Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 5, **Number** 1, Maret 2025
https://doi.org/10.47709/digitech.v5i1.5552

Analisis Keamanan Jaringan *Modem Zte* Terhadap Serangan *Packet Sniffing* Menggunakan Metode *Penetration Testing*

Yuliana Tissya Kantari[1], I Made Widiarta[2], Dimas Wiryatari[3], Shinta Esabella[4], Yunanri.W[5*]
[1,2,3,4,5]Universitas Teknologi Sumbawa, Indonesia
yulianakantari@gmail.com[1], made.widiarta@uts.ac.id[2], dimas.wiryatari@uts.ac.id[3], shinta.esabella@uts.ac.id[4], yunanri.w@uts.ac.id[5*]

open access
Histori Artikel:
Diajukan: 17 Februari 2025
Disetujui: 10 April 2025
Dipublikasi: 16 April 2025
Kata Kunci:
Analisis; Security; Network; Sniffing; Penetration Testing

Abstrak
Dinas Komunikasi, Informatika, dan Statistik (Kominfotik) Sumbawa mengelola jaringan Wifi yang penting untuk akses internet. Namun, potensi ancaman seperti serangan Packet Sniffing dapat membahayakan data sensitif. Penelitian ini bertujuan menganalisis keamanan jaringan Wifi menggunakan metode Penetration Testing dan Wireshark, serta memberikan rekomendasi untuk meningkatkan keamanan jaringan dan melindungi data. Penelitian ini menggunakan analisis kualitatif deskriptif dengan tahapan pengumpulan data melalui observasi, wawancara, dan studi pustaka. Selanjutnya, dilakukan penetration testing yang mencakup pengumpulan informasi, deteksi kerentanan, simulasi serangan menggunakan Wireshark, dan penyusunan laporan. Kebutuhan sistem meliputi perangkat keras seperti laptop Acer dan perangkat lunak seperti Windows 10 dan Wireshark untuk mendukung penelitian. Pengumpulan data observasi dalam penelitian ini dilakukan dengan mengamati langsung infrastruktur jaringan WiFi di Kominfo dan Informatika (Kominfotik) Sumbawa. Proses ini mencakup identifikasi perangkat keras seperti router, access point, dan perangkat klien yang terhubung. Selain itu, pengamatan juga dilakukan terhadap konfigurasi jaringan, termasuk jenis enkripsi yang diterapkan (WPA2 atau WPA3), pengaturan keamanan, dan kebijakan yang berlaku. Penelitian ini menunjukkan bahwa protokol WPA2, meskipun lebih aman, masih rentan terhadap serangan packet sniffing seperti deauthentication dan dictionary attack. Penting untuk memahami kerentanan ini dan menerapkan strategi mitigasi untuk melindungi data sensitif serta integritas jaringan Wi-Fi. Disarankan untuk migrasi ke WPA3, menerapkan kata sandi kuat, melakukan pemantauan jaringan, menggunakan VPN, dan meningkatkan edukasi pengguna tentang keamanan siber untuk melindungi jaringan Wi-Fi.

PENDAHULUAN

Dinas Komunikasi, Informatika, dan Statistik (Kominfotik) Kabupaten Sumbawa berperan penting dalam pengelolaan teknologi informasi dan komunikasi (TIK) untuk mendukung aktivitas pemerintahan dan pelayanan publik. Salah satu fasilitas utama yang dikelola adalah jaringan nirkabel (Wifi) yang menyediakan akses internet bagi pegawai dan masyarakat sekitar. Untuk memastikan akses internet yang optimal, pengelolaan jaringan Wifi perlu ditingkatkan, sehingga memudahkan akses layanan digital, berbagi informasi, dan mempercepat komunikasi(Parsaorantua et al., 2017).

Namun, di balik kemudahan yang ditawarkan oleh jaringan *Wifi,* terdapat potensi ancaman keamanan yang serius. Salah satu bentuk ancaman yang umum adalah serangan *Packet Sniffing*, yaitu metode di mana penyerang memantau dan menangkap paket data yang ditransmisikan melalui jaringan tanpa izin. Melalui teknik ini, penyerang dapat memperoleh data sensitif seperti informasi *login, email,* hingga komunikasi rahasia lainnya yang dikirim melalui jaringan. Resiko ini semakin besar apabila jaringan *Wifi* tidak dilindungi dengan baik, misalnya dengan enkripsi yang lemah atau pengaturan keamanan yang kurang memadai(Adiguna & Widagdo, 2022)(Arini et al., 2024)(Arsalan, 2023).

Dalam konteks Kominfotik Sumbawa, keamanan jaringan *Wifi* sangat penting karena dapat melibatkan data-data penting pemerintahan yang harus dilindungi. Kegagalan dalam melindungi jaringan ini dapat mengakibatkan kebocoran informasi yang tidak hanya membahayakan institusi tetapi juga menurunkan tingkat kepercayaan publik terhadap layanan yang diberikan(Danuasmo et al., 2023)(Darmawan et al., 2024).

Penetration testing merupakan serangan jaringan yang disimulasikan pada sistem komputer untuk menemukan kerentanan, ancaman, dan resiko dalam sistem dan aplikasi perangkat lunak, jaringan atau aplikasi *web* yang dapat digunakan penyerang. Dalam keamanan jaringan *wireless*, *pentesting* sering digunakan untuk

menambahkan *firewall* pada router. *Vulnerability* atau kerentanan adalah sebuah resiko resmi bahwa penyerang dapat mengganggu atau mendapatkan sistem dan data apapun yang ada pada sumber daya target. Dalam tahap pengembangan dan implementasi sistem, *Vulnerability* sering kali dimasukkan secara tidak sengaja. *Vulnerability* umum termasuk kesalahan desain atau konfigurasi, kesalahan perangkat lunak dan lainnya(Farhan & Kusuma, 2023)(Fatimah et al., 2022)(Ummah, 2019).

Hasil dari penelitian ini diharapkan dapat menjadi referensi dari pihak DISKOMINFOTIK untuk mempertimbangkan keamanan yang relevan digunakan dalam mengamankan data-data penting yang ada di Dinas Komunikasi dan Informatika Sumbawa(Mursyidah et al., 2019).

