Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI) p-ISSN: 2620 – 5327
Volume 7 Nomor 1, April 2024 e-ISSN: 2715 – 5501
DOI : 10.57093/jisti.v7i1.195

Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System (WIDS)

Andi Irfan[1], **Andi Zulkifli Nusri**[2], **Zul Rachmat**[3], **Sri Wulandari**[4]
Program Studi Teknik Informatika, Universitas Lamappapoleonro[1,2]
Jl. Kesatria No.56, Kabupaten Soppeng, Sulawesi Selatan, Indonesia[1,2]
Program Studi Manajemen Informatika, STMIK AMIKA SOPPENG[3,4]
Jl. Bukit Tujuh Wali-wali, Kabupaten Soppeng, Sulawesi Selatan, Indonesia[3,4]
irfan.andi2211@gmail.com[1] , andizulkifli51@gmail.com[2], zulrachmat@amiklps.ac.id[3] ,
sriwulan452@gmail.com[4]

Kata Kunci :
Keamanan jaringan;
Wireless intrusion detection;
Wireshark.

ABSTRAK

Penelitian ini membahas tentang analisis kualitas jaringan nirkabel pada kantor DPRD Kabupaten Soppeng. Penelitian ini bertujuan untuk mengimplementasikan *tools Wireless Intrusion Detection System* (WIDS) pada kantor DPRD Kabupaten Soppeng. Penelitian ini menggunakan metode yang mengadaptasi metode *System Development Life Cycle* (SDLC) mulai dari tahapan perencanaan, analisa, perancangan dan implementasi dengan cara memahami dan menyeleksi keadaan dan proses yang dilakukan pengguna untuk dapat mendukung kebutuhan pengguna, setelah melakukan tahapan perencanaan dan analisa. Adapun metode yang digunakan adalah *metode Wireless Intrusion Detection System (WIDS)* dengan menggunakan *Wireshark* sebagai *Tools*. Hasil penelitian menunjukkan *wireshark* dapat mendeteksi serangan yang dilakukan penyusup dengan melihat informasi dari hasil *capture* paket data yang dilakukan, mulai dari IP yang digunakan dan protokol apa yang digunakan. Setelah melakukan serangkaian pengujian dan analisis data, penggunaan metode WIDS dengan *Wireshark*, dapat mendeteksi serangan yang terjadi didalam sistem jaringan pada kantor DPRD Kabupaten Soppeng.

Keywords
Network security;
Wireless intrusion detection,
Wireshark.

ABSTRACT

This research discusses the analysis of the quality of the wireless network at the Soppeng Regency DPRD office. This research aims to implement Wireless Intrusion Detection System (WIDS) tools at the Soppeng Regency DPRD office. This research uses a method that adapts the System Development Life Cycle (SDLC) method starting from the planning, analysis, design and implementation stages by understanding and selecting the conditions and processes carried out by users to be able to support user needs, after carrying out the planning and analysis stages. The method used is the Wireless Intrusion Detection System (WIDS) method using Wireshark as a tool. The research results show that Wireshark can detect attacks carried out by intruders by looking at information from the data packet capture results, starting from the IP used and what protocol is used. After carrying out a series of tests and data analysis, using the WIDS method with Wireshark, was able to detect attacks that occurred in the network system at the Soppeng Regency DPRD office.

---Jurnal JISTI @2024---

PENDAHULUAN

Penggunaan internet dengan perangkat nirkabel berkembang sangat cepat sejalan dengan kebutuhan penggunaan sistem informasi. Teknologi wireless (tanpa kabel / nirkabel) saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi.

Komputer, Notebook, telepon seluler dan peripheralnya mendominasi pemakaian teknologi wireless. Penggunaan teknologi wireless yang diimplementasikan dalam suatu jaringan lokal sering dinamakan WLAN (Wireless Local Area Network). Namun perkembangan teknologi wireless yang terus berkembang sehingga terdapat istilah yang mendampingi WLAN seperti WMAN (Metropolitan), WWAN (Wide) dan WPAN (Personal/Private).

