ANALISIS SISTEM KEAMANAN *WIRELESS LOCAL AREA NETWORK* (WLAN) PADA PROSES *TETHERING*

M. R. Kurniawan*, Linna Oktaviana Sari**
*Teknik Elektro Universitas Riau **Jurusan Teknik Elektro Universitas Riau
Kampus Binawidya Km 12,5 Simpang Baru Panam, Pekanbaru, Riau
Jurusan Teknik Elektro Universitas Riau
Email: mr.kurniawan@student.unri.ac.id

.

ABSTRACT

Various types of technology facilities currently continue to develop in various ways, network security needs to be considered as the technology facilities develop. Tethering is a technology facility that is widely used today, such as in office areas, homes, boarding houses and campuses. In analyzing network security when using tethering as a media connection to the internet, testing and analysis are carried out when the test results are obtained. The testing techniques used are sniffing and scanning using inSSIDer home software, kismet, and aircrack-ng and airodump-ng tools. The results obtained from this test are that the inSSIDer and kismet software get open or encrypted security, then aircrak and airodump-ng can find the password used by Access Point (AP) tethering. From the tests carried out it can be concluded that the security of WLAN networks when using tethering is still categorized as not safe.

Keyword: *Wireless Local Area Network* (WLAN**)**, *tethering, aircrack-ng, airodump-ng,* inSSIDer, kismet.

PENDAHULUAN

Teknologi informasi berubah dan berkembang sangat pesat dan secara umum sudah banyak digunakan pada zaman modern saat ini, peranan teknologi didalam kehidupan tidak dapat dihindari terutama dalam dunia kerja, bisnis, serta pendidikan. Salah satu fasilitas teknologi saat ini memanfaatkan sebuah *smartphone* menjadi sebuah *Access Point* (AP) agar dapat terhubung ke internet, dengan memanfaatkan sebuah teknik *sharing* koneksi yaitu *tethering* dalam sebuah jaringan *wireless local area network* (wlan) dan mejadikan udara sebagai media penyaluran informasi pada jaringan tersebut.

Teknologi *tethering* ini memanfaatkan gelombang radio untuk mentransmisikan data dengan frekuensi 2,4 GHz. Secara umum WLAN seperti *tethering* ini telah banyak digunakan dari pada koneksi menggunakan kabel (LAN), padahal dari segi keamanan komunikasi data pada jaringan tersebut rentan terhadap aktivitas ilegal seperti *sniffing* dan *scanning* serta kejahatan lainnya.

Beberapa jenis keamanan pada jaringan *wireless* antara lain WEP(*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*), WPA2(*Wi-Fi Protected Access II*). Pada jaringan *tethering* sering terjadi kegagalan koneksi atau pemberian hak akses dari *client* ke *access point*, bagaimanapun masing-masing jenis keamanan pada WLAN ada kelebihan dan kelemahannya, setiap keamanan mempunyai sistem autentikasi dan tipe enkripsi yang berbeda agar setiap *user* bisa dilindungi datanya serta dapat diberikan hak akses yang semestinya.

Berdasarkan hal tersebut, pada penelitian ini akan dilakukan pengujian serta analisa untuk melihat tingkat keamanan jaringan *wireless local area network* (wlan) saat menggunakan *tethering*. Penelitian ini menggunakan 2 buah laptop. Yang mana digunakan sebagai *attacker* dan *client* serta *smartphone* sebagai *Access Point* (AP) untuk media koneksi ke internet.

TINJAUAN PUSTAKA

Jaringan komputer merupakan sebuah hubungan antara dua atau lebih komputer yang menjadikan kabel maupun nirkabel (*wireless*) sebagai media transmisinya.

Secara umum jaringan komputer terbagi menjadi empat bagian berdasarkan jangkauannya, yaitu:

a. WPAN: hanya menjangkau jarak yang sangat dekat seperti dalam ruangan dengan jarak sekitar 30 *feet*.
b. WLAN: hanya menjangkau jarak seperti antar gedung/perkantoran.
c. WMAN: menjangkau area dalam suatu kota.

d. WWAN: menjangkau area yang sangat luas, seperti koneksi antar negara atau benua, dan menggunakan media *wireless* atau kabel *fiber optic*.