STUDI LITERATUR

a.Kemanan Jaringan

Keamanan jaringan merupakan sistem yang bekerja untuk pencegahan aktifitas yang tidak diinginkan dengan melakukan identifikasi pengguna yang tidak memiliki hak akses dalam suatu jaringan. Menghubungkan komputer dengan komputer lain baik menggunakan jaringan kabel atau nirkabel memungkinkan orang lain untuk mengakses data, mengubah isi, sampai menghapus data dalam jaringan tersebut(Arini et al., 2024).

Keamanan komputer (*computer security*)juga dapat dia artikan sebagai keamanan informasi yang terdapat pada komputer atau jaringan. Keamanan komputer juga dikenal sebutan *Cybersecurity* atau *IT Security*. Keamanan komputer bertujuan membantu pengguna agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi(Umasugi, 2022).

b. *Packet Sniffing*

Packet sniffing adalah teknik pemantauan setiap paket yang melintas pada jaringan. *Packet sniffing* merupakan bagian dari perangkat lunak atau perangkat keras yang memonitor semua lalu lintas jaringan. Ini tidak seperti jaringan host standar yang hanya menerima lalu lintas yang dikirimkan khusus untuk mereka(Arsalan, 2023).

Serangan *sniffing* adalah jenis serangan siber yang melibatkan penyadapan atau pengambilan data yang dikirimkan melalui jaringan, seperti jaringan lokal (LAN) atau internet. Dalam *sniffing*, seorang penyerang menggunakan alat khusus (sniffer) untuk memantau dan mengumpulkan paket data yang melewati jaringan. Paket-paket ini dapat berisi informasi sensitif seperti kata sandi, data *login*, atau informasi pribadi pengguna. Serangan *sniffing* terbagi menjadi dua jenis utama :

1. *Passive Sniffing :* Penyerang hanya mengamati lalu lintas jaringan tanpa mengubah atau memodifikasi data yang lewat. Biasanya terjadi di jaringan tanpa enkripsi (seperti jaringan *Wi-Fi* publik yang tidak aman).
2. *Active Sniffing:* Penyerang secara aktif berusaha mengintervensi atau memodifikasi lalu lintas jaringan untuk mendapatkan akses ke data. Teknik yang digunakan dalam *active sniffing* termasuk ARP *spoofing* dan MAC *flooding*.

c. WireShark

Wireshark adalah salah satu dari alat analisa jaringan yang biasa dipakai oleh seorang *Network* Administrator untuk melakukan pemecahan masalah yang ada dalam jaringan, menganalisa, perangkat lunak atau untuk pengembangan sebuah protokol dalam komunikasi, dan atau dalam pendidikan. Pertama kali *wireshark* muncul dengan nama *Ethereal*, lalu pada bulan Mei tahun 2006 proyek ini mengganti namanya menjadi *Wireshark* karena ada permasalahan mengenai merek dagang. Bahasa Pemrograman yang dipakai dalam *wireshark* adalah bahasa C dengan *public license* GNU. *Wireshark* banyak digemari karena *interface wireshark* yang telah menggunakan tampilan grafis atau GUI(Farhan & Kusuma, 2023).

Seperti namanya, aplikasi *Wireshark* dapat menangkap beberapa paket data yang berkeliaran dalam lalu lintas jaringan yang dilihat. Seluruh jenis informasi paket dalam bermacam-macam format protokol pun bisa dengan mudah ditangkap dan dianalisis. Oleh karena itu, tool ini sering digunakan untuk *sniffing* (mendapatkan informasi penting seperti *username* dan *password*) dengan menangkap paket yang berkeliaran dalam lalu lintas jaringan dan menganalisanya. Proses yang dilakukan tersebut diawasi oleh *wireshark* agar uses dapat dengan aman meng-upload data tanpa perlu mengkhawatirkan ada yang menyusupi pada saat melakukan upload data(Farhan & Kusuma, 2023).

d. Kali Linux

Kali Linux merupakan penerus dari distribusi pengujian penetrasi Linux yang paling populer, Backtrack. Kali Linux 2.0 yang diluncurkan pada 11 Agustus 2015, merupakan versi perbaikan dari Kali Linux, yang memiliki fitur kernel 4.0 yang baru, dan didasarkan pada Debian versi Jessie dengan cakupan perangkat keras dan driver nirkabel yang lebih baik. Kali Linux 2.0 mencakup lebih dari 300 alat keamanan. Anda sekarang bisa mendapatkan alat keamanan yang paling disukai oleh para profesional di seluruh dunia, semuanya di satu tempat yang terinstal, terkonfigurasi, dan siap digunakan (Ishan Girdhar & Dhruv Shah, 2017).

Kali Linux (Kali) adalah penerus platform pengujian penetrasi BackTrack yang secara umum dianggap sebagai paket alat standar de facto yang digunakan untuk memfasilitasi pengujian penetrasi guna mengamankan jaringan data dan suara. Kali untuk mendukung beberapa aspek lanjutan dari pengujian penetrasi (Robert W. Beggs, 2014).
Jadi, Kali Linux alat yang menjadi standar dalam pengujian penetrasi guna mengamankan jaringan yang dimana Kali Linux mendukung beberapa aspek lanjutan dari ppengujian penetrasi.

e.Penetrasion Testing

Pengujian penetrasi, atau pentesting melibatkan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan. Pada pentest (berlawanan dengan penilaian kerentanan), penguji tidak hanya menutupi kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, jika memungkinkan, untuk menilai apa yang mungkin diperoleh penyerang setelah eksploitasi yang berhasil(Introduction, n.d.).