Kantor DPRD Kabupaten Soppeng menerapkan sistem akses jaringan menggunakan media kabel dan nirkabel untuk penggunaan sistem informasi yang ada pada kantor tersebut, baik sistem informasi *online* ataupun *offline*, juga untuk akses informasi menggunakan media internet, penggunaan jaringan komputer yang cukup krusial tentu memerlukan penanganan masalah dari segi keamanan pendeteksian lalulintas data atau paket-paket yang masuk. Serta permasalahan lainnya seperti penggunaan jaringan yang tidak semestinya, juga tidak adanya sistem keamanan jaringan yang bertujuan membatasi hak akses masuk ke dalam sistem jaringan, sehingga dapat menjadikan celah pada sistem keamanan jaringan dimana setiap orang dapat dengan lebih mudah masuk ke dalam lingkup jaringan Kantor DPRD Kabupaten Soppeng.

Keamanan jaringan adalah proses untuk melindungi sistem dalam jaringan dengan mendeteksi penggunaan yang berhak dalam jaringan. Pengelolahan terhadap pengendalian keamanan jaringan dapat dilihat dari sisi pengelolahan resiko (*Risk Management*). *Wireless Intrusion Detection System* (WIDS) dapat didefinisikan sebagai *tools*, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktifitas jaringan komputer. *Wireless Intrusion Detection System* secara khusus berfungsi sebagai proteksi secara keseluruhan dari sistem yang telah di instal WIDS. WIDS tidak berdiri sendiri dalam melindungi suatu sistem. Selain WIDS, juga terdapat sistem keamanan yang lain seperti *Intrusion Prevention System* (IPS), namun sistem ini hanya menggunakan parameter penyebaran *inline* atau satu jalur dan ketika mendeteksi potensi ancaman pengiriman peringatan sifatnya opsional sehingga bisa saja terjadi ancaman tapi tidak ada peringatan dari sistem. Sedangkan WIDS parameter penyebarannya melalui *spanning port* atau *network tap* dan ketika mendeteksi ancaman, peringatan akan secara otomatis terkirim.

Dalam upaya untuk meningkatkan keamanan jaringan komputer yang ada pada kantor DPRD Kabupaten Soppeng salah satunya adalah dengan *firewall*. Implementasi dari sistem *firewall* ini dapat berupa software ataupun hardware yang bersifat aktif dengan melakukan penyaringan paket data yang lewat berdasarkan pengaturan yang diinginkan. Cara lain adalah dengan mengimplementasikan *Wireless Intrusion Detection System* (WIDS) pada sebuah Jaringan Komputer. Sedikit berbeda dengan *firewall*, *Wireless Intrusion Detection System* (WIDS) adalah sebuah sistem yang digunakan untuk. melakukan deteksi adanya usaha-usaha penyusupan terhadap sebuah sistem dengan melakukan pengamatan trafik data secara real-time

KAJIAN PUSTAKA

1. Pengertian Jaringan Komputer.

Jaringan komputer adalah salah satu teknologi yang menjadi tulang punggung dari dunia komunikasi dan pertukaran informasi di era digital saat ini. Secara sederhana, jaringan komputer adalah kumpulan perangkat komputer yang terhubung bersama-sama untuk berbagi data, sumber daya, dan layanan. Menurut (Wardana & Nusri, 2022) Sebuah jaringan biasanya terdiri dari dua atau lebih PC yang saling berhubungan satu sama lain, dan berbagi sumber daya misalnya, CD ROM, printer, pertukaran data, atau memungkinkan untuk berkomunikasi dengan lain secara elektronik,sedangkan menurut (Arman Muhajir & Kasran, 2023) Definisi jaringan komputer mencakup berbagai elemen

teknis dan konseptual yang memungkinkan komputer dan perangkat lainnya untuk berkomunikasi dan berinteraksi satu sama lain.

2. Konsep dan Arsitektur Jaringan

Menurut (Sofana, 2013) jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer, dalam bahasa populer dapat di jelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer, dan perangkat lain seperti *router, switch* dan sebagainya. Sedangkan menurut (Wardana & Nusri, 2022) Sebuah jaringan biasanya terdiri dari dua atau lebih PC yang saling berhubungan satu sama lain, dan berbagi sumber daya misalnya, CD ROM, printer, pertukaran data, atau memungkinkan untuk berkomunikasi dengan lain secara elektronik.

