GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

Analisis Keamanan Jaringan Wifi dengan Teknik Packet Sniffing pada Lembaga Penyiaran Publik RRI Bengkulu

Analysis of Wifi Network Security with Packet Sniffing Technique at RRI Bengkulu Public Broadcasting Institution

Yulia Astuti[1)]; Hari Aspriyono[2)]; Ricky Zulfiandry[2)]
[1,2)]***Department of Informatics, Faculty of Computer Science, Universitas Dehasen Bengkulu***
Email: [1)] yuliaastuti161117@gmail.com

How to Cite :
Astuti, Y., Aspriyono, H., Zulfiandry, R. (2021). *Analysis of Wifi Network Security with Packet Sniffing Technique at RRI Bengkulu Public Broadcasting Institution*. Gatotkaca Journal, 2(2) page: 163-172. DOI: **https://doi.org/10.37638/gatotkaca.2.1.163-172**

ARTICLE HISTORY
Submited [29 Desember 2021]
Received [29 Desember 2021]
Revised [30 Desember 2021]
Accepted [31 December 2021]

KEYWORDS
Sniffing, Wifi, Internet, RRI Bengkulu

ABSTRAK
Masalah teknologi wireless menawarkan berbagai kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi wireless miliki cukup banyak kelebihan dibandingkan teknologi kabel yang sudah ada, diantaranya kemudahan akses komunikasi data dan akses internet di posisi manapun selama masih berada dalam jaringan wireless. Tujuan penelitian ini adalah menganalisis keamanan di dalam jaringan WLAN (Wireless Local Area Network) menggunakan teknik packet Sniffing. Metode yang digunakan adalah metode (NDLC) Network Development Life Cycle suatu siklus tahapan perancangan jaringan yang dapat menuntun sebuah perancangan jaringan, yang bergantung pada besarnya proyek yang akan dilaksanakan dan tujuan dari pembuatan proyek tersebut. Pengujian keamanan wireless menggunakan airodamp-ng sebagai media penyerangan dan analisis keamanan menggunakan metode wireless packetsniffing yang akan di uraikan pada aplikasi wireshak. packet sniffing merupakan sebua proses untuk menangkap paket yang melintas melalui jaringan komputer. Berdasarkan dari analisis dan percobaan serangan yang dilakukan maka masih perlu peningkatan, hal ini di dengan aplikasi airodamp-ng mendeteksi WiFi yang ada di sekitar dan serangang packet sniffing dapat menampilkan username dan password dengan menggunakan aplikasi wireshak.

ABSTRACT
The problem of wireless technology offers a variety of convenience, freedom and high flexibility. Wireless technology has quite a lot of advantages compared to existing wired technology, including easy access to data communication and internet access in any position as long as it is still in a wireless network. The method used is the Network Development Life Cycle (NDLC) method, a cycle of network design stages that can guide a network design, which depends on the size of the project to be implemented and the purpose of the project. Wireless security testing uses airodump-ng as an attack medium and security analysis uses wireless packet sniffing method which will be described in the wireshak application. Packet sniffing is a process for capturing packets passing through a computer network. Based on the analysis and attack experiments carried out, it still needs improvement, this is with the airodump-ng application detecting nearby WiFi and packet sniffing attacks can display usernames and passwords using the wireshak application.

PENDAHULUAN

Masalah Teknologi wireless menawarkan berbagai kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi wireless memiliki cukup banyak kelebihan dibandingkan teknologi kabel yang sudah ada, diantaranya kemudahan akses komunikasi data dan akses internet di posisi manapun selama masih berada dalam jangkauan wireless.

Selain menawarkan berbagai kemudahan, dalam jaringan wireless atau WLAN (Wireless Local Area Network), terdapat resiko keamanan yang lebih kritis dibandingkan dengan jaringan kabel karena medium udara dalam jaringan wireless tidak bisa dikontrol secara fisik. Hal ini membuat para penyerang atau penyusup (hacker) menjadi tertarik untuk melakukan berbagai aktivitas yang biasanya ilegal terhadap jaringan wireless (WLAN). Penyerangan yang dilakukan oleh hacker sangat bervariasi, mulai

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

dari Sniffing packet, packet injection, illegal authentication, sampai cracking WEP (Wired Equivalent Privacy), dan Cracking WPA (Wifi Protected Access) / WPA2.

RRI Bengkulu adalah suatu lembaga penyiaran publik yang terletak di jalan S. Parman No.31 Bengkulu. Lembaga Penyiaran Publik (LPP) Radio Republik Indonesia (RRI) Bengkulu bertugas untuk menyiarkan siaran-siaran pemerintah pada umumnya dan pemerintah daerah pada khususnya. Disamping juga mengadakan siaran hiburan bersama dengan itu dibentuk

pula badan pengasuh siaran RRI persiapan Bengkulu dengan kepala Studio AMRAH AHMAD BE. Dalam menunjang siaran RRI Bengkulu. menggunakan server Freenas untuk menyimpan lagu pro 1, 2, dan 4. Selain menggunakan server freenas RRI juga menggunakan jaringan internet indihome dengan bandwidth 100 Mbps yang didistribusikan ke pengguna melalui media WLAN (Wireless Local Area Network).

