# EVALUASI TINGKAT KEAMANAN JARINGAN KOMPUTER NIRKABEL PADA KEJAKSAAN TINGGI SUMATERA SELATAN

**Asmania, Tamzir Ariyadi[2]**
Fakultas Ilmu Komputer, Universitas Bina Darma
Email: asmania161997@gmail.com [1)], tamsirariyadi@binadarma.ac.id [2]

**ABSTRAK**

Pada era industri 4.0, teknologi informasi sangat dibutuhkan karena sebagai sarana penunjang dalam melakukan kontrol terhadap mesin – mesin yang sedang bekerja.Teknologi informasi sangat berkaitan dengan jaringan komputer Semakin meningkatnya jaringan komputer maka semakin tinggi juga tingkat kejahatan terhadap jaringan komputer.Walaupun alat yang digunakan sebagai jaringan mempunyai harga yang relatif mahal tidak menjamin keamanan dari serangan *cyber* ini. Tetapi, harus juga didukung dari pengguna yang menggunakan alat tersebut seperti sering melakukan monitoring, selalu melakukan *update software* dan memberi *password* yang sulit diretas.Pada penelitian ini penulis akan melakukan pengujian terhadap jaringan wireless yang ada di Kejaksaan Tinggi Sumatera Selatan. Kejaksaan Tinggi Sumatera Selatan memiliki file file dokumen yang bersifat *privacy* yang harus dilindungi. Karena jika jaringan yang ada mudah untuk diretas maka akan mendapatkan berbagai masalah seperti file tersebut terenkripsi dan hilang, jaringan lalu lintas data terganggu dan membuat sarana dan prasarana menjadi rusak.

**Keywords:** *Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel Pada Kejaksaan Tinggi Sumatera Selatan*

## 1. PENDAHULUAN

Seiring perkembangan teknologi hingga zaman sekarang, jaringan komputer terus mengalami perkembangan secara terus menerus baik melalu kabel maupun nirkabel. Namun, WPA2-PSK memiliki kemampuan yang sangat tinggi tapi masih ada celah untuk menerobos keamanan tersebut.Celah tersebut biasanya pada client itu sendiri. Client yang tidak menggunakan password yang lebih dari 6 digit akan mudah bagi *hacker* untuk mengeskploitasi jaringan nirkabel tersebut. Dengan menggunakan *tools* yang tersedia pada kali linux *hacker* akan melakukan teknik *brute-force* dengan berusaha menebak password tersebut dengan kata-kata yang ada pada *wordlist* yang dia miliki. Untuk itu penulis melakukan penelitian pada Kejaksaan Tinggi Semuatera Selatan.Kejaksaan tinggi sumatera selatan merupakan objek vital yang harus dilindungi karena terdapat banyak data yang sangat penting baik untuk masyarakat maupun negara.Dalam melakukan pengujian penulis mengambil judul yaitu Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel Pada Kejaksaan Tinggi Sumatera Selatan.

Jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain(a *network is a interconnection of a set of devices capable of* communication). Jaringan computer himpunaan interkoneksi sejumlah komputer *autonomous* yang berarti bahwa komputer tersebut memiliki kendali atas dirinya sendiri dan bukan merupakan bagian komputer lain (Sofana, 2011). Jaringan nirkabel merupakan jaringan komputer yang tidak mengunakan kabel jaringan (UTP, Coaxial, maupun fiber optic), namun memanfaatkan sinyal elektromagnrtis.(Pratama, 2015).

Keamanan jaringan adalah aktifitas yang dilakukan untuk mengamankan jaringan khususnya untuk melindungi usability, reliability, integrity, dan safety dari jaringan dan data. Target keamanan jaringan adalah bagaimana mencegah dan menghentikan berbagai potensi serangan agar tidak memasuki dan menyebar pada jaringan tersebut (Primartha, 2018). Seperti

definisi yang pertama dikembangkan oleh: Ralph Tyler beliau mengatakan, bahwa evaluasi merupakan proses pengumpulan data untuk menentukan sejauh mana, dalam hal apa, dan bagian mana tujuan penelitian sudah tercapai. Jika belum, bagaimana yang belum ada dan apa sebabnya(Abdul Jabar,2007:1). Berikut ini merupakan jenis serangan yang sering terjadi pada jaringan wireless :

1) *MAC Address Spoofing*. Metode penyerangan ini dilakukan dengan cara memalsukan / menggunakan *MAC Address* dari sebuah komputer yang memiliki hak untuk mengakses suatu jaringan nirkabel.
2) *WEP Attack.* Saat ini, serangan ini merupakan metode yang cukup populer digunakan dibanyak *hotspot*. Sebabnya boleh jadi karena metode pengamanan WEP kini sudah menjadi pengamanan default dalam setiap access point yang ada dipasaran
3) *Man in the middle attack.* Metode penyerangan ini memang tidak mudah. Penyerang dengan keahliannya akan mencegat data yang lewat dari dua titik (misalnya dari *access point* ke client atau sebaliknya), lalu "meracuni" salah satunya.
4) *Rouge Access Point.* Pada metode ini, penyusup membuat sebuah access point palsu. Tujuannya adalah agar user akan tertipu sehingga akan mengakses access point palsu ini.
5) *DoS Attack/Brute Force Attack.* Serangan ini bertujuan untuk melumpuhkan layanan akses yang disediakan access point.