1. Keamanan Jaringan

Keamanan jaringan sangat diperlukan dalam sebuah sistem jaringan, baik skala kecil maupun skala besar, komputer yang terhubung ke internet beresiko besar mendapatkan ancaman dari jaringan luar yang tidak dikenali.

Prinsip keamanan jaringan sering disebut dengan segitiga CIA (*Confidentiality, Integrity, Availability*) (Mydza, 2011):

a. *Confidentiality* (Kerahasiaan): menjaga infrastruktur jaringan agar tidak dapat diakses oleh pihak yang tidak berhak untuk mengaksesnya.
b. *Integrity* (Integritas): menjaga data agar tetap asli dan tidak dimodifikasi selama perjalanan dari sumber ke tujuan (penerima).
c. *Availability* (Ketersediaan): *user* yang mempunyai hak akses (*authorized user*) diberi akses tepat waktu dan tidak terkendala apapun.

2. Perbandingan Model Infrastruktur

Router	***Tethering Android***
- Bisa terhubung dengan 2 (dua) buah atau lebih *router*. - Bisa membentuk jaringan LAN. - Bisa menghubungkan banyak *client*.	- Hanya menggunakan 1 (satu) buah *Access Point* (AP) yaitu *smartphone android*. - Tidak dapat membentuk jaringan LAN. - *Client* yang dapat terhubung terbatas, maksimal 5 *client*.

Tabel diatas menunjukkan perbedaan model jaringan WLAN infrastruktur antara menggunakan perangkat *tethering* dengan jaringan yang menggunakan .*router*.

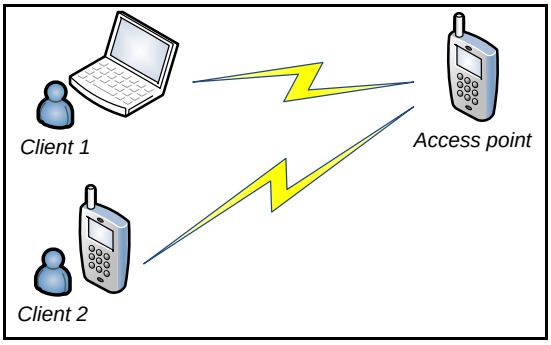
3. Keamanan Jaringan *Wireless*

Keamanan jaringan yang ada pada *wireless* antara lain:

a. *Service Set Identifier* (SSID)
Merupakan keamanan rendah yang ada pada pada suatu sistem jaringan, SSID ini berbentuk nama suatu jaringan.
b. MAC *Filtering*
MAC *filtering* memfilter jaringan diatas standar 802.11b untuk mengamankan jaringan dan berbentuk bilangan *hexadecimal* 12 digit.
c. Wi-Fi *Protected Access* (WPA dan WPA2)
WPA merupakan sebuah sistem keamanan jaringan yang ada pada jaringan *wireless*, WPA berbentuk *key* yang dienkripsi yang di-*set* terlebih dahulu oleh admin.

4. *Hotspot Tethering*

Tethering merupakan sebuah cara yang bisa *sharing* koneksi internet dari sebuah perangkat *mobile* ke perangkat lain yang membutuhkan koneksi internet.



Gambar 1. Koneksi *Hotspot Tethering*

5. Jenis – Jenis Ancaman Pada Jaringan

a. *Bruce Force and Dictionary attack*
Serangan jenis ini menggunakan berbagai kombinasi angka, huruf maupun simbol untuk menemukan *password* dari *account user*.
b. *Denial of Service* (DoS)
Cara ini merupakan ancaman keamanan jaringan dengan membuat trafik layanan jaringan menjadi macet dan *down*.
c. ARP *Spoofing*
Cara ini menggunakan data IP dan *node source* yang diubah dari data asli ke data yang

lain, sehingga penyerang mendapatkan data dari *source* sebelum sampai ke *destination*.

d. *Sniffer*

Tipe ini menggunakan sebuah program penangkap paket yang bisa menduplikasi isi paket yang lewat.

e. *Spamming*

Serangan ini berbentuk iklan atau trojan.

f. *Scanning*

Scanning terbagi dua, antara lain:

- *Port Scanning* : bertujuan menemukan *port-port* yang terbuka pada sistem jaringan.
- *Network Scanning* : bertujuan menemukan *host* yang aktif pada suatu jaringan.