3. Sistem Keamanan Jaringan

Menurut (Nugroho, 2019) Kehandalan jaringan menjadi tujuan utama dari proses awal sebuah perencanaan jaringan. Pengguna jaringan akan merasa lebih 'nyaman' jika menggunakan jaringan handal (*reliable*). Jaringan dapat dikatakan handal apabila sudah memenuhi parameter berikut:

a) Fault tolerance

Parameter *fault tolerance* didefinisikan sebagai istilah yang mengijinkan jalur utama yang digunakan untuk mengalirkan data dari sumber ke tujuan menjadi tidak berfungsi, namun harus disediakan jalur cadangan agar ketika jalur utama putus, data masih bisa dialirkan ke perangkat tujuan.

b) Skalabilitas

Tujuan dari adanya skalabilitas adalah untuk menjaga performasi dari sebuah jaringan. Skalabilitas dari sebuah jaringan mempunyai definisi bahwa keberadaan jaringan yang baru harus tidak mempengaruhi performasi jaringan yang lama.

c) *Qos* (*Quality of Service*)

Menurut (Nurnaningsih et al., 2022) bahwa terdapat 3 tingkat Qos yang umum dipakai, yaitu *Best-effort service, intergrated service* dan *Differentiated service*. *Quality of Service* digunakan untuk mengukur tingkat kinerja koneksi jaringan TCP/IP internet atau jaringan komputer. Qos memungkinkan administrator jaringan untuk memprotitaskan lalu lintas tertentu. *Quality of Service (QoS)* memberikan kemampuan untuk mendefinisikan atribut layanan yang disediakan baik secara kualitas ataupun kuantitas Qos akan menjamin data yang penting mendapatkan prioritas utama untuk diteruskan keperangkat tujuan. Data yang penting identik dengan data yang sifatnya *real time*, misalnya data suara atau video. Kedua jenis antrian perangkat sebuah jaringan dibandingkan data yang sifatnya unreal time seperti data teks dan gambar.

d) Keamanan

Keamanan jaringan menjadi bagian yang sangat penting dalam proses komunikasi data dalam sebuah jaringan. Data yang dikirim oleh penerima yang sah. Sehingga hal terpenting dalam keamanan jaringan adalah bagaimana menjamin data tidak diambil dan dibaca oleh pengguna lain yang tidak sah.

4. Definisi Denial of Service (DDoS)

Dalam komputasi, sebuah serangan *denial-of-service* (serangan DoS) adalah serangan dunia maya di mana pelaku berupaya membuat mesin atau sumber daya jaringan tidak tersedia bagi pengguna yang dituju dengan mengganggu layanan *host* yang terhubung ke Internet untuk sementara atau tanpa batas. *Denial of service* biasanya dicapai dengan membanjiri mesin atau sumber daya yang ditargetkan dengan permintaan yang berlebihan dalam upaya untuk membebani sistem dan mencegah beberapa atau semua permintaan yang sah agar tidak terpenuhi (Santoso, 2018). Dalam

sebuah serangan penolakan layanan secara terdistirbusi, Lalu lintas masuk yang membanjiri korban berasal dari berbagai sumber. Ini secara efektif membuat tidak mungkin menghentikan serangan hanya dengan memblokir satu sumber. Menurut (Kurniawan, 2012) Serangan DoS atau DDoS dapat dianalogikan dengan sekelompok orang yang memenuhi pintu masuk toko, sehingga menyulitkan pelanggan yang sah untuk masuk, sehingga mengganggu perdagangan. Pelaku kriminal serangan DoS sering menargetkan situs atau layanan yang dihosting di *Server web* profil tinggi seperti bank atau *gateway* pembayaran kartu kredit. Balas dendam, pemerasan dan aktivisme dapat memotivasi serangan ini

5. Definisi Intrusion Detection System

Menurut (Santoso, 2018) *Intrusion Detection System* dapat didefinisikan sebagai tool, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap jaringan computer. *Intrusion Detection System* (IDS) sebenarnya tidak cocok di beri peringatan tersebut karena IDS tidak mendeteksi penyusup tetapi hanya mendeteksi aktivitas pada lalu lintas jaringan yang tidak layak terjadi. *Intrusion Detection System* secara khusus berfungsi sebagai proteksi secara keseluruhan dari sistem yang telah diinstall IDS. IDS tidak berdiri sendiri dalam melindungi suatu sistem. IDS melakukan scanning terhadap lalu lintas yang masuk dan keluar dalam sebuah jaringan kemudian melakukan analisis dan mencari bukti dari percobaan penyerangan yang dilakukan peretas

