Prosiding Seminar Nasional SMIPT 2020
Sinergitas Multidisiplin Ilmu Pengetahuan dan Teknologi, vol. 3, nol. 1, 2020
p-ISSN: 2622-0520; e-ISSN: 2622-593X

Analisis Kelemahan Sistem Authentication Pengguna Pada Wireless IEEE 802.11i

Berkat Fa'atulo Halawa[1], Ahmad Suwardi[2], Robby Toro[3], Rahmalia Syahputri[4]
[1-4]*Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Institut Informatika & Bisnis Darmajaya*

Corresponding Author:
Penulis Pertama: Berkat Fa'atulo Halawa Telp: 085206691321
E-mail: berkathalawa.1711010164@mail.darmajaya.ac.id

Abstrak

Jaringan WiFi memanfaatkan gelombang radio sebagai media penghantar komunikasi, sehingga jaringan ini memiliki kerentanan keamanan yang lebih tinggi dibanding dengan teknologi komunikasi lainnya. Berbagai tindakan pengamanan telah diterapkan seperti teknologi WPA2-PSK. Teknologi ini menggunakan sistem keamanan algoritma AES dan CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) sebagai pengganti TKIP (Temporal Key Integrated Protocol) yang digunakan oleh WPA. Untuk keamanan sistem jaringan WPA2-AES, penyerang dapat memanfaatkn gelombang radio untuk mendapatkan kata sandi pada saat pengguna terhubung ke jaringan tersebut. Untuk mengetahui jenis serangan password dan waktu yang diperlukan telah dibangun simulasi serangan password cracking dalam bentuk dictionary attack. Berdasarkan uji coba yang telah dilakukan, bahwa tipe kata sandi yang menggunakan abjad kecil dan angka, memiliki durasi waktu yang lebih cepat, Sedangkan tipe password kombinasi abjad besar, kecil, angka dan karakter, merupakan jenis password yang memiliki durasi paling lama dalam memecahkan kunci kata sandi. Semakin banyak kombinasi kata sandi yang di gunakan maka akan membutuhkan waktu yang lebih lama untuk memecahkan kata sandi tersebut. Sebaliknya, semakin sedikit kombinasi kata sandi yang di gunakan maka akan lebih mudah untuk diretas. Teknik dan pengujian ini semata-mata dilakukan untuk penetrasi terhadap keamanan jaringan WPA2-PSK, yang bertujuan untuk mengetahui password WPA2-PSK serta untuk menambah wawasan tentang keamanan jaringan tersebut

Kata Kunci: Wireless, Password, WPA2-PSK, IEEE

1. PENDAHULUAN

Jaringan wireless atau nirkabel mulai berkembang pada 1997 hingga sekarang dan terus mengalami perkembangan yang sangat pesat. Jaringan ini banyak di manfaatkan oleh individu, organisasi, dan perusahaan yang menerapkan jaringan nirkabel di berbagai lokasi seperti rumah dan bisnis.

Jaringan wireless memiliki keuntungan yaitu pengguna dapat dengan mudah dapat mengakses informasi dimana saja dan kapan saja. Selain itu, jaringan wireless dapat diterapkan pada lokasi yang tidak terjangkau jaringan berbasis kabel, karena teknologi wireless mampu mendukung pengiriman data dalam rentang jarak yang cukup jauh (Agus dan Basir, 2011).

Meskipun jaringan wireless menawarkan banyak keuntungan namun jaringan nirkabel memiliki beberapa masalah keamanan, antara lain disebabkan penggunaan gelombang radio yang telah membuat sistem keamanan wireless menjadi rentan (Syahputri dan Sriyanto, 2012).

Pemakaian teknologi keamanan wireless secara umum dibagi atas tanpa pengamanan (open) dan dengan pengamanan (shared key). Open (non secure), yaitu tanpa menggunakan pengaman, dimana perangkat yang memiliki pancaran gelombang dapat mendengar transmisi dari perangkat lain seperti access point dapat langsung masuk kedalam jaringan tanpa perlu memberikan informasi untuk proses identifikasi. Sedangkan shared key, menggunakan kunci sebagai identitas untuk membuktikan keaslian perangkat untuk mengakses jaringan .

Standar keamanan shared key yang diterapkan dijaringan wireless saat ini adalah WPA2 (Wi-Fi Protected Access) yang merupakan penyempurnaan dari WPA yang telah menggantikan WEP (Wired Equivalent Privacy).

**Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id*

***Article History**: Received: September 02, 2020, Accepted: Oktober 01, 2020*

WPA2 menggunakan sistem keamanan algoritma AES dan CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) sebagai pengganti TKIP (Temporal Key Integrated Protocol) yang digunakan oleh WPA. TKIP memiliki kelemahan apabila terlalu banyak pengguna yang memakai channel yang sama dan terhubung dengan access point yang sama, maka bandwith yang bisa di lewatkan akan menurun. Sehingga, WPA rentan terhadap MAC address yang sangat mudah di spoofing yaitu ditiru atau di duplikasi (Alulu, 2007).