Dalam hal ini penulis akan menganalisis keamanan jaringan WLAN (Wireless Local Area Network) dengan teknik packet sniffing. Sniffing adalah proses monitoring dan capturing semua paket yang melewati jaringan tertentu dengan menggunakan alat sniffing. Teknik sniffing pada jaringan WLAN (Wireless Local Area Network) di LPP RRI Bengkulu akan dilakukan uji coba serangan sniffing menggunakan Software Airodump-ng sebagai media penyerangan dan wireshark sebagai media pengurai paket yang telah ditangkap.

LANDASAN TEORI

Jaringan Komputer

Menurut Herman (2018:4) Jaringan komputer adalah sekumpulan komputer (lebih dari satu) yang berhubungan satu dengan lainnya menggunakan media tertentu sehingga memungkinkan antar komputer tersebut untuk berinteraksi, bertukar data, dan berbagi peralatan bersama misalkan printer, scanner dan lain-lain. Dan dalam membentuk sebuah jaringan komputer terdapat komponen-komponen dasar yang perlu diketahui yaitu:

1. Host atau Node Merupakan komputer yang bertindak sebagai prosesor utama dalam sebuah jaringan.
2. Link Atau Saluran Merupakan media yang digunakan untuk menghubungkan antara komputer dalam sebuah jaringan, link atau saluran dapat berupa media kabel, fiber optic dan wireless.
3. Perangkat Lunak (Software). Perangkat lunak menjadi bagian penting dalam sebuah jaringan, dikarenakan fungsinya yang bertugas untuk mengatur jalannya informasi, pengelolaan antara satu simpul dengan simpul yang lain.

Topologi jaringan

Menurut Charles (2018:20) Topologi jaringan adalah salah satu aturan bagaimana menghubungkan komputer (node) satu sama lain secara fisik dan pola hubungan antara komponen-komponen yang berkomunikasi melalui media atau peralatan jaringan, seperti server, workstation, hub/switch, dan pemasangan kabel (media transmisi data).

Wireless LAN

Menurut Efvy (2016:1), jaringan Wireless atau disebut juga Wireless LAN merupakan jaringan tanpa kabel yang menggunakan udara sebagai media transmisinya untuk menghantarkan gelombang elektromagnetik.

1. Antena merupakan perangkat eksternal yang digunakan untuk memperkuat sinyal. Perangkat ini juga termasuk dalam komponen jaringan WLAN yang bersifat opsional, kita bisa menggunakannya atau tidak.
2. Router adalah sebuah perangkat yang berfungsi untuk menghubungkan dua jaringan atau lebih sehingga pengiriman data dari satu perangkat ke perangkat lain bisa diterima.
3. 3.Modem merupakan singkatan dari Modulator Demodulator. Modem merupakan alat untuk mengubah sinyal digital komputer (aliran data) menjadi sinyal analog (sinyal-sinyal telepon), dan sebaliknya.
4. 4.Switch menghubungkan semua komputer yang terhubung ke LAN, sama seperti hub. Perbedaannya adalah switch dapat beroperasi dengan mode full-duplex dan mampu mengalihkan jalur dan menyaring informasi ke dan dari tujuan yang spesifik.
5. 5.Kabel jaringan, kabel dalam sebuah jaringan digunakan sebagai penghubung. Meskipun sekarang sudah ada teknologi jaringan tanpa kabel (wireless) namun kabel masih sering digunakan karena mudah dalam pengoprasiannya.

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

Packet Sniffing

Menurut Gede (2014:151) Packet Sniffing, network analyzers atau penyadapan paket merupakan sebuah proses untuk menangkap paket paket yang melintas melalui jaringan komputer. Untuk melakukan proses packet sniffing memerlukan aplikasi tertentu. Aplikasi ini menangkap tiap-tiap paket dan kadang-kadang menguraikan isi dari RFC (Request for Comments) atau spesifikasi yang lain. Berdasarkan pada struktur jaringan (seperti hub atau switch), salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu lintas dari salah satu mesin di jaringan. Perangkat pengendali jaringan dapat pula diatur oleh aplikasi penyadap untuk bekerja dalam mode campur-aduk (promiscuous mode) untuk "mendengarkan" semuanya (umumnya pada jaringan kabel).

TCP/IP

Menurut Siswo (2014:107), TCP/IP (Transmission Control Protocol/Internet Protocol) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar menukar data dari satu komputer ke komputer lain di dalam suatu jaringan.

METODE PENELITIAN

NDLC (Network development life Cycle) Network Development merupakan suatu siklus tahapan perancangan jaringan yang dapat menuntun sebuah perancangan jaringan, yang bergantung pada besarnya proyek yang akan dilaksanakan dan tujuan dari pembuatan proyek tersebut. Setiap tahapan siklus merupakan proses yang akan menentukan bagaimana proses kelanjutan dari proyek yang akan dilaksanakan.

