu sistem yang dapat mendeteksi adanya kesalahan di dalam jaringan atau yang biasa disebut sistem intrusi deteksi yang dapat memantau *traffic* data dalam jaringan komputer dengan metode sistem intrus detekti berbasis jaringan atau yang biasa disebut dengan *Network Intrusion Detection System* (NIDS). Dimana NIDS ini merupakan suatu teknik yang dapat digunakan untuk memantau *Traffic* data keluar dan *Traffic* data masuk ataupun *Traffic* data yang terjadi dalam jaringan komputer antara masing – masing node host yang berada dalam satu segmen jaringan lokal[5].

Salah satu aplikasi ataupun tools yang dapat digunakan sebagai NIDS ini adalah shorewall. Shorewall ini merupakan salah satu aplikasi *firewall* yang dapat di install pada sistem operasi linux dengan memanfaatkan iptables, shorewall juga menerapkan konsep zona yang dapat mempermudah dalam penentuan aturan dari firewall untuk mengamankan jaringan komputer.[6].

Dengan adanya sistem keamanan ini dapat membantu seorang administrator jaringan pada sekolah ini untuk mendeteksi lebih dini demi mengambil langkah pancegahan kerusakan ataupun gangguan dalam jaringan.

2. KERANGKA TEORITIS

A. Sistem Keamanan Jaringan

Sistem Keamanan jaringan pada dasarnya merupakan proses dalam mengendalikan akses terhadap sumberdaya jaringan, sehingga akses data pada jaringan komputer dapat dikontrol agar bisa diakses oleh siapa saja yang berhak dan menghalangi orang atau subjek yang tidak terdaftar untuk mengaksesnya[7].

B. *Intrusion Detection System* (IDS)

Intrution Detection *System* adalah singkatan dari IDS, dimana IDS ini merupakan sebuah sistem yang melakukan pengawasan terhadap *Traffic* data pada jaringan komputer serta dapat melakukan pengawasan terhadap kegiatan - kegiatan yang mencurigakan didalam sebuah sistem jaringan. IDS akan memberikan notifikasi Jika ditemukan kegiatan yang mencurigakan berhubungan dengan *Traffic* data dalam jaringan dalam bentuk pesan kepada sebuah sistem ataupun administrator jaringan[8].

IDS terbagi dalam 2 jenis berdasarkan penempatannya, yaitu:

1. *Host Based IDS* (HIDS)

Host Based IDS dapat digunakan untuk pemantauan tertentu dalam jaringan. Dimana HIDS ini hanya digunakan untuk memantau komputer *host* dalam mendeteksi kejadian seperti kesalahan login berkali-kali dan melakukan pengecekan pada file sistem.

2. *Network Based IDS* (NIDS)

Network Based IDS dapat digunakan dalam melakukan pemantauan terhadap satu segmen jaringan dengan mengumpulkan paket - paket data yang lewat pada jaringan tersebut serta melakukan analisa dan mengelompokkan paket - paket tersebut sesuai dengan aturan yang akan dibuat dalam sistem.

C. Shorewall

Shorewall (*Shoreline Firewall*) merupakan salah satu *firewall* yang handal dan murah untuk digunakan di sistem operasi Linux selain *Ipchains* dan *Iptables*, shorewall juga mudah dikonfigurasi bagi penggunanya dan mengatur data yang diterima dan pengiriman data. Serta melakukan Ping pesan ICMP dalam proses Ping ACCEPT, DROP dan *REJECT*[9].

D. Jaringan Komputer

Jaringan komputer merupakan hubungan dari beberapa perangkat jaringan yang dapat berkomunikasi antara satu dan lainnya. Perangkat jaringan yang dimaksudkan ini mencakup semua jenis perangkat komputer, baik itu komputer *desktop*,

laptop, smartphone, *tablet* serta perangkat penghubung seperti *router, switch, modem, wireless access point*[10].

