PENGUJIAN KEAMANAAN JARINGAN NIRKABEL(WPA2-PSK)DENGAN METODE PENETRATION TESTING(Sudi Kasus: Access Point Tp-Link WA701ND, Tenda F3 dan Hotspot Smartphone Realmi 5i)

Sulpan[1], Wahyat[2]
Politeknik Negeri Bengkalis
sulpanuciha@mail.com[1],wahyat@polbeng.ac.id[2]

Abstract

Wireless network is a technology used to receive or transmit on a local network without using cables or via radio waves. The weakness of wireless networks is that people around can carry out hacking attacks, the wireless network security that will be tested is wpa2-psk, which looks for security holes in wpa2-psk. Tools available on Kali Linux, such as airmon-ng, airdump-ng, aireplay-ng, aircrack-ng and wifite/wifite kill, this test is carried out on smartphone access points and hotspots, the type of access point is tp-link wa701nd, Tenda f3 and hotspot realmi 5i. The method used in this test is penetration testing. The results of this study can be used and applied to the types of smartphone access points and hotspots that have been carried out in this test. And increase access point security from unwanted attacks.

Keywords — Wireless Networks, Network Security, Penetration Tests, Wireless LAN, Kali Linux

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer memudahkan orang untuk memenuhi kebutuhan informasi. Salah satu teknologi yang berkembang pesat adalah teknologi media transmisi nirkabel atau *wireless.* Media transmisi yang digunakan *wireless* adalah gelombang radio yang dipancarkan kesemua area yang bisa dijangkau oleh gelombang radio tersebut.(sabdho & ulfa, 2018).Para *hacker* sering melakukan aksi untuk menguji kemampuan yang telah di pelajari sebelumnya. Kemudian terhubung dalam satu jaringan yang sama dan mengambil data pengguna lainnya secara ilegal.(Pratama & Syamsuar, 2021) Pada saat para *hacker* melancarkan aksinya ditempat umum seperti kafe, *public hostpot* dan restoran. Karena sebagian pengguna tidak peduli dengan keamanan komunikasi data di tempat publik, maka tempat *hacker* untuk melakukan uji coba ilegal melalui jaringan *wireless* yang terhubung ke *hacker.* Jika dibandingkan dengan jaringan kabel. Jaringan *wireless* lebih rentan dan mudah masuk kedalam jaringan *wireless* yang tersedia. Cukup mendapatkan *password wifi* sudah bisa terhubung ke jaringan yang dituju oleh *hacker*(Haeruddin & Kurniadi, 2021). Menguji keamanan wpa2-psk dari serangan *hacker* yang ingin mendapatkan *password* tanpa teridentifikasi oleh sistem perangkat access point dan hotspot samrtphone.Tahap pengujian akan di lakukan pada *access point* Tp-link WA701ND, Tenda F3 dan *Hotspot Smartphone* Realmi5i.Tahap pengujian diawali dengan melakukan *Network mapping* yaitu mengumpulkan data-data yang diperlukan sebelum melakukan *penetration testing* pada jaringan nirkabel pada 3 perangkat tersebut, serta mengidentifikasi sistem keamanan yanga ada pada perangkat *acces point* dan *hotspot smartpone*. Penggunaan *tools* akan dilakukan saat proses pengujian ini sehingga mempermudah dalam pengujian. Sistem operasi yang digunakan dalam pengujian ini yaitu sistem operasi *kali linux*. Pengujian ini bertujuan untuk meningkatkan keamanan pada *access point* dan *hotspot smartphone.*

2. TINJAUAN PUSTAKA

a. Penelitian yang berjudul "Analisis Keamanan Jaringan WLAN Dengan Metode *Penetration Testing*" (Bayu dkk, 2017) menggunakan metode *penetration testing* sebagai bentuk simulasi serangan yang akan terjadi atau mencari celah keamanan di jaringan *wireless.* Singkatnya, tujuan pengujian penetrasi hanya untuk melindungi organisasi

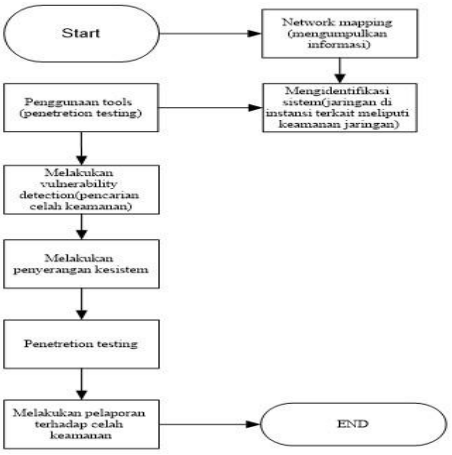
b. Penelitan yang berjudul "Analisis Sistem Keamanan Jaringan *Wireless (*WEP,WPA-PSK/WPA2-PSK*) MAC Address*, Menggunakan Metode *Penetration Testing*" (Sari dkk 2017) menjelaskan bahwa sebuah jaringan bisa dikatakan aman harus memenuhi enam persyaratan, yaitu kerahasiaan yang hanya bisa diakses oleh pihak yang berwenang dan cegah pihak yang tidak berwenang membaca informasi rahasia dan harus aman. Lalu integritas yang pastikan data yang diterima tetap tidak berubah selama transmisi.