1. Analisis

   Tahap awal sebelum penelitian dilakukan maka peneliti terlebih dahulu melakukan pengumpulan data untuk dijadikan bahan dalam menentukan sistem baru. Metode pengumpulan data yang peneliti lakukan adalah wawancara dengan pengguna. Setelah data terkumpul, selanjutnya dilakukan analisis permasalahan. Analisis permasalahan dilakukan untuk menjawab sistem baru yang akan dibuat. Data hasil analisis tersebut selanjutnya disajikan dan diberikan pembahasan. Dari analisis permasalahan tersebut, peneliti mencoba menjawab (memberikan solusi) yang diperoleh dari pencarian teori-teori yang relevan.
2. Desain

   Peneliti merancang desain pengujian sistem yang akan digunakan dalam analisis keamanan jaringan wifi.
3. Implementation

   Peneliti menggambarkan pengujian sistem dalam bentuk diagram blok dan flowchart kerja sistem.
4. Pengujian Sistem

   Setelah melakukan implementasi, maka tahap terakhir adalah Pengujian Sistem. Kesimpulan adalah hasil dari pengujian sistem apakah sistem diterima atau sistem ditolak. Kesimpulan ditulis dengan singkat, padat dan jelas. Selanjutnya eksploitasi lubang keamanan (exploitation), merupakan tahap dimana penguji mencoba menguji kerentanan yang didapatkan pada tahap sebelumnya. Yang terakhir yaitu post eksploitasi (post exploitation), merupakan tahap melaporkan hasil uji yang telah dilakukan dan memberikan rekomendasi untuk mengatasi kerentanan yang ditemukan.

HASIL DAN PEMBAHASAN

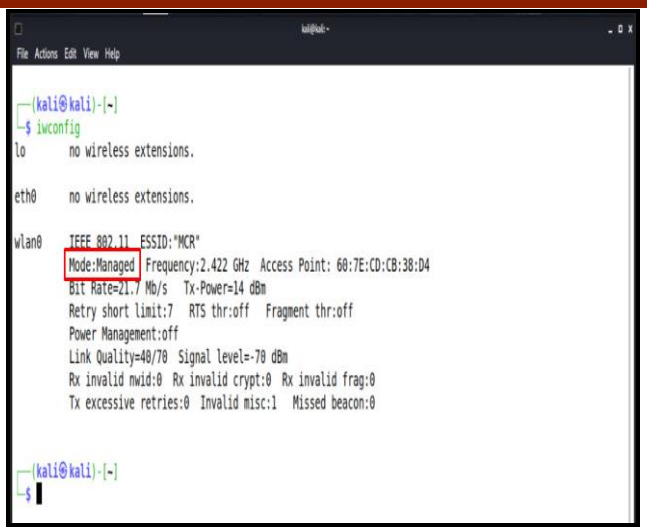
Hasil dan Pembahasan

Metode perancangan sistem yang digunakan dalam penelitian adalah metode *Network Development Life Cycle (NDLC*). Berdasarkan rancangan menggunakan metode NDLC yang sudah diperjelas pada bab III. Beriku adalah desain Topologi pada Lembaga Penyiaran Publik Radio Republik Indonesia Bengkulu.

Pengecekan *wireless interface* mode dan mengubah mode=managed ke mode=monitor

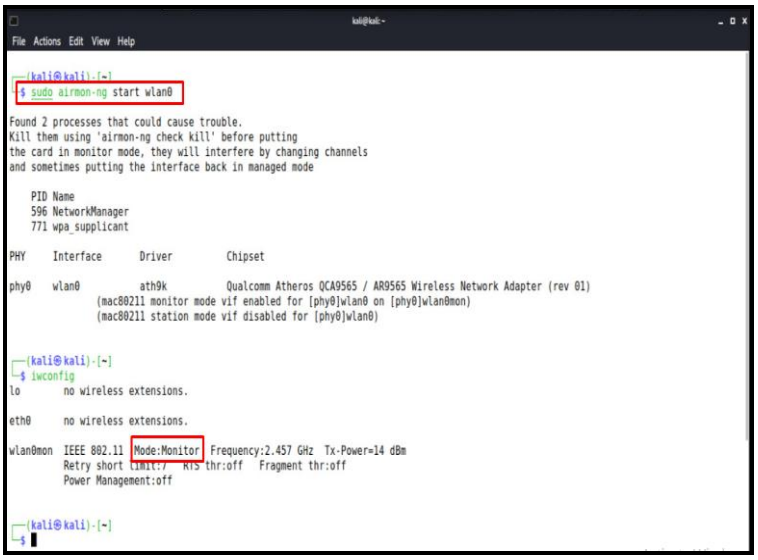
Langkah pertama adalah proses pengecekan mode *interface* yang terhubung ke wifi dengan mengetikkan perintah **$iwconfig**

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)



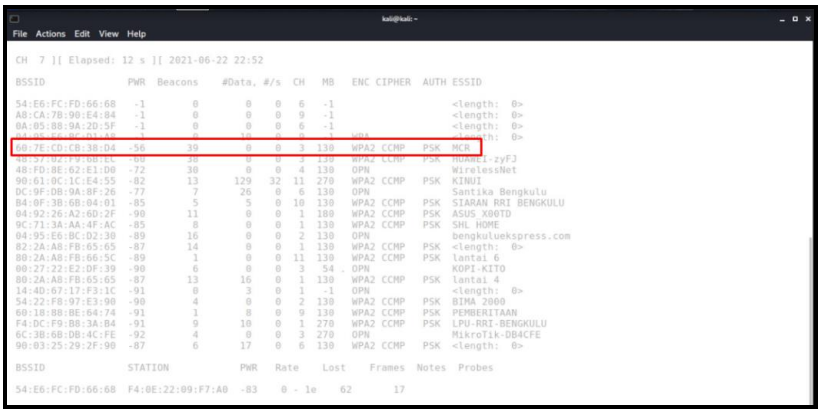
Gambar 1. Pengecekan *wireless interface* mode

Selanjutnya ketikkan perintah $**sudo airmon-ng start wlan0** untuk mengaktifkan *mode monitor* pada wifi.