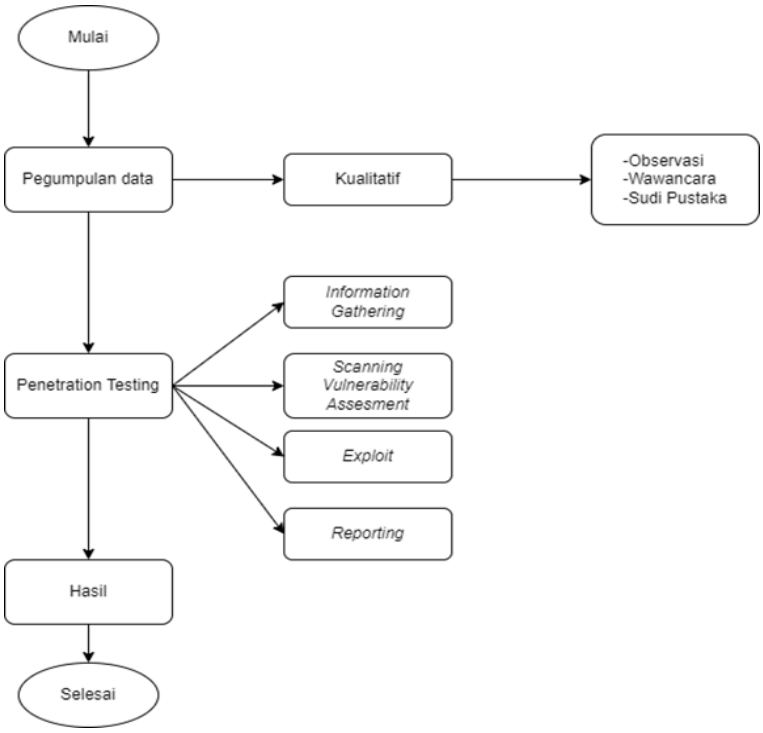
Pengujian penetrasi (Pentest) adalah proses mengeksploitasi kerentanan dengan aman tanpa banyak berdampak pada jaringan atau bisnis yang ada. Keterbatasan dengan Pentest hanya pada eksploitasi yang tersedia untuk umum saat ini dan sebagian besar merupakan pengujian yang berfokus pada proyek. Di Pentest, kita sering mendengar *Yay! Got Root*, tetapi kita tidak pernah mempertanyakan *What's next?*. Hal ini bisa jadi karena berbagai alasan seperti proyek membatasi Anda untuk segera melaporkan masalah berisiko tinggi kepada klien atau klien hanya tertarik pada satu segmen jaringan dan ingin Anda berkompromi(Velu, 2016).

Jadi, dapat disimpulkan bahawa Pengujian Penetrasi (*Penetration Testing)* adalah proses pengujian dengan melakukan serangan yang tidak hanya berfokus pada kerentanannya saja tetapi bisa menilai kerentanan yang memungkin penyerang untuk menyalahgunakannya. Berikut langkah – langkah yang perlu dilakukan dalam *penetration testing* menurut (EC-Council, 2012) :

1. *Information Gathering :* Pengumpulan data merupakan kunci utama untuk pengujian. Kita dapat mengumpulkan data secara manual atau dapat menggunakan layanan alat seperti teknik analisis kode sumber halaman web, dll) tersedia bebas secara online.
2. *Scanning Vulnerability Assesment :* Setelah data dikumpulkan, kemudian melakukan pengujian kerentanan untuk mengetahui kelemahan keamanan dan mengambil langkah-langkah pencegahan yang sesuai menampilkan level tingkat kelemahan dari *alert vulnerability* yang ditemukan.
3. *Exploit*
   Langkah pengujian ini adalah metode yang menggunakan tester untuk melancarkan serangan pada sistem target dan juga mengurangi resiko penyerangan.
4. Reporting
   Setelah penetrasi dilakukan, kemudian menyiapkan laporan akhir yang menjelaskan segala sesuatu tentang sistem. Akhirnya laoran tersebut dianalisis untuk mengambil langkah – langkah untuk melindungi sistem target.

METODE

Dalam melakukan melakukan penelitian ini, peneliti menggunakan analisa kualitatif yang menggunakan analisa deskriptif. Hal ini dikarenakan sifat permasalahan yang menggambarkan atau mendeskripsikan keadaan subjek atau objek yang diteliti. Adapun tahapan yang analisa keamanan jaringan yaitu.



Gambar 1 Metode Penelitian

Dari gambar diagram alir di atas terdapat beberapa tahapan yang dilakukan. Tahapan pertama merupakan tahapan pengumpulan data yang menggunakan metode kualitatif yaitu dengan melakukan observasi, wawancara, dan studi pustaka. Setelah pengumpulan data, tahapan selanjutnya adalah penetration testing yang dimana pada tahapan ini penelti mengumpulkan data-data yang akan digunakan dalam pengujian yang akan dilakuakan *(Information Gathering)*, menguji kerentanan (*scanning vulnerability assesment*), Selanjutnya setelah melakukan pengujian terhadap kerentanan dari jaringan nya maka akan dilakukannya simulasi serangan (*exploit*), dan hasil akhir dari bagan alir atau metode yang digunakan yaitu membuat laporan (*reporting*).

HASIL

Skenario Penyerangan Sniffing

Dalam penelitian ini, skenario penyerangan sniffing dirancang untuk menggambarkan bagaimana seorang penyerang dapat mengeksploitasi kerentanan dalam jaringan WiFi di Kominfo dan Informatika (Kominfotik) Sumbawa. Skenario dimulai dengan penyerang yang berada dalam jangkauan fisik jaringan WiFi target, menggunakan perangkat yang telah dikonfigurasi untuk melakukan serangan. Penyerang memanfaatkan alat seperti Aircrack-ng untuk mengaktifkan mode monitor pada adapter WiFi, yang memungkinkan mereka untuk menangkap paket data yang dikirimkan antara perangkat klien dan access point. Setelah berhasil menangkap handshake, penyerang kemudian mencoba untuk mendekripsi kata sandi jaringan menggunakan teknik brute force atau dictionary attack. Dengan akses ke jaringan, penyerang dapat melakukan sniffing terhadap lalu lintas data, termasuk informasi sensitif seperti username, password, dan data pribadi lainnya yang tidak terenkripsi(Huzairi, 2023). Skenario ini menyoroti pentingnya penerapan langkah-langkah keamanan yang kuat, seperti penggunaan enkripsi yang lebih baik dan pengaturan kebijakan akses yang ketat, untuk melindungi jaringan dari potensi serangan sniffing yang dapat mengakibatkan kebocoran data dan pelanggaran privasi(Rizqi Nurdiana et al., 2021).

a. Install Virtual Box

Menginstal VirtualBox adalah langkah awal yang penting untuk memulai pengujian jaringan WiFi dalam penelitian ini. Proses ini dimulai dengan mengunjungi situs resmi VirtualBox, di mana pengguna dapat mengunduh versi terbaru dari perangkat lunak virtualisasi tersebut, yang tersedia untuk berbagai sistem operasi seperti Windows, macOS, dan Linux.