Pengujian keamanan dalam jaringan nirkabel yaitu menggunakan metode *brute-force attack.*Aplikasi yang digunakan yaitu *Aircrack-ng*.
Alur penyerangan menggunakan *Aircrack-ng*yaitu :

1) Pemantauan : Packet capture dan ekspor data ke file teks untuk diproses lebih lanjut oleh aplikasi pihak ketiga.
2) Menyerang : Serangan ulang, deauthentication, membuat akses point palsu dan melalui via injeksi paket.
3) Pengujian : Memeriksa kartu WiFi dan kemampuan driver (capture and injection).
4) Cracking : Cracking pada WEP dan WPA PSK (WPA 1 dan 2).

MikroTik RouterOS merupakan sistem operasi yang diperuntukkan sebagai network router. MikroTik routerOS sendiri adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan *wireless*(Ino Irvanto 2014:1).

## 2. METODOLOGI PENELITIAN

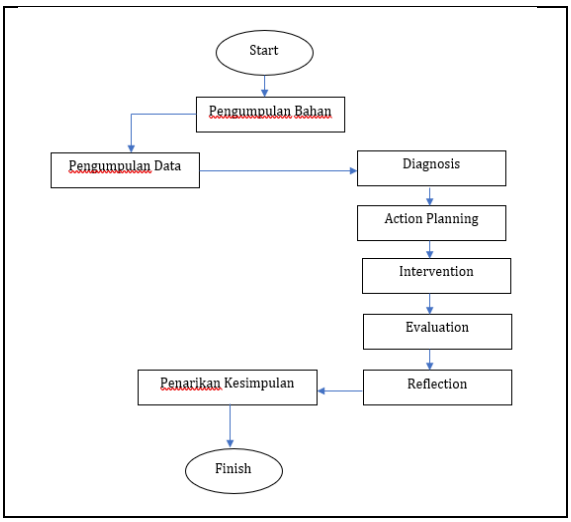
### 2.1 *Alat dan Bahan*

Alat dan bahan yang digunakan adalah :

1) Perangkat Keras berupa Laptop HP 14 cm0068AU,Processor AMD-9,Memori 4 GB dan Wireless Network Card Realtek 802.11 b/g/n.
2) Sistem Operasi berupa Sistem Operasi Kali Linux dan Sistem Operasi Windows 7.
3) Perangkat Lunak berupa *Virtual box* untuk menjalankan Kali Linux, Airmon-ng untuk mengaktifkan mode monitor pada perangkat wireless, airdump-ng untuk memantau semua kegiatan Access Point, airodump-ng –write untuk meng-Capture paket ke dalam sebuah file dan aircrack-ng untuk meretas password Wifi menggunakan file hasil capture.

### 2.2 *Alur Penelitian*

Untuk mempermudah dalam penyusunan alur penelitian maka akan disajikan dalam bentuk *flowchart*, sehingga penelitian akan menjadi lebih terstruktur.




**Gambar 1.** *Flowchat* Pengujian

### 2.3. *Pengumpulan Informasi*

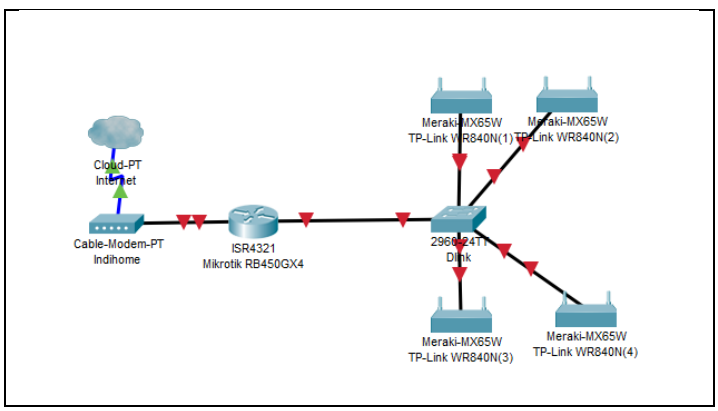
Pengumpulan informasi dilakukan dengan cara :

1) **Wawancara.** Penguji akan melakukan tanya jawab atau wawancara kepada pihak pengelola atau *staff* IT yang bertanggung jawab terhdapa jaringan yang ada di Kejaksaan Tinggi Sumatera Selatan untuk medapatkan informasi lebih lanjut terkait masalah yang ada
2) **Studi Kepustakaan.** Untuk mengetahui secara detail peneliti akan mengambil informasi dari beberapa buku, jurnal dan internet untuk menyelesaikan dan mengevaluasi masalah tersebut.