Gambar 2. *Wireless interface mode Managed* ke *mode monitor*

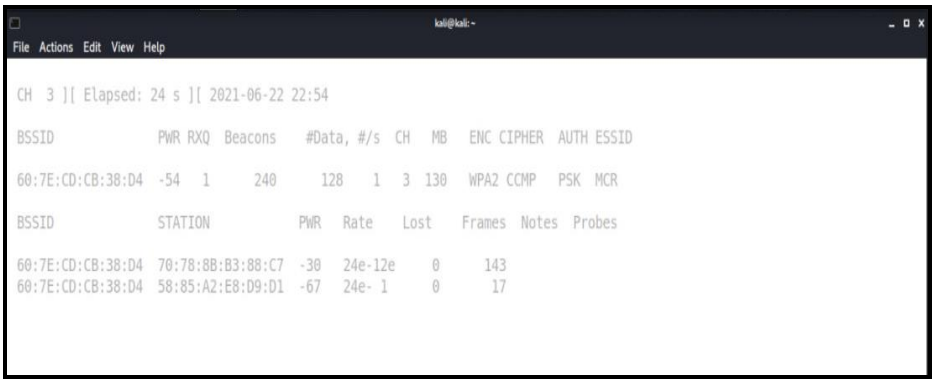
Jika sudah berubah menjadi *mode managed* lalu jalankan *airmon-ng* dan *scanning* wifi semua jaringan *nirkabel* yang ada disekitar akan ditampilkan, sekaligus informasi yang bermanfaat tentang jaringan tersebut. Temukan jaringan yang akan di uji. dengan menggunakan perintah **$sudo airodump-ng wlan0mon**.



Gambar 3 *Scanning* wifi

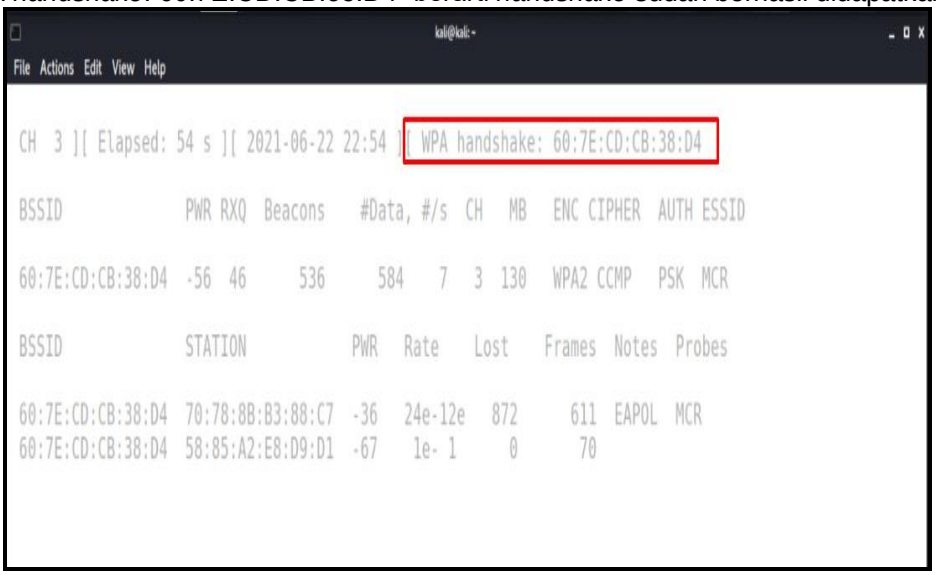
Setelah selesai *scanning* maka didapatkan beberapa essid. selanjutnya tentukan *wifi* yang akan kita *sniffing*. disini wifi yang akan di *sniffing* yaitu dengan SSID MCR. **$sudo airodump-ng wlan0mon –bssid 60:7E:CD:CB:38:D4 --essid MCR –channel 3 –write sniffingwifi –output-format pcap.**

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)