c. Penelitiannya yang berjudul "*Penetration Testing* Pada Jaringan *Wifi* Menggunakan *Kali Linux*" (Rusdi & Prasti, 2019) menjelaskan bahwa dikarenakan kemudahan untuk instalasi jaringan nirkabel, sangat rentan terhadap gangguan keamanan eksternal. Enkripsi ganda ini telah diterapkan untuk melindungi kemanan jaringan *wireless* ini. Namun, Enksripsi ini mudah dipecahkan oleh *hacker*. Oleh karena itu perlu ditingkatkan keamanan jaringan di perusahaan tersebut.

3. METODE PENELITIAN

Data yang di butuhkan dalam pengujian keamanan jaringan nirkabel wpa2-psk. Pada penelitian oleh(Haeruddin & Arif Kurniadi 2021) Penelitian ini menggunakan metode Penetration Testing untuk menganalisis sistem keamanan jaringan WLAN ditempat umum, hotspot, dan kafe. Tujuannya untuk mensimulasikan bentuk serangan jaringan menggunakan tools yang tersedia di kali linux. Hasil dari penelitian ini menunjukan bahwa hanya dua dari tiga serangan yang berhasil. Oleh karena itu, harus meningkatkan keamanan pada simulasi yang berhasil dilaksanakan. Sesuai dengan hasil implementsi pada *access point* Tp-link WA701ND, Tenda F3 dan *Hotspot Smartphone.* Peralatan dan bahan yang digunakan untuk penelitian adalah *Access Point*, Kabel UTP, Laptop, *Processor*, *Ram*, *Kali Linux*, *Airmong- Ng, Airodump-Ng, Aireplay-Ng, Aircrack-Ng* dan *Wifite/Wifite –Kill.* Prosedut penelitian meliputi Identifikasi Masalah, Pengumpulan Data, Analisa, Perancangan, Pembuatan Pengujian Keamanan Jeringan Nirkabel WPA2-PSK dengan Metode *Penetration Testing* menggunkan Sistem Operasi *Kali Linux* dan terakhir Pembuatan Laporan.

3.1 Prosedur Penelitian



Gambar 1. Flowchart Penelitian

Pada penelitian ini sistem pengujian yang diusulkan adalah melakukan tahap awal penelitian, Maka dilakukan *Network Mapping* mengumpulkan semua ketersediaan referensi sebagai literatur seperti jurnal, buku, artikel dengan tujuan sebagai penunjang pelaksaan penelitian. Mengidentifikasi sistem jaringan di instansi terkait meliputi keamanan jaringan. Menggunakan *tools* sebagai percobaan *penetration testing.*Melakukan *Vulnerabality Detection* untuk pencarian celah keamanan. Melakukan penyerangan ke sistem, Jika benar maka percobaan penetrasi berhasil dan apabila gagal maka tahap penetrasi akan di uji kembali.

