

Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux

M. I. Rusdi*, D. Prasti
Universitas Cokroaminoto Palopo
Email : *Muhammad.idham.unm@gmail.com

Abstrak

Sinyal wireless merupakan sinyal gelombang elektromagnetis yang dapat berjalan tanpa media tetapi melalui ruang hampa atau media seperti udara. Karena tidak dibutuhkan media fisik sebagai perantara, maka hal ini akan sangat menguntungkan pada saat membangun jaringan pada daerah atau area yang luas. Kemudahan dalam hal instalasi dan biaya yang relatif murah membuat para praktisi jaringan banyak menggunakan wireless ini. Namun dibalik dari kemudahan dan biaya yang murah, jaringan wifi ini rentan terhadap gangguan keamanan dari luar. Beberapa enkripsi telah diterapkan untuk mengamankan jaringan wifi ini antara lain WEP, WPA, WPA2. Namun enkripsi WEP sudah dapat dengan mudah di cracking atau dapat dijebol oleh seorang penyusup. Kini penulis melakukan audit atau penetration testing keamanan WPA/WPA2 enkripsi jaringan wifi menggunakan system operasi Kali Linux

Kata kunci: *wireless, enkripsi, kali, linux,*

1. Pendahuluan

a. Latar Belakang

Sinyal *wireless* merupakan merupakan sinyal gelombang *elektromagnetis* yang dapat berjalan tanpa media tetapi melalui ruang hampa atau media seperti udara. Karena tidak dibutuhkan media fisik sebagai perantara, maka hal ini akan sangat menguntungkan pada saat membangun jaringan pada daerah atau area yang luas.

Sudah bukan rahasia lagi kalau ternyata standar jaringan nirkabel IEEE 802.11 yang menggunakan enkripsi WEP memiliki kelemahan yang memungkinkan seorang penyusup mengetahui kode enkripsinya. Akan tetapi bukan sesuatu yg tidak memungkinkan untuk membuat jaringan nirkabel bisa mempunyai tingkat keamanan yang tinggi dengan mengkombinasikan pengukuran keamanan tradisional, keamanan standar terbuka dari jaringan nirkabel dan keamanan yang dimiliki perangkat itu sendiri. Perbaikan untuk menyikapi kelemahan pada WEP telah dikembangkan suatu teknik pengamanan baru yang disebut dengan WPA (*Wi-Fi Protected Access*). Teknik WPA ini adalah model pengamanan yang kompartibel dengan draft standar 802.11i yang masih dalam proses pengembangan untuk menggantikan standar 802.11. Pada teknik WPA ini selain pengembangan dari proses enkripsi juga menambahkan proses *user authentication* yang tidak ada pada pada WEP. Proses otentifikasi pada WPA menggunakan 802.1X dan EAP (*Extensible Authentication Protocol*) [1].

Kali linux adalah salah satu distribusi Linux tingkat lanjut untuk **Penetration Testing** dan audit keamanan. Kali Linux merupakan pembangunan kembali BackTrack

Linux secara sempurna, mengikuti sepenuhnya kepada standar pengembangan Debian. Semua infrastruktur baru telah dimasukkan ke dalam satu tempat, semua *tools* telah direview dan dikemas, dan kami menggunakan Git untuk VCS nya [2]. Fitur-fitur Kali Linux adalah sebagai berikut:

- 1) Lebih dari 300 *tools penetration testing*
- 2) Gratis dan akan selalu gratis
- 3) Mengikuti FHS *compliant*
- 4) Dukungan perangkat *wireless* yang luas
- 5) Lingkungan pengembangan yang aman
- 6) Dukungan banyak bahasa

b. Rumusan Masalah

Berdasarkan latar belakang di atas maka penulis merumuskan permasalahan dalam penelitian ini yaitu “Eksplorasi fitur keamanan WPA-PSK dan WPA2-PSK jaringan wifi menggunakan system operasi kali linux “

c. Tujuan Penelitian

Adapun tujuan dari penelitian adalah:

- 1) Menganalisa fitur sistem keamanan WPA-PSK, WPA2-PSK pada jaringan *wireless*, dengan menggunakan sistem operasi Kali Linux
- 2) Memberikan solusi dan memperbaiki sistem keamanan jaringan *wireless* agar jaringan tersebut dapat bekerja dengan baik dan aman.

