Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 3, **Number** 2, September 2023
https://doi.org/10.47709/digitech.v3i2.3402

Analisis Keamanan Jaringan Komputer Menggunakan Metode Intrusion Detection System (IDS) dan Firewall

Yudi Mulyanto[1*], Eri Sasmita Susanto[2], Muhammad Ilham Akbar[3], Farida Idifitriani[4]
[1,2,3,4]Program Studi Informatika, Universitas Teknologi Sumbawa
[1]yudi.mulyanto@uts.ac.id, [2]eri.sasmita.susanto@uts.ac.id, [3]mi.akbar03@gmail.com, [4]farida.idifitriani@uts.ac.id

open access
Histori Artikel:
Diajukan: 5 Januari 2024
Disetujui: 8 Januari 2024
Dipublikasi: 9 Januari 2024
Kata Kunci:
Analisis, Jaringan, *Intrusion Detection System* (IDS), *Firewall, Router Mikrotik*

Abstrak
Sistem keamanan jaringan DISKOMINFOTIK Sumbawa masih terbilang sederhana dikarenakan sistem keamanan jaringan yang masih menggunakan *Firewall* dari Router *Mikrotik*. Keamanan jaringan seperti ini rentan terhadap serangan karena celah atau hak akses untuk masuk ke jaringan belum dibatasi. Tujuan dari penelitian ini yaitu untuk mengidentifikasi dan mengevaluasi sebuah potensi terjadinya resiko keamanan jaringan serta menerapkan solusi yang mampu melindungi sistem jaringan dari serangan yang berbahaya. Metode pengumpulan data yang digunakan adalah *Mixed Method* yang merupakan gabungan antara Kuantitatif dan Kualitatif seperti Observasi, Studi Pustaka, Wawancara dan Dokumentasi serta menggunakan analisa penelitian dengan metode *Intrusion Detection System* (IDS). Hasil penelitian ini menunjukan bahwa pengujian parameter QoS sebelum diterapkannya sistem keamanan jaringan seperti nilai Throughput 5734 Kb/s, Packet Loss 10,1% yang terbilang tinggi dan nilai Delay 1,159116 ms, Jitter 1,159147 ms yang terbilang rendah, Sedangkan hasil ketika sudah dterapkannya sistem keamanan jaringan menunjukan bahwa nilai Throughput 387 Kb/s, Packet Loss 0,1% yang terbilang rendah dari sebelumnya dan nilai Delay 14,821861 ms, Jitter 14,822145 ms yang terbilang tinggi dari sebelumnya.

PENDAHULUAN

Perkembangan jaringan internet yang pesat menjadikan keamanan suatu data dan arus lalu lintas jaringan meningkat seiring dengan penggunaan jaringan *internet* pada *Server* yang terhubung dengan publik. Hal ini menjadi suatu persoalan yang harus diperhatikan karena dapat menyebabkan kerentanan terhadap serangan kejahatan jaringan internet seperti pencurian data, pemalsuan data, pengubahan data (Halaman muka pada situs *web*site), pembocoran data, penyalahgunaan data seseorang dan kejahatan lainnya.

Dinas Komunikasi, Informatika dan Statistika (DISKOMINFOTIK) merupakan sebuah instansi yang menyediakan pelayanan informasi yang didirikan berdasarkan Surat Keputusan Bupati Sumbawa Nomor 68 Tahun 2016. Dinas Komunikasi, Informatika dan Statistika (DISKOMINFOTIK) sendiri memiliki tugas dan wewenang dalam meningkatkan kualitas pelayanan dan pengelolaan informasi yang berkualitas, benar dan tanggung jawab, serta membangun dan mengembangkan sistem penyediaan dan layanan informasi.