6. Monitoring Jaringan

Perkembangan jaringan komputer yang semakin pesat memberikan tantangan tersendiri bagi para administrator jaringan dalam menganalisis keamanan jaringannya secara tepat. Monitoring jaringan adalah suatu fungsi pengumpulan informasi dari manajemen jaringan. Tujuan dari monitoring jaringan adalah pengumpulan informasi yang berguna dari berbagai macam bagian dari jaringan sehingga jaringan tersebut dapat dikelola dan dikontrol dengan menggunakan informasi yang telah dikumpulkan tersebut (Ernawati, 2012).

7. Keamanan Jaringan.

Keamanan jaringan adalah suatu cara untuk mencegah penyerang yang tidak mempunyai hak akses dan pakai terhadap sistem komputer dan jaringan. Keamanan ini bertujuan agar pemilik sistem informasi dapat menjaga sistem informasinya tidak disusupi oleh orang lain yang akan masuk ke sistem(Ernawati, 2012).

Pengguna ponsel akhir-akhir ini lebih banyak terhubung ke *hotspot* dari pada modem biasa. Persentase akses ponsel pintar ke *hotspot* setinggi 90% dari koneksi telepon. Seperti yang telah disebutkan sebelumnya, jenis resiko dan ancaman meningkat seiring dengan meningkatnya penggunaan mekanisme *Ad hoc* (Khoula, 2016).

8. Ancaman serangan pada *hotspot smartphone*.

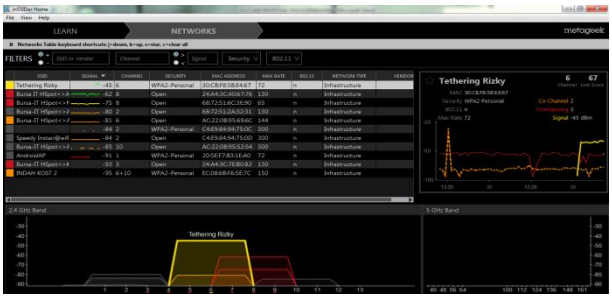
Scanning yaitu kegiatan yang dilakukan *hacker* untuk menentukan aktif atau tidaknya *host* target dalam jaringan. Hasil *scanning* dapat berupa IP *address*, sistem operasi, *service* maupun aplikasi yang dijalankan serta informasi mengenai *host* target, sedangkan *sniffing* yaitu penyusupan dengan cara memonitoring dan menganalisis jaringan komputer yang berjalan dengan sebuah *software.*

9. Pengertian *Tethering*

Tethering merupakan suatu cara yang dapat dilakukan oleh setiap orang yang memiliki sebuah perangkat *mobile* seperti *smartphone* untuk membagi atau men-*share* koneksi internet dari perangkat *mobile* tersebut ke perangkat lain yang membutuhkan koneksi internet.

10. *Software* inSSIDer *Home*

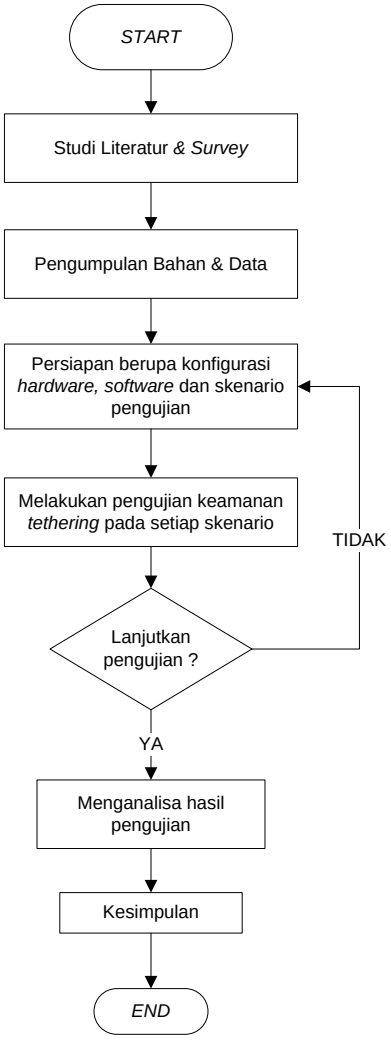
Software inSSIDer *Home* adalah *software* yang dapat digunakan untuk melakukan pemindaian/*scan* dan meng-*caputure* jaringan dengan parameter utama SSID dalam jangkauan antena Wi-Fi Komputer/Laptop, melacak kekuatan sinyal dari waktu ke waktu, dan menampilkan tipe keamanan pada suatu jaringan dan aplikasi ini akan memindai seluruh perangkat yang ada dalam jaringan. Gambar 2 dibawah ini merupakan tampilan dari *software* inSSIDer *Home*.