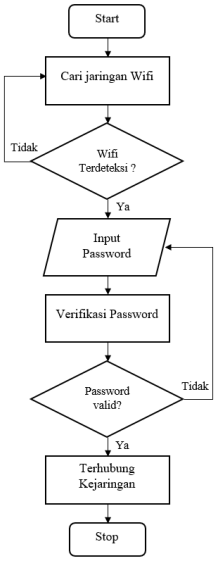
METODE PENELITIAN

1. Teknik Pengumpulan Data

Teknik pengumpulan data yang dilakukan penulis dalam mengumpulkan data untuk penelitian ini adalah :

a) Observasi
   Teknik pengumpulan data yang dilakukan penulis dengan cara pengamatan langsung ditempat penelitian. Tujuan dari observasi ini adalah untuk memperoleh data yang diinginkan dalam objek penelitian.
b) Wawancara
   Teknik pengumpulan data yang dilakukan penulis dengan cara melakukan wawancara secara langsung dengan pihak yang berkompeten di tempat penelitian. Penulis melakukan wawancara dengan staf bagian teknologi informasi (IT).
c) Studi Literatur
   Teknik pengumpulan data yang dilakukan penulis dengan cara mencari referensi mengenai objek penelitian yang diperoleh dari buku, jurnal, dan penelitian terdahulu

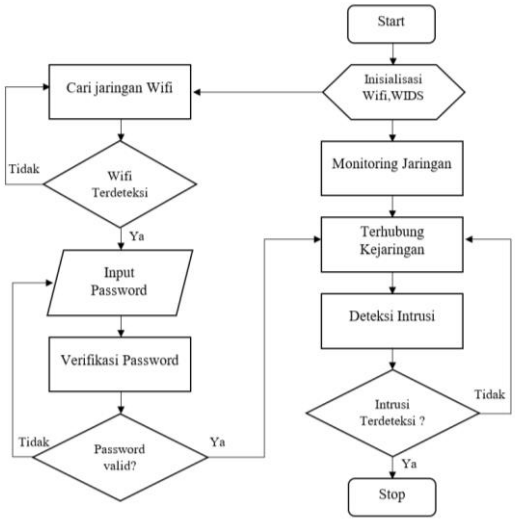
2. Flowchart Sistem yang Berjalan



Gambar 1. Flowchart Sistem yang diUsulkan

Penggunaan jaringan dapat dilihat pada flowchart, dimana pengguna mencari jaringan wifi, jika jaringan terdeteksi maka pengguna harus menginput password, jika password benar maka akan terhubung kejaringan melalui wifi, penggunaan jaringan ini sangat berbahaya karena tidak adanya sistem keamanan jaringan yang bertujuan memantau pengguna yang masuk dalam sistem jaringan, sehingga dapat menjadi celah pada sistem keamanan jaringan dimana setiap orang dapat dengan mudah masuk kesistem jaringan dan pengguna bisa saja melakukan aktivitas berbahaya seperti *phising, sniffing, bruteforce* dan aktifitas lain yang membahayakan keamanan data

3. Flowchart Sistem yang diUsulkan



Gambar 2. Flowchart Sistem yang diUsulkan

Pada flowchart sistem yang diusulkan, proses pertama kali yang lakukan adalah inisialisasi perangkat dan aplikasi yang digunakan dalam jaringan, pengguna mencari jaringan wifi yang tersedia kemudian melakukan koneksi dengan menginput password, setelah berhasil terhubung dijaringan, aplikasi WIDS akan memonitoring pengguna yang terhubung kejaringan tersebut. Jika WIDS

mendeteksi intrusi maka akan memutuskan jaringan pengguna tersebut dan jika tidak maka akan terus terhubung kejaringan.