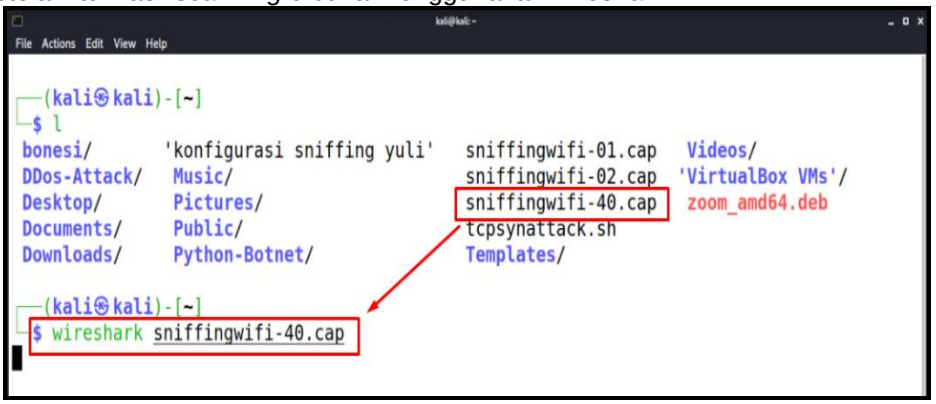
Gambar 4. *wifi running*

Pada saat proses *scanning* berjalan. AP mengirimkan paket *deauth* atau pemutusan koneksi dan *client* mencoba menghubungkan ulang, barulah kita akan mendapatkan *handshake*nya. Jika sudah muncul "*WPA handshake*: 60:7E:CD:CB:38:D4" berarti *handshake* sudah berhasil didapatkan.



Gambar 5. Hasil menangkap *wpa handshake*

Setelah itu Hasil *scanning* dibuka menggunakan *wireshark.*



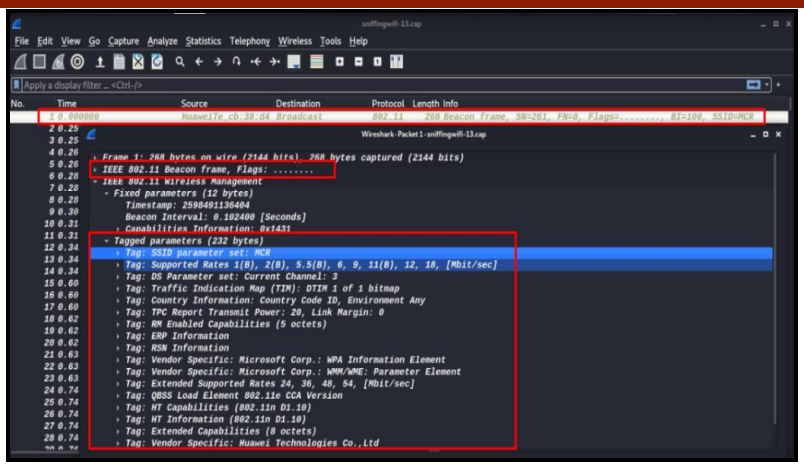
Gambar 6. Hasil *Sniffing* tersimpan di home direktori dan dibuka menggunakan *wireshark*

Analisis *wireshark*

Analisis *four way handshake* yang terjadi antara akses point dengan client/station dengan filter **mac : wlan.sa =70:78:8B:B3:88:C7**

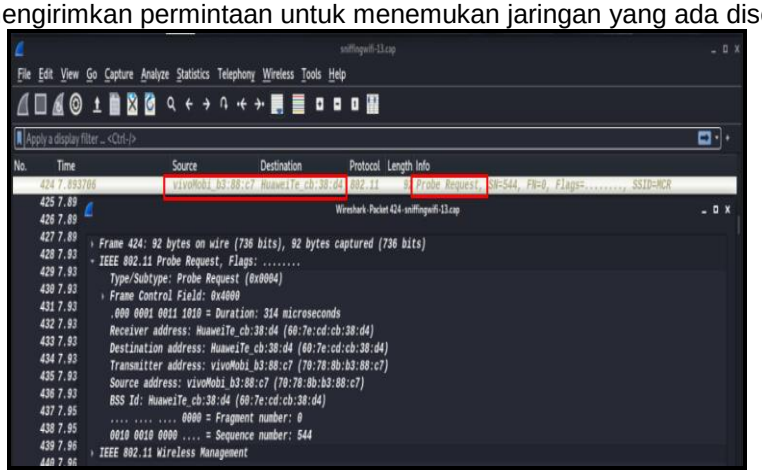
1. Akses point melakukan *broadcast* dengan menggunakan *beacon frame*. Pada saat akses point melakukan *broadcast* akan didapatkan informasi seperti SSID: MCR, *Chanel*: 3

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)



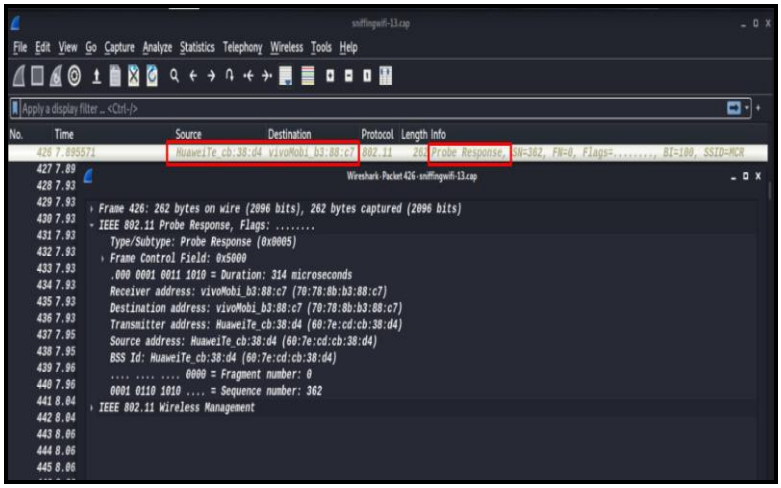
Gambar 7. *Beacon frame*

1. *Client* mengirimkan permintaan untuk menemukan jaringan yang ada disekitar.