## 3. HASIL DAN PEMBAHASAN

### 3.1. *Topologi Jaringan Nirkabel Kejaksaan Tinggi Sumatera Selatan*

Berikut ini merupakan topologi jaringan yang ada pada Kejaksaan Negeri Sumatera Selatan, dapat dilihat dari gambar dibawah ini :




**Gambar 2.** Topologi Jaringan Kejaksaan Tinggi Sumatera Selatan

### 3.2. *Access Point Kejaksaan Tinggi Sumatera Selatan*

Adapun jumlah dan tipe access point yang dipasang pada setiap lantai sebagai berikut :

**Tabel 1.** Jumlah dan Merek Acces Point di Setiap Lantai

| Lantai | Jumlah Acces Point (Unit) | Merek |
|---|---|---|
| 1 | 2 | TENDA AC6 |
| 2 | 2 | TENDA AC6 |
| 3 | 2 | TENDA AC6 |
| 4 | 2 | TENDA AC6 |
| 5 | 2 | TENDA AC6 |
| 6 | 2 | TENDA AC6 |

### 3.3. *Jenis Enkripsi Password Jaringan*

Jaringan Nirkabel di kantor kejaksaan tinggi sumatera selatan memiliki jenis password yang digunakan berbeda yaitu WPA-PSK atau WPA2-PSK yang dipadu dengan autentikasi hostpot di route atau mikrotik untuk mengatur jalan lewat hotspot. Adapun jenis enskripsi password yang digunakan WPA-PSK atau WPA2-PSK**.** WPA atau *wifi protected access* merupakan teknologi kemanan wifi sebagai pengganti dari WEP yang memiliki kekurangan .Ada dua jenis WPA yaitu WPA personal (WPA-PSK), dan WPA-Radius.Pada jaringan nirkabel kejaksaan tinggi sumatera selatan menggunakan access point yang diberikan *security* berupa WPA-PSK.

### 3.4. *Analisis Kerentanan (Vulnerability Analysis)*

Sistem *wireless* atau nirkabel memiliki permasalahan kerentanan secara khusus yang berhubungan dengan perangkat atau jalur data . Beberapa hal yang mempengaruhi aspek keamanan dari sistem *wireless* antara lain: (Supriyanto 2006)

a. Perangkat pengakses informasi yang menggunakan sistem wireless.
b. Penyadapan pada jalur komunikasi data (*man-inthe-middle attack*).
c. Perangkat *wireless* yang kecil membatasi kemampuan perangkat dari sisi CPU, RAM, kecepatan komunikasi, satu daya.
d. Pengguna tidak dapat membuat sistem pengaman sendiri.
e. Adanya batasan jangkauan radio dan interferensi menyebabkan ketersediaan servis menjadi terbatas.

**Tabel 2.** Data *Access Point* Target

| SSID | Channel | Encryption | Authentication | ESSID |
|---|---|---|---|---|
| D8:07:B6:77:83:CO | 2 | WPA2 | Personal | KT-SUMSEL |

### 3.5. *Model Ancaman (ThreatModelling)*

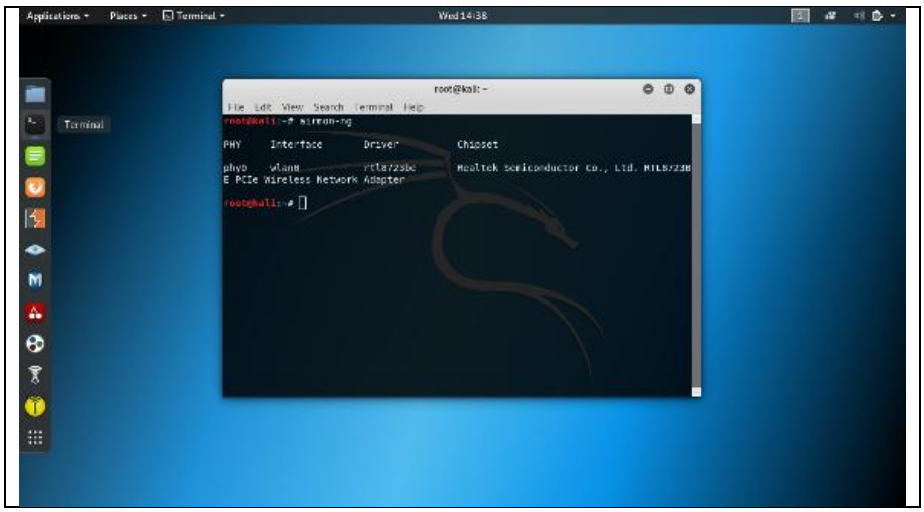
Adapun ancaman yang akan dilakukan antara lain :