Gambar 2. Tampilan *Software* inSSIDer *Home*

METODE PENELITIAN

Metode penelitian yang digunakan menggunakan metode *action research*. Arsitektur jaringan yang digunakan menggunakan 1(satu) buah *smartphone android* yang menjadi *access point* (AP) *hotspot tethering*, 1(satu) buah laptop yang digunakan sebagai *client* yang menggunakan *tethering*, serta 1(satu) buah laptop sebagai *attacker*.



Gambar 3. Diagram Alir Penelitian

Penjelasan kegiatan pada *flowchart* penelitian diatas sebagai berikut :

1. Studi literatur & *survey*.

   Dengan membaca teori-teori yang berkaitan dengan topik skripsi ini, yang terdiri dari jurnal, artikel-artikel, skripsi-skripsi, *ebook*, layanan internet, dan lain-lain. Setelah itu melakukan *survey* terhadap *access point* yang akan menjadi target penelitian.
2. Pengumpulan bahan & data.

   Bahan dan data yang dikumpulkan disini seperti tutorial-tutorial pengujian, *operating system* yang akan digunakan, serta *tools-tools* dan *software* yang diperlukan dalam penelitian ini.
3. Konfigurasi *hardware*, *software* dan topologi jaringan.

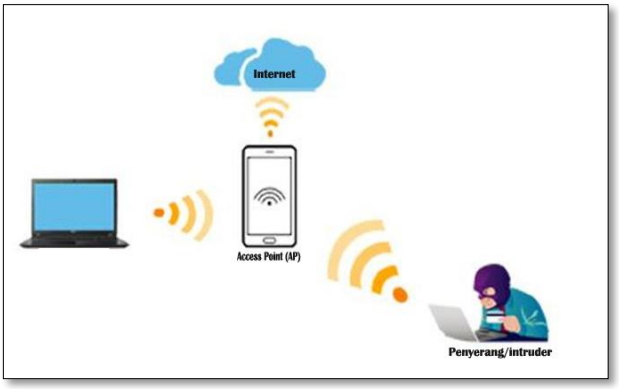
   Setelah semua bahan dan data didapatkan, maka dilakukan konfigurasi *hardware* dan *software* agar pengujian dapat dijalankan, setelah itu dilakukan perancangan topologi dengan beberapa skenario pengujian yang akan dilakukan nantinya.

   Topologi yang digunakan pada penelitian ini menggunakan konsep *tethering/portable* yang dapat menjadikan *smartphone android* sebagai *access point* untuk memanfaatkan koneksi internet dan digunakan oleh *client*.
4. Melakukan pengujian jaringan.

   Pengujian keamanan jaringan ini menggunakan beberapa skenario pengujian, antara lain :
   - Skenario pengaruh penggunaan perangkat *user* berupa laptop yang mengakses jaringan.
   - Skenario pengaruh penggunaan perangkat *user* berupa *smartphone* yang mengakses jaringan.
   - Skenario pengaruh layanan data yang diakses seperti *email*, *video streaming* dan *facebook*.

Konfigurasi Jaringan *Tethering*

Pada penelitian ini dirancang desain jaringan yang digunakan dan disesuaikan dengan model infrastruktur jaringan pada *Wireless Local Area Network* (WLAN), berikut desain jaringan yang digunakan pada penelitian ini.