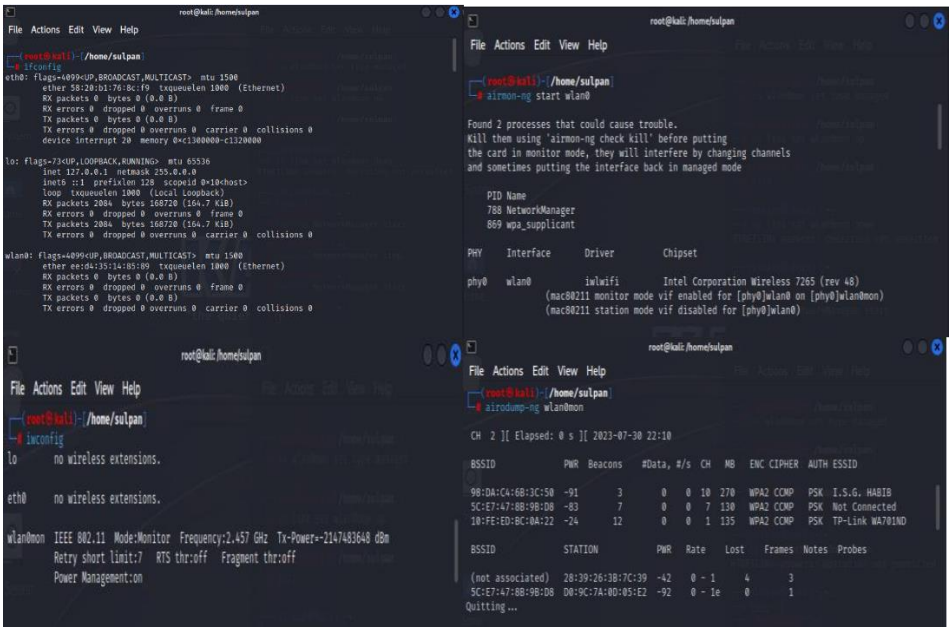
4. HASIL PENELITIAN DAN PEMBAHASAN

Pengujian kali ini ditujukan pada sebuah *Access Point*, yaitu TP-Link WA701ND, Tenda F3 dan *Hotspot Smartphone* Realmi 5i. Pada tahap ini, penulis menggunakan sistem operasi yaitu *kali linux* dan menggunakan *tools airmon-ng, airodump-ng, aireplay-ng, aircrack-ng* dan *wifite/wifite --kill.*

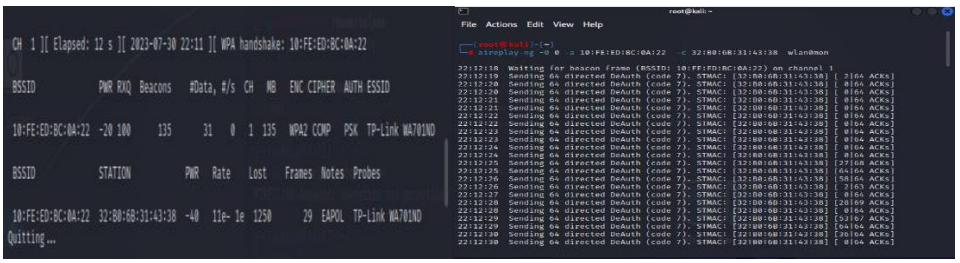
4.1 *Cracking* The *Encryption*

a. Implementasi pada *Access Point* Tp-link WA701ND

Perintah *ifconfig* pada terminal untuk mengecek apalah kartu jaringan terdeteksi di *kali linux*, berpindah ke mode monitor dengan perintah airmon-ng start wlan0. Sehingga kartu jairngan sudah berada pada mode monitor, tahap berikutnya mendeteksi jaringan *wifi* di sekitar dengan perintah *airodump-ng*.



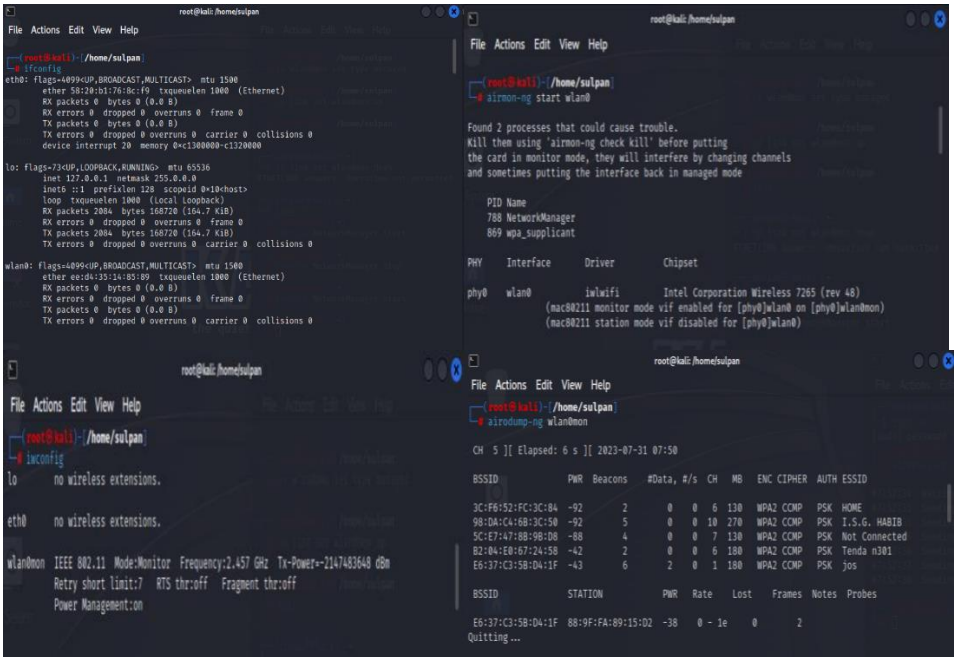
Gambar 2 Tampilan *airmon-ng* dan *airodump-ng*