Aplikasi yang digunakan untuk melakukan monitoring adalah *snort*, *Snort* adalah salah satu aplikasi deteksi intrusi (intrusion detection system/IDS) yang populer dan dapat digunakan untuk memantau lalu lintas jaringan guna mendeteksi dan mencegah serangan pada sistem komputer. Ada pun yang dimonitoring adalah Deteksi Intrusi yaitu mendeteksi aktivitas yang mencurigakan atau serangan pada jaringan komputer, Analisis Protokol yaitu *Snort* dapat menganalisis lalu lintas jaringan pada berbagai protokol seperti TCP/IP, UDP, ICMP, dan lainnya. Hal ini memungkinkan *Snort* untuk mengenali serangan yang menggunakan kerentanan dalam protokol tersebut. Logging dan Pemantauan yaitu *Snort* dapat mencatat aktivitas jaringan dalam bentuk log yang mencakup informasi penting seperti sumber dan tujuan serangan, protokol yang digunakan, tipe serangan, waktu terjadinya, dan lainnya. Log ini dapat dianalisis untuk mengevaluasi serangan, mengidentifikasi tren, atau mengambil tindakan yang diperlukan

HASIL DAN PEMBAHASAN

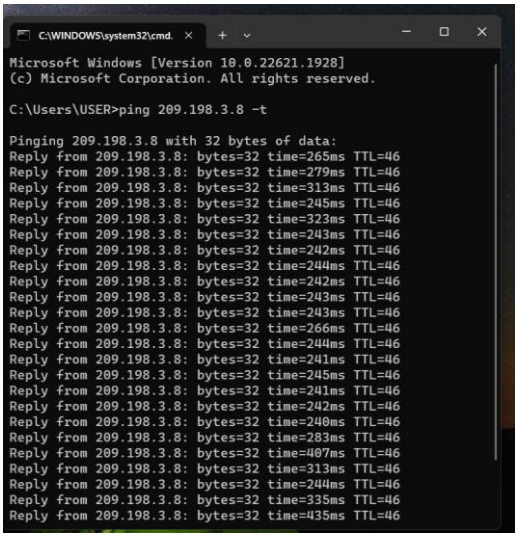
1. Implementasi

Implementasi sistem kemanan jaringan wireless menggunakan aplikasi *wireshark* yang dipasan pada komputer yang menggunakan sistem operasi windows untuk melakukan monitoring jaringan. Simulai intrusi pada jaringan dilakukan pemasangan aplikasi *NMap* yang berfungsi sebagai *scanner port* yang aktif, dan aplikasi *open source LOIC* sebagai penyerang *DDOS*

2. Pengujian

a) Pengujian tanpa aplikasi

Pengujian awal dilakukan tanpa menggunakan aplikasi khusus, pengujian ini menggunakan *command prompt* untuk mengetahui apakah kedua perangkat telah terhubung dengan baik dengan menggunakan perintah ping. IP target adalah 209.198.3.8 dan IP penyerang adalah 10.153.186.227, seperti pada gambar berikut :

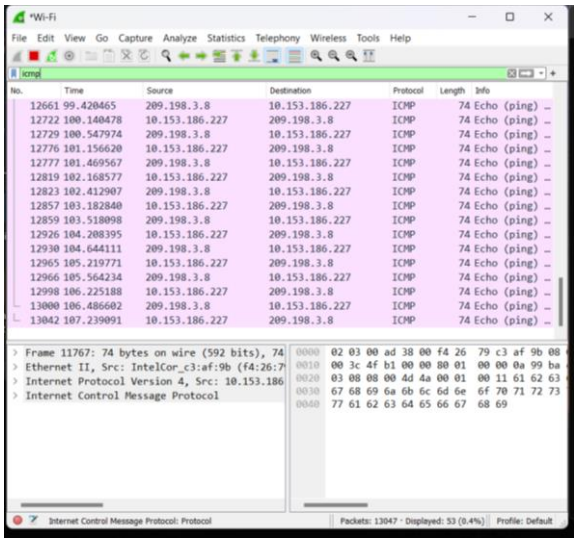


Gambar 3. Pengujian Ping ke Target

Gambar 3 menunjukkan bahwa ada reply dari IP 209.198.3.8 yang menandakan telah terjadi komunikasi antara komputer target dan komputer penyerang. Pada pengujian ini juga dilakukan monitoring oleh wireshark dengan mengcapture lalu lintas jaringan dalam keadaan

p-ISSN: 2620 – 5327
e-ISSN: 2715 – 5501

normal atau hanya menunjukkan kegiatan lalulintas yang biasa yaitu hanya melakukan ping antara dua komputer seperti terlihat pada gambar berikut :



