DOI: https://doi.org/10.62017/tektonik

Analisis Keamanan *Wireless* Terhadap Serangan *Denial of Service* menggunakan Metode *Penetration Testing* pada Dinas XYZ

Jhamary Syahronny *[1]
Agus Tedyyana [2]

[1,2] Politeknik Negeri Bengkalis
*e-mail: arilangot3@gmail.com [1], agustedyyana@polbeng.ac.id[2]

Abstrak

Penelitian ini adalah untuk menganalisis keamanan jaringan wireless terhadap serangan DoS dengan menerapkan metode Penetration testing di dinas XYZ. Penelitian ini akan memfokuskan pada identifikasi kelemahan potensial dalam jaringan wireless yang membuatnya rentan terhadap serangan DoS dan menguji efektivitas Penetration testing dalam mendeteksi dan merespons serangan DoS. Penulis pada penelitian ini mengusulkan dua solusi yang dimana untuk meningkatkan keamanan jaringan wireless di kantor dinas XYZ. Solusi pertama adalah dengan melakukan analisis Hping3 untuk mendeteksi jaringan pada Wireless. Tujuannya adalah untuk memastikan Penetration testing yang telah diimplementasikan berfungsi dengan baik dan mampu mendeteksi serangan DoS secara efektif. Masalah dalam konfigurasi atau kegagalan sistem dapat mengurangi efektivitas Penetration testing dalam mendeteksi serangan DoS. Selanjutnya, adapun hasil dalam penelitian ini dalam melakukan serangan DoS berhasil dilakukan , solusi yang diusulkan adalah melakukan analisis dengan Wireshark Tools Kali Linux untuk pertukaran paket data pada wireless yang melakukan serangan DoS secara manual agar dapat memonitoring hasil serangan DoS berhasil dibuktikan. Untuk solusi selanjutnya agar tidak terjadinya serangan DoS, sebaiknya bisa menerapkan pendaftaran Mac address filtering unuk mengamankan jaringan dari ancaman serangan DoS sebagai solusi terakhir dalam penelitian ini.

Kata Kunci: *Serangan Dos, penetration testing, kali linux*

Abstract

This research is to analyze the security of wireless networks against DoS attacks by applying the Penetration testing method in the XYZ service. This research will focus on identifying potential weaknesses in wireless networks that make them vulnerable to DoS attacks and examine the effectiveness of penetration testing in detecting and responding to DoS attacks. The author of this research proposes two solutions to improve the security of the wireless network at the XYZ office. The first solution is to carry out Hping3 analysis to detect wireless networks. The aim is to ensure that the penetration testing that has been implemented functions well and is able to detect DoS attacks effectively. Problems in configuration or system failures can reduce the effectiveness of penetration testing in detecting DoS attacks. Furthermore, as for the results of this research in carrying out a successful DoS attack, the proposed solution is to carry out an analysis with the Wireshark Tools Kali Linux for exchanging data packets on wireless that carry out a DoS attack manually so that monitoring the results of the DoS attack can be proven to be successful. For the next solution to prevent DoS attacks from occurring, it is best to be able to apply Mac address filtering registration to secure the network from the threat of DoS attacks. This is the final solution in this research.

Keywords: *DoS attacks, penetration testing, Kali Linux*

PENDAHULUAN

Saat ini, informasi dan komunikasi telah menjadi kebutuhan dasar yang esensial, dengan teknologi wireless sebagai solusi utama untuk memenuhi kebutuhan akses informasi kapan pun dan di mana pun. Kemajuan teknologi memaksa sistem keamanan jaringan komputer untuk terus diperbarui guna melindungi dari ancaman di dunia maya, terutama mengingat internet adalah jaringan dengan akses yang sangat terbuka. Meskipun teknologi *wireless* memfasilitasi mobilitas dan meningkatkan produktivitas, ia juga memperkenalkan tantangan baru terkait keamanan. Jaringan wireless lebih rentan terhadap serangan dibandingkan dengan jaringan kabel, sehingga penting untuk meningkatkan perlindungan terhadap potensi pencurian data dan peretasan. Serangan DoS, yang mengakibatkan gangguan layanan dengan membanjiri sistem dengan lalu

DOI: https://doi.org/10.62017/tektonik

lintas berlebihan, adalah salah satu ancaman utama yang harus diwaspadai. Jenis serangan ini dapat menyebabkan gangguan serius dalam operasional dan kerugian finansial yang signifikan. Oleh karena itu, penting untuk melakukan penetration testing (pentest) sebagai metode untuk mengidentifikasi dan mengeksploitasi kelemahan keamanan sistem. Penelitian ini bertujuan untuk menyelidiki keamanan jaringan wireless, khususnya dalam konteks kantor dinas XYZ, dengan menggunakan alat pengujian seperti Kali Linux dan tool terkait.