E. *Quality Of Service*

Quality Of Service (QOS) merupakan kualitas pelayanan dari suatu jaringan dalam menyediakan layanan yang baik dengan teknologi yang berbeda – beda. [11]. Beberapa parameter yang dapat digunakan untuk mengukur QoS, antara lain:

1. *Delay*

Delay merupakan waktu yang diperlukan untuk mengirimkan data melalui jaringan atau kanal komunikasi. Faktor yang mempengaruhi delay pengiriman meliputi kecepatan transmisi data, jarak fisik antara pengirim dan penerima, serta kondisi jaringan yang dapat menyebabkan tumpang tindih lalu lintas atau konflik. Berikut Tabel standar delay berdasarkan ITU G.114. [12]

TABEL 1
Standar Delay Berdasarkan ITU G.114

Delay (ms)	Kualitas
0 - 150	Baik
150 – 400	Cukup, masih dapat diterima
> 400	Buruk

2. *Jitter*

Jitter merupakan variasi waktu antara dua atau lebih kejadian yang seharusnya berulang secara periodik dalam sistem komunikasi dan komputer. Jitter dapat menyebabkan dampak negatif pada kualitas layanan dan kinerja jaringan. jitter. Berikut tabel standar *delay* berdasarkan ITU G.114.[12]

TABEL 2
Standar *Jitter* Berdasarkan ITU G.114

Jitter (ms)	Kualitas
0 - 20	Baik
20 – 50	Dapat diterima
> 50	Tidak dapat diterima

3. Packet Loss

Packet Loss merupakan kondisi di mana paket data hilang atau tidak sampai ke tujuan saat dikirim melalui jaringan komunikasi. Penyebabnya bisa beragam, mulai dari kemacetan jaringan hingga gangguan pada saluran komunikasi. Dampak dari packet loss bisa sangat merugikan, terutama dalam hal kualitas layanan dan kinerja jaringan. Berikut Tabel Standar nilai Packet Loss.[12]

TABEL 3
Standar *Packet Loss* Berdasarkan ITU G.114

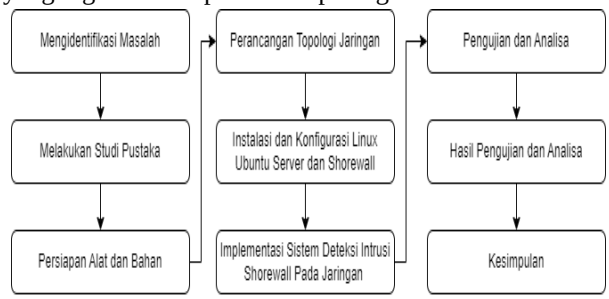
Packet Loss (%)	Kualitas
0 – 1 %	Baik
1 – 5 %	Dapat diterima
> 10 %	Tidak dapat diterima

4. *Throughput*

Throughput merupakan ukuran kuantitatif yang menggambarkan jumlah data atau informasi yang berhasil dikirim atau diterima dalam jaringan atau sistem komputer dalam satu periode waktu tertentu. Throughput adalah indikator penting dalam mengevaluasi kinerja jaringan, meningkatkan kualitas layanan, melakukan perencanaan kapasitas, dan mengidentifikasi *bottleneck*. Dengan memahami dan memantau throughput, administrator jaringan dan sistem dapat mengoptimalkan kinerja dan efisiensi dalam operasi sehari-hari.[12]

3. METODE RISET

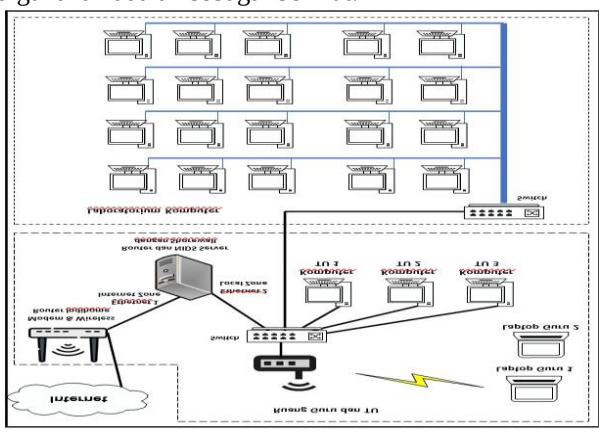
Dalam penelitian ini digunakan metode penelitian *Eksperimen.* D a l a m penelitian ini dilakukan analisa yang akan dijadikan sebagai bahan untuk Implementasi sistem deteksi intrusi menggunaakn metode *Network Intrusion Detection System* (NIDS) dengan memanfaatkan aplikasi shorewall. Adapun metode riset yang digunakan dapat dilihat pada gambar 1.