Gambar 4. Capture Ping Wireshark

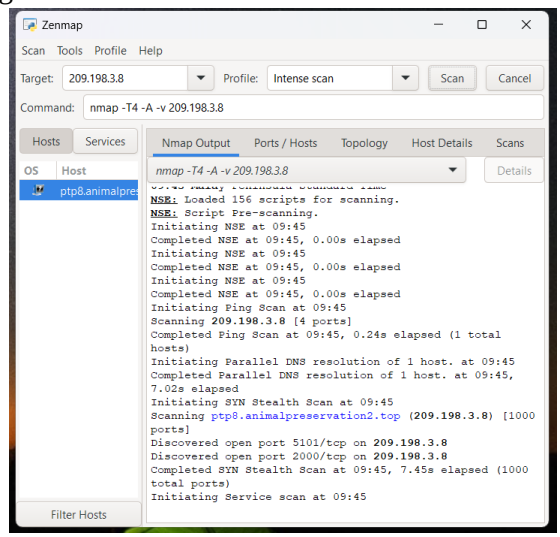
Dari gambar 4 dapat dilihat *wireshark* mengcapture paket-paket data yang dinyatakan sebagai lalulintas normal dari jaringan tersebut. Pada kolom *destination* terdapat IP masing-masing komputer dalam melakukan komunikasi

b) Pengujian menggunakan Aplikasi

Setelah melakukan pengujian awal tanpa aplikasi khusus, selanjutnya dilakukan pengujian dengan menggunakan aplikasi yang akan melakukan penyerangan menggunakan aplikasi *Nmap dan LOIC*

1) Scanning port menggunakan Nmap

Simulasi pertama dilakukan dengan *scanning port* terhadap komputer target dengan memasukkan IP 209.198.3.8 dan melakukan scan maka akan terlihat *port-port* yang terbuka seperti pada gambar berikut :

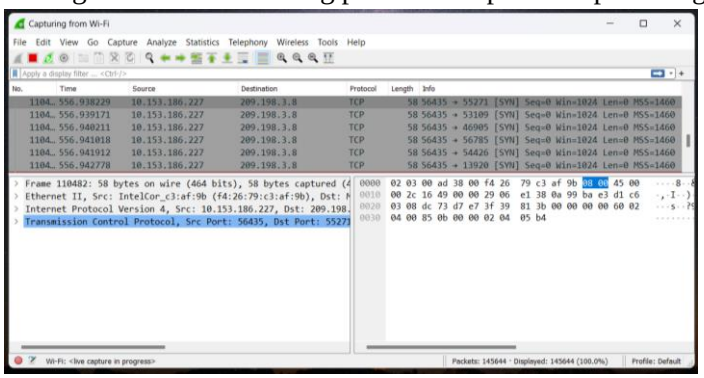


Gambar 5. Scanning port nmap

Setelah melakukan *scanning port* pada Nmap, selanjutnya pada wireshark bisa dilihat adanya lalulintas data yang tidak biasa yang menunjukkan adanya kegiatan penyerangan *port scanning*, dari kolom *source* terdapat IP dari komputer penyerang yaitu

p-ISSN: 2620 – 5327
e-ISSN: 2715 – 5501

10.153.186.227. pada kolom destination adalah IP 209.198.3.8 yang merupakan komputer target. Protocol yang digunakan adalah TCP dan pada kolom info menunjukkan bahwa port dari penyerang sedang melakukan scanning pada semua port komputer target



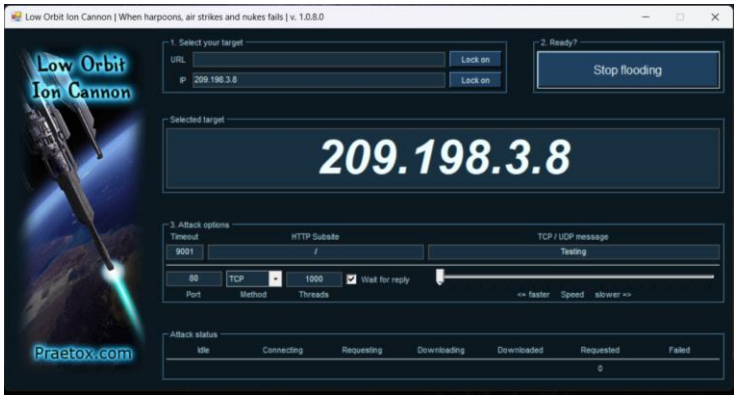
Gambar 6. Wireshark Mendeteksi Scanning Port Nmap

2) Serangan DDoS menggunakan LOIC

Pengujian berikutnya menggunakan aplikasi *open source LOIC.* Penyerangan menggunakan *LOIC* ini akan mengirimkan data terus menerus sehingga komputer target lumpuh.