Sistem keamanan DISKOMINFOTIK Sumbawa masih terbilang sederhana dikarenakan sistem keamanan jaringan yang masih menggunakan *Firewall* dari *Router mikrotik*. Keamanan seperti ini sangat rentan terhadap serangan karena celah atau hak akses untuk masuk ke jaringan belum dibatasi. Hal ini terbukti dengan adanya serangan yang terjadi pada sistem keamanan jaringan DIKOMINFOTIK seperti *XSS* dan *MySQL Injection*. Oleh karena itu diperlukannya suatu usaha pencegahan dan pendeteksian untuk membantu keamanan data pada suatu jaringan komputer.

Dalam sebuah penelitian yang berjudul "Deteksi Penyusupan Pada *Server* Menggunakan Metode *Intrusion Detection System* (IDS) Berbasis *SNORT*" menyatakan bahwa IDS *SNORT* mampu mendeteksi adanya penyusupan kedalam *Server* atau jaringan (Wijaya & Pratama, 2020). Adapula penelitian lain yang berjudul "Mengoptimalkan Keamanan Jaringan Komputer Menggunakan *SNORT* dan Telegram Bot Yang Terintegrasi Dengan Mikrotik" menyatakan bahwa Penerapan *Intrusion*

Detection System (IDS) *SNORT* dan Telegram Bot berhasil dan dapat diintegrasikan dengan *router mikrotik* setelah dilakukannya pengujian dengan hasil 95% yang menunjukan bahwa pengguna *SNORT* dan Telegram Bot dapat mengoptimalkan sistem keamanan jaringan informasi (I Putu Gede Abdi Sudiatmika, dkk., 2022). Serta Penelitian lainnya yang berjudul "Keamanan Jaringan Menggunakan Teknik *Network Intrusion Detection System* (NIDS) Di Kantor Setwan Kepulauan Riau" Menyatakan bahwa Penelitian penelitian ini menyimpulkan bahwa apapun penyerangan yang dilakukan terhadap sistem keamanan jaringan dapat dideteksi oleh mesin sensor sehingga dapat dilakukan pencegahan sebelum terjainya kerusakan data yang luas (CL Ari Setiawan, dkk., 2020).

Maka dari itu tujuan dari dilakukannya penelitian ini untuk mengidentifikasi dan mengevaluasi sebuah potensi terjadinya resiko keamanan jaringan serta menerapkan solusi yang mampu melindungi sistem jaringan dari serangan yang berbahaya.

STUDI LITERATUR

1. Analisis

Analisis adalah kegiatan berpikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda komponen, hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu (Nalil Khairiah Dr. Siti Hajar & Pd, 2022). Pendapat lain juga mengatakan bahwa analisis proses memahami suatu fenomena atau peristiwa dengan mengidentifikasi pola atau tema yang muncul dari data yang dikumpulkan (John W. Creswell, 2007).

2. Jaringan

Jaringan merupkan sebuah jaringan yang terdiri dari banyak komputer dan peragkat lain yang terhubung bersama sehingga mereka dapat berkomunikasi satu sama lain (Andrew S. Tanenbeum 2017). Jaringan juga adalah kumpulan node atau host yang terhubung untuk bertukar data dan sumber daya (W. Richard Stevens 2001). Pendapat lain juga mengatakn bahwa jaringan adalah kumpulan dari dua atau lebih perangkat komunikasi yang saling berhubungan dan dapat berkomunikasi satu sama lain (Douglas E. Comer 2004).

3. *Intrusion Detection System (IDS)*

Intrusion Detection System (IDS) adalah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan (Indonesia, 2018). Pendapat lain juga mengatakan bahwa IDS adalah sistem yang memantau aktivitas jaringan dan memberi peringatan saat aktivitas mencurigakan atau aneh terdeteksi (Bejtlich, 2013).

4. *Firewall*

Firewall adalah sistem keamanan jaringan yang bertugas melindungi jaringan dari serangan yang tidak diinginkan dengan cara membatasi akses ke jaringan (William Stallings, 2013). Pendapat lain juga mengatakan bahwa *Firewall* adalah sistem atau perangkat lunak yang dirancang untuk mengontrol dan memantau lalu lintas jaringan dari jaringan yang dapat mencegah akses dari sumber yang tidak dipercaya (Andrew S.Tanenbaum, 2011).