Proyek akhir yang berjudul "Analisis Keamanan Wireless terhadap Serangan DoS (Denial of Service) menggunakan Penetration Testing pada Kantor Dinas XYZ". Fokus utama penelitian ini adalah meningkatkan keamanan jaringan wireless terhadap serangan DoS. Serangan DoS merupakan ancaman serius yang dapat menyebabkan gangguan signifikan pada kinerja sistem dengan membanjiri target dengan lalu lintas berlebihan, sehingga membuat sistem tidak dapat diakses oleh pengguna yang sah. Jaringan nirkabel di kantor Dinas XYZ menghadapi beberapa kelemahan keamanan yang berpotensi dimanfaatkan oleh penyerang untuk melancarkan serangan DoS. Kelemahan tersebut meliputi penggunaan enkripsi yang lemah atau tidak memadai, konfigurasi default pada perangkat jaringan seperti router dan access point, kurangnya pemantauan dan pengawasan jaringan, serta kerentanan pada perangkat keras atau perangkat lunak yang digunakan. Masalah-masalah ini dapat mengakibatkan gangguan layanan, penurunan produktivitas, dan kerugian lainnya. Untuk mengatasi masalah ini, diperlukan analisis mendalam terhadap keamanan jaringan *wireless* dengan menggunakan metode *penetration testing* dan alat seperti *Kali Linux, Hping3, Wireshark, dan Aircrack-ng*. Penelitian ini bertujuan untuk mengidentifikasi kelemahan yang ada dan mengevaluasi efektivitas metode penetration testing dalam mencegah serangan DoS. Hasil dari penelitian ini diharapkan dapat memberikan wawasan berharga bagi kantor dinas XYZ untuk memperbaiki sistem keamanan jaringan mereka dan mengurangi risiko serangan DoS di masa depan.

Berangkat dari permasalahan di atas, peneliti mengusulkan beberapa solusi untuk meningkatkan keamanan jaringan wireless di kantor dinas XYZ. Pertama, dianjurkan untuk menggunakan Hping3 dalam analisis jaringan *wireless* untuk memastikan bahwa penetration testing yang diterapkan efektif dalam mendeteksi serangan DoS. Kegagalan konfigurasi atau sistem dapat mengurangi efektivitas deteksi serangan. Solusi berikutnya adalah memanfaatkan *Wireshark* dalam *Tools* Kali Linux untuk memantau pertukaran paket data, khususnya dalam mendeteksi dan mencegah serangan DoS secara manual, sehingga penyerang tidak dapat terhubung ke jaringan. Peneliti juga merekomendasikan penerapan metode penetration testing yang menyeluruh, termasuk simulasi serangan DoS pada jaringan untuk mengidentifikasi titik lemah, memberikan rekomendasi perbaikan, dan tindakan pencegahan guna meningkatkan ketahanan sistem terhadap serangan. Selain itu, perlu dilakukan evaluasi terhadap potensi kerentanan yang dapat dimanfaatkan oleh pihak tidak berwenang. Teknologi ini akan membantu mendeteksi dan menghentikan lalu lintas berbahaya sebelum mencapai infrastruktur utama, memperkuat pertahanan jaringan secara menyeluruh. Dengan menerapkan solusi ini, tingkat keamanan wireless di kantor dinas XYZ akan meningkat, melindungi informasi sensitif, dan mencegah penyadapan alur lalu lintas jaringan. Selain itu, solusi ini akan memberikan wawasan yang lebih baik tentang serangan-serangan yang mungkin terjadi pada jaringan wireless. Penelitian ini bertujuan untuk meningkatkan kesadaran akan pentingnya keamanan jaringan wireless dan memberikan langkah-langkah yang konkret untuk melindungi dari serangan DoS di kantor dinas XYZ.

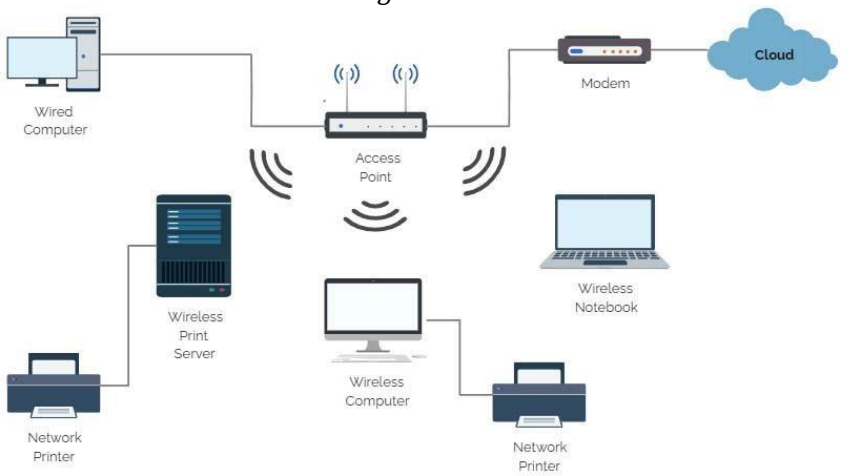
METODE

Dalam tahap penelitian analisis keamanan *Wireless LAN* terhadap serangan *DoS* menggunakan metode penetration testing, peneliti mempersiapkan alat dan bahan yang diperlukan. Persiapan ini mencakup perangkat keras dan perangkat lunak. Untuk perangkat keras, peneliti menggunakan laptop Lenovo dengan prosesor AMD E2, RAM 8GB, hardisk 500 GB, serta perlengkapan tambahan seperti wifi, access point, Mikrotik, kabel LAN, dan konektor RJ 45. Sementara itu, untuk perangkat lunak, peneliti menyiapkan aplikasi dan tools seperti *Aircrack-ng,*

DOI: https://doi.org/10.62017/tektonik

OS Kali Linux, Hping3, dan Wireshark. Kemudian pengumpulan data dilakukan dengan mengamati lingkungan jaringan nirkabel dalam kondisi normal dan saat serangan DoS terjadi. Data yang dikumpulkan akan digunakan untuk melatih dan menguji kinerja penetration testing. Metode pengumpulan data meliputi wawancara, baik tatap muka maupun melalui media seperti telepon, email, atau video call, serta observasi langsung untuk mencatat fenomena dan sikap responden.