Gambar 4**.** Desain Skenario Serangan

Topologi yang digunakan pada penelitian ini menggunakan konsep *tethering/portable* Wi-Fi yang dapat menjadikan *smartphone android* sebagai *access point* atau *gateway* untuk memanfaatkan koneksi internet dan digunakan oleh laptop maupun *smartphone*.

Pengujian *Sniffing* Jaringan WLAN

Software inSSIDer yang digunakan untuk *sniffing* berjalan diatas sistem operasi *windows* dan terletak di laptop *attacker*. Berikut gambar 5 yang

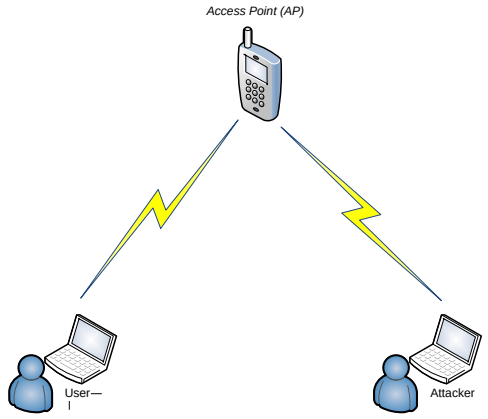
menggambarkan hasil *sniffing* pada laptop penyerang (*attacker).*

Gambar 5**.** Hasil *sniffing* pada *software* inSSIDer

Pengujian pada gambar 5 diatas dilakukan proses *sniffing* ke jaringan WLAN yang ada disekitar area penelitian dan didapatkan 1 (satu) *access point* (AP) yang *online*.

Konfigurasi Skenario Pengujian

Pada penelitian ini jarak antara *client* ke *access point* (AP) yaitu 1 meter dan jarak *attacker* 2,5 meter. Berikut gambar 6 desain jaringan yang digunakan.



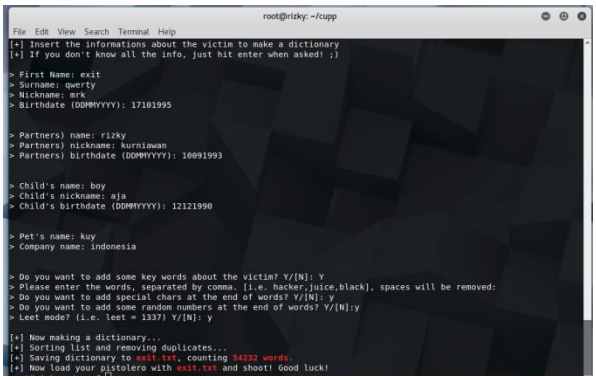
Gambar 6. Desain Topologi Jaringan

Penjelasan topologi :

- *Client* yang digunakan disini menggunakan laptop Lenovo™ ideapad™ Core i3 yang menggunakan *wireless adapter* sehingga dapat terhubung dengan jaringan WLAN. *Client* tersebut terhubung dengan *smartphone android* dengan menggunakan koneksi *hostpot tethering*.
- *Smartphone* yang digunakan memiliki fitur *Hostpot Tethering* dan dijadikan sebagai *hotspot access point.*
- *Attacker* melakukan proses *scanning* dan *sniffing* untuk mendapatkan informasi dari *access point* (*smartphone*).

Membuat *file wordlist.txt*

File wordlist.txt merupakan *file* yang berisi kamus kata-kata yang akan menjadi acuan untuk mendapatkan kata sandi dari *Access Point* (AP) yang menjadi target pengujian, *file* ini bisa dibuat manual maupun di *download* pada *website* yang menyediakan *wordlist* untuk menguji keamanan jaringan.

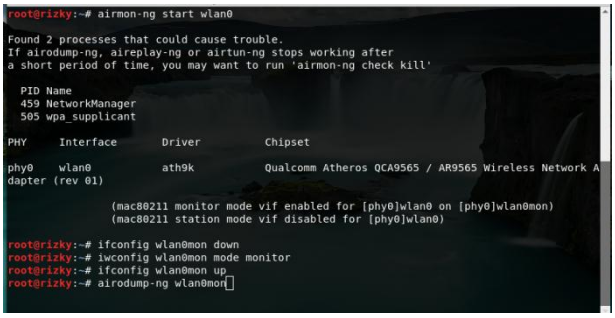


Gambar 7. Proses Membuat *Wordlist.txt*

Pada gambar 7 diatas, *wordlist* dibuat menggunakan bantuan *tool* cupp *python*.