AES merupakan algoritma kriptografi chipper blok dan bekerja menggunakan operasi matematika dan logis berdasarkan algoritma Rijndael. Metode ini menggabungkan kunci dan blok data 128 bit (tidak terenkripsi) untuk membuat blok data yang berbeda (terenkripsi) (Edney et al, 2004).

Dalam 802.11i juga dikenal sebagai Keamanan Jaringan Kuat (RSN), membangun protokol keamanan di AES disebut Counter Mode-Cipher Blok Chaining MAC Protocol (CCMP). CCMP mendefinisikan seperangkat aturan yang menggunakan chipper blok AES untuk mengaktifkan enkripsi dan perlindungan frame data IEEE 802.11 di tingkat MPDU (Edney, 2004).

Pemanfaatan AES diharapkan dapat mengatasi serangan terhadap kunci enkripsi yang lemah (Kumar dan Gambhir, 2014).

Sistem jaringan tanpa kabel bertujuan untuk mengirimkan paket data secepat mungkin. Peggunaan sistem keamanan enkripsi akan memperlambat proses pengiriman data maka, pemakaian sistem keamanan enkripsi masih belum mendapat menjadi pilihan utama. Setelah proses pengiriman data sudah cukup cepat dan harganya menjadi murah, maka akan melihat kemajuan di bagian keamanan dengan menggunakan enkripsi.

Ada dua jenis kelemahan yang dimiliki pada jaringan tanpa kabel, yaitu kelemahan pada sistem konfigurasi dan kelemahan pada metode enkripsi yang diterapkan. Penyebab kelemahan pada konfigurasi karena pada saat merancang sebuah jaringan tanpa kabel cukup mudah. Banyak vendor yang menyiapkan fasilitas dan perangkat yang mempermudah pengguna jaringan sehingga banyak penggunaan jaringan tanpa kabel yang saat ini menggunakan konfigurasi wireless default bawaan vendor. Banyak pengguna jaringan tanpa kabel yang merancang jaringan dengan menggunakan cara setting default yang di sediakan vendor seperti SSID, alamat IP, remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user (password) untuk pengguna jaringan tersebut. WEP (Wired Equivalent Privacy) adalah standart keamanan jaringan tanpa kabel sebelumnya, hanya saja sistem keamanan yang disediakan WEP bisa dengan mudah retas atau dipecahkan dengan berbagai perangkat aplikasi yang tersedia gratis di internet. WPA-PSK dan LEAP merupakan sebuah sistem keamanan yang menjadi solusi pengganti WEP, sudah dapat diretas atau dipecahkan dengan teknik serangan dictionary secara offline. Celah keamanan pada jaringan tanpa kabel terletak pada empat bagian lapisan, keempat bagian lapisan tersebut adalah metode dari terjadinya hubungan komunikasi data pada media jaringan. Pada lapisan metode hubungan komunikasi melewati media jaringan terdapat celah-celah keamanan yang bisa dijadikan jalur untuk dimasuki. Sistem keamanan jaringan tanpa kabel memiliki kelemahan yang perlu dicermati dengan ekstra teliti.

Tulisan ini menganalisa kelemahan autentikasi pada teknologi WPA2 dengan cara melakukan simulasi serangan password cracking. Tulisan ini dibagi menjadi lima bagian. Bagian pertama memberikan gambaran tentang hal yang melatarbelakangi serangan terhadap wireless, sedangkan bagian kedua memaparkan serangan-serangan yang terjadi pada komunikasi wireless. Bagian ketiga metode penelitian yang berisi bahan dan alat serta langkah yang dilakukan dalam penelitian. Pada bagian yang keempat memaparkan hasil dan pembahasan penelitian, sedangkan bagian kelima memaparkan kesimpulan dari penelitian yang dilakukan.

2. METODE

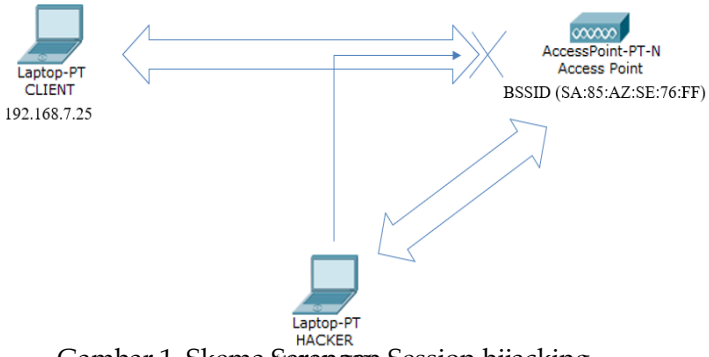
Pada penelitian ini, metode yang digunakan adalah simulasi cracking terhadap keamanan jaringan nirkabel WPA2/AES untuk mengetahui kelemahan teknologi tersebut. Setelah itu, hasil ditabulasi dan dianalisa. Password cracking merupakan metode yang dipergunakan untuk mendapatkan kata sandi pada sebuah sistem jaringan tanpa kabel.