Pengujian dilakukan dengan mengirimkan serangan DoS simulasi ke jaringan *wireless* yang diamati. Tujuan dari pengujian ini adalah untuk menilai respons Penetration Testing terhadap serangan tersebut. Evaluasi mencakup kemampuan Penetration Testing dalam mendeteksi dan menangkal serangan DoS, serta mengukur tingkat keberhasilan deteksi dan kesalahan seperti *False Positive atau False Negative.*



Gambar di atas menunjukkan sistem jaringan wireless yang saat ini digunakan di kantor dinas XYZ. Sistem keamanan yang ada belum efektif dan efisien dalam menilai tingkat keamanan jaringan internet, dengan celah yang dapat dimanfaatkan oleh pihak tidak berwenang. Untuk mengatasi masalah ini, penulis memutuskan menerapkan konfigurasi khusus dalam Metode Penetration Testing. Pentester akan mengikuti langkah-langkah terstruktur untuk mengidentifikasi kelemahan keamanan sistem secara menyeluruh, sehingga temuan yang akurat dan relevan dapat digunakan untuk meningkatkan keamanan sistem tersebut.

Berikut adalah langkah-langkah dalam penetration testing menggunakan metode white-box secara ringkas:

1. Analisis Kode Sumber: Pemeriksaan struktur kode, algoritma, dan data untuk memahami cara aplikasi dibangun dan mendesain kasus uji yang mencakup seluruh aspek kode.
2. Identifikasi Jalur Eksekusi: Menggunakan diagram alur atau kendali aliran untuk menentukan jalur eksekusi kode dan memvisualisasikan kondisi serta keputusan yang diambil dalam aplikasi.
3. Menentukan Kasus Uji: Membuat kasus uji berdasarkan jalur eksekusi untuk memastikan aplikasi berfungsi dengan benar di berbagai skenario, termasuk kondisi batas dan penanganan kesalahan.
4. Menyiapkan Lingkungan Pengujian: Mengonfigurasi perangkat keras, perangkat lunak, dan dependensi untuk meniru lingkungan produksi guna memastikan hasil pengujian yang valid.
5. Melakukan Pengujian: Menjalankan kasus uji, memonitor hasil, dan menggunakan alat seperti Wireshark untuk melacak eksekusi kode dan mengidentifikasi titik kerentanan.
6. Analisis Hasil Pengujian: Membandingkan hasil aktual dengan yang diharapkan untuk mengidentifikasi penyimpangan.
7. Dokumentasi: Mencatat temuan, kesalahan, dan jalur kode yang diuji sebagai referensi untuk pengembangan lebih lanjut.
8. Laporan Pengujian: Menyusun laporan komprehensif yang merangkum metodologi, hasil, dan rekomendasi untuk tim pengembangan dan stakeholder.

DOI: https://doi.org/10.62017/tektonik

Langkah-langkah ini memastikan bahwa kode aplikasi berkualitas tinggi, bebas dari kesalahan, dan berfungsi sesuai harapan. Pengujian White Box adalah bagian krusial dari siklus pengembangan perangkat lunak, memungkinkan identifikasi dan perbaikan masalah secara efektif.

HASIL DAN PEMBAHASAN

Dalam eksperimen ini, pentester menggunakan Kali Linux, Aircrack-ng, Wireshark, dan Hping3 untuk mensimulasikan serangan DoS dan menganalisis kerentanannya. Kali Linux berfungsi sebagai platform utama, Aircrack-ng untuk pengujian keamanan jaringan, Wireshark untuk analisis lalu lintas data, dan Hping3 untuk simulasi paket jaringan. Penggunaan alat-alat ini memungkinkan evaluasi menyeluruh terhadap kesiapan sistem terhadap serangan DoS dan membantu merumuskan rekomendasi keamanan yang lebih akurat.

A. Prosedur Eksperimen

Prosedur penelitian mencakup serangkaian langkah-langkah untuk melakukan simulasi serangan DoS pada jaringan nirkabel, seperti yang dijelaskan dalam ilustrasi berikut. Setiap tahapan dirancang untuk memberikan panduan yang jelas dalam mengidentifikasi, melaksanakan, dan menganalisis serangan guna memahami lebih dalam tentang kerentanan jaringan wireless terhadap ancaman DoS.

Menghubungkan Komputer Jaringan Wifi

Dalam simulasi ini, penulis menghubungkan komputer ke jaringan Wi-Fi di kantor dinas XYZ, memastikan perangkat terintegrasi dengan jaringan tersebut. Langkah ini penting karena memungkinkan penulis untuk mengakses dan memantau sistem secara langsung, mempermudah pengujian keamanan yang lebih rinci dan menyeluruh. Dengan demikian, penulis dapat lebih efektif mengidentifikasi dan menganalisis potensi kerentanan, serta memahami bagaimana serangan dapat mempengaruhi jaringan secara *real-time*.

Analisis Penetration Testing

Penelitian ini menganalisis sistem keamanan jaringan *wireless* dengan metode penetration testing. Pada tahap identifikasi kerentanan *(Vulnerability Identification),* ditemukan beberapa potensi serangan, seperti *WPA Cracking* dan *DoS* pada login *router wireless*. Proses pengumpulan informasi *(Information Gathering)* mencakup pengumpulan data seperti *SSID target*, *MAC Address,* serta keamanan access point yang menggunakan WPA2 key. Melalui penggunaan *tools Kali Linux* seperti *Aircrack-ng, Hping3*, dan *Wireshark*, peneliti berhasil mengidentifikasi *access point target* di dinas XYZ dengan *SSID* dan *MAC Address* 50:c7:bf:40:e9:48. *Penetration testing* kemudian dilakukan dengan mensimulasikan serangan terhadap *access point target* berdasarkan hasil identifikasi kerentanan. Tahap awal dari *penetration testing* ini melibatkan proses cracking untuk menguji kekuatan sistem keamanan.