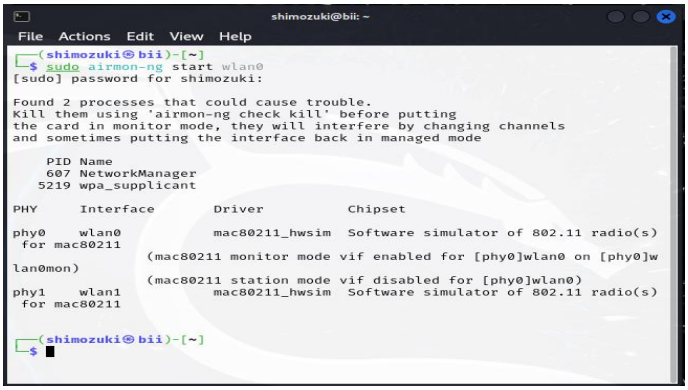
sistem operasi (dalam hal ini, Linux), dan versi yang sesuai (Kali Linux). Setelah itu, pengguna harus mengalokasikan memori (RAM) yang cukup untuk mesin virtual, biasanya antara 2GB hingga 4GB, tergantung pada spesifikasi sistem host dan kebutuhan aplikasi yang akan dijalankan. Selanjutnya, pengguna akan diminta untuk membuat hard disk virtual, di mana mereka dapat memilih ukuran dan

jenis penyimpanan (VDI, VHD, atau VMDK). Setelah semua pengaturan selesai, pengguna dapat menyelesaikan proses pembuatan mesin virtual. Mesin virtual yang baru dibuat kini siap untuk diinstal dengan sistem operasi Kali Linux, memungkinkan pengguna untuk melakukan pengujian keamanan dan analisis jaringan tanpa mempengaruhi sistem operasi utama mereka. Dengan demikian, langkah ini sangat penting dalam mempersiapkan lingkungan pengujian yang aman dan efisien

Gambar 2 Virtual Mesin Kali Linux

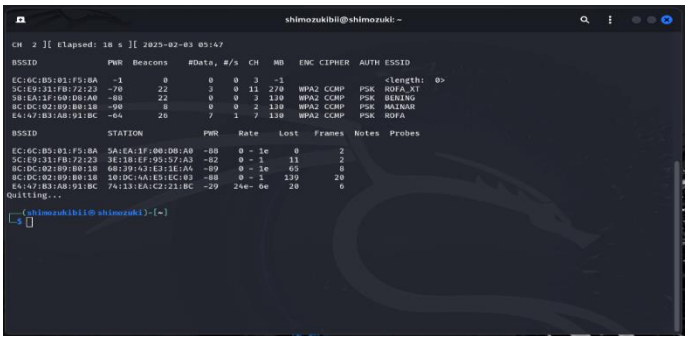
b. Menangkap Handshake

Handshake adalah proses komunikasi yang terjadi antara perangkat klien dan access point (AP) saat klien mencoba untuk terhubung ke jaringan WiFi. Proses ini melibatkan pertukaran beberapa paket data yang berisi informasi penting, termasuk identifikasi jaringan dan kunci enkripsi. Untuk menangkap handshake, penyerang atau penguji keamanan biasanya menggunakan alat seperti airodump-ng, yang berfungsi untuk memonitor lalu lintas jaringan dalam mode monitor. Dengan menjalankan perintah yang tepat, pengguna dapat mengidentifikasi jaringan target dan mulai menangkap paket data yang dikirimkan. Untuk meningkatkan peluang menangkap handshake, teknik deauthentication dapat diterapkan, di mana penyerang mengirimkan paket deauth ke klien yang terhubung, memaksa mereka untuk terputus dan mencoba terhubung kembali. Ketika klien mencoba untuk terhubung kembali, handshake akan terjadi, dan paket-paket tersebut dapat ditangkap. Data handshake yang berhasil ditangkap kemudian dapat digunakan untuk analisis lebih lanjut, seperti mencoba mendekripsi kata sandi jaringan menggunakan alat seperti Aircrack-ng. Dengan demikian, menangkap handshake merupakan langkah penting dalam mengidentifikasi kerentanan jaringan dan menguji efektivitas langkah-langkah keamanan yang diterapkan. Berikut adalah hasil masuk ke mode monitor dengan printah *sudo airmon-ng start wlan0*(Riadi et al., 2020).



Gambar 3 Mode Monitor

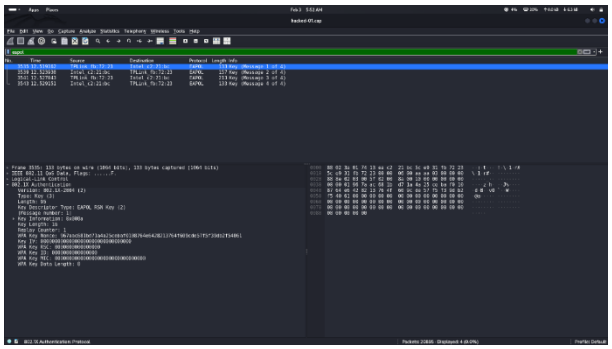
Pada gambar 4.4 tersebut, terlihat bahwa mode monitor telah berhasil diaktifkan dengan status "enable". Setelah mengaktifkan mode monitor, kita dapat memverifikasi perubahan ini dengan menggunakan perintah iwconfig, yang menunjukkan bahwa adaptor jaringan WiFi yang sebelumnya bernama wlan0 kini telah berubah menjadi wlan0mon. Perubahan nama ini menandakan bahwa adaptor sekarang siap untuk menangkap paket data dari jaringan. Selanjutnya, untuk menemukan titik akses dari jaringan yang tersedia, kita akan menggunakan perintah sudo airodump-ng wlan0mon, yang memungkinkan kita untuk memindai dan menganalisis jaringan WiFi di sekitar(Esabella & Bella Fitriana, 2023).