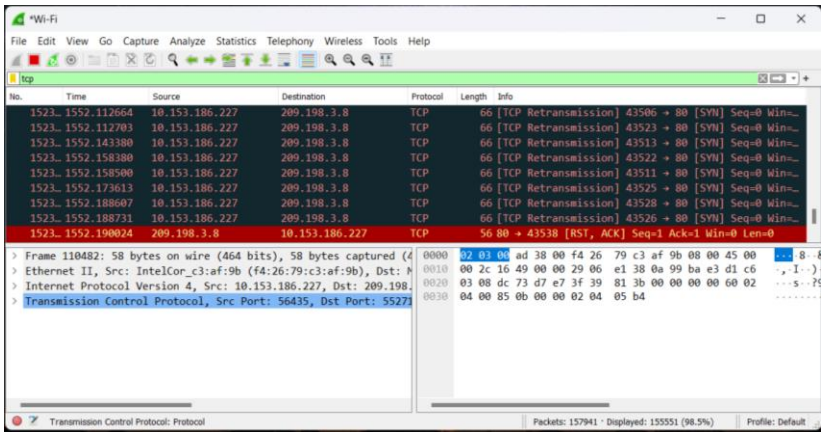
a. Serangan DDoS TCP

Pada pengujian ini dilakukan penyerangan dengan mengirim data sebanyak mungkin yang mengakibatkan peningkatan kinerja pada CPU bahkan terjadi *hang* bahkan mati. Tampilan *LOIC* dapat dilihat pada gambar 7 berikut dimana simulasi serangan dilakukan dengan menginput IP target 209.198.3.8 selanjutnya memilih port TCP dan protocol target.



Gambar 7. DDoS Attack menggunakan LOIC TCP

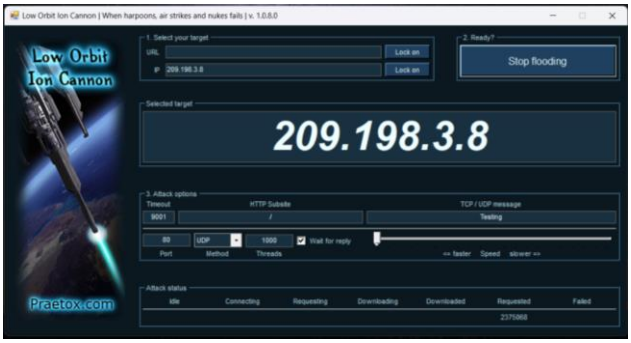
Setelah melakukan serangan, *wireshark* mendeteksi adanya lalulintas data yang tidak biasa seperti pada gambar 8, dari kolom *source* terdapat IP dari komputer yang melakukan serangan yaitu 10.153.186.227. Dan kolom destination adalah IP 209.198.3.8 yang merupakan komputer target, dikolom info dapat dilihat adanya pengiriman data yang dilakukan secara teru menerus dengan inisial paket SYN dari IP 10.153.186.227 melalui banyak *port* kesatu *port* yaitu *port* 80 dengan protocol TCP



Gambar 8. Wireshark Mendeteksi serangan DDoS TCP

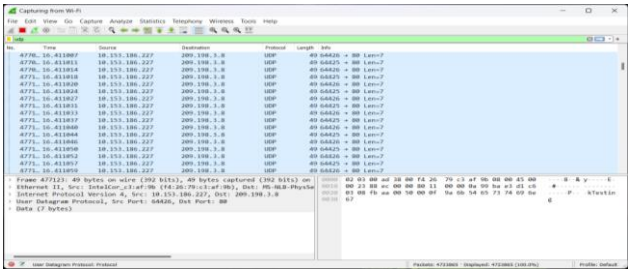
b. Serangan DDoS UDP

Simulasi berikutnya dilakukan serangan DDoS melalui protokol UDP dengan menentukan *port* mana yang akan diserang dengan mengirimkan banyak paket data. LOIC mengirim serangan berupa DDoS melalui port 80 hingga komputer target lumpuh seperti pada gambar 9 berikut :



Gambar 9. DDoS Attack menggunakan LOIC UDP

Pada simulasi ini *wireshark* mendeteksi adanya kegiatan yang tidak normal seperti pada gambar 0 ditandai dengan adanya IP penyerang pada kolom source menggunakan protocol UDP. Dari paket yang terkirim pada jaringan dapat dilihat adanya aktivitas mencurigakan menuju port 80 secara terus menerus dari IP 10.153.186.227, dari kolom info dapat dilihat banyak pengiriman data secara terus menerus.