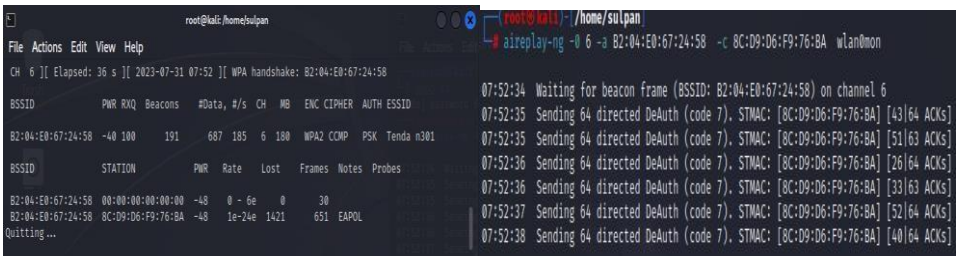
Gambar 3 Tampilan *airodump-ng* dan *aireplay-ng*

b. Implementasi pada *Access Point* Tenda F3

Perintah *ifconfig* pada terminal untuk mengecek apalah kartu jaringan terdeteksi di *kali linux*, berpindah ke mode monitor dengan perintah airmon-ng start wlan0. Sehingga kartu jairngan sudah berada pada mode monitor, tahap berikutnya mendeteksi jaringan *wifi* di sekitar dengan perintah *airodump-ng*.



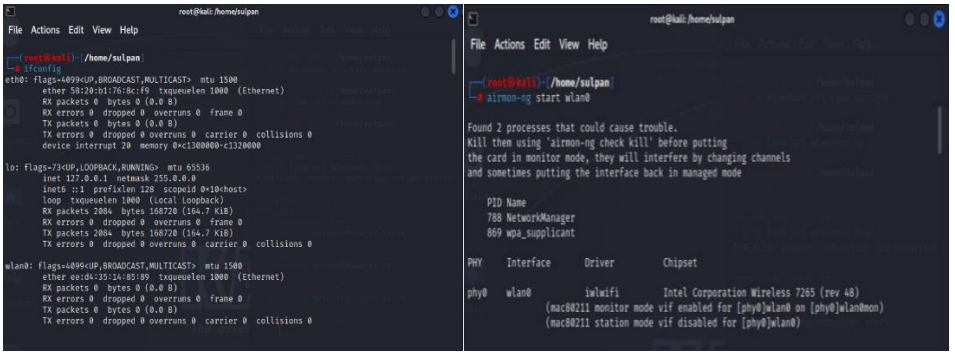
Gambar 4 Tampilan *airmon-ng* dan *airodump-ng*

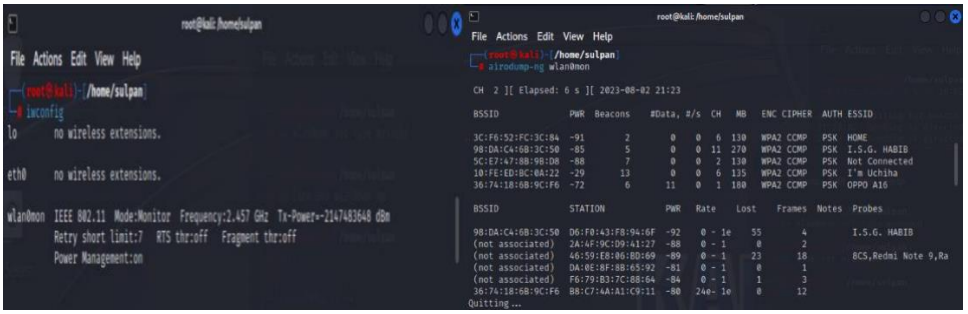


Gambar 5 Tampilan *airodump-ng* dan *aireplay-ng*

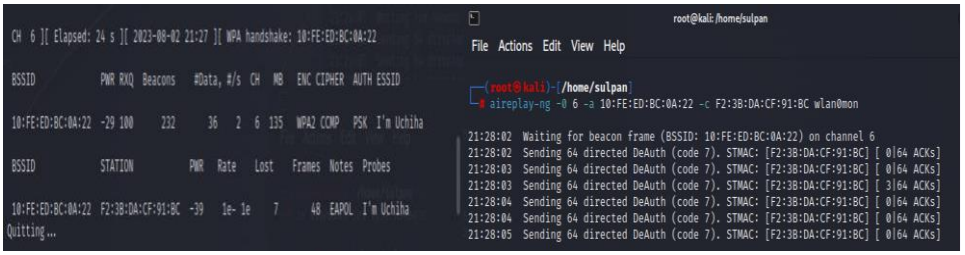
c. Implementasi pada *Hotspot Smartphoe*

Perintah *ifconfig* pada terminal untuk mengecek apalah kartu jaringan terdeteksi di *kali linux*, berpindah ke mode monitor dengan perintah airmon-ng start wlan 0. Sehingga kartu jairngan sudah berada pada mode monitor, tahap berikutnya mendeteksi jaringan *wifi* di sekitar dengan perintah *airodump-ng*.