Simulasi serangan cracking yang dilakukan dibagi menjadi dua serangan, yaitu :

*Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id

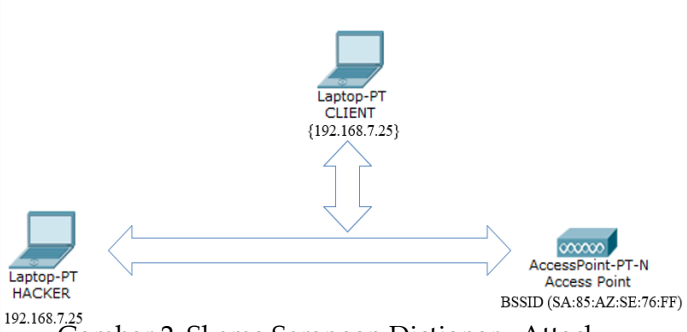
***Article History**: Received: September 02, 2020, Accepted: Oktober 01, 2020*

- Session hijacking merupakan salah satu serangan efektif pada jaringan, cukup mudah dan apabila jalur akses target tidak menggunakan enkripsi WEP/WPA. Dengan melakukan session hijacking, seorang peretas dapat memperoleh akses ke suatu jaringan, dimana peretas menyamar sebagai pengguna yang sah. Metode ini juga dapat menjadi langkah pertama dalam berbagai teknik serangan yang lebih rumit.



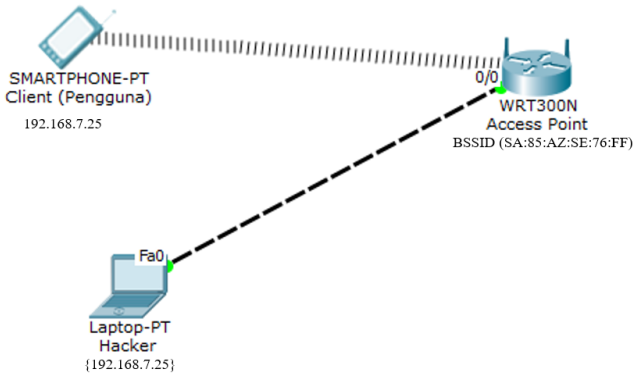
Gambar 1. Skema Serangan Session hijacking

- Dictionary Attack merupakan metode mombobol komputer atau server yang dilindungi kata sandi dengan secara sistematis memasukkan setiap kata dalam kamus sebagai kata sandi. Serangan ini juga dapat digunakan dalam upaya menemukan kunci yang diperlukan untuk mendeskripsi suatu pesan atau dokumen yang terenkripsi.



Gambar 2. Skema Serangan Dictionary Attack

Mekanisme serangan :



Gambar 3. Skema Serangan Password Cracking

*Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id
***Article History**: Received: September 02, 2020, Accepted: Oktober 01, 2020*

Simulasi yang dilakukan pada penelitian ini sebanyak 19 kali percobaan yang terbagi dari 9 kombinasi kata sandi, sebagai berikut:

a. Kata sandi dengan menggunakan abjad kecil
b. Kata sandi dengan menggunakan abjad besar
c. Kata sandi dengan menggunakan angka
d. Kombinasi kata sandi abjad besar dan abjad kecil
e. Kombinasi kata sandi abjad kecil dan angka
f. Kombinasi kata sandi abjad besar dan angka
g. Kombinasi kata sandi angka dan karakter
h. Kombinasi kata sandi abjad besar, abjad kecil dan angka
i. Kombinasi kata sandi abjad besar, abjad kecil, angka dan karakter.

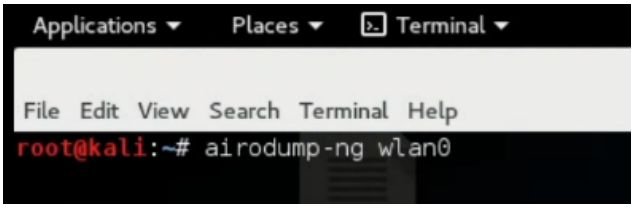
Alat dan bahan yang digunakan:

Alat : - PC
- Telepon genggam
- AP

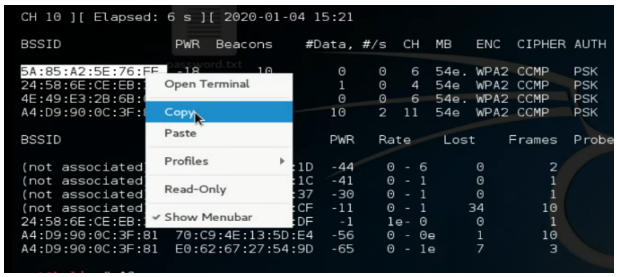
Software : - Kali Linux

Langkah-langkah yang dilakukan:

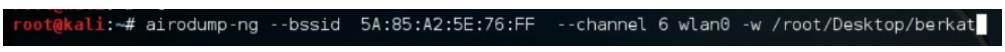
1. Membuka terminal kali linux dan masuk ke root untuk menjalankan simulasi
2. Menampilkan semua jaringan di sekitar untuk mendapatkan BSSID dan informasi seputar jaringan yang tersedia



3. Memilih salah satu BSSID yang akan di serang (access point target) SA:85:AZ:SE:76:FF



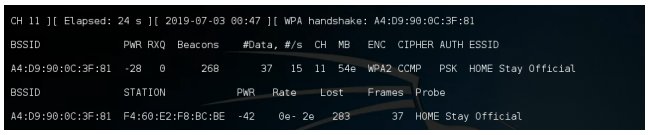
4. Menempatkan file yang akan didapat dari bssid dan channel yang di tuju.



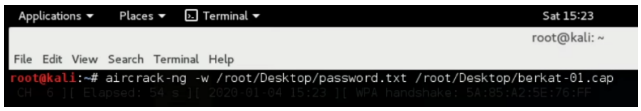
*Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id

***Article History**: Received: September 02, 2020, Accepted: Oktober 01, 2020*

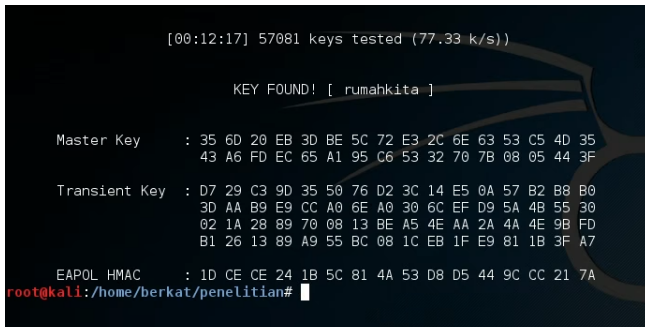
5. Akan muncul tampilan yang memuat koneksi ke access pointt (handshake), handshake akan muncul apabila ada client yang mau terhubung ke access point target.



6. Memulai cracking password access point.



7. Menunggu beberapa saat sampai proses craking selesai maka aka muncul KEY FOUND!



Penelitian ini telah di lakukan secara berkala dengan perangkat yang sama namun dengan kombinasi kata sandi WPA2/PSK yang berbeda-beda. Berikut tabulasi simulasi atau percobaan yang telah dilakukan:

Tabel 1. Tabulasi simulasi atau percobaan

No	Tipe Kata Sandi	Jumlah Karakter	Key Found	Durasi cracking	Keys Tested	Speed k/s
1	Abjad kecil	9	rumahkita	00:12:17	57081	77,33
2	Abjad kecil	9	cafetaria	00:05:03	44388	293,56
3	Abjad besar	10	WIFIGRATIS	00:09:43	62792	77,01
4	Abjad besar	10	ERKATRAVEL	00:08:21	41460	99,00
5	Angka	8	08021999	00:04:05	56124	204,42
6	Angka	9	987654321	00:10:01	293	161,22
7	Abjad besar dan abjad kecil	9	ModalDong	00:11:59	82584	146,56
8	Abjad besar dan abjad kecil	10	BUCINbucin	00:15:52	84348	83,77
9	Abjad kecil dan angka	12	belikuota123	01:27:56	519492	90,74
10	Abjad kecil dan angka	12	0852bagibagi	00:35:07	493168	305,58

*Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id
***Article History**: Received: September 02, 2020, Accepted: Oktober 01, 2020*

11	Abjad besar dan angka	10	KERJA12345	00:38:57	501444	145,40
12	Abjad besar dan angka	8	AKU3KAMU	00:39:29	542764	437,25
13	Angka dan karakter	9	12345_321	01:02:31	465596	136,60
14	Angka dan karakter	9	4321&1234	00:57:14	504992	251,22
15	Abjad besar, kecil dan angka	13	BeloveCorp123	03:07:35	1334160	147,37
16	Abjad besar, kecil dan angka	8	Usaha001	01:24:45	1067688	223,08
17	Abjad besar, kecil, angka dan karakter	10	Xiaomi_123	02:03:49	1676028	331,36
18	Abjad besar, kecil, angka dan karakter	10	Kuota&DU1T	04:50:45	2044836	111,54
19	Abjad besar, kecil, angka dan karakter	17	War03Ng_M4M1&P4P1	08:56:01	4297512	148,90

3. HASIL DAN PEMBAHASAN

WPA menggunakkan teknologi atau algoritma untuk autentikasi pengguna, tetapi teknologi tersebut tidak bisa melindungi sistem dari serangan password cracking.