Kali Linux

Dalam penelitian ini, Kali Linux berperan sebagai sistem operasi untuk melaksanakan uji penetrasi (Penetration testing). Proses ini melibatkan beberapa program seperti Aircrack-ng, Hping3, dan Wireshark, yang masing-masing memiliki fungsi spesifik dalam mengeksploitasi target dan mengendalikan perangkat yang sedang diuji. Aircrack-ng digunakan untuk meretas kata sandi jaringan nirkabel dan melakukan serangan DoS, sementara Hping3 mensimulasikan serangan DoS pada lalu lintas jaringan dan mendeteksi penyusup dalam sistem pengguna. Wireshark berfungsi untuk menganalisis dan mengatasi masalah jaringan, mengidentifikasi gangguan, mengoptimalkan kinerja jaringan, serta menyelesaikan masalah keamanan. Ilustrasi dari penggunaan alat-alat ini dapat dilihat pada gambar di bawah.

DOI: https://doi.org/10.62017/tektonik

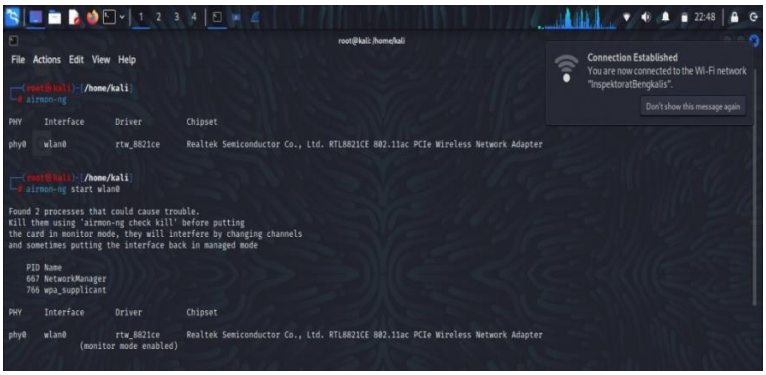
Gambar 1. *Kali Linus*

Untuk melakukan uji penetrasi *(penetration testing)* menggunakan *Kali Linux*, langkah-langkah yang ditempuh adalah sebagai berikut: Pertama, jalankan Kali Linux, lalu masukkan username *"root"* dan *password "toor".* Setelah masuk ke tampilan desktop, pilih menu *"Applications"* di *Kali Linux.* Di sana, berbagai alat yang dapat digunakan untuk pengujian penetrasi atau audit keamanan sistem tersedia untuk dipilih sesuai kebutuhan.

B. Pengujian Menggunakan Aircrack-ng

Ada beberapa metode pengujian yang dapat dilakukan dengan menggunakan *Aircrack-ng*, yang masing-masing memiliki tujuan dan pendekatan berbeda dalam mengevaluasi keamanan jaringan nirkabel. Metode-metode ini mencakup berbagai teknik untuk menguji kerentanan. Setiap metode ini memainkan peran penting dalam proses pengujian penetrasi, memungkinkan penguji untuk secara menyeluruh menganalisis dan mengeksploitasi potensi kelemahan yang ada dalam jaringan *wireless.*

- Tahap pertama memasukan perintah *airmon-ng*



Gambar 2. *Airmon-ng*

Pada tahap awal penelitian yang ditunjukkan pada Gambar 2, metode Kali Linux digunakan untuk menguji keamanan jaringan wireless dengan memanfaatkan Aircrack-ng. Pengujian dimulai dengan memasukkan perintah *"airmon-ng*" untuk mengaktifkan mode monitor pada antarmuka jaringan, diikuti dengan perintah *"airodump-ng"* untuk menangkap dan menganalisis paket data yang dikirimkan melalui jaringan wireless. Proses ini memungkinkan peneliti untuk mengidentifikasi perangkat yang terhubung ke jaringan dan mengeksplorasi potensi celah keamanan yang dapat dieksploitasi.

- Tahap kedua hasil dari *scanning* menggunakan perintah *Airodump-ng*

DOI: https://doi.org/10.62017/tektonik

Gambar 3. Hasil *Scanning*

Pada tahap kedua, seperti yang ditunjukkan pada Gambar 3, pentester melaksanakan tahap Intelligence Gathering, yaitu proses pengumpulan informasi tentang target yang akan diserang. Informasi ini dikumpulkan melalui pemindaian jaringan wireless menggunakan perintah Airodump-ng. Hasil dari pemindaian ini memberikan data penting tentang jaringan, seperti SSID, kekuatan sinyal, dan perangkat yang terhubung, yang akan digunakan untuk merencanakan serangan lebih lanjut.

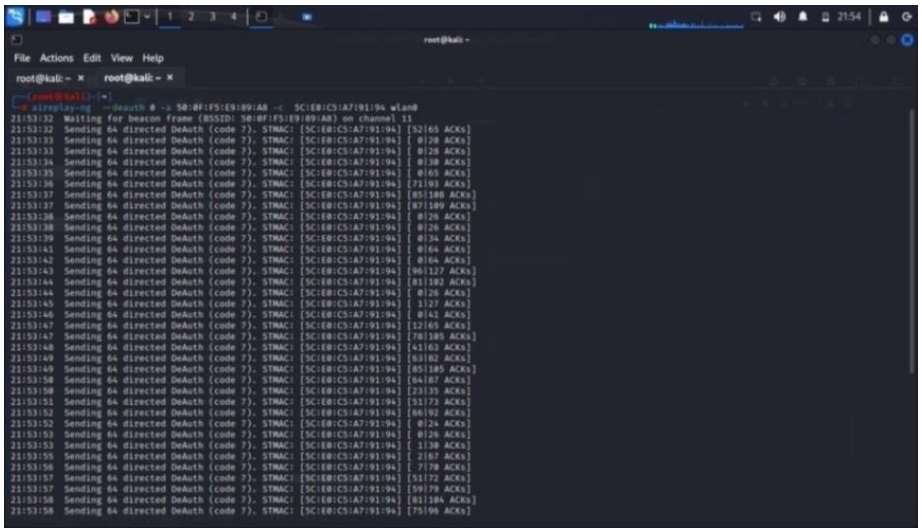
- Tahap ke tiga memasukan perintah *Airodump-ng*