Gambar 4 Menampilkan Titik Akses

Pada gambar di atas, terlihat hasil dari pemindaian jaringan WiFi yang dilakukan menggunakan perintah airodump-ng. Dalam output ini, terdapat informasi penting mengenai jaringan yang terdeteksi. Jaringan dengan BSSID 5C:E9:31:FB:72:23 menggunakan enkripsi WPA2 dengan cipher CCMP dan memiliki ESSID "Persandian2". Jaringan ini berada di channel 11 dan menunjukkan kekuatan sinyal yang cukup baik. Selain itu, terdapat informasi mengenai klien yang terhubung ke jaringan tersebut. Klien dengan alamat MAC 02:00:00:00:01:00 menunjukkan status "not associated", yang berarti klien tersebut belum terhubung ke jaringan. Namun, informasi mengenai jumlah frame yang hilang dan jumlah probe yang dilakukan oleh klien tersebut juga ditampilkan. Selanjutnya jalankan perintah sudo airodump-ng --bssid 5C:E9:31:FB:72:23 -c 11 --write [filename] wlan0mon untuk menangkap handshake dari jaringan yang ingin Anda analisis. Pada penelitian ini saya mengunakan jaringan 5C:E9:31:FB:72:23 dan nama file hacked-01.cap(Esabella & Bella Fitriana, 2023).

Perintah wireshark hacked-01.cap digunakan untuk membuka dan menganalisis file capture yang berisi data jaringan yang telah ditangkap sebelumnya, dalam hal ini file hacked-01.cap. Gambar yang ditampilkan menunjukkan hasil analisis dari file tersebut menggunakan Wireshark, sebuah alat analisis jaringan yang populer. Berikut adalah hasil dari wireshark.

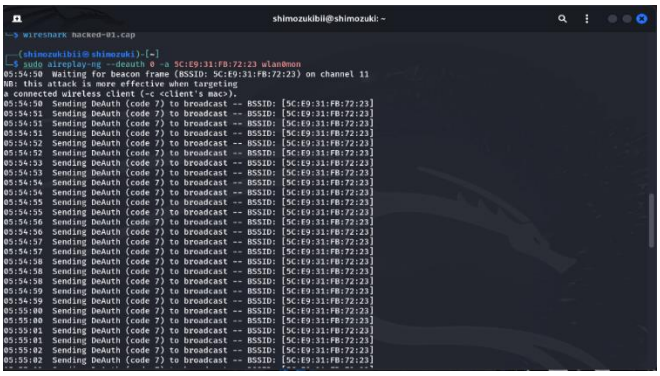


Gambar 5 File Tangkapan Di Wireshark

Pada gambar 4.7, terlihat bahwa Wireshark menampilkan beberapa frame yang berisi pesan EAPOL (Extensible Authentication Protocol over LAN), yang merupakan bagian dari proses handshake WPA2. Proses ini terdiri dari empat pesan kunci yang diperlukan untuk mengautentikasi perangkat yang terhubung ke jaringan. Frame pertama menunjukkan pesan kunci pertama dari empat pesan yang diperlukan, diikuti oleh pesan kedua, ketiga, dan keempat. Setiap pesan berisi informasi penting seperti nonce, ID kunci, dan informasi lainnya yang diperlukan untuk proses otentikasi.

c. Deauthentication Attack

Deauthentication Attack adalah teknik yang digunakan dalam keamanan jaringan untuk memutuskan koneksi antara perangkat klien dan access point (AP) secara paksa. Proses ini sering digunakan oleh penyerang untuk mengumpulkan *informasi lebih lanjut, seperti handshake WPA/WPA2, yang dapat digunakan untuk mencoba memecahkan kunci jaringan*.



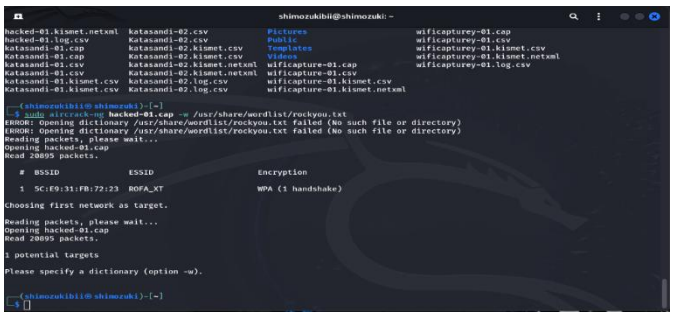
Gambar 6 Deauthentication

Pada gambar 6 tersebut menampilkan proses Deauthentication Attack yang dilakukan menggunakan utilitas aireplay-ng. Perintah yang dieksekusi adalah sudo aireplay-ng --deauth 0 -a 5C:E9:31:FB:72:23 wlan0mon. Hasil dari perintah ini adalah pengiriman paket deauthentication secara berulang ke access point dengan BSSID 5C:E9:31:FB:72:23 melalui interface wlan0mon. Pesan "Sending Deauth (code 7) to broadcast" menunjukkan bahwa paket deauthentication dengan kode alasan 7 (berarti "alasan yang tidak ditentukan") dikirimkan ke alamat broadcast. Pengiriman ke alamat broadcast ini bertujuan untuk memutuskan koneksi semua klien yang terhubung ke access point target. Serangan ini efektif untuk memaksa klien terputus dan kemudian mencoba terhubung kembali, sehingga memungkinkan penyerang untuk menangkap four-way handshake yang diperlukan untuk proses cracking password WPA/WPA2. Pesan "Waiting for beacon frame" menunjukkan bahwa aireplay-ng sedang menunggu beacon frame dari access point untuk memastikan target masih aktif dan untuk menyinkronkan serangan.