Gambar 1 Metode Riset

A. Topologi Jaringan

Pada penelitian ini akan dilakukan pengembangan terhadap jaringan yang sudah ada dengan menerapkan sistem keamanan jaringan menggunakan deteksi itrusi berbasis Network Intrusion Detection System (NIDS) dengan tools shorewall. Adapun topologi yang akan digunakan adalah sebagai berikut.



Gambar 2. Topologi Jaringan

Dari Gambar 2 terlihat bahwa adanya penambahan Router yang akan berperan sebagai NIDS *Server* untuk sistem deteksi intrusi shorewall yang akan digunakan untuk memberikan alokasi internat dan juga memantau ataupun melakukan deteksi di dalam satu segmen jaringan, sehingga semua kegiatan komunikasi data yang terjadi pada jaringan SMK Negeri 3 Kepahiang akan terpantau oleh Server yang sudah ditanamkan tools shorewall. Selain itu koneksi wifi yang ada pada SMK Negeri 3 Kepahiang juga akan di rubah berada di bawah Server shorewall, sehingga wifi yang ada pada modem dan wireless router ISP yidak akan digunakan lagi.

B. Prinsip Kerja Sistem

Prinsip kerja dari sistem deteksi intrusi shorewall berbasis *Network Intrusion Detection System* (NIDS) pada jaringan internet SMK Negeri 3 Kepahiang adalah dengan adalah dengan menerapkan zona yaitu zona koneksi internet dan zona koneksi lokal. Dimana masing – masing zona ini kan di atur dan dipantau oleh Shorewall yang akan menjadi *router* serta NIDS *Server* untuk memberikan koneksi internet sekaligus sebagai sistem deteksi intrusi di jaringan SMK Negeri 3 Kepahiang. *Penetration* testing dilakukan dalam jaringan SMK Negeri 3 Kepahiang

4. HASIL DAN PEMBAHASAN

Hasil dari penelitian yang dilakukan difokuskan pada deteksi terhadap serangan Mac *Clone* dan juga deteksi terhadap serangan DDoS serta kualitas layanan dari jaringan SMK Negeri 3 Kepahiang. Berikut hasil dari penerapan sistem deteksi intrusi shorewall

A. Hasil Deteksi Serangan *Mac Clone*

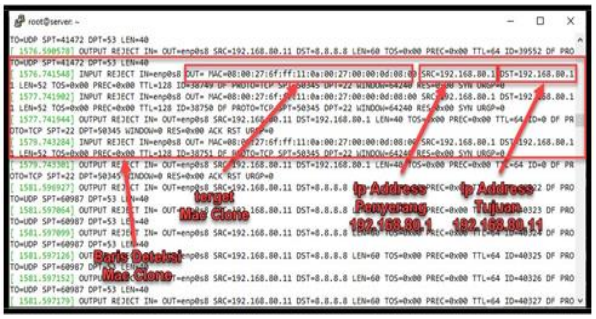
Pengujian ini dilakukan dengan dilakukan dengan skenario saat shorewall belum diaktifkan dan setelah shorewall diaktifkan. Berikut skenario pengujian dengan shorewall belum diaktifkan.

Gambar 3. Hasil Pengujian Mac Clone Sebelum Shorewall Aktif

Dari gambar 3 diatas, terlihat aplikasi netcut yang berjalan pada komputer client dapat melihat mac address dari beberapa komputer yang terhubung satu jaringan dan dapat melakukan cut off terhadap komputer yang terhubung. Kemudian penulis melakukan pengujian terhadap kembali dengan skenario shorewall sudah diaktifkan seperti yang terlihat pada gambar 3 berikut.