Gambar 8. *probe Request*

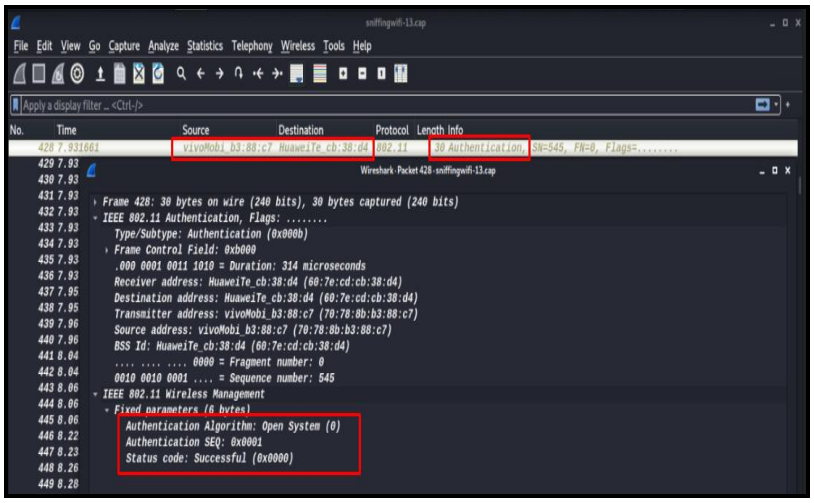
2. Akses point menerima *probe response* dari *client* dan Akses point menerima permintaan pemeriksaan untuk melihat apakah stasiun memiliki kecepatan data umum yang dapat didukung. Jika mereka memiliki kecepatan data yang kompatibel, maka *probe response* dikirim untuk mengiklankan SSID (nama jaringan *nirkabel*), kecepatan data yang didukung, jenis enkripsi jika diperlukan, dan kemampuan data lainnya dari AP.



Gambar 9 *Probe response*

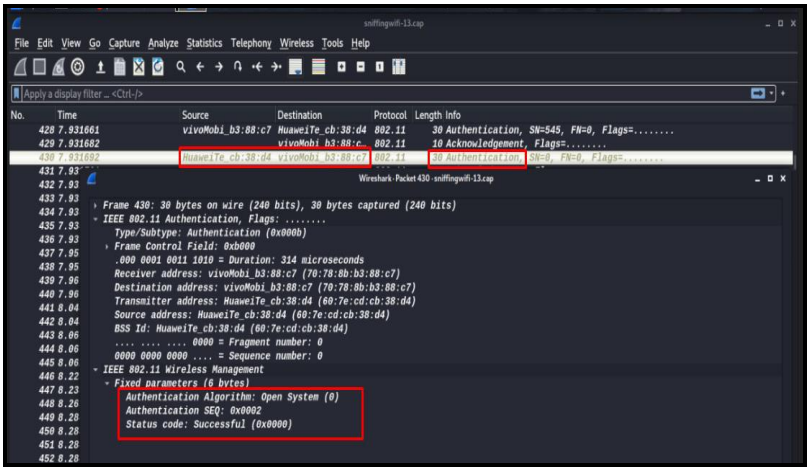
3. *Client* melakukan *authentication* ke akses point dengan mengirimkan otentikasi 802.11 tingkat rendah ke akses point yang mengatur otentikasi untuk dibuka dan urutan ke 0x0001

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)



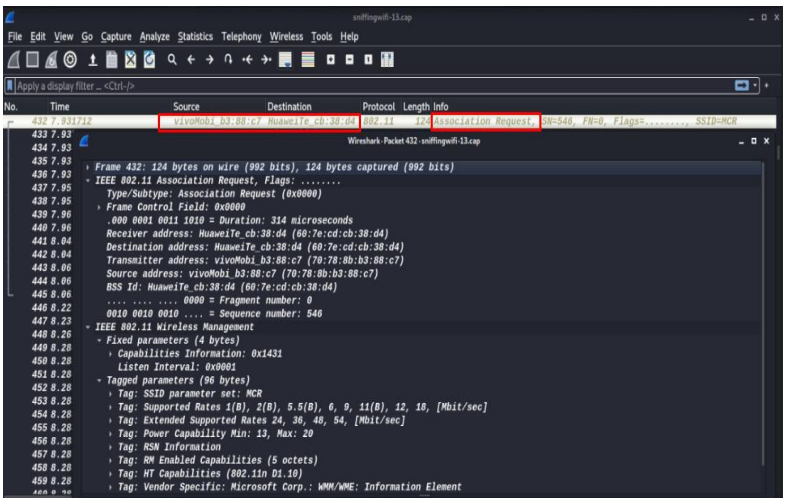
Gambar 10. *Authentication*

4. Akses point menerima *authentication* dan merespon ke *client* dengan *authentication* yang menunjukkan urutan 0x0002. Jika AP menerima *authentication* selain permintaan dari *client*, maka ia akan mengerimkan pesan pemutusan (*Deauthentication*).