2. Metode

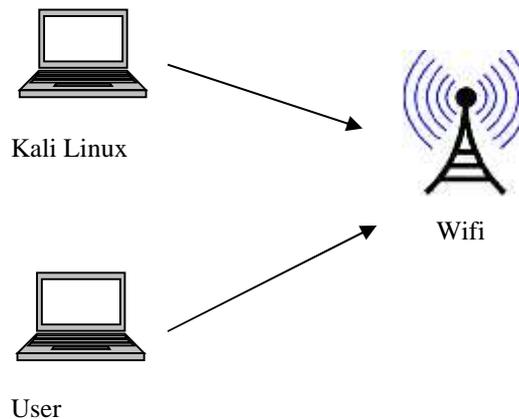
a. Lokasi Penelitian

Penelitian ini dilakukan pada lab mini dengan menggunakan Akses Point berupa smartphone yang telah dilengkapi enkripsi keamanan WPA-PSK, WPA2-PSK dan sebuah laptop yang telah terinstal Kali linux



Gambar 1. Pengaturan keamanan pada smartphone

b. Rancangan Uji Penetrasi



Gambar 2. Rancang uji penetrasi

Dilihat dari gambar diatas maka rancangan uji penetrasi ini, penulis langsung mencoba melakukan audit keamanan terhadap sebuah wifi yang telah dilengkapi dengan enkripsi keamanan WPA-PSK dan WPA2-PSK dan membandingkan kedua enkripsi keamanan tersebut.

c. Metode Penelitian

Dalam penelitian ini menggunakan metode penelitian tindakan atau *action research*. Adapun tahapan penelitian yang merupakan siklus dari *action research* adalah:

- 1) *Diagnosing*, dengan melakukan identifikasi masalah-masalah pokok yang ada.
- 2) *Action Planning*, memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.
- 3) *Action Taking*, mengimplementasikan rencana tindakan yang telah dibuat dengan harapan dapat menyelesaikan masalah.
- 4) *Evaluating*, melaksanakan evaluasi terhadap hasil implementasi yang telah dilakukan.
- 5) *Learning*, melakukan *review* terhadap tahapan-tahapan yang telah berakhir kemudian penelitian ini dapat berakhir.

d. Metode Analisis Data

Analisis data dimulai dengan menganalisis sistem keamanan WPA-PSK, WPA2-PSK jaringan wifi. Serta melakukan uji penetrasi terhadap jaringan *wireless* tersebut menggunakan sebuah laptop yang telah terinstal system operasi kali linux, sehingga dapat diketahui letak kelebihan dan kelemahan dari sistem keamanan wifi tersebut. Setelah menemukan masalah yang terjadi maka penulis memberikan suatu pemecahan atau solusi dari masalah yang sedang dihadapi.

3. Hasil dan Pembahasan

a. Perbedaan Security Wireless WPA, WPA2 dan WPA-PSK

1) WPA

WPA (bahasa Inggris: Wi-Fi Protected Access) adalah suatu sistem yang juga dapat diterapkan untuk mengamankan jaringan nirkabel. Metoda pengamanan dengan WPA ini diciptakan untuk melengkapi dari sistem yang sebelumnya, yaitu WEP. Para peneliti menemukan banyak celah dan kelemahan pada infrastruktur nirkabel yang menggunakan metoda pengamanan WEP. Sebagai pengganti dari sistem WEP, WPA mengimplementasikan layer dari IEEE, yaitu layer 802.11i. Nantinya WPA akan lebih banyak digunakan pada implementasi keamanan jaringan nirkabel.