Gambar 4. Hasil Pengujian Mac Clone Setelah Shorewall Aktif

Dari gambar 4 diatasterlihat aplikasi netcut tidak dapat lagi menampilkan IP address dan mac address komputer yang terhubung dalam satu jaringan. Hal ini disebabkan shorewall melakukan reject terhadap koneksi yang diminta oleh aplikasi netcut melalui komputer client, untuk lebih jelasnya dapat dilihat pada gambar 5 berikut.

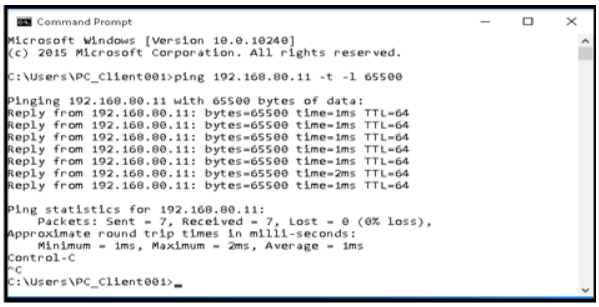


Gambar 5. Hasil Deteksi Mac Clone pada Shorewall

Dari gambar 5 diatas, terlihat informasi pemutusan koneksi (*Reject*) yang bersumber dari *port ethernet* enp0s8 yang dalam penelitian ini merupakan *port ethernet* yang mengarah ke jaringan lokal. *Reject* tersebut terjadi karena adanya percobaan Mac *clone* dan juga DDoS *attack*. Percobaan mac *clone* yang berhasil di deteksi dan langsung mendapatkan *reject* oleh shorewall dapat dilihat pada baris 1576.741548 sampai dengan 1579.743284 yang menunjukkan adanya *reject* mac dengan tujuan 192.168.80.11 yang merupakan IP *address* tujuan dari serangan mac *clone*.

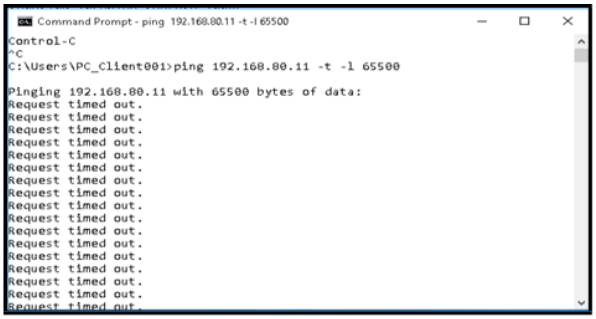
B. Hasil Deteksi *DDOS Attack*

Pengujian DDoS *attack* bertujuan untuk membanjiri jalur komunikasi pada jaringan dengan byte data yang tidak normal yaitu 65500 bytes dimana untuk normalnya hanya 32 bytes. Pengujian ini dilakukan dengan dua skenario pengujian. Skenario pengujian pertama adalah melakukan DDoS *attack* saat shorewall belum diaktifkan menggunakan perintah "ping 192.168.80.11 -t -l 65500", dimana -t menunjukkan ping akan terus dilakukan sampai host menghentikan, sedangkan -l adalah *buffer size* dengan besaran paket tertentu yang dalam pengujian ini adalah 65500 byte. Adapun hasilnya dapat dilihat seperti gambar berikut.