Gambar 11. *Authentication*

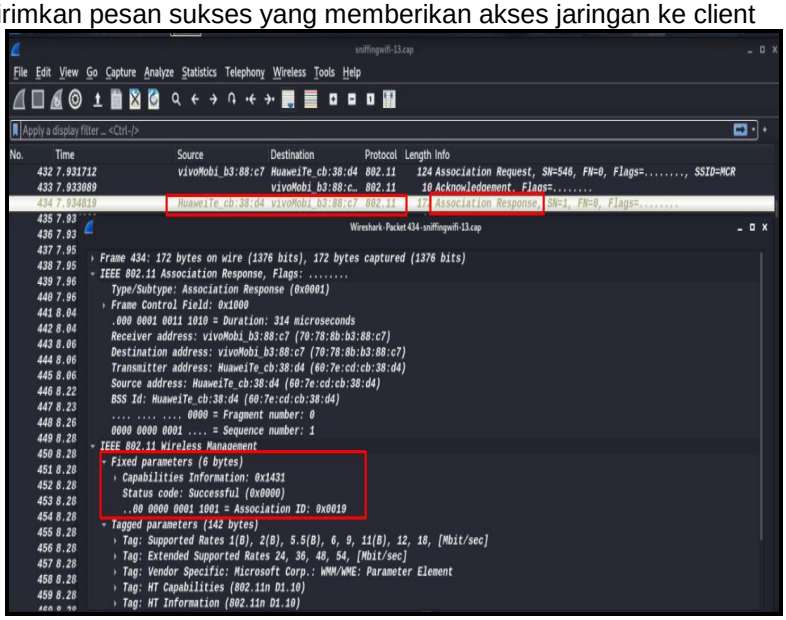
5. Setelah *authentication* selesai, maka selanjutnya client menentukan AP mana yang ingin di *Association,* ia akan mengirimkan permintaan *Association request* ke AP. Permintaan *Association* berisi jenis enskripsi yang dipilih jika diperlukan dan kemampuan 802.11 lainnya.



Gambar 12. *Association request*

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

6. Akses point membalas dengan *association respon* ke client. Jika elemen dalam permintaan *Association* cocok dengan kemampuan AP, maka AP akan membuat ID untuk *client* dengan mengirimkan pesan sukses yang memberikan akses jaringan ke client

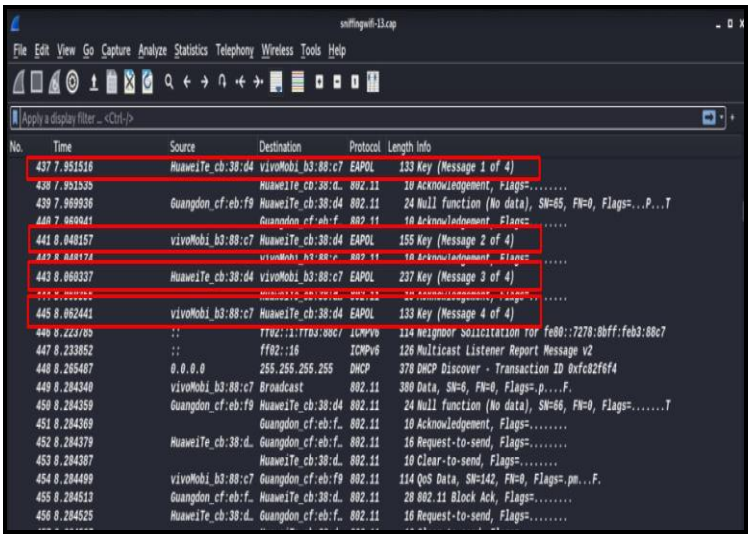


Gambar 13. *Association respond*

7. Setelah client berhasil bergabung ke *Akses point*, tahap selanjutnya adalah pembentukan kunci atau bisa disebut dengan *four way handshake*. Dalam pembentukan kunci terdapat 4 Message (pesan) yaitu:

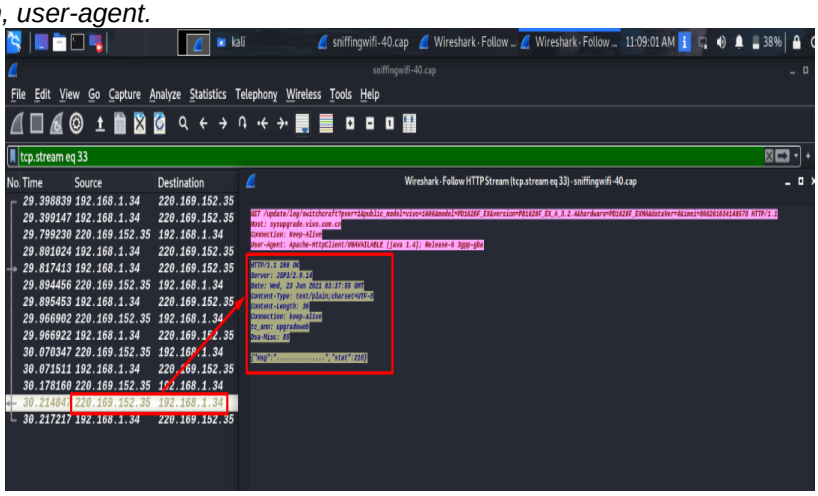
   1) **Message 1** : titik akses mengirim pesan EAPOL dengan Anonce (nomor acak) ke perangkat untuk menghasilkan PTK. Jangan lupa clien harus tahu MAC Ap karena terhubung ke mac. Ini memiliki PMK, Snonce dan alamat MAC sendiri. Setelah menerima Anonce dari titik akses, ia memiliki semua input untuk membuat PTK.
      PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))
      Alamat Mac 5E:66:6C:CF:EB:F9 adalah alamat sumber atau alamat mac titik akses yang mengirim pesan EAPOL pertama ke perangkat dan 70:78:8B:B3:88:C7 adalah perangkat Mac client.
   2) **Message 2** : Setelah perangkat membuat PTK, ia mengirimkan SNonce yang dibutuhkan oleh titik akses untuk menghasilkan PTK. Perangkat mengirim EAPOL ke AP dengan MIC (pemeriksaan integritas pesan) untuk memastikan kapan titik akses dapat memverifikasi apakah pesan ini rusak atau dimodifikasi. Setelah SNonce diterima oleh AP itu dapat menghasilkan PTK juga untuk enkripsi lalu lintas unicast.
   3) **Message 3** : Pesan EAPOL ketiga dikirim dari AP ke perangkat client yang berisi GTK. AP membuat GTK tanpa keterlibatan klien dari GMK.
   4) **Message 4** : Pesan EAPOL keempat dan terakhir akan dikirim dari client ke AP hanya untuk mengonfirmasi bahwa Kunci telah diinstal.

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)



Gambar 14. Pembentukan kunci

8. Sekarang client berhasil terhubung ke AP dan transfer data dapat dimulai. Selanjutnya melakukan *capture* pada protocol HTTP, setelah itu lakukan analisis paket yang berisi POST. Pada data POST ada beberapa informasi seperti alamat IP 220.169.152.35 *source* dan 192.168.1.34 *destination,* serta HTTP yang berisi *Host, Connection, connect-length, origin, user-agent.*



Gambar 15 Paket http dan *password*

Solusi untuk mencegah serangan *Packet Sniffing*

1. Bedakan antara jaringan wifi kantor dengan jaringan wifi untuk fasilitas umum, agar ketika seorang *hacker* menyerang menggunakan teknik *Packet Sniffing* tidak dapat menembus jaringan wifi kantor.
2. Harus menggunakan sertifikat SSL (*secure socket layer*) pada *website*. Karena dengan menggunakan sertifikat SSL informasi akan terjaga selama proses pengiriman melalui internet dengan cara dienskripsi, sehingga hanya penerima pesan yang dapat memahami hasil dari enskripsi tersebut.

KESIMPULAN DAN SARAN

Kesimpulan

1. Aplikasi airodump-ng mendeteksi wifi yang ada di sekitar.
2. Penyerangan packet sniffing yang dapat merekam dan menampilkan username dan password dengan menggunakan aplikasi wireshark.
3. Penyerangan packet sniffing hanya dapat di lakukan pada http sedangkan untuk yang sudah menggunakan https tidak dapat di lakukan, karena https sudah menggunakan secure socket layer (SSL).

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

Saran

Kelebihan dan kekurangan di atas dapat dijadikan pelajaran serta referensi kedepannya. Saran yang dapat dipertimbangkan untuk ke depannya diperlukan pembagian jaringan untuk membedakan jaringan untuk umum dan jaringan untuk karyawan agar tidak terjadi serangan yang dilakukan melalui jaringan wifi umum oleh pihak yang tidak bertanggung jawab untuk mendapatkan informasi penting yang dapat merugikan instansi.

DAFTAR PUSTAKA

Juliharta, I Gede P. K. 2014. Bussiness Impact Analysis Aplikasi Jaringan Komputer Dengan Teknik Packet Sniffing. Jurnal Sistem Dan informatika: Vol 110 No. 1 November 2015-151.

Santoso dan Radna Nurmalina. 2017. Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut). Jurnal Integrasi: Vol. 9 No. 1. Hal 86.

Widodo, Charles, dkk. 2018. Implementasi Topologi Hybrid Untuk Pengoptimalan Aplikasi Edms Pada Project Office Pt Phe Onwj. Jurnal Teknik Informatika: Vol 11 No.1.Hal 21

Wardoyo, Siswo, dkk. 2014. Analisis Performa File Transport Protocol Pada Perbandingan Metode Ipv4 Murni, Ipv6 Murni Dan Tunneling 6to4 Berbasis Router Mikrotik. Jurnal Nasional Teknik Elektro: Vol: 3 No. 2 September 2014: 107.

Yuliandoko, Herman. 2018. Jaringan Komputer Wire dan Wireless berserta penerapannya. Jakarta: Deepublish

Zam, Efvy. 2016. Wireless Hacking. Jakarta. PT Elex Media Komputindo