d. *Cracking Dictionary Attack*

Cracking Dictionary Attack adalah metode yang digunakan untuk memecahkan kata sandi dengan memanfaatkan daftar kata sandi yang umum atau kata-kata yang mungkin digunakan oleh pengguna. Metode ini berfungsi dengan *mencocokkan hash dari kata sandi yang dicoba dengan hash yang telah ditangkap dari proses otentikasi, seperti dalam kasus jaringan Wi-Fi yang menggunakan WPA/WPA2.*

Fungsi utama dari serangan ini adalah untuk mengidentifikasi kata sandi yang lemah atau umum yang mungkin digunakan oleh pengguna untuk mengamankan jaringan mereka. Dalam konteks keamanan jaringan, serangan ini sangat berguna karena banyak pengguna cenderung menggunakan kata sandi yang mudah diingat, seperti nama hewan peliharaan, tanggal lahir, atau kata-kata umum lainnya. Dengan menggunakan alat seperti Aircrack-ng, penyerang dapat mengotomatiskan proses pencocokan hash dengan daftar kata sandi yang telah disusun sebelumnya, yang dikenal sebagai "dictionary."

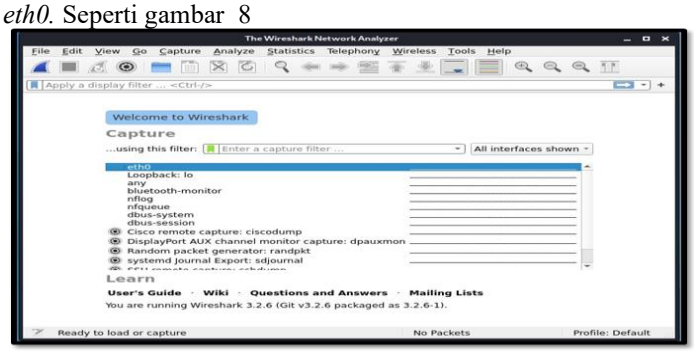


Gambar 7 Proses Cracking Dictionary Attack

Pada gambar 4.9 yang ditampilkan menunjukkan proses dari aircrack-ng yang menggunakan data hasil handshake sebelumnya untuk memecahkan kata sandi pada enkripsi WPA. Dalam proses ini, aircrack-ng berhasil mendeteksi satu jaringan target dengan BSSID 5C:E9:31:FB:72:23 dan ESSID PERSANDIAN2. Meskipun terjadi kesalahan dalam penggunaan file kamus, alat ini tetap dapat membaca paket dari file capture yang ada. Namun, untuk melanjutkan proses cracking dan mendapatkan kata sandi, diperlukan file kamus yang valid. Jika file kamus yang tepat tersedia, proses ini berpotensi untuk berhasil memecahkan kata sandi yang digunakan pada jaringan tersebut

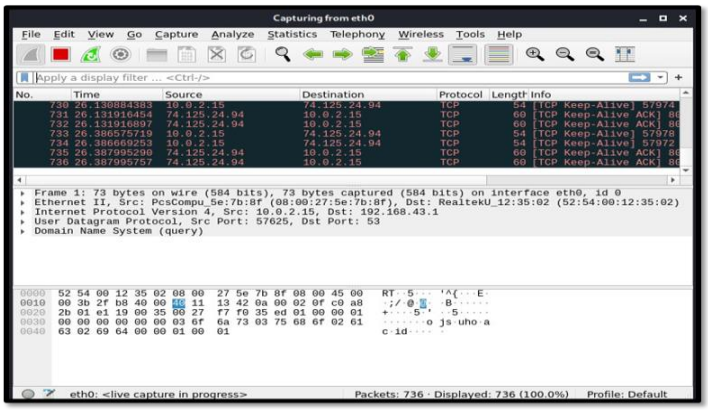
PEMBAHASAN

Selanjutnya penulis membuka *software wireshark.* Langkah pertama penyerangan adalah pilih *interface* jaringan yang diinginkan.Terdapat beberapa *interface* yang bertugas untuk meng*capture packet.* Pada tahap ini penulis memilih *interface eth0.* Seperti gambar 8



Gambar 8 Tampilan Interface Pada wireshark

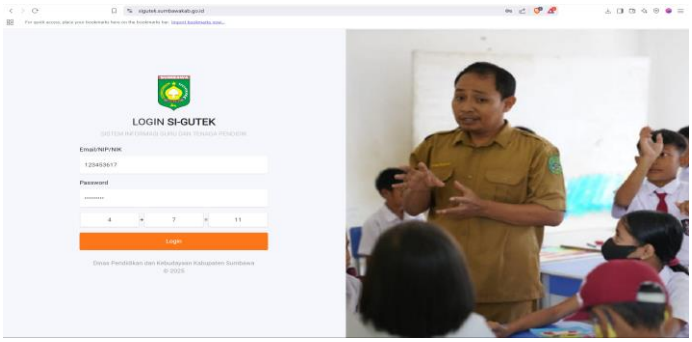
Setelah melakukan start pada interface yang sudah dipilih tadi, maka dengan otomatis tools pada wireshark berjalan dan menangkap hasil capture packet dari web browser yang telah dibuka. Seperti pada Gambar 9



Gambar 9 Proses Capture Pada interface eth0

e. *Penyerangan Website Sigutek*

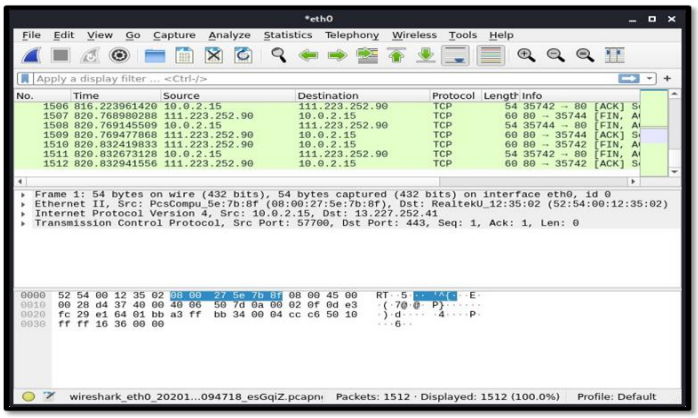
Pada tampilan login website unpad, penyerang mencoba melakukan serangan packet sniffing terhadap website sigutek. Pada tahap ini penyerang target melakukan proses login menginput nip, password yang salah dengan tujuan ingin mencoba kerentanan terhadap website tersebut. Seperti pada gambar 10