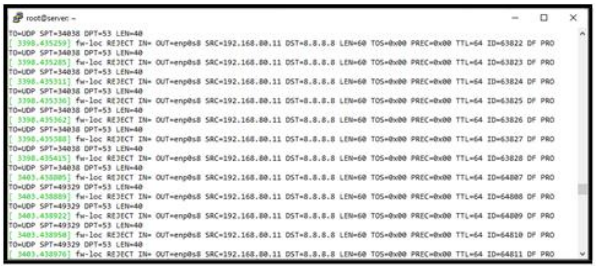
Gambar 6. Hasil Pengujian DDoS Sebelum Shorewall Aktif

Dari Gambar 6 terlihat bahwa Ping dengan data (*buffer size*) yang tidak normal (DDoS) dapat dilakukan dengan adanya *reply* dari IP *address* tujuan yaitu 192.168.80.11. Selanjutnya pada skenario pengujian yang kedua penulis melakukan pengujian DDoS dengan kondisi shorewall yang sudah diaktifkan, dimana hasilnya dapat dilihat seperti gambar berikut



Gambar 7. Hasil Pengujian DDoS Setelah Shorewall Aktif

Dari gambar 7 diatas, terlihat hasil dari DDoS yang tidak diterima oleh komputer tujuan dengan menampilkan hasil *Request Timed Out* (RTO), hal ini disebabkan oleh *Server* shorewall sudah melakukan *reject* pada percobaan DDoS oleh *client* seperti informasi yang diberikan shorewall pada gambar berikut.

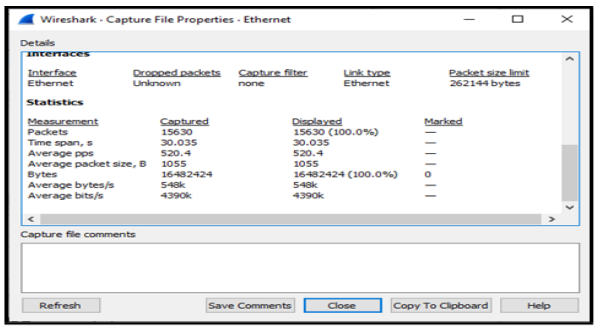


Gambar 8. Hasil Deteksi Intrusi DdoS Attack

Dari gambar 8 diatas, terlihat staus *reject* dilakukan oleh shorewall dengan tujuan ke IP *address* 192.168.80.11 dengan *Time to Live* (TTL) sebesar 64 *Second* dengan ID paket yang dikirim terus meningkat hingga sesuai dengan jumlah paket yang dibuat saat melakukan DdoS *Attack.*

C. Hasil Kualitas Layanan Jaringan

Berikut ini hasil dari pengujian kualitas layanan dengan tujuan untuk memastikan bahwa implementasi shorewall dalam jaringan tidak mempengaruhi penggunaan jaringan. Pengujian ini dilakukan dengan aplikasi wireshark seperti yang terlihat pada Gambar berikut ini.



Gambar 9. Hasil Capture File Properties

Dari Gambar 9 diatas, terlihat hasil *capture file properties* menggunakan wireshark. Untuk melakukan perhitungan terhadap parameter kualitas layanan dapat dilihat seperti berikut ini.

1. *Delay*

Delay dapat dihitung menggunakan rumus sebagai berikut :

Rata-rata *delay* = Total *delay* / Total packet yang diterima

= 30.035 s / 15630

= 0.00192 s

= 1.92 ms

Keterangan :
Total *Delay* : *time span*
Total *Packet* yang diterima : *Packet Caputre*

2. Jitter

Jitter dapat dihitung dengan menggunakan rumus sebagai berikut :

$$\text{Jitter} = \frac{\text{Total variasi } \textit{delay (Average pps)}}{(\text{Total packet yang diterima} - 1)}$$

= 520.4 s / (15630 -1) = 520.4 s / 15629

= 0.03330 s

= 33.3 ms

3. *Packet Loss*

Packet Loss dapat dihitung menggunakan rumus sebagai berikut :

$$\text{Packet Loss} = \frac{(\text{Paket dikirim} - \text{Paket diterima}) \times 100\%}{\text{Paket dikirim}}$$

$$= \frac{(15630-15630) \times 100\%}{15630}$$

= 0 %

4. *Througput*

Throughput dapat dihitung dengan menggunakan rumus sebagai berikut :

$$\text{Throughput} = \frac{\text{Paket data yang diterima (Bytes)}}{\text{Rentang Waktu Pengamatan}}$$

$$= \frac{16482424 \text{ byte}}{30.035 \text{ s}}$$

$$= 548773.8971 \text{ byte}$$

$$= 548 \text{ kb}$$

Dari perhitungan berdasarkan parameter dalam pengujian kualitas layanan, diperoleh hasil dengan nilai dari *delay* 1.92 ms, nilai dari *jitter* 33.3 ms, nilai *packet loss* 0%, dan nilai dari *throughput* 548 kb.