Gambar 6 Tampilan *airmon-ng* dan *airodump-ng*

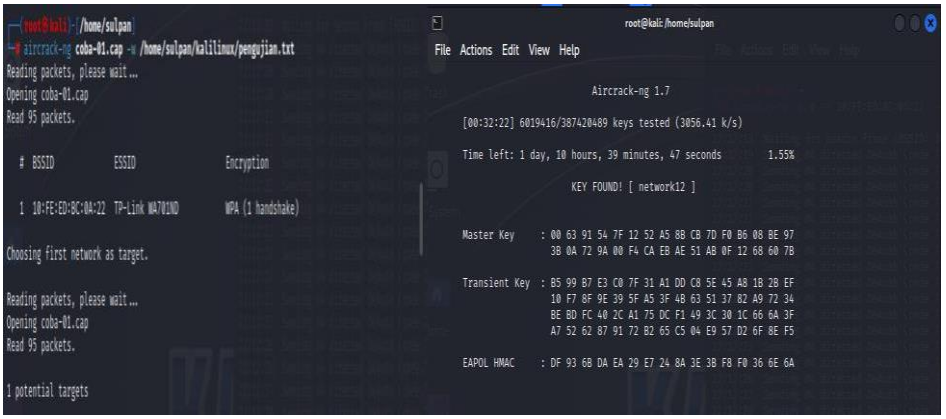


Gambar 7 Tampilan *airodump-ng* dan *aireplay-ng*

4.2 *Attacking* Wpa2 *key*

a. *Attacking* pada *Access Point* Tp-link WA701ND

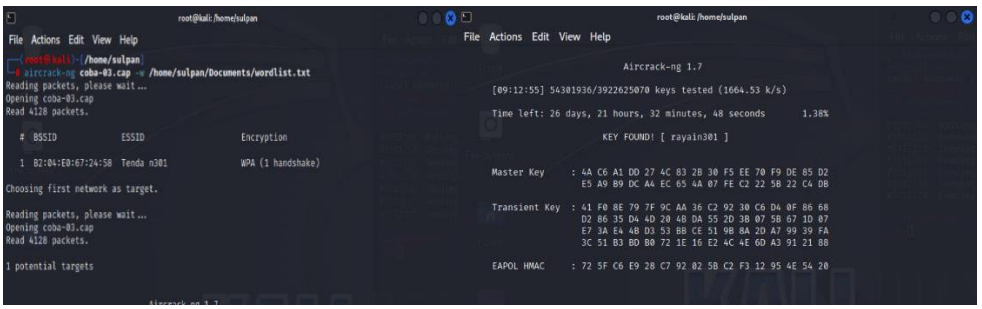
pada tahap kedua, BSSID pada *Access Point* Tp-nlink WA701ND di uji dalam mode CLI menggunakan *tools aircrack-ng.*



Gambar 8 Tampilan *aircrack-ng*

b. *Attacking* pada *Access Point* Tenda F3

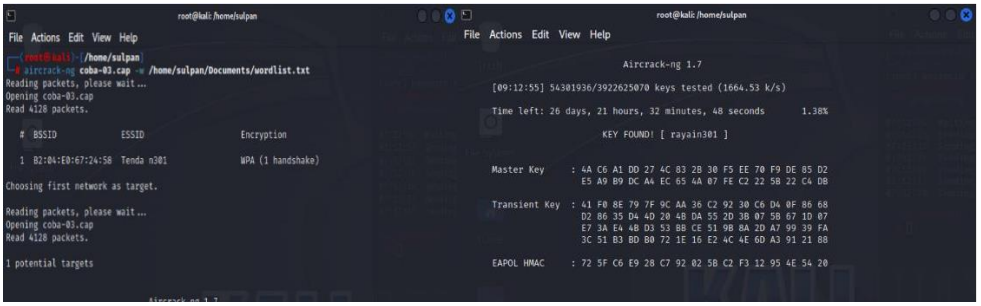
pada tahap kedua, BSSID pada *Access Point* Tenda F3di uji dala mode CLI menggunakan *tools aircrack-ng*.