Gambar 10 Tampilan Halaman Login Sigutek

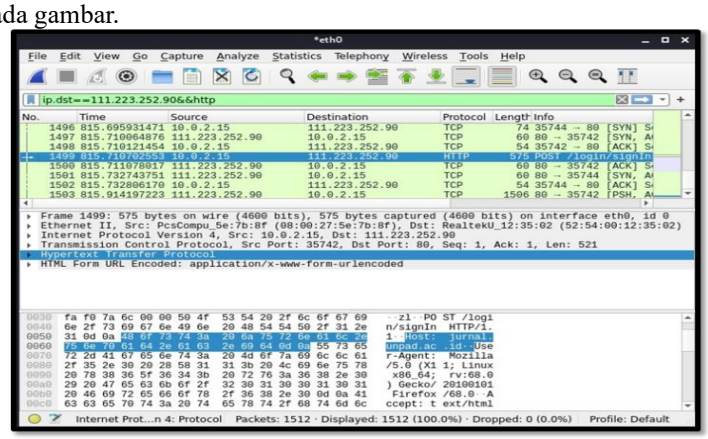
Selanjutnya proses capture packet akan terjadi, lalu penyerang menekan stop untuk menghentikan proses capturing packet. Pada tampilan capturing packet dapat dilihat beberapa informasi seperti packet list dan packet byte. Pada packet list dapat dilihat beberapa informasi packet yang terurut secara numerik informasi dari packet list yaitu waktu, sumber paket, ip tujuan, protocol yang digunakan,panjang peket dan

informasi lebih lanjut tentang paket sedangkan pada packet byte hasil paket ditampilkan dalam bilangan Hexadecimal dan ASCII, Seperti pada gambar 11



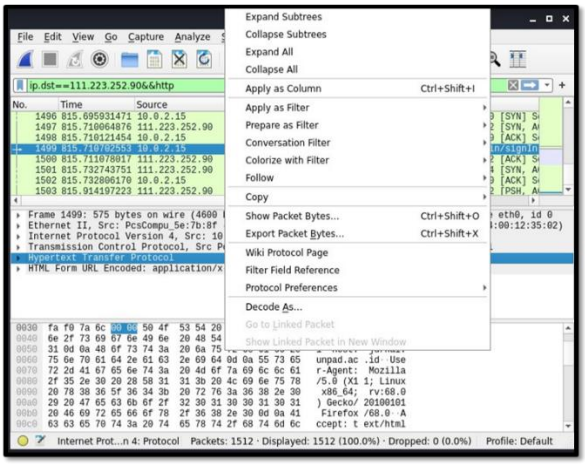
Gambar 11 Proses Stop Capture Packet

Pada proses ini dilakukan pencarian *ip address* atau alamat website pada terminal jika tidak ditemukan *ip address* pada *capture packet* yang tertangkap. Selanjutnya proses pencarian *packet* penyerang memasukkan perintah pada *display filter* untuk menampilkan parameter login pada *packet* yang *tercapture.*Seperi pada gambar.



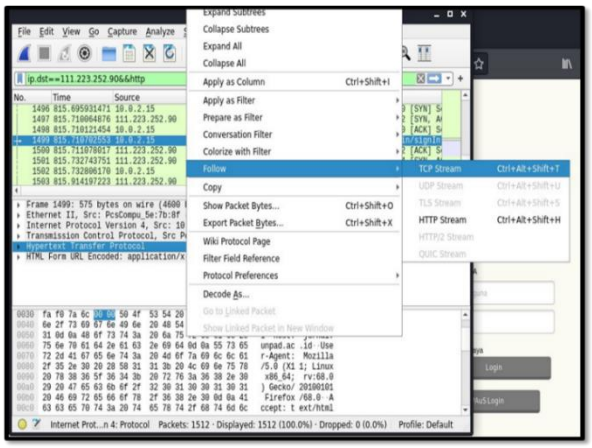
Gambar 12 Pencarian Packet Display Filter

Selanjutnya pada proses ini penyerang melakukan klik kanan pada Hypertext Transfer Protocol (HTTP). Seperti pada gambar 13



Gambar 13 Proses Follow Pada HTTP

Pada proses ini setelah melakukan klik kanan pada Hypertext Transfer Protocol (HTTP) selanjutnya pilih Follow –TCP Stream. Sepeti pada gambar



Gambar 14 Proses Follow TCP Stream

f. Reporting

Berdasarkan hasil uji enkripsi yang telah dilakukan menggunakan alat aircrack-ng, terlihat bahwa proses cracking terhadap jaringan Wi-Fi yang terdeteksi menunjukkan beberapa variabel penting yang dapat dianalisis. Dalam pengujian ini, kami menggunakan file capture hacked-01.cap, yang berisi data handshake dari jaringan dengan BSSID 5C:E9:31:FB:72:23 dan ESSID PERSANDIAN2. Meskipun alat berhasil membaca paket dan mendeteksi satu potensi target, terdapat kendala dalam penggunaan file kamus yang diperlukan untuk melanjutkan proses cracking. Dari pengujian ini, kami mendapatkan beberapa hasil data yang relevan, antara lain :

Table 1 Hasil Reporting

Jenis serangan	Informasi Yang di Temukan	Status
Capture Traffic AP	BSSID, Enkripsi, Channel, dan ESSID	Berhasil
Deauthentication	MAC Address Beacon	Berhasil
Capture Handsake	Auth system	Berhasil
Cracking Dictionary Attack	Kata Sandi dari Enkripsi	Tidak Berhasil

Berdasarkan hasil uji enkripsi yang disajikan dalam Tabel 4.1, terdapat beberapa jenis serangan yang dilakukan untuk menguji keamanan jaringan. Pertama, pada serangan **Capture Traffic AP**, informasi yang berhasil ditemukan mencakup BSSID, enkripsi, channel, dan ESSID, yang menunjukkan bahwa proses ini berhasil dilakukan. Selanjutnya, pada serangan **Deauthentication**, informasi yang diperoleh adalah MAC Address Beacon, yang juga berhasil ditangkap. Proses **Capture Handshake** berhasil mengidentifikasi sistem otentikasi yang digunakan, menandakan bahwa langkah ini juga sukses. Namun, pada serangan **Cracking Dictionary Attack**, meskipun telah dilakukan, proses ini tidak berhasil mendapatkan kata sandi dari enkripsi yang diuji. Hasil ini menunjukkan bahwa meskipun beberapa langkah dalam pengujian berhasil, tantangan tetap ada dalam proses cracking, yang sangat bergantung pada ketersediaan dan keakuratan file kamus yang digunakan.