5. PENUTUP

Berdasarkan hasil penelitian yang telah dilakukan, berikut ini beberapa kesimpulan yang didapatkan:

1. Aplikasi shorewall dapat diterapkan pada jaringan dengan 2 *interface*, dimana 1 *interface* digunakan untuk terhubung ke jaringan internet dan 1 *interface* digunakan untuk terhubung ke jaringan lokal.
2. Shorewall dapat melakukan deteksi intrusi dan reject terhadap permintaan informasi IP address dan Mac address oleh aplikasi netcut untuk tujuan Mac clone.
3. Shorewall dapat melakukan deteksi intrusi dan reject terhadap percobaan DDoS dengan buffer size 65500.
4. Penerapan shorewall sebagai sistem deteksi intrusi tidak mempengeruhi kualitas layanan, dimana dari hasil pengujian berdasarkan ITU G.114 masih dikategorikan baik dengan dengan nilai dari *delay* 1.92 ms, nilai dari *jitter* 33.3 ms, nilai *packet loss* 0%, dan nilai dari *throughput* 548 kb.

6. REFERENSI

[1] Amarudin and Faruk Ulum, "Desain Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode Port Knocking," 2018.

[2] Pusiknas Bareskrim Polri, "Kejahatan Siber di Indonesia Naik Berkali-kali Lipat," *Pusiknas Bareskrim Polri*, Dec. 22, 2022.

[3] S. Dwi Ratnasari and D. Safiroh Utsalina, "Implementasi Penanganan Serangan Mac-Clone Pada Hotspot Mikrotik Di Stmik Pradnya Paramita Malang (Studi Kasus: STMIK PRADNYA PARAMITAMALANG)," 2017.

[4] M. N. Faiz, O. Somantri, A. R. Supriyono, and A. W. Muhammad, "Impact of Feature Selection Methods on Machine Learning-based for Detecting DDoS Attacks : Literature Review," *JOURNAL OF INFORMATICS AND TELECOMMUNICATION ENGINEERING*, vol. 5, no. 2, pp. 305–314, Jan. 2022, doi: 10.31289/jite.v5i2.6112.

[5] M. Muqorobin, Z. Hisyam, M. Mashuri, H. Hanafi, and Y. Setiyantara, "Implementasi Network Intrusion Detection System (NIDS) Dalam Sistem Keamanan Open Cloud Computing," *Majalah Ilmiah Bahari Jogja*, vol. 17, no. 2, pp. 1–9, Jul. 2019, doi: 10.33489/mibj.v17i2.205.

[6] I. Riadi, E. Brillianto, U. Ahmad, D. Yogyakarta, J. Soepomo, and Y. Telp, "Visualisasi Monitoring Port Menggunakan Shorewall Dan Log Analizer," *Seminar Nasional Informatika*, 2008.

[7] D. Juardi, "Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus," 2017.

[8] H. Alamsyah, Riska, and A. Al Akbar, "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System," 2018.

[9] Y. Yanti and R. Effendi, "'Analisa Sistem Keamanan Jaringan Komputer Firewall Menggunakan Shorewall Pada PT. Indofarma Global Medika,'" 2020.

[10] T. Sanjaya and D. Setiyadi, "Network Development Life Cycle (NDLC)

Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim."

[11] S. Ayom Cahyadi, I. Santoso, and A. Ajulian Zahra, "Analisis Quality Of Service (Qos) Pada Jaringan Lokal Session Initiation Protocol (Sip) Menggunakan Gns3."

[12] INTERNATIONAL TELECOMMUNICATION UNION, "One-way transmission time," *INTERNATIONAL TELECOMMUNICATION UNION*.