Gambar 9 Tampilan *aircrack-ng*

c. *Attacking* pada *Hotspot Smartphone*

pada tahap kedua, BSSID pada *Hotpspot Smartphone* di uji dala mode CLI menggunakan *tools aircrack-ng*.

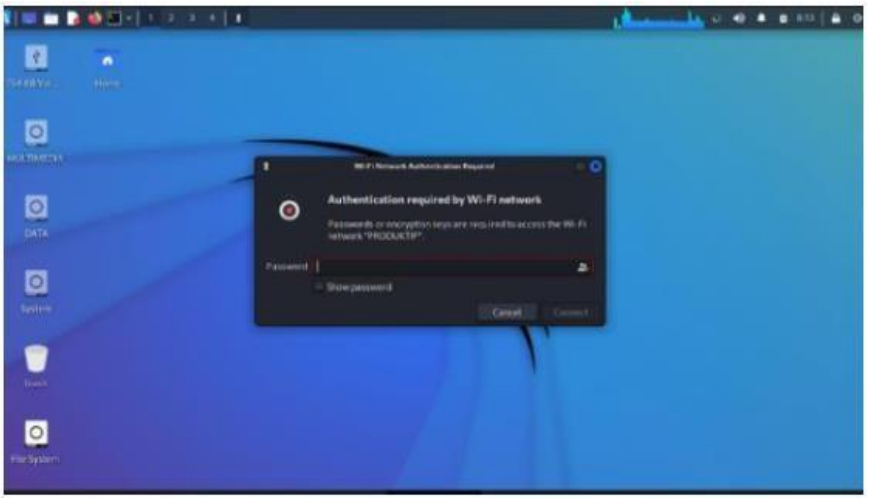


Gambar 10 Tampilan *aircrack-ng*

4.3 *Autentication Wifi Password*

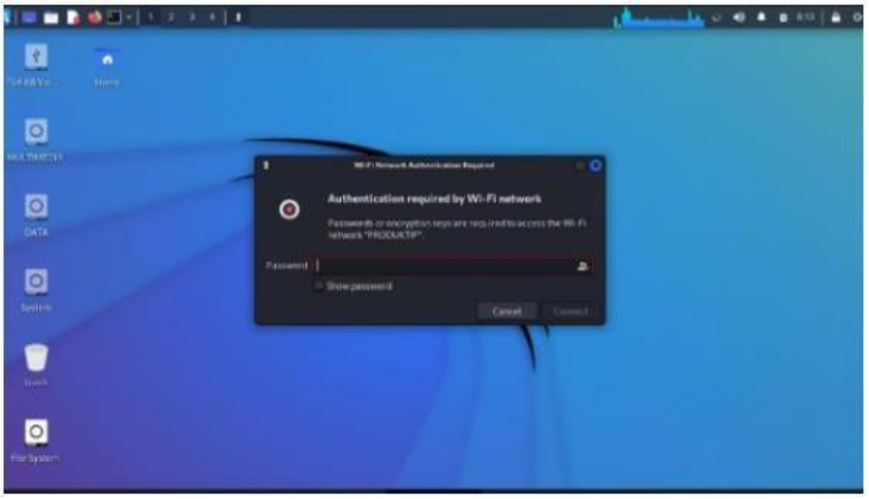
Pada tahap ketiga menguji WPA key yang sudah di dapat dari hasil Cracker BSSID dan Attack BSSID di tampilan gambar.

a. *Authentication* pada *access point* Tp-link WA701ND



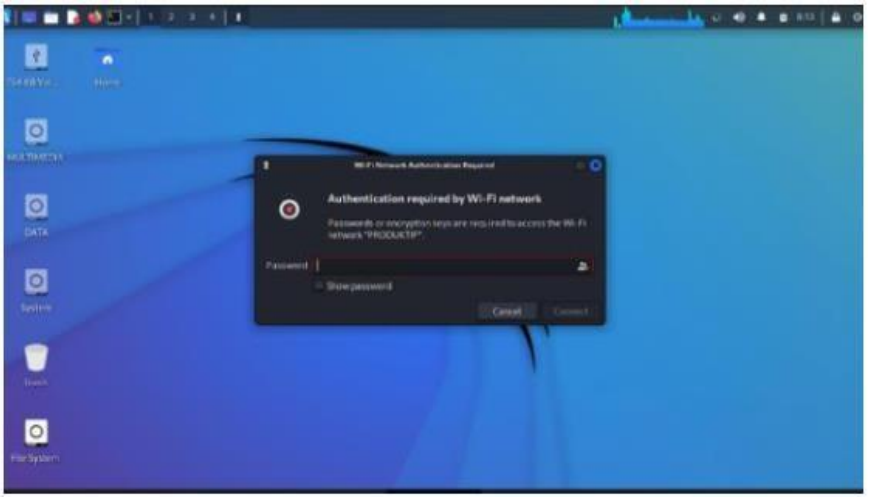
Gambar 11 *Authentication wifi password*