5. *Quality of Service (QoS)*

Quality of Service (QoS) merupakan mekanisme jaringan yang memungkinkan aplikasi-aplikasi atau layanan dapat beroperasi sesuai dengan yang diharapkan (com, 2014). Pendapat lain juga mengatakan bahwa *Quality of Service (QoS*) merupakan kemampuan jaringan mengelola lalu lintas data berdasakan kecepatan, keandalan, dan latency memastikan kualtas layanan yang optimal kepada para pengguna (Alhazzazi, 2018).

a. Throughput

Throughput adalah jumlah bit atau byte data yang berhasil ditransfer pada satu waktu (perdetik) antara pengirim dan penerima dalam jaringan telekomunikasi (Forouzan, 2013). Pendapat lain juga mengatakan bahwa *Throughput* adalah jumlah data yang berhasil dikirim dari satu titik jaringan ke titik jaringan lainnya pada waktu tertentu (Stallings, 2013).

b. Jitter

Jitter adalah variasi waktu kedatangan paket data karena perbedaan jarak, rute dan beban lalu

lintas jaringan. Getaran diukur dalam satuan waktu seperti, mikrodetik atau milidetik (Forouzan, 2013). Pendapat lain juga mengatakan bahwa jitter adalah variasi *Delay*, yaitu perbedaan selang waktu kedatangan antar paket di terminal tujuan. Untuk mengatasi jitter maka paket data ditentukan sampai paket dapat diterima pada sisi penerima dengan urutan yang benar (Yuliandoko, 2018).

Tabel 1. Standarisasi *Jitter* Versi *TIPHON*

Kategori Degradasi	Peak Jitter
Sangat bagus	0 ms
Bagus	0 s/d 75 ms
Sedang	76 s/d 125 ms
Jelek	125 d 255 ms

c. Packet Loss

Packet Loss adalah paket terjadi Ketika paket data hilang saat dikirim dari satu perangkat jaringan ke perangkat lainnya. Ini bisa jadi karena kapasitas jaringan yang terbatas atau kemacetan jaringan (Kurose, 2017).

Tabel 2. Standarisasi *Packet Loss versi TIPHON*

Kategori Degradasi	*Packet Loss*
Sangat bagus	0
Bagus	3 %
Sedang	15 %
Jelek	25 %

d. Latency

*Latenc*y didefinisikan sebagai waktu yang dibutuhkan pesan untuk mencapai tujuannya dari sumbernya (William Stallings, 2017). Pendapat lain juga mengatakan bahwa latency adalah waktu yang dibutuhkan pesan untuk melakukan perjalanan dari sumber ke tujuannya (Andrew S.Tanenbaum, 2011).

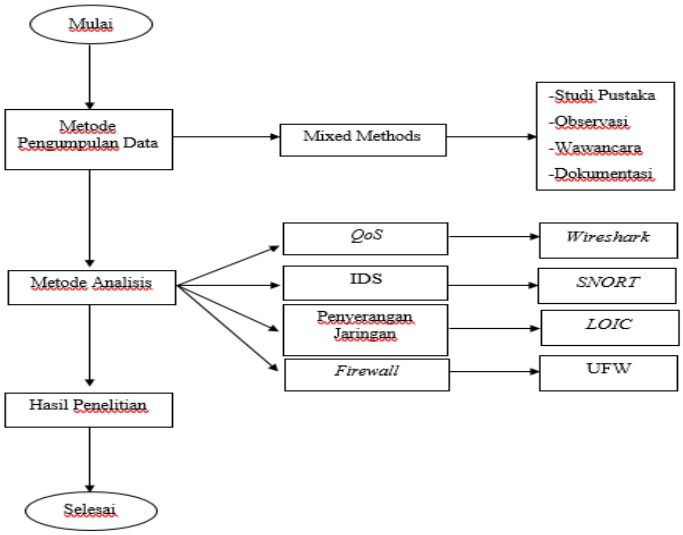
Tabel 3. Standarisasi *Latency/Delay versi TIPHON*