Gambar 4. *Capture Pad*

Pada tahap ini, seperti yang ditunjukkan pada Gambar 4, langkah pertama adalah menjalankan perintah *`airodump-ng`* untuk membuat *Capture Pad*. Langkah ini adalah bagian dari proses *penetration testing* menggunakan teknik *Threat Modeling*. Teknik ini melibatkan identifikasi dan pencarian celah keamanan dalam jaringan nirkabel dengan cara memasukkan BSSID untuk memantau dan menganalisis lalu lintas jaringan. *Capture Pad* yang dihasilkan akan berfungsi sebagai dasar untuk mengumpulkan data yang diperlukan untuk evaluasi lebih lanjut terhadap potensi kerentanan dalam sistem.

- Tahap keempat melakukan perintah terhadap *Aireplay-ng*

DOI: https://doi.org/10.62017/tektonik



Gambar 5. *Aireplay-ng*

Pada tahap ini, pentester melakukan Threat Modeling dengan menggunakan Aireplay-ng untuk mengidentifikasi celah keamanan. Proses ini melibatkan pengiriman port untuk memperoleh handshake BSSID dari jaringan wireless target. Hasilnya dapat dilihat pada gambar 5 di atas.

- Tahap Kelima melakukan perintah terhadap *wireshak*

Pada tahap ini, pentester menggunakan Wireshark untuk melakukan *Vulnerability Analysis. Wireshark* membantu dalam memeriksa dan mencari celah keamanan jaringan *wireless* dengan membuka *file Capture-cap* yang ditemukan melalui pemindaian. Analisis ini penting untuk mengidentifikasi kelemahan potensial dalam lalu lintas jaringan, seperti paket data yang tidak terenkripsi atau pola lalu lintas yang mencurigakan. Hasil analisis memberikan wawasan tentang potensi titik lemah yang dapat dimanfaatkan dalam serangan lebih lanjut.

- Tahap Keenam memasukkan perintah *Aircrack-ng*

Tahap keenam, melibatkan penggunaan *Aircrack-ng* untuk mendapatkan password jaringan *wireless* target. Setelah melakukan pemindaian *Capture-cap* dengan *Wireshark, pentester* menggunakan *Aircrack-ng* untuk mendekripsi password. Analisis ini membantu menentukan efektivitas metode *cracking* dan mengukur kekuatan password serta keamanan jaringan secara keseluruhan. Hasil dari tahap ini menunjukkan seberapa rentan jaringan terhadap pengambilalihan akses.

- **Memulai Serangan DoS dengan Aircrack-ng**

Gambar 6. Tahap Awal Serangan DoS

Gambar diatas menunjukkan tahap awal penyerangan DoS terhadap jaringan *wireless* setelah memperoleh password dengan *Aircrack-ng. Pentester* memanfaatkan perintah *Aircrack-ng* untuk

DOI: https://doi.org/10.62017/tektonik

mematikan jaringan di kantor dinas XYZ. Analisis dari tahap ini mengungkapkan bagaimana serangan DoS dapat mempengaruhi ketersediaan dan stabilitas jaringan, serta mengidentifikasi potensi dampak terhadap operasional jaringan yang lebih luas.

- **Scanning Target Penyerangan**

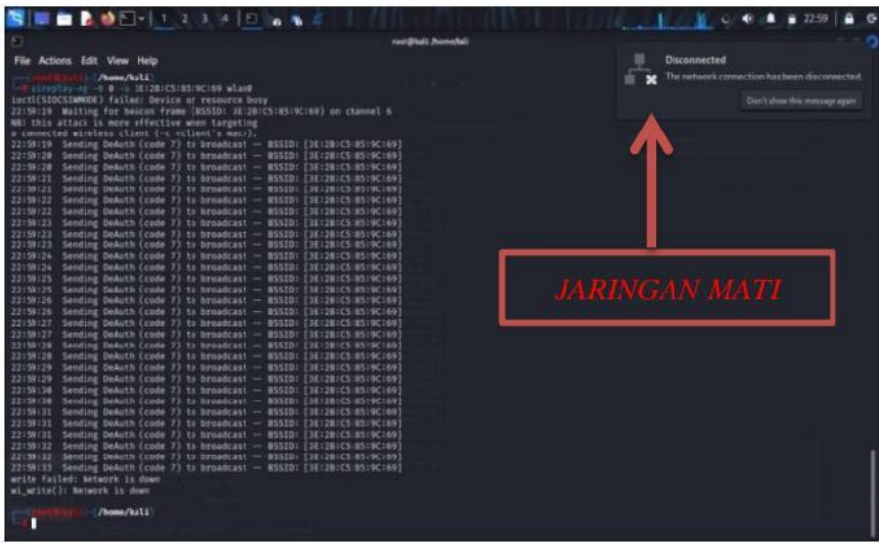
Pentester melakukan scanning target sebagai bagian dari eksploitasi terhadap jaringan wireless di dinas XYZ. Tahap ini melibatkan pemetaan dan penilaian lebih mendalam terhadap target untuk menemukan celah tambahan atau kelemahan yang dapat dieksploitasi. Analisis ini memberikan gambaran tentang efektivitas serangan dan area yang mungkin memerlukan perhatian lebih lanjut untuk mengoptimalkan metode eksploitasi.