b. *Authentication* pada *Access point* Tenda F3



Gambar 12 *Authentication wifi password*

c. *Authentication* pada *Hotspot Smartphone*



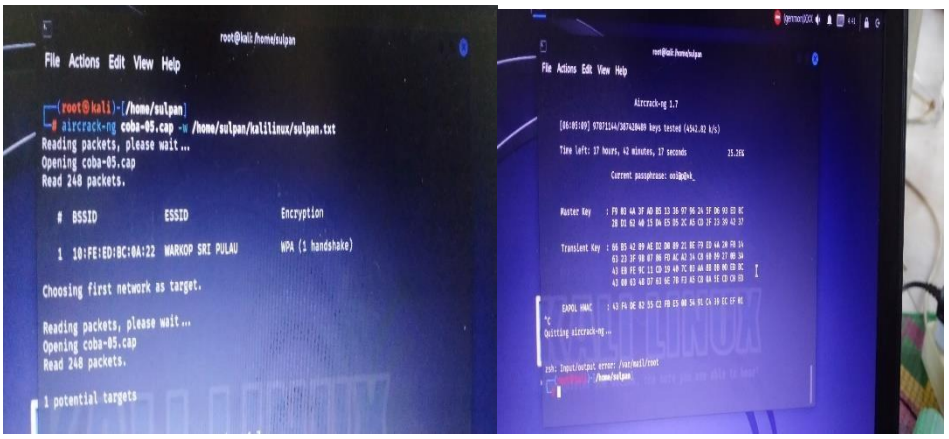
Gambar 13 *Authentication wifi password*

4.4 Peningkatan Keamanan Jaringan Nirkabel Wpa2-Psk

Dalam meningkatkan keamanan jaringan nirkabel wpa2-psk yaitu dengan cara paling efektif adalah menggunakan kombinasi *password* dengan berbagai karakter dengan menggunakan jumlah karakter yang panjang, wpa2-psk bisa 8 sampai dengan 15 karakter, bisa juga mengkombinasikan angka dengan huruf serta bisa mengkombinasikan karakter "@,#,$,%,*" dan jangan menggunakan kombinasi karakter atau kata yang terlalu simple dan baku, misalnya seperti book, rooms, nama orang, makanan dan nama gedung/ruangan.

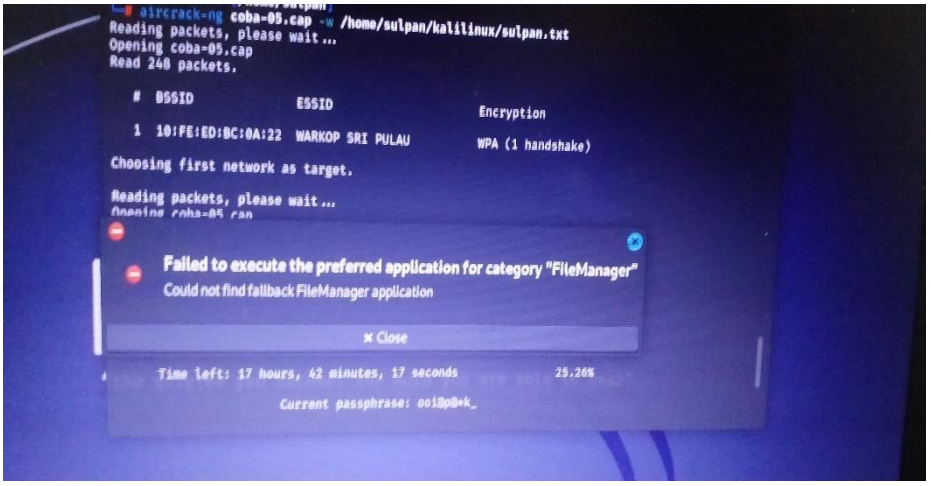
a. Pengujian peningkatan keamanan

1. Mengkombinasikan angka, huruf dan karakter.
   Peningkatan yang dilakukan yaitu mengkombinasikan angka, huruf dan karakter, sehingga penyerangan membutuhkan waktu yang cukup lama, dan setting di access point itu di Wpa2-psk AES.



Gambar 14 Kombinasi *password*

Dan dalam proses mendapatkan *password* kondisi laptop dari pengujian ini suhu meningkat drastis. Sehingga membuat sistem operasi *kali linux* menjadi *error*.