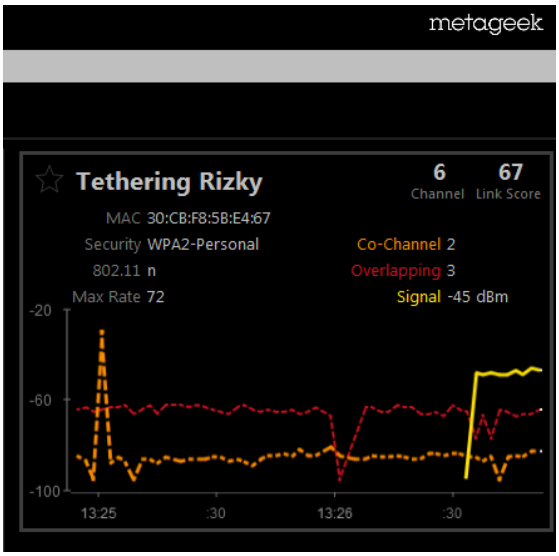
HASIL DAN PEMBAHASAN

Hasil dari pengujian yang dilakukan berupa beberapa informasi mengenai jaringan *tethering* yang digunakan.



Gambar 8. Mengaktifkan Mode Monitoring

Proses seperti gambar 8 diatas berguna agar *traffic* jaringan dapat dimonitoring dan ditandai dengan "wlan0mon".



Gambar 9. Hasil *Sniffing* Menggunakan inSSIDer *home*

Dari Gambar 9 diatas didapatkan data bahwa informasi pada *access point* yaitu *smartphone* didapat nilai MAC 30:CB:F8:5B:E4:67 dengan tipe Wi-Fi 802.11n dengan keamanan WPA2-Personal.

Tujuan dari analisa ini adalah untuk mengetahui informasi dari *access point* yang akan menjadi pusat akses ke internet serta mendapatkan data yang bisa menjadi acuan *attacker* dapat masuk ke jaringan target.

Sniffing **menggunakan** ***airodump.ng***

Gambar 10. Hasil *sniffing* dari *airodump.ng*

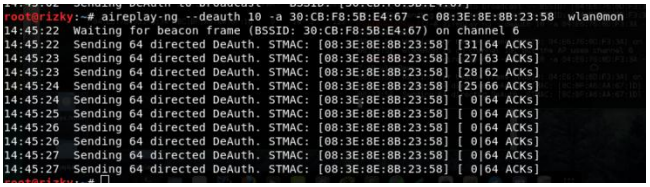
Gambar 10 diatas terdapat saat *client-client* yang belum terhubung ke *access point*, terdapat 2 *client* pada jaringan yang di monitoring.

Gambar 11. *Client* yang terhubung

Gambar 10 diatas telah terdeteksi *client* yang terhubung dengan *access point* dengan ESSID "*Tethering* Rizky".

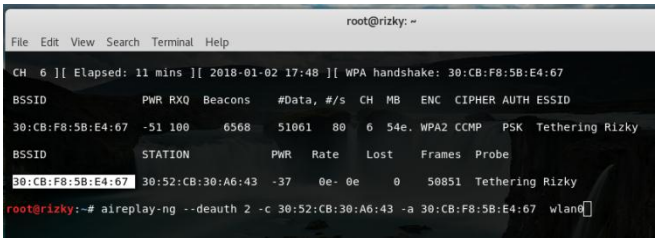
Mendapatkan Paket ***handshake***

Setelah interface wlan0 telah dimonitoring, langkah selanjutnya yaitu mendapatkan paket *handshake* untuk menyesuaikan data *wordlist* atau *dictionary file* yang telah dibuat dengan AP target pengujian yang berguna sebagai *list* data kemungkinan *password* yang digunakan oleh *client* ketika mengakses *access point* pada *hostpot tethering.*