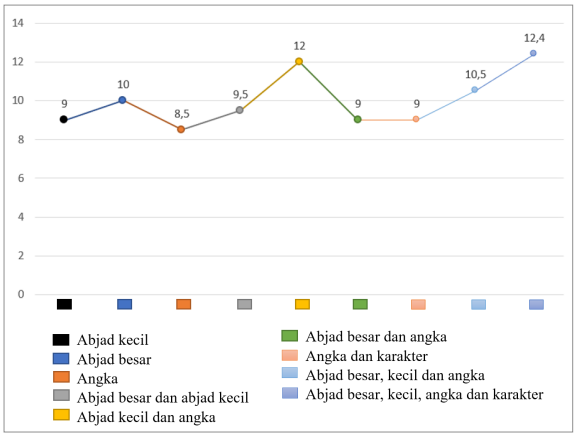
Pada penelitian ini, semua percobaan berhasil mendapatkan kata sandi access point dengan variasi jumlah karakter, tipe password, durasi cracking, keys tested dan kecepatan crack yang berbeda-beda seperti pada (tabel 1).

a. Jumlah Karakter

Berdasarkan penelitian yang telah dilakukan, maka didapat rata-rata jumlah karakter sebagai berikut.

*Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id

***Article History**: Received: September 02, 2020, Accepted: Oktober 01, 2020*



Grafik 1. Rata-rata jumlah karakter

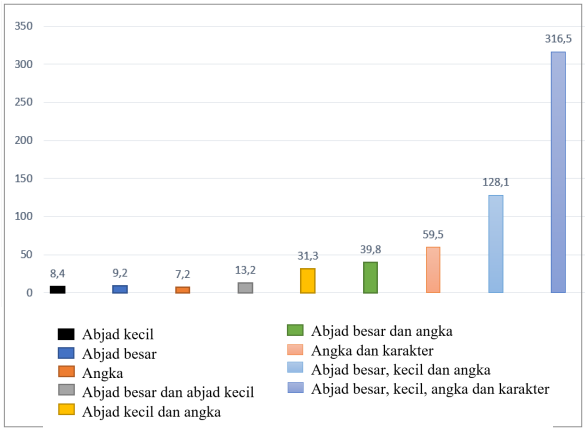
Jumlah karakter sangat mempengaruhi proses peretasan yang dilakukan. Apabila jumlah karakter pendek, maka akan lebih mudah dan lebih cepat untuk mendapatkan kata sandi. Terlihat pada percobaan 1 yang memiliki 9 jumlah karakter, apabila dibandingkan dengan percobaan 19 yang memiliki 17 jumlah karakter maka dapat dibuktikan bahwa percobaan 1 lebih mudah dan lebih cepat untuk mendapatkan kata sandi yaitu berdurasi 12 menit 17 detik. Seperti halnya pada percobaan 5 yang memiliki 8 jumlah karakter, jika dibandingkan dengan percobaan 4 yang memiliki 10 jumlah karakter maka dapat dibuktikan bahwa percobaan 5 lebih cepat untuk mendapatkan kata sandi yaitu berdurasi 4 menit 5 detik. Selain itu, percobaan 10 dan 15 juga membuktikan pengaruh jumlah karakter pada proses peretasan. Apabila dibandingkan, percobaan 10 yang memiliki 12 jumlah karakter dan percobaan 15 yang memiliki 13 jumlah karakter maka dapat dibuktikan bahwa percobaan 12 lebih mudah dan lebih cepat untuk mendapatkan kata sandi yaitu berdurasi 35 menit 7 detik.

Sedangkan, jika jumlah karakternya panjang akan memperlambat proses peretasan karena akan memperlama peluang munculnya kata sandi. Hal ini terjadi oleh karena pada proses cracking dimulai secara terstruktur yaitu dimulai dari angka 0-9, abjad a-z, dan seluruh karakter ASCII. Terlihat pada percobaan 19 yang memiliki 17 jumlah karakter, apabila dibandingkan dengan percobaan 15 yang memiliki 13 jumlah karakter maka dapat dibuktikan bahwa percobaan 19 lebih sulit dan lebih lama untuk mendapatkan kata sandi yaitu berdurasi 8 jam 56 menit 1 detik. Seperti halnya pada percobaan 4 yang memiliki 10 jumlah karakter, jika dibandingkan dengan percobaan 2 yang memiliki 9 jumlah karakter maka dapat dibuktikan bahwa percobaan 4 lebih lama untuk mendapatkan kata sandi yaitu berdurasi 8 menit 21 detik. Selain itu, percobaan 9 dan 16 juga membuktikan pengaruh jumlah karakter pada proses peretasan. Apabila dibandingkan, percobaan 9 yang memiliki 12 jumlah karakter dan percobaan 16 yang memiliki 8 jumlah karakter maka dapat dibuktikan bahwa percobaan 9 lebih sulit dan lebih lama untuk mendapatkan kata sandi yaitu berdurasi 1 jam 27 menit 56 detik.

*Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id
***Article History**: Received: September 02, 2020, Accepted: Oktober 01, 2020*

b. Durasi Cracking

Penelitian ini juga menghasilkan durasi cracking yang berbeda. Berdasarkan penelitian yang telah dilakukan, maka didapat rata-rata durasi cracking sebagai berikut.



Grafik 2. Rata-rata durasi cracking dalam menit

Perbedaan durasi cracking dapat terjadi karena perbedaan kombinasi tipe kata sandi, jumlah karakter, percobaan kunci dan kecepatan pada proses cracking.

Dari data rata-rata percobaan yang dilakukan, kombinasi tipe kata sandi abjad kecil, abjad besar dan angka berada pada posisi terendah. Pada percobaan 1 dan 2 yang menggunakan kombinasi tipe kata sandi abjad kecil, rata-rata durasi cracking yang diperlukan yaitu 8 menit 4 detik. Pada percobaan 3 dan 4 yang menggunakan kombinasi tipe kata sandi abjad besar, rata-rata durasi cracking yang diperlukan yaitu 9 menit 2 detik. Sedangkan, pada percobaan 5 dan 6 yang menggunakan kombinasi tipe kata sandi angka, rata-rata durasi cracking yang diperlukan yaitu 7 menit 2 detik. Hal ini membuktikan bahwa kombinasi kata sandi abjad kecil, abjad besar dan angka tersebut sangat cepat untuk mendapatkan kata sandi.

Selain itu, dari rata-rata percobaan yang dilakukan, kombinasi tipe kata sandi abjad besar dan abjad kecil, kombinasi abjad kecil dan angka, serta kombinasi abjad besar dan angka berada pada posisi menengah atau sedang. Pada percobaan 7 dan 8 yang menggunakan kombinasi tipe kata sandi abjad besar dan abjad kecil, rata-rata durasi cracking yang diperlukan yaitu 13 menit 2 detik. Pada percobaan 9 dan 10 yang menggunakan kombinasi tipe kata sandi abjad kecil dan angka, rata-rata durasi cracking yang diperlukan yaitu 31 menit 3 detik. Sedangkan, pada percobaan 11 dan 12 yang menggunakan kombinasi abjad besar dan angka, rata-rata durasi cracking yang diperlukan yaitu 39 menit 8 detik. Hal ini membuktikan bahwa kombinasi kata sandi abjad besar dan abjad kecil, kombinasi abjad kecil dan angka, serta kombinasi abjad besar dan angka tersebut sangat cepat untuk mendapatkan kata sandi.

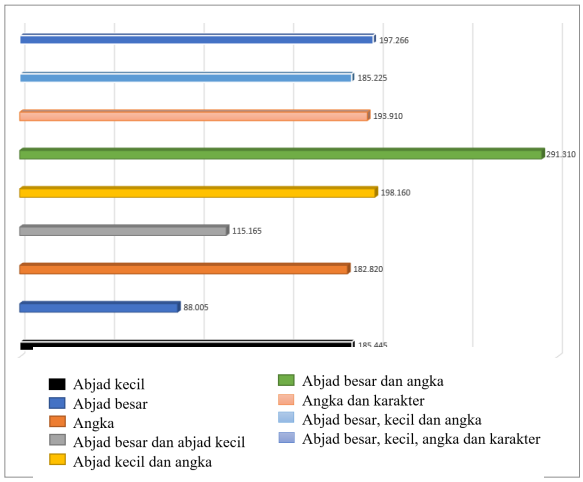
Selain itu juga, dari rata-rata percobaan yang dilakukan, kombinasi tipe kata sandi angka dan karakter, kombinasi abjad besar, kecil dan angka, serta kombinasi abjad besar kecil, angka dan karakter berada pada posisi teratas. Pada percobaan 13 dan 14 yang menggunakan kombinasi tipe kata sandi angka dan karakter, rata-rata durasi cracking yang diperlukan yaitu 59 menit 5 detik. Pada

*Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id
***Article History**: Received: September 02, 2020, Accepted: Oktober 01, 2020*

percobaan 15 dan 16 yang menggunakan kombinasi abjad besar, kecil dan angka, rata-rata durasi cracking yang diperlukan yaitu 2 jam 13 menit 5 detik. Sedangkan, pada percobaan 17, 18 dan 19 yang menggunakan kombinasi abjad besar kecil, angka dan karakter, rata-rata durasi cracking yang diperlukan yaitu 5 jam 27 menit 5 detik. Hal ini membuktikan bahwa kombinasi tipe kata sandi angka dan karakter, kombinasi abjad besar, kecil dan angka, serta kombinasi abjad besar kecil, angka dan karakter tersebut susah dan sangat lama untuk mendapatkan kata sandi.

c. Kecepatan Cracking

Proses peretasan juga dipengaruhi oleh kecepatan jaringan target yang diretas.. Berdasarkan penelitian yang telah dilakukan, maka didapat rata-rata kecepatan cracking sebagai berikut.