KESIMPULAN

Penelitian ini menganalisis kerentanan protokol WPA2 terhadap serangan *packet sniffing*. Hasil analisis menunjukkan bahwa meskipun WPA2 menawarkan peningkatan keamanan dibandingkan dengan pendahulunya, protokol ini masih rentan terhadap berbagai jenis serangan, termasuk *deauthentication attack* dan *dictionary attack*. Keberhasilan serangan-serangan ini berpotensi mengakibatkan akses tidak sah ke jaringan dan pencurian data sensitif. Temuan ini menggarisbawahi pentingnya pemahaman yang komprehensif terhadap kerentanan keamanan jaringan Wi-Fi dan perlunya implementasi strategi mitigasi yang efektif untuk melindungi integritas dan kerahasiaan data yang ditransmisikan. Penelitian ini menyoroti perlunya pendekatan keamanan berlapis untuk meminimalkan risiko eksploitasi celah keamanan pada protokol WPA2

REFERENSI

Adiguna, M. A., & Widagdo, B. W. (2022). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r). *Jurnal SISKOM-KB (Sistem Komputer Dan Kecerdasan Buatan)*, *5*(2), 1–8. https://doi.org/10.47970/siskom-kb.v5i2.268

Arini, A., Luthfi Arsalan, M., & Teja Sukmana, H. (2024). Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus : Pt. Akurat.Co). *Cyber Security Dan Forensik Digital*, *6*(2), 30–38. https://doi.org/10.14421/csecurity.2023.6.2.4075

Arsalan, M. L. (2023). Keamanan Jaringan Wireless Fidelity (Wi-Fi) Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus: PT Akurat Sentra MediaA. *Repository.Uinjkt.Ac.Id*.

Danuasmo, S., Nazuarsyah, N., & Ginting, R. B. (2023). Rancang Bangun Jaringan Wireless Lan Dan Internet Berbasis Cloud Pada Universitas Bina Bangsa Getsempena. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *7*(1), 15. https://doi.org/10.22373/cj.v7i1.16865

Darmawan, M. A., Ningsih, R., & Jurnaidi, A. (2024). *Analisis Keamanan Jaringan Terhadap Sniffing*. *14*(3), 228–233.

Farhan, R. M., & Kusuma, G. H. A. (2023). Teknik Sniffing Jaringan Menggunakan Wireshark. *Journal of Informatics and Advanced Computing (JIAC)*, *4*(1), 87–93.

Fatimah, F., Mary, T., & Pernanda, A. Y. (2022). Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing di Universitas PGRI Sumatera Barat. *JURTEII: Jurnal Teknologi Informasi*, *1*(2), 7–11. https://doi.org/10.22202/jurteii.2022.5707

Introduction, A. H. (n.d.). *Penetration testing to Hacking*.

Kunang, Y. N., Ibadi, T., Nugroho, B. A., Mursyidah, Husaini, Atthariq, Arhami, M., Hidayat, H. T., Anita, Ramadhona, Meena, R. C., Nawal, M., Bundele, M. M., Rengaraju, P., Kumar, S. S., Lung, C. H., & Purnama, R. A. (2019). Analysis and implementation of the Port Knocking method using Firewall-based Mikrotik RouterOS. *IOP Conference Series: Materials Science and Engineering*, *8*(4), 1907–5022.

Muhyidin, Y., Hafid Totohendarto, M., Undamayanti, E., & Tinggi Teknologi Wastukancana, S. (2020). Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking Comparison of Website Security Levels Using Nmap and Nikto With Ethical Hacking Methods. *Jurnal Teknologika*, 1–10.

Peminatan, B., Komputer, T., Mahasiswa, J., Tarbiyah, F., & Keguruan, D. (2023). *Analisis keamanan fasilitas(wifi) terhadapap serangan packet sniffing pada protokol http dan https*.

Rizqi Nurdiana, F., Gunawan, I., Cahya Viollita, R., Faizal, Ma., Nurcahyadi abcde Teknik informatika, D., & Tinggi Teknologi Ronggolawe Cepu Penulis Korenspondensi, S. (2021). Analisis Keamanan Jaringan Wifi Menggunakan Wireshark. *JES (Jurnal Elektro Smart)*, *1*(1), 10–12. https://www.sttrcepu.ac.id/jurnal/index.php/jes/article/view/159

Alam, M. A. J., & Agus, M. (2008). *Mengenal Wifi, Hotspot, LAN, dan Sharing Internet* .Jakarta: PT Elex Media Komputindo.

Riadi, I., Yudhana, A., & Yunanri.W Korspondensi, P. (2020). *Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment*. *7*(4). https://doi.org/10.25126/jtiik.202071928

Safira, R. (n.d.). *Analisis Kinerja Jaringan Komputer Pada Smkn 1 Sumbawa Besar Dengan Menggunakan Metode Network Performance Analysis (NPA)* (Vol. 1, Issue 1). https://jurnal.uts.ac.id/index.php/jurtikom

Yunanri.W, Esabella, S., & Bella Fitriana, (2023). KLIK: Kajian Ilmiah Informatika dan Komputer Analisis Keamanan Jaringan Menggunakan Metode Security Policy Development Life Cycle (SPDLC). *Media Online*, *4*(1), 634–641. https://doi.org/10.30865/klik.v4i1.1157

Yunanri.W, Riadi, I., & Yudhana, A. (2016). *Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST)* (Vol. 2, Issue 1). http://ars.ilkom.unsri.ac.id300