1) **Meretas Enkripsi.** Dimana tujuan dari serangan ini untuk mengetahui apakah semua *Access Point* dilindungi dengan sistem keamanan enkripsii secara WEP, WPA, ataupun WPA2.
2) **Menyerang Infrastruktur.** Tahap ini dilakukan serangan pada layanan *wireless* untuk *client* sehingga dapat mempengaruhi kinerja jaringan.
3) **Meretas Password.** Pada tahap ini pennguji melakukan serangan dengan menggunakan *tools aircrack-ng* yang bertujuan untuk mengetahui *password* dari *user*.

### 3.6. *Pengujian*

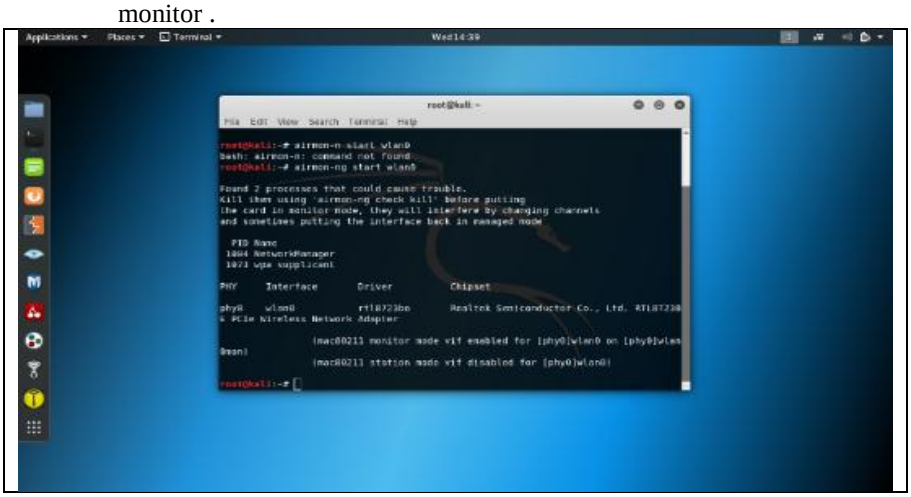
Adapun beberapa tahapan pengujian sebagai berikut :

1) **Tahapan- Tahapan Instalasi dan Konfigurasi Software.**
   Untuk menjalankan Kali Linux harus menginstal terlebih dahulu *virtual box* agar bisa berjalan secara bersamaan di windows.
2) **Tahapan Pengujian Dengan Bruce – Attack**
   Pengujian dilakukan dengan 3 tahapan , yaitu :
   a. Peretasan Enkripsi atau *Cracking The Encryption* bertujuan dari serangan ini adalah untuk mengetahui access point tersebut menggunakan *system security* jenis WPA,WPA/PSK, atau WEP.
      a) Buka terlebih dahulu terminal
      b) Lalu ketik airmon-ng untuk melihat devices wifi yang ada di notebook.



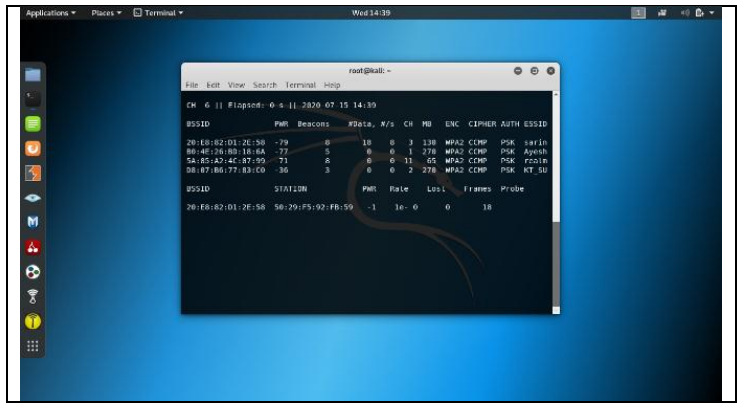

**Gambar 3.** Daftar Driver Wifi

c) Ketikkan airmon- ng start wlan0 untuk mengaktifkan wifi *card* sebagai mode monitor .