Kategori Latency	Besar *Delay*
Sangat bagus	<150 ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Jelek	>450 ms

METODE

3.1 Metode Peneltian

Dalam melakukan penelitian ini, Peneliti menggunakan analisa penelitian dengan metode *Intrusion Detection System* (IDS). Hal ini dikarenakan permasalahan yang menggambarkan atau mendeskripsikan keadaan subjek atau objek yang diteliti. Adapun pada tahapan analisis sistem jaringan yaitu sebagai berikut :



Gambar 1. Alur Metode Penelitian

Berdasarkan dari kerangka berpikir dalam metode penelitian ini ada beberapa tahapan yang dilakukan Tahapan pertama yaitu metode pengumpulan data dimana peneliti disini menggunakan metode mixed methods yang merupakan gabungan antara metode kuantitatif dan kualitatif sehingga ada beberapa langkah yang dilakukan dalam melakukan metode pengumpulan data seperti melakukan observasi, wawancara, studi Pustaka, dan dokumentasi. Selanjutnya tahapan kedua yaitu metode analisis dimana peneliti disini melakukan pengukuran parameter *QoS* Menggunakan Tools *Wireshark*, *Intrusion Detection System* (IDS) dengan tools *SNORT*, Penyerangan Jaringan melalui aplikasi *LOIC*, dan penerapan *Firewall* menggunakan Uncomplicated *Firewall* (UFW).

3.2 Metode Analisis Sistem

1. *Quality of Service (QoS)*

   Dalam metode analisis sistem ini *QoS* digunakan untuk mengukur parameter pada jaringan komputer menggunakan Tools *Wireshark* dengan cara mengukur *Throughput, Packet Loss, Jitter, dan Latency* sebelum dan sesudah diterapkannya metode IDS ini
2. *Intrusion Detection System (IDS)*

   IDS akan memantau dan memonitoring lalu lintas jaringan menggunakan Tools *SNORT* dengan database yang menyimpan informasi tentang berbagai jenis intrusi atau serangan. Jika kecocokan ditemukan maka IDS dapat mendeteksi adanya serangan dan memberikan peringatan.
3. Penyerangan Jaringan

   Penyerangan jaringan disini dilakukan dengan menggunakan Tools *LOIC* untuk mengirimkan serangan berupa packet data yang banyak sesuai request yang diinginkan. Sehingga nantinya mampu menyebabkan adalah permasalahan pada *Server* atau jaringan.
4. *Firewall*

   Dalam keamanan jaringan disini menggunakan UFW agar dapat memblokir serangan sesuai dari hasil monitoring jaringan yang terjadi apabila ada jaringan yang mencurigakan..Dengan menginput beberapa konfigurasi didalam sistem UFW ini.
5. Hasil Penelitian

   Setelah dilakukannya uji coba analisis sistem tahapan selanjutnya yaitu membuat laporan hasil yang dimana laporan ini menjadi bukti bahwa telah dilakukannya penelitian

dengan judul Analisis Keamanan Jaringan *Menggunakan Intrusion Detection System (IDS)* dan *Firewall.*

HASIL

Hasil penelitian ini menunjukan bahwa pengujian parameter QoS sebelum diterapkannya sistem keamanan jaringan seperti nilai Throughput 5734 Kb/s, Packet Loss 10,1% yang terbilang tinggi dan nilai Delay 1,159116 ms, Jitter 1,159147 ms yang terbilang rendah, Sedangkan hasil ketika sudah dterapkannya sistem keamanan jaringan menunjukan bahwa nilai Throughput 387 Kb/s, Packet Loss 0,1% yang terbilang rendah dari sebelumnya dan nilai Delay 14,821861 ms, Jitter 14,822145 ms yang terbilang tinggi dari sebelumnya.