- **Bukti Penyerangan dengan Aircrack-ng**

Gambar 7. Bukti Target untuk Melakukan Serangan DoS

Gambar 7 di atas menunjukkan bukti penyerangan yang dilakukan menggunakan *Aircrack-ng*. *Pentester* melakukan scanning terhadap Target BSSID jaringan *wireless* untuk memverifikasi keberhasilan serangan DoS. Analisis bukti ini membantu dalam mengkonfirmasi apakah serangan berhasil dan memberikan rincian tentang bagaimana serangan dapat dilakukan dengan lebih efektif.

- **Hasil Penyerangan *DoS***



Gambar 8. Hasil Penyerangan

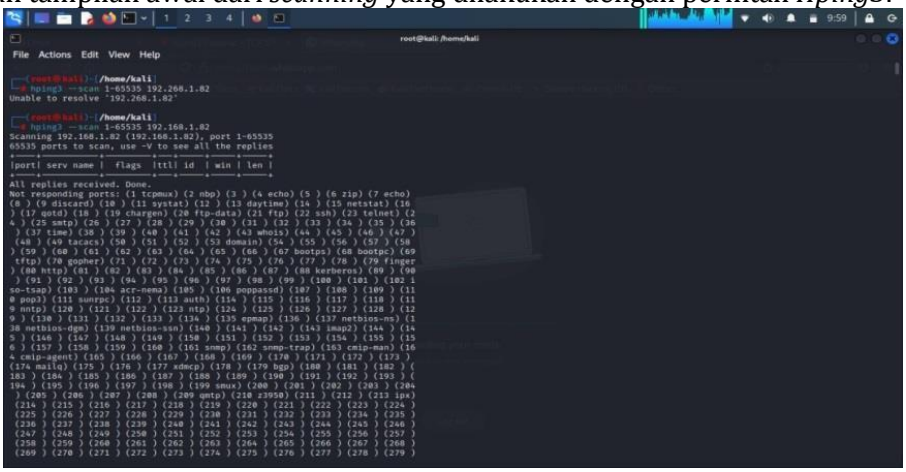
Hasil dari penyerangan DoS yang dilakukan dengan Aircrack-ng, sebagaimana ditampilkan pada Gambar 8, menunjukkan bahwa jaringan wireless di dinas XYZ berhasil mengalami serangan DoS. Pentester mengirimkan paket secara berlebihan untuk menguji ketahanan jaringan. Analisis hasil ini mengidentifikasi kelemahan signifikan dalam sistem keamanan jaringan dan menunjukkan bahwa perlindungan yang ada tidak memadai untuk menghadapi serangan DoS. Temuan ini

DOI: https://doi.org/10.62017/tektonik

menyoroti kebutuhan mendesak untuk memperkuat keamanan jaringan guna menghindari gangguan operasional di masa depan.

C. Pengujian Menggunakan Hping3

Dalam pengujian ini, Hping3 digunakan untuk melancarkan serangan *DoS tipe ICMP Flood* pada jaringan *wireless.* Proses pengujian dimulai dengan memeriksa kecepatan jaringan sebelum serangan dilakukan, di mana jaringan beroperasi pada kecepatan normal. Pada tahap pertama, *Hping3* digunakan untuk melakukan *scanning*, yang hasilnya terlihat pada Gambar 9. Gambar ini menunjukkan tampilan awal dari *scanning* yang dilakukan dengan perintah *Hping3*.



Gambar 9. Tampilan *Scanning Hping3*

Selanjutnya, pada tahap kedua, serangan DoS dilakukan menggunakan ICMP Flood, seperti yang ditunjukkan pada Gambar 10. Iptables mencatat 361.509 paket, sebagian besar dengan prefix log "ICMP Flood". Dari total 34.464 paket yang dikirim oleh Hping3, hanya 40 paket yang berhasil dicatat dalam log. Perbedaan ini disebabkan oleh keterbatasan kecepatan penulisan log oleh Iptables, yang menyebabkan pesan lama tertimpa sebelum dapat ditulis ke file log (/var/log/hasil-log.log).

Gambar 10. Melakukan Serangan *DoS Hping3 ICMP Flood*

Pada tahap ketiga, hasil serangan DoS menggunakan *Hping3* menunjukkan penurunan kinerja jaringan akibat pengiriman paket dalam jumlah besar. Terakhir, monitoring kecepatan jaringan dilakukan, menunjukkan penurunan signifikan dalam kecepatan jaringan dan akhirnya kegagalan koneksi *(Down)* setelah serangan. Pengujian ini menunjukkan bahwa serangan *DoS* berhasil menyebabkan jaringan menjadi sangat lambat dan akhirnya tidak dapat berfungsi, mengindikasikan adanya kelemahan serius dalam sistem pertahanan jaringan yang diuji.