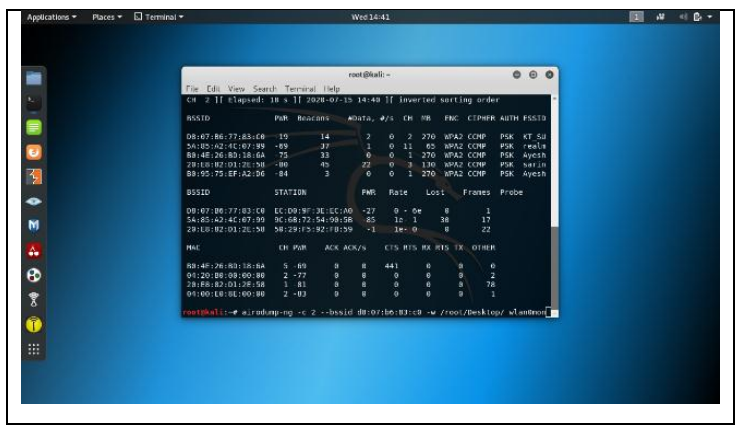

**Gambar 4.** Mengaktifkan Driver Wlan0mon

d) Setelah mengaktifkan mode monitor, selanjutnya akan melakukan *capture wireless packet* .



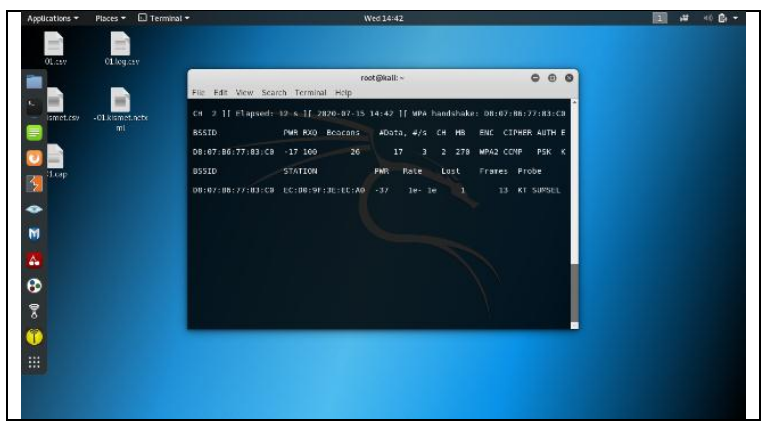
**Gambar 5.** Mengaktikan AiroDump-ng wlan0mon

e) Kemudian ketikkan "airodump-ng -2 –bssid d8:07:b6:83:c8 -w /root/Desktop/ wlan0mon".