WPA didesain dan digunakan dengan alat tambahan lainnya, yaitu sebuah komputer pribadi (PC). Fungsi dari komputer pribadi ini kemudian dikenal dengan istilah authentication server, yang memberikan key yang berbeda kepada masing-masing pengguna/client dari suatu jaringan nirkabel yang menggunakan akses point sebagai media sentral komunikasi. Seperti dengan jaringan WEP, metoda enkripsi dari WPA ini juga menggunakan algoritma RC4. Pengamanan jaringan nirkabel dengan metoda WPA ini, dapat ditandai dengan minimal ada tiga pilihan yang harus diisi administrator jaringan agar jaringan dapat beroperasi pada mode WPA ini. Ketiga menu yang harus diisi tersebut adalah:

a) Computer Server

Komputer server yang dituju oleh akses point yang akan memberi otentikasi kepada client. beberapa perangkat lunak yang biasa digunakan antara lain freeRADIUS, openRADIUS dan lain-lain.

b) Port

Nomor port yang digunakan adalah 1812.

c) SharedSecret

Shared Secret adalah kunci yang akan dibagikan ke komputer dan juga kepada client secara transparant.

Setelah komputer diinstall perangkat lunak otentikasi seperti freeRADIUS, maka sertifikat yang dari server akan dibagikan kepada client. Untuk menggunakan Radius server bisa juga dengan tanpa menginstall perangkat lunak di sisi komputer client. Cara yang di gunakan adalah Web Authentication dimana User akan diarahkan ke halaman Login terlebih dahulu sebelum bisa menggunakan Jaringan Wireless. Dan Server yang menangani autentikasi adalah Radius server.

b. WPA-PSK

WPA-PSK (Wi-Fi Protected Access – Pre Shared Key) adalah pengamanan jaringan nirkabel dengan menggunakan metoda WPA-PSK jika tidak ada autentikasi server yang digunakan. Dengan demikian accesspoint dapat dijalankan dengan mode WPA tanpa menggunakan bantuan komputer lain sebagai server. Cara mengkonfigurasikannya juga cukup sederhana. Perlu diketahui bahwa tidak semua access point akan mempunyai fasilitas yang sama dan tidak semua access point menggunakan cara yang sama dalam mendapatkan Shared-Key yang akan dibagikan ke client. Pada access point Dlink DWL-2000AP, pemberian Shared-Key dilakukan secara manual tanpa mengetahui algoritma apa yang digunakan. Keadaan ini berbanding terbalik dengan akses point Linksys WRT54G, dimana administrator dapat memilih dari dua algoritma WPA yang disediakan, yang terdiri dari algoritma TKIP atau algoritma

AES. Setelah Shared-Key didapat, maka client yang akan bergabung dengan access point cukup memasukkan angka/kode yang diijinkan dan dikenal oleh access point. Prinsip kerja yang digunakan WPA-PSK sangat mirip dengan pengamanan jaringan nirkabel dengan menggunakan metoda Shared-Key[3].

c. WPA2

WPA2 adalah sertifikasi produk yang tersedia melalui Wi-Fi Alliance. WPA2 Sertifikasi hanya menyatakan bahwa peralatan nirkabel yang kompatibel dengan standar IEEE 802.11i. WPA2 sertifikasi produk yang secara resmi menggantikan wired equivalent privacy (WEP) dan fitur keamanan lain yang asli standar IEEE 802.11. WPA2 tujuan dari sertifikasi adalah untuk mendukung wajib tambahan fitur keamanan standar IEEE 802.11i yang tidak sudah termasuk untuk produk-produk yang mendukung WPA.

d. Serangan Terhadap jaringan Wifi

Setiap device yang memiliki wireless adapter dapat membaca Wi-Fi yang ada di sekitar area nya [4]. Artinya Wi-Fi dapat dikatakan tidak aman apabila setiap orang dapat terkoneksi dalam jaringan tersebut hanya dengan menggunakan autentikasi berupa password. Masih ada celah pada sisi user dimana hal tersebut dapat dimanfaatkan hacker untuk masuk ke dalam Wi-Fi, dan mencuri data para pengguna yang terkoneksi ke jaringan tersebut [5]

Wifi menggunakan gelombang radio pada frekwensi milik umum yang bersifat bebas digunakan oleh semua kalangan dengan batasan batasan tertentu. Setiap wifi memiliki area jangkauan tertentu tergantung *power* dan antenna yang digunakan. Tidak mudah melakukan pembatasan area yang dijangkau pada wifi. Hal ini menyebabkan berbagai dimungkinan terjadi aktifitas aktifitas antara lain:

1) *Interception* atau penyadapan

Hal ini sangat mudah dilakukan, dan sudah tidak asing lagi bagi para hacker. Berbagai tools dengan mudah di peroleh di internet. Berbagai teknik kriptografi dapat di bongkaroleh tools tools tersebut.