Grafik 3. Rata-rata kecepatan cracking

Semakin besar kecepatan jaringan yang dituju, maka akan semakin cepat mendapatkan kata sandi. Terlihat pada percobaan 3 dan 4 dengan kecepatan rata-rata 88,005 k/s, apabila dibandingkan dengan percobaan 7 dan 8 dengan kecepatan rata-rata 115,165 k/s maka dapat dibuktikan bahwa percobaan 3 dan 4 lebih mudah dan lebih cepat untuk mendapatkan kata sandi yaitu berdurasi rata-rata 9 menit 2 detik sedangkan rata-rata durasi percobaan 7 dan 8 yaitu 13 menit 2 detik. Seperti halnya pada percobaan 5 dan 6 dengan kecepatan rata-rata 182,820 k/s, apabila dibandingkan dengan percobaan 13 dan 14 dengan kecepatan rata-rata 193,910 k/s maka dapat dibuktikan bahwa percobaan 5 dan 6 lebih mudah dan lebih cepat untuk mendapatkan kata sandi yaitu berdurasi rata-rata 7 menit 2 detik sedangkan rata-rata durasi percobaan 13 dan 14 yaitu 59 menit 5 detik. Selain itu, percobaan 1 dan 2 dengan kecepatan rata-rata 185,445 k/s, apabila dibandingkan dengan percobaan 9 dan 10 dengan kecepatan rata-rata 198,160 k/s maka dapat dibuktikan bahwa percobaan 1 dan 2 lebih mudah dan lebih cepat untuk mendapatkan kata sandi yaitu berdurasi rata-rata 8 menit 4 detik sedangkan rata-rata durasi percobaan 9 dan 10 yaitu 31 menit 3 detik.

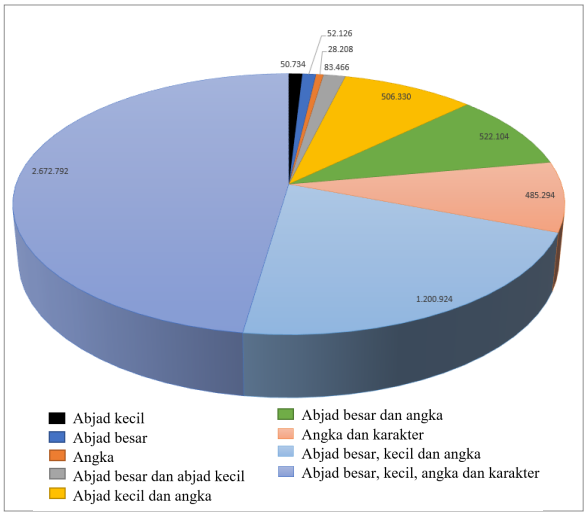
Apabila kecepatan jaringan yang dituju lemah, maka akan memperlambat proses peretasan yang dilakukan. Hal ini dapat dilihat pada percobaan 11 dan 12 dengan kecepatan rata-rata 291,310 k/s, apabila dibandingkan dengan percobaan 9 dan 10 dengan kecepatan rata-rata 198,160 k/s maka

*Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id
Article History: Received: September 02, 2020, Accepted: Oktober 01, 2020

dapat dibuktikan bahwa percobaan 11 dan 12 lebih sulit dan lebih lama untuk mendapatkan kata sandi yaitu berdurasi rata-rata 39 menit 8 detik sedangkan rata-rata durasi percobaan 9 dan 10 yaitu 31 menit 3 detik. Pada percobaan 13 dan 14 dengan kecepatan rata-rata 193,910 k/s, apabila dibandingkan dengan percobaan 3 dan 4 dengan kecepatan rata-rata 88,005 k/s maka dapat dibuktikan bahwa percobaan 13 dan 14 lebih sulit dan lebih lama untuk mendapatkan kata sandi yaitu berdurasi rata-rata 59 menit 5 detik sedangkan rata-rata durasi percobaan 3 dan 4 yaitu 9 menit 2 detik. Sedangkan, pada percobaan 17, 18 dan 19 dengan kecepatan rata-rata 197,266 k/s, apabila dibandingkan dengan percobaan 15 dan 16 dengan kecepatan rata-rata 185,225 k/s maka dapat dibuktikan bahwa percobaan 17, 18 dan 19 lebih sulit dan lebih lama untuk mendapatkan kata sandi yaitu berdurasi rata-rata 5 jam 27 menit 5 detik. Sedangkan rata-rata durasi percobaan 15 dan 16 yaitu 2 jam 13 menit 5 detik.

d. Keys Tested

Penelitian ini juga menghasilkan keys tested yang berbeda. Berdasarkan penelitian yang telah dilakukan, maka didapat rata-rata keys tested sebagai berikut.