**Gambar 6.** Monitoring Airodump-ng terhadap 1 SSID

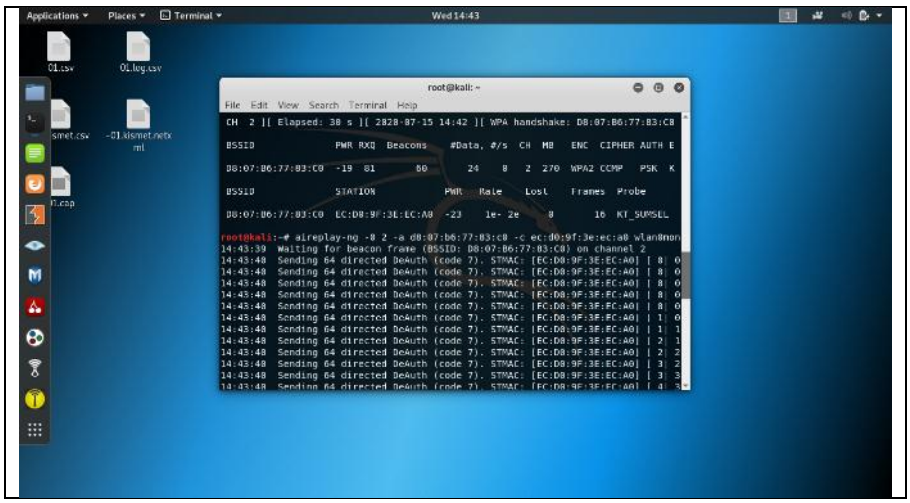
b. *Attacking The Infrastructure*,



**Gambar 7.** Hasil WPA handshake wifi KT-SUMSEL

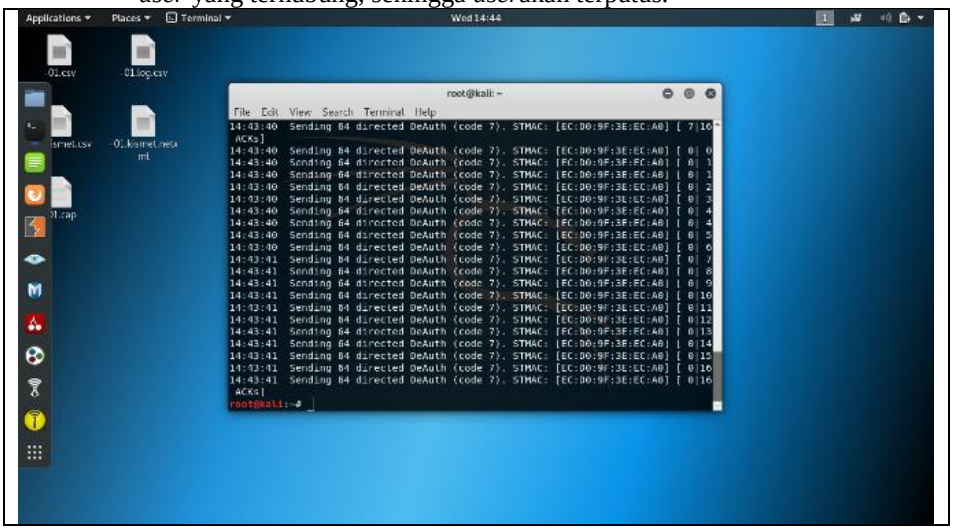
Untuk mendapatkan handshake maka penulis akan memutuskan *client* yang terhubung dalam *access point* .. Langkahnya sebagai berikut ini :

a. Ketikkan perintah untuk memutuskan jaringan client sehingga akan melakukan autentikasi Kembali dan mendapatkan password enkripsi "aireplay-ng -0 2 -a d8:07:b6:77:83:c0 -c ec:d8:9f:3e:ec:a0 wlan0mon".

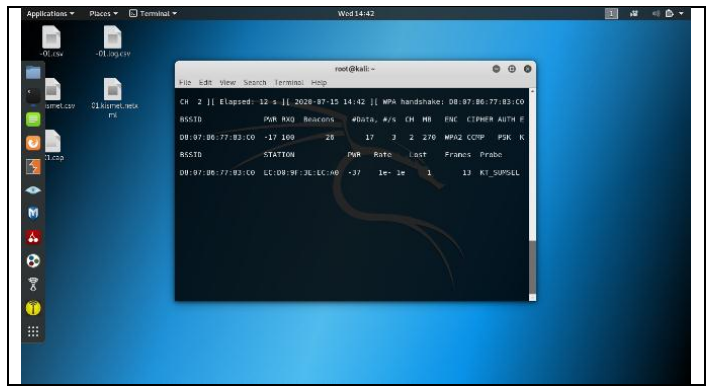



**Gambar 8.** Proses *Deauthenticate Wireless Client*

b. Pada gambar terlihat bahwa penulis mengirim data paket *deauthentication* ke *user* yang terhubung, sehingga *user*akan terputus.



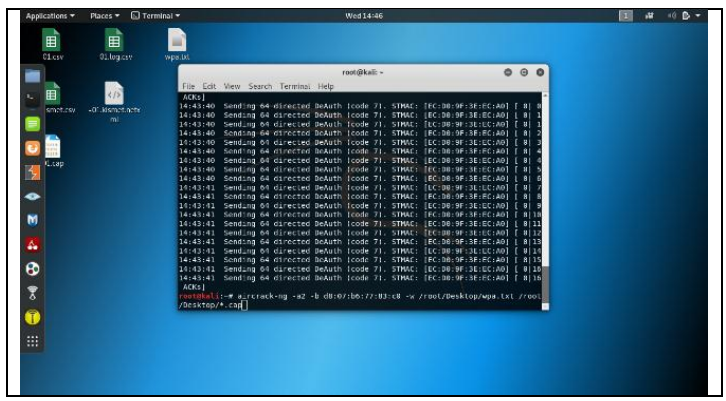

**Gambar 9.** Melakukan Airreplay-ng untuk Mendapatkan *Handshake*



**Gambar 10.** *Handshake* yang Telah Diperoleh Dari Channel Target

c. *Cracking Password* tahap ini penulis melakukan serangan dengan menggunakan *tools* aircrack-ng yang bertujuan untuk mengetahui *password* dari *user*.