2) *Injection*

Pada saat transmisi melalui radio, dimungkinkan dilakukan *injection* karena berbagai kelemahan pada cara kerja wifi dimana tidak ada proses validasi siapa yang sedang terhubung atau siapa yang memutuskan koneksi saat itu.

3) *Jamming*

Jamming sangat dimungkinkan terjadi, baik disengaja maupun tidak disengaja karena ketidaktahuan pengguna wireless tersebut. Pengaturan penggunaan kanal frekwensi merupakan keharusan agar jamming dapat di minimalisir. *Jamming* terjadi karena frekwensi yang digunakan cukup sempit sehingga penggunaan kembali channel sulit dilakukan pada area yang padat jaringan nirkabelnya.

4) *Locating Mobile Nodes*

Dengan berbagai software, setiap orang mampu melakukan *wireless site survey* dan mendapatkan informasi posisi letak setiap Wifi dan beragam konfigurasi masing masing. Hal ini dapat dilakukan dengan peralatan sederhana spt PDA atau laptop dengan di dukung GPS sebagai penanda posisi.

5) *Access Control*

Dalam membangun jaringan wireless perlu di design agar dapat memisahkan node atau host yang dapat dipercaya dan *host* yang tidak dapat dipercaya. Sehingga diperlukan *access control* yang baik

Langkah selanjutnya yaitu melakukan *injection test* menggunakan aireplay-ng

```
root@id:~# aireplay-ng -9 wlan0
15:50:52 Trying broadcast probe requests...
15:50:54 % Answer...
15:50:54 Found 1 AP

15:50:54 Trying directed probe requests...
15:58:54 EA:BB:A8:A4:9D:3D channel: 1 'pentest-ID'
15:58:54 Ping (min/avg/max): 1.218ms/2.535ms/8.418ms Power: 25.67
15:58:54 33/30: 100%

15:58:54 Injection is working
```

Gambar 6. *Injection test*

Maksud dari *Injection is working* adalah kepastian bahwa interface wireless siap di gunakan. Dan dengan otomatis aireplay akan melakukan probe ke AP yang dapat dideteksi dan masuk pada range scanner. Kemudian kita lanjutkan dengan mengumpulkan aliran data dari AP, kembali lagi dengan “airodump-ng” Kali ini lebih spesifik dengan bssid target AP dan opsi channel

```
root@id:~# airodump-ng -c 1 -b EA:BB:A8:A4:9D:3D -w wpadump wlan0
Notice: Channel range already given
```

Gambar 7. Aliran data AP direkam

keterangan:

c (channel AP yang di gunakan)

b (bssid target AP)

w (nama file hasil capturing yang akan disimpan dengan ekstensi *.cap)

wlan0 (interface wireless)

```
CH 1 | Elapsed: 52 s | 2014 07 31 16:24

BSSID          PWR RX0 Beacons #Data, #/s CH  WEP ENC CIPHER WITH BSSID
EA:DD:AB:A4:9D:3D -37 166      524      0  0  1  54e WPA TKIP PSK pentest-ID

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated) 60:02:04:00:41:56 -77  0 - 1  0      6
(not associated) 24:E2:71:5C:71:AC  89  0 - 1  0      1

root@id:~#
```

Gambar 8. Hasil capturing aliran data AP

Hasil perintah di atas pada gambar terlihat adanya client dengan BSSID 60:02:B4:03:41:56 dan 24:E2:71:5C:71:AC yang telah melakukan probe terhadap SSID target. Anda dapat menemukan informasi client yang terkoneksi dengan baik pada AP di kolom STATION pada output “airodump-ng”.