Grafik 4. Rata-rata keys tested cracking,

untuk proses peretasan kombinasi kata sandi dengan menggunakan abjad kecil, diperlukan rata-rata peluang munculnya kata sandi yaitu 50,73 keys tested. Hal ini sangat berpengaruh pada durasi dan kecepatan jaringan selama peretasan berlangsung. Kombinasi kata sandi dengan menggunakan abjad besar, diperlukan rata-rata 52,12 peluang munculnya kata sandi. Kombinasi kata sandi dengan menggunakan angka, diperlukan rata-rata 28.208 peluang munculnya kata sandi. Kombinasi kata sandi abjad besar dan abjad kecil, diperlukan rata-rata 83.466 peluang munculnya kata sandi. Kombinasi kata sandi abjad kecil dan angka, diperlukan rata-rata 506.330 peluang munculnya kata sandi. Kombinasi kata sandi abjad besar dan angka, diperlukan 522.104 rata-rata

*Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id
Article History: Received: September 02, 2020, Accepted: Oktober 01, 2020

peluang munculnya kata sandi. Kombinasi kata sandi angka dan karakter, diperlukan 485.294 rata-rata peluang munculnya kata sandi. Kombinasi kata sandi abjad besar, abjad kecil dan angka, diperlukan 1.200.924 rata-rata peluang munculnya kata sandi. Kombinasi kata sandi abjad besar, abjad kecil, angka dan karakter, diperlukan rata-rata 2.672.792 peluang munculnya kata sandi.

4. KESIMPULAN

Keamanan pada jaringan wireless LAN sangat penting khususnya untuk menjamin agar pihak yang mengakses jaringan adalah yang sah. Untuk itu, WPA2 menggunakan sistem keamanan yang cukup baik, yakni AES (Advanced Encryption Standar) meskipun demikian, kata sandi dalam jaringan wireless LAN tetap dapat di pecahkan dengan salah satunya menggunakan serangan password cracking.

Untuk mengetahui ketahanan sistem terhadap serangan session hijacking dan password cracking, telah dilakukan uji coba dengan menggunakan beberapa kombinasi kata sandi, baik huruf, angka, dan simbol.

Berdasarkan uji coba yang telah dilakukan, bahwa tipe kata sandi yang menggunakan abjad kecil dan angka, memiliki durasi waktu yang lebih cepat, Sedangkan tipe password kombinasi abjad besar, kecil, angka dan karakter, merupakan jenis password yang memiliki durasi paling lama dalam memecahkan kunci kata sandi.

Dapat di simpulkan bahwa semakin banyak kombinasi kata sandi yang di gunakan maka akan membutuhkan waktu yang lebih lama untuk memecahkan kata sandi tersebut. Sebaliknya, semakin sedikit kombinasi kata sandi yang di gunakan maka akan lebih mudah untuk diretas.

DAFTAR RUJUKAN

[1] B., Yanti, Y., & . Z. (2018). Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi. *Jurnal Serambi Engineering*, *3*(1), 248–254. https://doi.org/10.32672/jse.v3i1.353

[2] Basir, A., Studi, P., & Komputer, I. (2011). Desain Teknis Jaringan Tulang Punggung "Wireless" Universitas Mulawarman Fahrul Agus, *Jurnal Informatika Mulawarman*, *6*(3), 93–97.

[3] Kumar, U., & Gambhir, S. (2014). *m nl ad in e e V by e th rsio is n fil O e is nly m nl ad in e e V by e th rsio is n fil O e*. *7*(4), 25–34.

[4] McCullough, Jack., 2004. *Wireless Networking: preventing a data disaster*. Indianapolis, Indiana: Wiley Publishing, Inc

[5] Prabowo W. Onno. 2010. Belajar Menjadi hacker. Buku Pintar : Jakarta.

[6] Satria, Lucky. 2014. Pengertian IP Spoofing, Cara Kerja dan Pencegahan IP Spoofing. Informatika : Bandung.

[7] Suryani, Izny. 2013. Contoh-contoh Kasus Cybercrime. Informatika : Bandung.

[8] Syahputri, R., & Sriyanto. (2012). Fast and secure authentication in IEEE 802.11i wireless LAN. *Proceeding of 2012 International Conference on Uncertainty Reasoning and Knowledge Engineering, URKE 2012*, 158–161. https://doi.org/10.1109/URKE.2012.6319534

*Corresponding Author: Berkat Fa'atulo Halawa, Email: berkathalawa.1711010164@mail.darmajaya.ac.id

***Article History**: Received: September 02, 2020, Accepted: Oktober 01, 2020*