Gambar 15 *Kali linux error*

4.5 Hasil Pengujian

Tabel 1. *Font size* 12pt

Kategori Serangan	Data yang dibutuhkan	Keterangan
Cracking The Encryption	*Wordlist dan password*	Berhasil
Attacking WPA key	*Wordlis dan password*	Berhasil
AuthenticationWifi Password	*Wordlis dan password*	Berhasil

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dari pengujian keamanan jaringan nirkabel(wpa2-psk)dengan metode penetration testing(studi kasus: warkop begawan) dapat di ambil kesimpulan yaitu :

a. Dari hasil implementasi pengujian keamanan wpa2-psk di beberapa merek dan type *access point*. Penyerangan yang di lakukan menggunakan *tools airmon-ng, airodump-ng, aireplay-ng, aircarck-ng dan wifite/wifite --kill*, wpa2-psk bisa diserang. Jika wordlist yang digunakan sesuai dengan karakter password.
b. Waktu yang dibutuhkan untuk mendapatkan password cukup lama karena, penyesuaian jumlah karakter yang di *wordlist* dengan karakter *password* di *access point* yang di serang.
c. Sebelum melakukan serangan pastikan sudah memiliki *wordlis*t, *wordlist* yang sempurna itu terdiri dari minimal 8 karakter dan maksimal 12 karakter dimana berisikan abjad a-z dan angka 0-9 serta simbol. Namun berpengaruh pada penyimpanan yang sangat besar. Bisa mempenaruhi penyimpanan sebesar 5-10 TB.

5.2 Saran

Adapun saran dari peneliti bahwasanya dalam meningkatkan keamanan pada jaringan nirkabel yang spesifikasi keamanannya masih Wpa2-psk adalah sebagai berikut:

a. Sebaiknya mengkombinasikan password dengan huruf, angka dan simbol dan buatlah karakternya sebanyak 12 karakter sehingga si penyerang membutuhkan waktu yang lama untuk mendapatkan *password wifi* tersebut.
b. Sebaiknya menggunakan *access point* yang sudah memiliki sistem keamanaan Wpa3, dimana Wpa3 memperpanjang enkripsi hingga 192 bit untuk meningkatkan kekuatan kata sandi, ini melindungi terhadap kata sandi yang lemah yang dapat di-*crack***.** dengan mudah melalui tebakan.

6. DAFTAR PUSTAKA

Alghifari, Q. (2021). Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing Di Pt . Indonesia Power Pltu Jabar 2 Palabuhanratu Omu.

Astri Saraun, Arie S.M. Lumenta, D. F. S. (2021). An Analysis of WLAN Security at the Minahasa Regency Office of Educational Affairs. *Jurnal* Teknik Informatika Unsrat, *17*(1), 19–26.

Haeruddin, H., & Kurniadi, A. (2021). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6). *CoMBInES-Conference on Management …*, *1*(1), 508–515. https://journal.uib.ac.id/index.php/combines/article/view/4475

Jordi Prayoga (2021) Memahami WPA2-PSK dalam keamanan Wifi https://gudangssl.id/blog/wpa2-psk-adalah/

Kholiq, A., & Khoirunnisa, D. (2019). Analisis Keamanan Wireless Local Area Network (WLAN) dengan Metode Penetration Testing Execution Standard (PTES) (Studi Kasus: PT. Win Prima Logistik). *Jurnal Ilmiah Fakultas Teknik LIMIT'S*, *1*(1), 46–55. https://teknik.usni.ac.id/jurnal/ABDUL KHOLIQ.pdf

Maulana, S. F., & Suhendi, H. (2021). Pengujian Celah Keamanan Jaringan Komputer Pt. Jiona Sejati Dengan Network Penetration Testing. *PROTEKTIF (EProsiding Teknik 2*(1), 44–50. http://eprosiding.ars.ac.id/index.php/pti/article/view/310

Mulyanto, Y., & Algi Fari, A. (2022). ANALISIS KEAMANAN LOGIN ROUTER MIKROTIK DARI SERANGAN BRUTEFORCE MENGGUNAKAN METODE PENETRATION TESTING (Studi Kasus: SMK NEGERI 2 SUMBAWA). *Jurnal Informatika, Teknologi Dan Sains*, *4*(3), 145–155.

https://doi.org/10.51401/jinteks.v4i3.1897

Santoso, N. A., Ainurohman, M., & Kurniawan, R. D. (2022). Penerapan Metode Penetrasion Testing Pada Keamanan Jaringan Nirkabel. *Jurnal Responsif : Riset Sains Dan Informatika*, *4*(2), 162–167. https://doi.org/10.51977/jti.v4i2.831

Sari, D. M., Yamin, M., & Aksara, L. B. (2017). Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration testing. *SemanTIK*, *3*(2), 203–208. https://doi.org/10.1016/j.neuropharm.2007.08.010