Gambar 12. Proses *deauthentication*

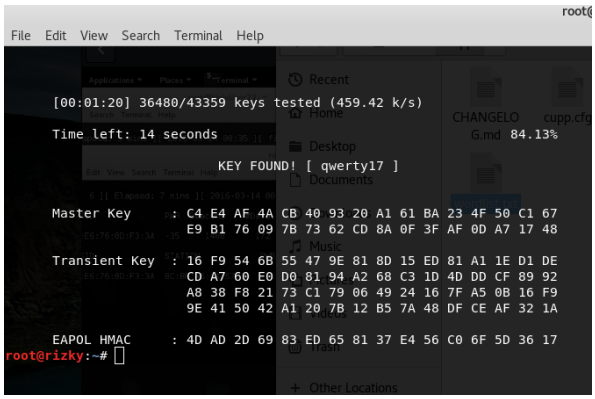
Proses *deauth* pada gambar 12 diatas yaitu cara untuk memutuskan koneksi dari *client* ke *access point* agar *client* melakukan *login* ulang ke *access point* dan dalam waktu yang sama aireplay-ng merekam paket *handshake* yang didapatkan dari *client* dan *access point*.



Gambar 13. Mendapatkan Paket *Handshake*

Paket *handshake* menandakan bahwa ada *client* yang terhubung dengan *Access Point* (AP), sehingga pengujian bisa dilanjutkan agar mendapatkan informasi mengenai kata sandi dari AP yang menjadi target pengujian.

Hasil Akhir ***Snffing*** **dan** ***Scanning***



Gambar 14. Hasil Akhir *Snffing* dan *Scanning*

Gambar 14 diatas didapatkan setelah beberapa langkah pengujian seperti *scanning* dan *sniffing* dilakukan pada jaringan *Wireless Local Area*

Network (WLAN) saat menggunakan akses *tethering*.

Dari hasil akhir seperti gambar 14 diatas didapatkan sebuah kata sandi dari *Access Point* (AP) *hotspot tethering* yang diuji, yaitu "qwerty17", yang mana kata sandi tersebut didapatkan dari proses *sniffing* yang menggunakan *wordlist* yang telah dibuat, kata sandi ditemukan pada *wordlist* ke 36480 dari 43359 kata sandi yang dibuat oleh proses *generate* menggunakan *tool cupp python*.

KESIMPULAN

Berdasarkan hasil dan analisa yang dilakukan pada penelitian ini, maka dapat disimpulkan:

1. Proses *tethering* yang banyak digunakan saat ini tidak cukup aman untuk digunakan.
2. Tipe enkripsi pada *hotspot tethering* masih bisa dibobol menggunakan bantuan *tool aircrack-ng* dan *airodump-ng*, dengan melakukan serangan *bruceforce* menggunakan *wordlist*.
3. Aplikasi inSSIDer dapat melakukan *sniffing* dan *scanning* dengan mudah pada jaringan WLAN sehingga mendapatkan informasi dari *Access Point* (AP) yang ada.
4. Sistem pengujian dengan *tools aircrack-ng* dan *airodump.ng* dapat menemukan kata sandi dari *Access Point* (AP) yaitu "qwerty17".

DAFTAR PUSTAKA

Atmaji, E. S. J. dan B. M. Susanto. 2016. Monitoring Keamanan Jaringan Komputer Menggunakan Network Intrussion Detection System (NIDS). Seminar Hasil Penelitian dan Pengabdian Masyarakat Dana BOPTN: 118-122.

Khoula, A. H., N. Shah., and A. N. S. Shankarappa, 2016. Smartphone's Hotspot Security Issues and Challenges. IEEE*:* 113-118.

Mutaqin, A. F. 2016. Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS *Alert* dengan *Snort*. *Jurnal Sistem dan Teknologi Informasi (JUSTIN)* 1(1): 1-6.

Mydza, D. M. 2011. Analisa dan Konfigurasi Network Intrusion Prevention System (NIPS) Pada Linux Ubuntu 10.04 LTS. *Skripsi*. Jurusan Teknik Informatika Universitas Islam Negeri Sultan Syarif Kasim Riau. Pekanbaru.

Rajab, M. 2010. Analisa Perancangan Wireless LAN Security Menggunakan WPA2-RADIUS. *Skripsi*. Program Studi Teknik Informatika. UIN Syarif Hidayatullah.