D. Pengujian Menggunakan Wireshark

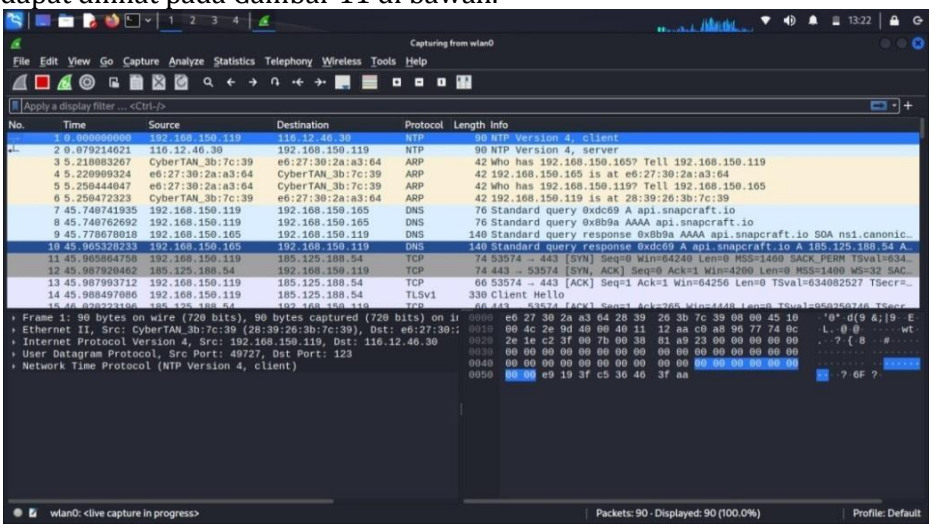
Wireshark digunakan sebagai alat untuk *Penetration Testing* pada sistem keamanan jaringan wireless di dinas XYZ, yang memerlukan koneksi *Local Area Network (LAN)* karena sistem yang

DOI: https://doi.org/10.62017/tektonik

diuji masih berada dalam lingkungan Localhost. Langkah-langkah implementasi *Penetration Testing* dijelaskan sebagai berikut.

- Menjalankan *Wireshark*

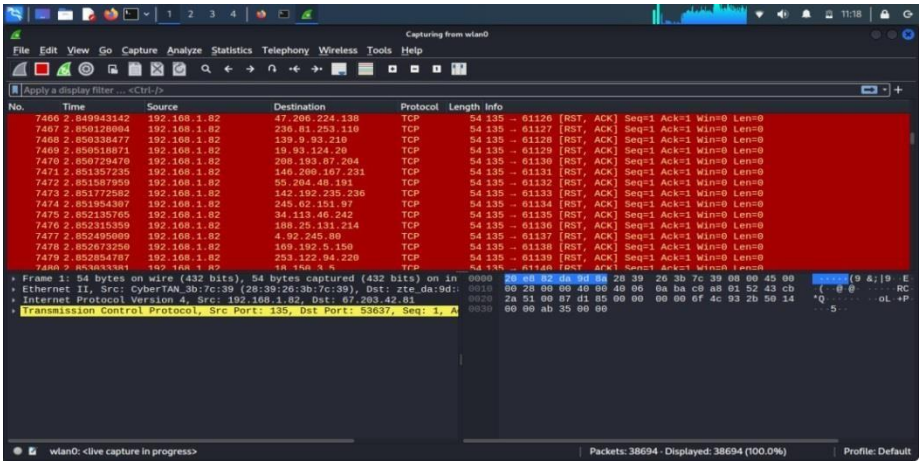
Untuk memonitor jaringan WiFi menggunakan Wireshark, pertama-tama, sambungkan ke jaringan WiFi atau hotspot yang relevan. Setelah itu, buka aplikasi Wireshark dan pilih menu "WiFi" atau "Wireless Network Connection" dari opsi yang tersedia. Tampilan awal aplikasi Wireshark dapat dilihat pada Gambar 11 di bawah.



Gambar 11. Tahap Awal *Wireshak*

Langkah awal ini penting untuk memastikan bahwa *Wireshark* dapat menangkap dan menganalisis lalu lintas jaringan dari koneksi yang tepat. Memilih menu yang sesuai memungkinkan aplikasi untuk memonitor data yang relevan dari jaringan WiFi yang sedang dipelajari, memberikan informasi yang dibutuhkan untuk analisis lebih lanjut terhadap potensi masalah atau ancaman dalam jaringan tersebut. Hasil dari proses *scanning* ini memberikan berbagai informasi penting yang telah dianalisis secara mendetail. Setelah analisis, aliran UDP *Stream* dapat dihentikan atau ditutup. Dari pemindaian paket data dan analisis menggunakan *Wireshark*, ditemukan bahwa proses tersebut berhasil. Analisis ini memungkinkan identifikasi potensi masalah dalam lalu lintas data dan membantu dalam merancang strategi perbaikan untuk memperkuat keamanan jaringan.

- Dari hasil percobaan mendapatkan sebagai berikut:



Gambar 12. Bukti Monitoring *DoS* menggunakan *Tools Wireshak*

Mengacu pada Gambar 12 di atas maka diperoleh hasil bahwa hasil dari serangan *Denial Of Service (DoS)* yang berhasil dilaksanakan menggunakan aplikasi Wireshark. Dalam serangan ini, sejumlah besar paket data destruktif dikirimkan, yang mengakibatkan dampak signifikan pada jaringan,

DOI: https://doi.org/10.62017/tektonik

seperti yang terlihat dalam dokumentasi gambar tersebut. Analisis menunjukkan bahwa *Wireshark* efektif dalam mendeteksi dan memvisualisasikan dampak dari serangan DoS, memperlihatkan betapa besar efek yang ditimbulkan oleh pengiriman paket yang tidak diinginkan pada jaringan.

E. Rekomendasi Perbaikan

Hasil pengujian keamanan jaringan wireless di kantor dinas XYZ menunjukkan bahwa serangan DoS berhasil mengakses password dan username jaringan serta menyebabkan jaringan wireless mengalami downtime. Temuan ini menegaskan bahwa jaringan dapat diserang dan dinonaktifkan oleh pihak yang tidak berwenang. Oleh karena itu, rekomendasi khusus diberikan untuk mengatasi serangan DoS terhadap jaringan wireless kantor dinas XYZ.