Masukkan file wordlist yaitu WPA.txt di folder /root/Desktop/ kemudian ketikkan aircrack-ng -a2 -b d8:07:b6:77:83:c0 -w /root/Desktop/wpa.txt /root/Desktop/*.cap

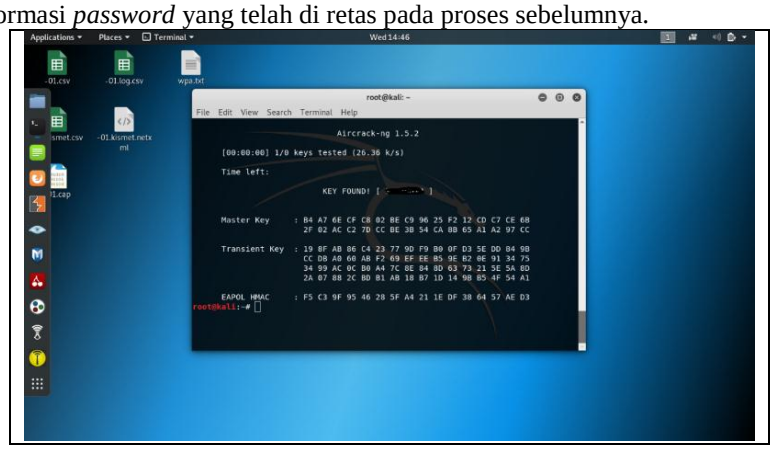


**Gambar 11.** Proses Cracking Password

Menjalankan aircrack-ng untuk memecahkan WPA PSK key.

### 3.7. *Laporan (Reporting)*

Hasil dari *cracking password* berupa *Command Prompt* yang ada di terminal yang berisikan informasi *password* yang telah di retas pada proses sebelumnya.



**Gambar 12.** Tampilan Password yang Ditemukan

### 3.8. *Mengevaluasi keamanan jaringan dari pengujian*

Setelah melakukan pengujian dalam jaringan *wireless* di Kejaksaan Tinggi Sumatera Selatan. Maka peneliti akan melakukan Evaluasi terhadap jaringan yang telah ada.

1) Untuk mengatasi serangan terhadap *brute-force attack* maka peneliti melakukan koordinasi terhadap staff yang terkait untuk merubah password dengan menambahkan beberapa karakter agar peretas kesulitan dalam melakukan serangan.
2) Mengatasi MAC Spoofing peneliti melakukan block terhadap mac – address yang tidak dikenali dan IP address yang tidak terdaftar pada jaringan Wireless Kejaksaan Tinggi Sumatera Selatan.
3) Mengatasi Man In The Middle Attack peneliti dan staff yang bertanggung jawab di bidang IT melakukan pemindahan beberapa access point di tempat yang tidak diketahui dan sulit dijangkau sehingga tidak memungkin orang lain untuk bisa mengeskploitasi alat tersebut dan menyusupkan *skrip* di dalamnya.

### 3.9. *Hasil Pengujian*

Untuk melakukan pengamanan agar jaringan nirkabel sulit ditembus dan tahan akan serangan *brute-force attack*. Jaringan nirkabel harus memiliki karakteristik sebagai berikut :

1) Gunakan kata sandidengan kombinasi huruf, angka, simbol, huruf kecil, dan huruf besar.
2) Isi kata sandi dengan Panjang karakter lebih dari 12 karakter.
3) Gunakan tipe pengaman seperti WPA, WPA-PSK, dan WPA2-PSK

Untuk melakukan *cracking* terhadap sistem keamanan ini membutuhkan *wordlist* atau *dictionary* yang banyak karena WPA/WPA2 bisa menggunakan karakter lebih dari 8 digit dan semua karakter bisa digunakan baik berupa simbol, angka, maupun huruf. Pada table dibawah menunjukkan bahwa serangan menggunkan teknik brute force :

**Tabel 3**. Hasil cracking password

| No. | Jenis Ancaman | WPA2-Personal (Bruto Force) |
|---|---|---|
| 1 | Perentasan Enkripsi | Berhasil |
| 2 | Melumpuhkan Pengguna | Berhasil |
| 3 | Perentasan PAssword | Berhasil |

Mengetahui daerah terjauh untuk tingkat keberhasilan melakukan pengujian ini.

**Tabel 4.** Hasil cracking password dengan jarak

| Jarak | Waktu Cracking | Status Serangan |
|---|---|---|
| 10 Meter | 1 Jam | Berhasil |
| 15 Meter | 2 Jam 10 menit | Berhasil |
| 30 Meter | 3 Jam | Gagal |
| 45 Meter | 4 Jam | Gagal |
| 60 Meter | 5 Jam | Gagal |

Semakin pendek jarak dalam melakukan cracking maka akan mempercepat pengiriman data sehingga tingkat keberhasilan meningkat dan semain jauh jarak maka akan memperlambat pengiriman data sehingga tingkat keberhasilan rendah.