Gambar 10. Wireshark Mendeteksi serangan DDoS UDP

3. Hasil analisis

Analisis yang didapat dari proses pengujian yang telah dilakukan adalah kondisi lalulintas pada jaringan berjalan dengan baik pada saat sebelum terjadi penyerangan dengan pengujian *ping* antara komputer penyerang dan komputer target, kemudian terjadi gangguan saat serangan *scanning port* menggunakan *Nmap*, serangan *DDoS* TCP dan UDP menggunakan *LOIC* dilakukan, hal ini membuat *wireshark* mendeteksi dan menampilkan informasi dan rincian data penyerang seperti IP dan *port* yang digunakan.

Dalam pengujian tersebut, kelebihan *wireshark* dapat mendeteksi serangan yang dilakukan penyusup dengan melihat informasi dari hasil *capture* paket data yang dilakukan, mulai dari IP yang digunakan dan protokol apa yang digunakan.

SIMPULAN

Sistem WIDS dalam mendeteksi serangan yang terjadi dilakukan dengan proses *scanning* terhadap sejumlah *source* dan lalulintas yang terjadi didalam jaringan. Implementasi WIDS menggunakan *tools wireshark* yaitu dengan mendeteksi serangan yang dilakukan penyusup dengan melihat informasi dari hasil *capture* paket data yang dilakukan, mulai dari IP yang digunakan dan protokol apa yang digunakan.

SARAN

Pendeteksian sistem keamanan jaringan yang dilakukan dikantor DPRD masih sederhana sehingga masih dapat dilakukan pengembangan untuk mencapai hasil yang lebih akurat. Integrasikan WIDS dengan infrastruktur keamanan yang ada, seperti firewall, SIEM (Security Information and Event Management), atau sistem keamanan lainnya. Kerjasama dan pertukaran informasi antara sistem keamanan dapat meningkatkan kemampuan deteksi dan respons terhadap ancaman.

DAFTAR PUSTAKA

Arman Muhajir, & Kasran. (2023). *Analisa Jaringan Nirkabel Pada Mesin ATM Berbasis IoT di PT . Bank*. *6*(April), 77–84.

Kurniawan, A. (2012). *Network Forensics : Panduan Analisis & Investigasi Paket Data Jaringan Menggunakan Wireshark* (1st ed.). Andi Offset. https://perpustakaan.wicida.ac.id/opac/detail-opac?id=3662

Nugroho, K. (2019). *Jaringan Komputer Menggunakan Pendekatan Praktis*. Mediatera.

Nurnaningsih, Riskayani, & Husnang, A. (2022). Analisis Keamanan Jaringan Hotspot Dengan Parameter Quality Of Service (Qos) Pada Kantor Dinas Komunikasi Dan Informatika Kabupaten Soppeng. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika "JISTI,"* *5*(1), 51–58. https://journal.jisti.unipol.ac.id/index.php/jisti/article/view/109

Santoso, J. D. (2018). KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN WIRELESS INTRUSION Joko Dwi Santoso Abstraksi Keywords : Pendahuluan. *INFOS Jurnal*, *1*(3).

Sofana, I. (2013). *Membangun Jaringan Komputer : Mudah Membuat Jaringan Komputer (Wire & Wireless) Untuk Pengguna Window Dan Linux*. Informatika. https://openlibrary.telkomuniversity.ac.id/pustaka/18686/membangun-jaringan-komputer-mudah-membuat-jaringan-komputer-wire-wireless-untuk-pengguna-window-dan-linux.html

Wardana, M. A., & Nusri, A. Z. (2022). *Jaringan Virtual Private Network (Vpn) Berbasis Mikrotik Pada Kantor Kecamatan Marioriawa Kabupaten Soppeng*. *5*, 107–116.