Pertama, penting untuk memastikan bahwa semua perangkat dalam jaringan, seperti *router* dan *access point,* telah diperbarui dengan patch keamanan terbaru untuk menutup kerentanan yang bisa dieksploitasi oleh serangan *DoS*.

Selanjutnya, konfigurasi *router* dan *access point* perlu ditingkatkan; matikan siaran SSID untuk mengurangi visibilitas jaringan dan gunakan enkripsi WPA2 atau WPA3 untuk melindungi komunikasi nirkabel. Selain itu, ubah kata sandi default router dan access point dengan yang lebih kuat dan sulit ditebak, serta filter alamat MAC untuk hanya mengizinkan perangkat dengan alamat MAC yang dikenal untuk terhubung.

Monitoring aktivitas jaringan juga krusial; terapkan sistem pemantauan yang efektif untuk mendeteksi aktivitas mencurigakan dan analisis log untuk memverifikasi adanya serangan serta dampaknya. Terakhir, konfigurasi *Quality of Service (QoS)* untuk membatasi penggunaan bandwidth oleh perangkat tertentu, sehingga serangan yang mencoba membanjiri jaringan dengan lalu lintas tidak sah dapat dibatasi. Dengan langkah-langkah ini, diharapkan keamanan jaringan nirkabel dapat ditingkatkan secara signifikan.

KESIMPULAN

Berdasarkan analisis yang dilakukan, peneliti menyimpulkan beberapa langkah untuk memperkuat keamanan jaringan *wireless* dari serangan *DoS (Denial of Service)* dengan metode *penetration testing*. Pertama, identifikasi titik kelemahan menunjukkan bahwa jaringan kantor dinas XYZ rentan karena penggunaan perangkat WiFi yang sudah usang dan tidak dilengkapi dengan fitur keamanan yang memadai. Selain itu, kurangnya pembaruan perangkat WiFi secara berkala meningkatkan risiko serangan DoS. Untuk mengatasi masalah ini, peneliti mengusulkan solusi preventif, yaitu pendaftaran alamat *MAC* untuk mengendalikan akses perangkat dan memastikan pembaruan perangkat WiFi secara rutin. Selain itu, peneliti merekomendasikan konfigurasi keamanan yang lebih ketat, termasuk penerapan standar keamanan WPA3 *(Wi- Fi Protected Access 3)*. untuk meningkatkan perlindungan jaringan wireless. Enkripsi data juga harus diterapkan pada semua transmisi melalui jaringan dengan menggunakan protokol yang kuat, seperti WPA3 untuk Wi-Fi dan SSL/TLS untuk transmisi data. Dengan menerapkan langkah-langkah ini, diharapkan keamanan jaringan *wireless* kantor dinas XYZ dapat diperbaiki, membuatnya lebih tahan terhadap serangan DoS dan memastikan perlindungan yang lebih baik dari ancaman yang ada.

DAFTAR PUSTAKA

Abdussalam, Z., & Basuki, A. (2022). Implementasi platform visualisasi dan analisis trafik jaringan menggunakan Arkime pada jaringan small-office/home-office. *Vol. 6*(11), 5454–5464.

Aryo, G., et al. (2022). Analisis keamanan jaringan wireless menggunakan metode penetration testing di SMK XYZ Tana Toraja. *Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing di SMK XYZ Tana Toraja, 2*(2), 1–7. https://doi.org/10.47178/infinity.v2i2

Fatimah, F., Mary, T., & Pernanda, A. Y. (2021). Analisis keamanan jaringan Wi-Fi terhadap serangan packet sniffing di Universitas PGRI Sumatera Barat. *JURTEII Jurnal Teknologi Informasi, 1*(1), 7–11. https://doi.org/10.22202/jurteii.2022.5707

Huda, I. A. (2020). Perkembangan teknologi informasi dan komunikasi (TIK) terhadap kualitas pembelajaran di sekolah dasar. *Jurnal Pendidikan dan Konseling, 2*(1), 121–125. https://doi.org/10.31004/jpdk.v1i2.622

Indonesia, N., Tbk, P., Watansoppeng, K. C. P., & Arman, M. (2023). Analisa jaringan nirkabel pada mesin ATM berbasis IoT di PT. Bank. *Vol. 6*(April), 77–84.

Kasus, S., Kota, D. I., Tekkamsisan, P., & Siber, B. (2019). Empirical study on Wi-Fi performance & security (case study in Depok City). *Jurnal Teknologi Informasi dan Ilmu Komputer, 6*(6), 671–676. https://doi.org/10.25126/jtiik.20196832

Maulana, A. B., Hertiana, S. N., & Fardan, F. F. (2022). Analisis serangan denial of service (DoS) pada jaringan privat seluler 5G stand alone berbasis open cellular. *Jurnal Elektro dan Telekomunikasi Terapan, 8*(6), 2792.

Rumalutur, S. (2015). Analisis keamanan jaringan wireless LAN (WLAN) pada PT. PLN (Persero) Wilayah P2B Area Sorong. *Electro Luceat, 1*(1), 62–74. https://doi.org/10.32531/jelekn.v1i1.15

Rusdi, M. I., & Prasti, D. (2019). Penetration testing pada jaringan Wi-Fi menggunakan Kali Linux. *Seminar Nasional Teknologi Informasi dan Komputasi 2019*, 260–269.

Santoso, J. D. (2019). Keamanan jaringan nirkabel menggunakan wireless intrusion detection system. *Infos, 1*(3), 44–50.