Tujuan sebenarnya adalah tercapainya WPA-handshake. mendapatkan key WPA tidaklah semudah WEP, karena key pada WPA tidaklah statik seperti pada WEP. Karena itu kemungkinan untuk menyerang WPA adalah dengan tehnik bruteforcing dan hal itu dapat terjadi jika adanya informasi “handshake” antara AP dan client legal berhasil di capture oleh hasil output *.cap airodump-ng. Untuk mendapatkan *handshake* kita harus mendiskonekan (deauthentication) *client* dari AP terlebih dahulu. Untuk itu

kita gunakan aireplay-ng. Perlu dicatat: karena alasan kondisi diatas, target AP harus memiliki client legal terlebih dahulu

Setelah WPA-Handshake tercapai, langkah selanjutnya yaitu Cracking WPA dapat dilakukan dengan metode *bruteforcing* yang memerlukan *password list* atau *wordlist dictionary*. Untuk mengumpulkan wordlist yang menyerang target tertentu dapat dilakukan metode Social Engineering, MITM, dll. Untuk cracking WPA berdasarkan hasil pengumpulan data dari “airodump-ng” yang terbentuk dengan file *.cap. Tools yang sangat terkenal digunakan melakukan serangan ini adalah CoWPAtty dan aircrack.

4. KESIMPULAN

WPA merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci WEP. Ada dua jenis yakni WPA personal (WPAPSK), dan WPARADIUS. Saat ini yang sudah dapat di crack adalah WPA-PSK, yakni dengan metode brute force attack secara offline. Brute force dengan menggunakan mencoba-banyak kata dari suatu kamus. Serangan ini akan berhasil jika passphrase yang digunakan wireless tersebut memang terapat pada kamus kata yang digunakan si hacker. Untuk mencegah adanya serangan terhadap keamanan wireless menggunakan WPA-PSK, gunakanlah passphrase yang cukup panjang (misal satu kalimat).

Wireless LAN yang aktif dengan konfigurasi default akan memudahkan para penyusup dapat memanfaatkan jaringan tersebut secara ilegal. Konfigurasi default dari tiap vendor perangkat wireless sebaiknya dirubah settingnya sehingga keamanan akses terhadap wifi tersebut lebih baik. Keamanan jaringan Wireless dapat ditingkatkan dengan cara:

- a. Mengganti nama dan password default pada perangkat access point
- b. mengaktifkan dan update fasilitas enkripsi
- c. Mengganti nama SSID
- d. Mengaktifkan MAC Address filtering
- e. Menonaktifkan fasilitas broadcast dari SSID
- f. Aktifkan pembatasan user
- g. Gunakan jika sedang ada keperluan sehingga keamanan lebih terjamin

Tata letak wireless dan pengaturan power/daya transmit sebuah Access Point juga dapat dilakukan untuk mengurangi resiko penyalahgunaan wireless. Pastikan area yang dijangkau hanya area yang memang digunakan oleh user. Untuk solusi keamanan wireless dapat menggunakan protokol yang sudah disediakan yakni WPA2Radius atau sering disebut RSN/802.11i.

3. Referensi

- [1] D. M. Sari *et al.*, “Analisis Sistem Keamanan Jaringan Wireless (Wep, Wpapsk/Wpa2psk) Mac Address, Menggunakan Metode Penetration Testing”, *semantik*, vol.3, no.2, pp. 203-208, 2017.
- [2] M. A. Rahmadani *et al.*, ”Implementasi Hacking Wireless dengan Kali Linux Menggunakan Kali Nethunter”, *Eproc*, vol.3, no.3, 2017
- [3] S. G. V. Vipin Poddar *et al.*, “Comparitive Analysis of Wireless Security Protocols (WEP and WPA2),” *Int. J. Ad Hoc Netw. Syst.*, vol. 4, no. 3, pp. 1–7, 2014
- [4] P. D. V. R. G. Vibhawari and V. Nanavare, “A Survey on Evil Twin Access Point Detection Technique,” *Int. J. Innov. Res. Comput. Commun. Eng.*, 2016.

- [5] C. Modi, V. Parekh, "Detection of Rogue Access Point to Prevent Evil Twin Attack in Wireless Network," *Int. J. Eng. Res. Technol.*, vol. 6, no. 4, pp. 23–27, 2014
- [6] M. G. H. Wibowo *et al.*, "Keamanan Jaringan Wlan Terhadap Serangan Wireless Hacking Pada Dinas Komunikasi & Informatika DIY" pada Prosiding sensei, 2017.