PEMBAHASAN

1. Pengukuran parameter QoS sebelum penyerangan keamanan jaringan
   a. Throughput
      Rumus = Jumlah Bytes : Time Span = 26480222 : 36,940 s
      = 716.844,125 Byte/s
      = 5.734,753 Bit/s
      = 5734 Kb/s

      Pada gambar dan rumus diatas adalah hasil dari *Throughput* pada pengujian pertama di DISKOMINFOTIK Sumbawa yang direkam melalui aplikasi *Wireshark* dan kemudian dilakukan penjumlahan untuk mendapatkan hasil yang benar.
   b. Packet Loss
      Rumus = ((Paket dikirim – Paket diterima) / Paket dikirim) x 100
      = ((31870 - 28639) / 31870) x 100
      = 10,1%

      Pada gambar dan rumus diatas, menunjukan bahwa total *Packet Loss* adalah 10,1% yang artinya menunjukan ada beberapa paket data yang hilang.
   c. Delay
      Total *Delay* = 36,939878
      Rata-rata *Delay* = 0,001159116
      = 1,159116 ms

      Pada gambar diatas, menunjukan hasil dari rekaman data pengujian *Wireshark* yang telah dimasukan ke dalam *Microsoft Excel* dan dilakukan penjumlahan pada *Excel*.
   d. Jitter
      Total Jitter = 36,940856
      Rata-rata Jitter = 0,001159147
      = 1,159147 ms

      Gambar diatas, menunjukan hasil yang didapatkan saat melakukan perjumlahan pada *Microsoft Excel*, yang dimana nilai jitter dicari setelah mendapatkan nilai dari proses *Delay*.

2. Pengukuran parameter QoS setelah penyerangan keamanan jaringan
   a. Throughput
      Rumus = Jumlah Bytes : Time Span = 21981146 : 453,668 s
      = 48,452.053 Byte/s
      = 387,616 Bit/s
      = 387 Kb/s

      Pada gambar dan rumus diatas adalah hasil dari *Throughput* pada pengujian kedua di DISKOMINFOTIK Sumbawa yang direkam melalui aplikasi *Wireshark* dan kemudian di lakukan penjumlahan untuk mendapatkan hasil yang benar.

b. Packet Loss
Rumus = ((Paket dikirim – Paket diterima) / Paket dikirim) x 100
= ((30609 – 30.565) / 30609 x 100
= 0,1%

Pada gambar dan rumus diatas, menunjukan bahwa total *Packet Loss* adalah 0,1% yang artinya ada beberapa paket yang hilang.

c. Delay
Total *Delay* = 453,667512
Rata-rata *Delay* = 0,014821861
= 14,821861 ms

Pada gambar diatas, menunjukan hasil dari rekaman data pengujian *Wireshark* yang telah dimasukan ke dalam *Microsoft Excel* dan dilakukan penjumlahan pada *Excel*.

d. Jitter
Total Jitter = 453,676211
Rata-rata Jitter = 0,014822145
= 14,822145 ms

Pada gambar diatas, menunjukan hasil yang didapatkan saat melakukan penjumlahan pada *Microsoft Excel*, yang dimana nilai jitter dicari setelah mendapatkan nilai dari proses *Delay*.

3. Perbandingan parameter QoS sebelun dan setelah dilakukannya penyerangan jaringan

a. Throughput

Berdasarkan gambar di atas, terlihat pada pengujian pertama yaitu sebelum memiliki nilai *Throughput* yang lebih tinggi yaitu 5734k, Pada pengujian kedua sesudah memiliki nilai *Throughput* 387k yang dimana lebih rendah dibandingkan dengan nilai *Throughput* sebelumnya.

Kesimpulannya *Throughput* sesudah dilakukannya penyerangan dan keamanan jaringan memiliki nilai yang bagus akan tetapi masih lebih baik hasil *Throughput* sebelum dilakukannya penyerangan dan keamanan jaringan.

b. Packet Loss

Berdasarkan gambar diatas, terlihat pada pengujian pertama yaitu sebelum memiliki nilai *Packet Loss* yang lebih tinggi yaitu 10,1% . Pada pengujian kedua sesudah memiliki nilai *Packet Loss* yang lebih rendah yaitu 0,1%.