WPA-PSK merupakan jenis keamanan tertinggi dalam keamanan jaringan nirkabel dikarenakan menggunakan kombinasi berupa huruf, simbol, dan angka. Selain itu, sistem ini menggunakan 8 digit sampai 64 digit karakter sehingga membutuhkan waktu yang lama untuk melakukan *cracking* dan *wordlist* yang sangat banyak. Untuk melakukan teknik ini hal yang

pertama yang harus dilakukan yaitu harus melakukan *scanning* terhdapa jaringan wireless sehingga bisa mendapatkan informasi berupa *ESSID,Channel,* dan jenis enkripsi yang digunakan. Untuk mendapatkan informasi tersebut digunakan *tools* airodump-ng. lalu kemudian handshake dengan menggunakan *toolsaireplay-ng* sehingga client akan terputus koneksi terhadap jaringan dan akan menghubungkan kembali. Pada tahap ini aireplay akan mencoba melakukan *brute-force* sampai menemukan *password encryptions* pada router dan menyimpannya.

Setelah mendapatkan *password encryptions,* dilanjutkan dengan melakukan cracking terhadap *password encryptions* tersebut dengan *tools* aircrack-ng untuk mengetahui password yang sebenarnya. Aircrack-ng akan mencari dalam sebuah wordlist atau kamus jika telah ditemukan makan aircrack-ng akan menampilkannya di terminal dengan keterangan" *Key Found* = ***** ".
ang dilakukan penulis adalah melakukan scanning pada jaringan wireless target dengan menggunakan *tools* airodump-ng yang tujuannya adalah untuk melihat client yang terhubung pada jaringan tersebut, setelah informasi didapat maka selanjutnya penulis memutuskan koneksi client dari jaringan dengan cara membuat jaringan sibuk dengan menggunakan aireplay-ng, fungsinya ialah untuk mendapatkan handshake dari client. Apabila proses tersebut berhasil, handshake akan langsung terdeteksi. Untuk proses selanjutnya adapun ancaman yang telah dilakukan antara lain :

Keberhasilan dalam pengujian dengan teknik *brute-force attack* ini disebabkan karena password dari wifi KT-SUMSEL dikarenakan terdapat didalam *wordlist* yang digunakan oleh penulis dalam melakukan proses pengujian. Keberhasilan juga ditunjang dari segi jarak karena semakin jauh jarak melakukan pengujian maka tingkat keberhasilan semakin rendah dikarenakan sinyal wifi terlalu lemah sehingga pengiriman data terhambat.

## 4. KESIMPULAN

Kesimpulan yang didapatkan dari hasil penelitian ini adalah :

1) Melakukan Pengujian menggunakan *brute force attack* dengan*handshake router* dengan *tools* aircrack-ng untuk mengetahui kelemahan dan celah keamanan pada jaringan nirkabell kejaksaan tinggi sumatera selatan.
2) jaringan nirkabel pada kejaksaan tinggi sumatera selatan dapat ditembus dengan *tools* aircrack-ng yang menandakan bahwa penguji mendapatkan *password* wifi tersebut.
3) Semakin jauh penguji melakukan *pentesting* terhadap wifi tersebut maka peluang keberhasilan semakin jauh dikarenakan pengiriman data yang terlalu jauh dan akibat gangguan sinyal lemah.

Saran yang didapatkan adalah :

1) Menggunakan sistem keamanan enckripsi yaitu WPA2-PSK,dikarenaka sistem keamanan ini bisa memasukkan karakter lebih dari 8 sampai 64 digit.
2) Gunakan *password* dengan Panjang karakter lebih dari 20 karakter dikarenakan tidak ada dalam dictionary atau wordlist. Jikalaupun ada maka membutuhkan waktu yang sangat lama untuk mendapatkan kata yang sama.
3) Gunakan *password* dengan melakukan kombinasi sepeti huruf, angka, simbol, huruf besar dan huruf kecil. Sebab WPA2-PSK mendukung semua jenis karakter tersebut.
4) Pengguna diharapkan untuk tidak membagikan *password* dengan sembarangan.
5) Selalu melakukan pentesting setiap akhir minggu untuk memastikan bahwa sistem keamanan jaringan aman dari berbagai ancaman.

## DAFTAR PUSTAKA

Irvanto, Ino.(2014).*Konfigurasi Routerboard Mikrotik RB-750*.Andi Offset

Madya, S, (2006) *Teori dan Praktik Penelitian Tindakan (Action Research)*, Alfabeta: Bandung.

Official kali linux documentation.(2013).*ebook kali linux 200 attack bahasa indonesia.*

Primartha, rifkie. (2018). *Security Jaringan Komputer Berbasis.CEH*.Informatika

Pratama, P. A. E. (2015). *HANDBOOK JARINGAN KOMPUTER*. Informatika Bandung.

Sofana, I. (2011). *Teori & Modul Praktikum Jaringan Komputer*. Modula.

Sofana, I. (2019). *Network Security dan Cyber Security*. Informatika Bandung.

Sofana, I. (2015). *Membangun Jaringan Komputer* . Informatika.