Kesimpulannya *Packet Loss* sesudah dilakukannya penyerangan dan keamanan jaringan memiliki nilai yang lebih baik daripada sebelum dilakukannya penyerangan dan keamanan jaringan.

c. Delay

Berdasarkan gambar diatas, terlihat pada pengujian pertama yaitu sebelum memiliki nilai *Delay* yang lebih rendah yaitu 1,159116 ms. Pada pengujian kedua sesudah memiliki nilai *Delay* 14,821861 ms yang dimana lebih tinggi dibandingkan dengan nilai *Delay* sebelumnya.

Kesimpulannya nilai *Delay* sesudah dilakukannya penyerangan dan keamanan jaringan memiliki nilai yang lebih baik daripada sebelum dilakukannya penyerangan dan keamanan jaringan.

d. Jitter

Berdasarkan gambar diatas, terlihat pada pengujian pertama yaitu sebelum memiliki nilai jitter yang lebih rendah yaitu 1,159147 ms. Pada pengujian kedua sesudah memiliki nilai jitter 14,822145 ms yang dimana lebih tinggi dibandingkan dengan nilai jitter sebelumnya.

Kesimpulannya nilai jitter sesudah dilakukannya penyerangan dan keamanan jaringan memiliki nilai yang bagus, akan tetapi masih lebih baik nilai jitter sebelum dilakukannya penyerangan dan keamanan jaringan.

KESIMPULAN

Dalam penelitian terhadap keamanan jaringan DISKOMINFOTIK Sumbawa, diketahui bahwa serangan menggunakan aplikasi LOIC berhasil menemukan celah keamanan pada jaringan komputer. Namun, implementasi sistem keamanan telah berhasil dalam menghadapi serangan ini dengan memberikan pemberitahuan "connection error: time out". Hasil penelitian ini memberikan gambaran bahwa teknisi dan admin jaringan perlu meningkatkan kualitas keamanan jaringan dengan langkah-langkah preventif dan responsif yang lebih efektif terhadap serangan-serangan potensial seperti yang diidentifikasi dalam penelitian tersebut sehingga Implementasi sistem keamanan yang efektiif dapat menjadi solusi untuk melindungi jaringan dari serangan di masa mendatang.

REFERENSI

Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press. https://books.google.co.id/books?id=QdLclhJhQecC

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and Conducting Mixed Methods Research*. SAGE Publications. https://books.google.co.id/books?id=eTwmDwAAQBAJ

Dian K. P., M. P. P. (2008). *75 Cara Ampuh Lolos Wawancara Kerja*. WahyuMedia. https://books.google.co.id/books?id=vMlAKAY4OTkC

Gede, I. P., Sudiatmika, A., Yesha, I. P., Ariwanta, A., Ayu, I. G., & Melati, S. (2022). *Mengoptimalkan Keamanan Jaringan Komputer Menggunakan Snort dan Telegram Bot yang Terintegrasi dengan Mikrotik*. *3*(4), 247–256. https://doi.org/10.47065/josyc.v3i4.2037

Setiawan, C. L. A., Tria, A., & Abza, P. (2020). *Keamanan Jaringan Menggunakan Teknik Network Intrusion Detection System (NIDS) Di Kantor Setwan Kepulauan Meranti*. *4*(2).

Wijaya, B., & Pratama, A. (2020). *Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort*. *09*, 97–101.

Com, V. (2014). *Tips & Trik Jaringan Wireless*. Elex Media Komputindo. https://books.google.co.id/books?id=C4lKDwAAQBAJ

Nalil Khairiah Dr. Siti Hajar, D. A. J. R. I. A. M., & Pd, M. A. M. P. W. M. (2022). *Prosiding Seminar Nasional Perencanaan Pembangunan Daerah Dan Kebijakan Daerah 2021*. umsu press. https://books.google.co.id/books?id=Y5VaEAAAQBAJ