Vol 3 (2022) No 1

Jitsi Jurnal Ilmiah Teknologi Sistem Informasi

http://jurnal-itsi.org ISSN 2722-4619 (Print) ISSN 2722-4600 (Online)

Keamanan Jaringan Wireless Dengan Kali Linux

Fajar Setyawan[#], Rasyidah[#], Hidra Amnur[#]

[#] *Jurusan Teknologi Informasi, Politeknik Negeri Padang, Limau Manis, Padang, 25164, Indonesia*
E-mail: rasyidah@pnp.ac.id, hidraamnur@gmail.com

A B S T R A C T S

The development of wireless technology or wireless produces something interesting to discuss. Wireless technology is not always about how fast communication can be done. Security issues are very important to discuss, especially in an era that is all digital and all minimalist which no longer requires cables. Security needs to be considered to provide a sense of security when using a device connected to a Wi-Fi. For that, it is necessary to do a security analysis on a wifi. This analysis is carried out using the Penetration Testing method by carrying out attacks to find weaknesss in the Wi-Fi network security system. So, you will see the strength of the password on the Wi-Fi network. Security testing is also carried out on the communication path between clients and access points. So that from the results of this test it will be seen how safe the Wi-Fi network security system is.

K A T A K U N C I

Penetration testing,
wifi,
keamanan,
wpa2,
nirkabel,
serangan,
hijacking network,
bandwidth.

A B S T R A K

Perkembangan dari teknologi wireless atau nirkabel selalu menghasilkan sesuatu yang menarik untuk dibahas. Teknologi nirkabel tidak selalu membahas tentang seberapa cepat komunikasi yang dapat dilakukan. Masalah keamanan sangat penting untuk dibahas, terlebih dijaman yang serba digital dan serba minimalis yang tidak lagi membutuh kan kabel. Keamanan perlu diperhatikan untuk memberi rasa aman saat menggunakan perangkat yang terhubung kesebuah Wi-Fi. Untuk itu, perlu dilakukan analisa keamanan yang ada pada sebuah Wi-Fi. Analisa ini dilakukan menggunakan metode Penetration Testing dengan melakukan penyerangan untuk mencari celah dari sistem keamanan jaringan wifi. Sehingga, akan terlihat kekuatan dari kata sandi yang ada pada jaringan Wi-Fi. Pengujian keamanan juga dilakukan terhadap jalur komunikasi antar client dan access point. Sehingga dari hasil pengujian ini akan terlihat seberapa aman sistem keamanan jaringan Wi-Fi.

1. PENDAHULUAN

Jaringan Wi-Fi tidak harus membahas tentang seberapa kencang dalam berinternet, namun juga tentang keamanan. Keamanan jaringan merupakan keharusan yang utama karena sebuah jaringan Wi-Fi merupakan pintu gerbang pertama yang dilewati sebelum berselancar di internet. Jika factor keamanan tidak di perhatikan, ada saja permasalahan yang akan dihadapi sederhananya seperti orang asing dengan mudah nya menggunakan jaringan Wi-Fi yang bukan hak nya. Akibatnya, tagihan Wi-Fi seseorang akan membengkak tanpa dipakai sekalipun karena digunakan oleh orang yang tidak berhak. Contoh kasus lain adalah seseorang yang bisa mengambil data hanya dengan cara terhubung dalam jaringan Wi-Fi yang sama, terutama Wi-Fi public. Mungkin untuk penggunaan biasa tidak terlalu berdampak, tetapi beda cerita jika sudah memasuki lingkup perusahaan serta privasi.

Dari hasil penelitian tahun 2015 yang dilakukan oleh Siti Zaim, WPA2 masih memiliki kelemahan walaupun sudah terenkripsi dengan AES (Advanced Ecryption Standar). Namun karena mekanisme handshake, memiliki kelemahan pada preshared key, yang digunakan, maka dekripsi paket data yang ditransmisikan menjadi mudah dilakukan. Oleh sebab itu, kesadaran akan pentingnya keamanan informasi (security awareness) menjadi hal yang

wajib. Dengan adanya kesadaran akan pentingnya keamanan informasi maka setiap pihak dapat melindungi datanya terutama pada saat ditransmisikan pada jaringan internet berbasis wireless (Wi-Fi) meskipun menggunakan mode pengamanan WPA2.

Tahun 2017, Imam K, Muh. Yamin, dan LM Fid Aksara telah melakukan penelitian tentang keamanan jaringan WLAN dengan menggunakan metode Penetration Testing yang menghasilkan sebuah kesimpulan mode keamanan WPA2-PSK masih memiliki celah keamanan. Hal ini dibuktikan dengan hasil penelitian yang dilakukan bahwa dari empat jenis serangan yang dilakukan, hanya satu yang berstatus gagal yaitu pada jenis serangan cracking the encryption. Selain itu pada pengujian Attacking The Infrastructure dan Man In The Middle, jaringan WLAN belum bisa memberi keamanan kepada user yang terkoneksi agar tidak mendapatkan gangguan maupun penyadapan dari user lain pada saat mengakses layanan internet yang sama[1].

2. METODOLOGI PENELITIAN

Jaringan nirkabel atau biasa disebut jaringan wireless merupakan salah satu teknologi jaringan yang dimana media transmisi nya menggunakan frekuensi radio atau infrared untuk memberi sebuah koneksi jaringan keseluruh pengguna dalam area disekitarnya. Sebuah teknologi tentu bersanding dengan sebuah protocol, begitu juga dengan jaringan nirkabel. Jaringan nirkabel mempunyai protocol yang sangat populer yaitu keluarga IEEE 802.11 atau biasa disebut dengan Wi-Fi. Ada beberapa standar jaringan nirkabel yang dibuat oleh IEEE, yaitu[5] :

1. *802.11b*
   Disahkan oleh IEEE pada tanggal 16 September 1999, 802.11b mungkin adalah protokol jaringan nirkabel yang paling populer yang dipakai saat ini. Banyak alat – alat yang compatible dengan standar ini. 802.11b menggunakan modulasi yang dikenal sebagai Direct Sequence Spread Spectrum (DSSS) di bagian dari ISM band dari 2.400 sampai 2.495 GHz dan mempunyai kecepatan maximum 11 Mbps, dengan kecepatan sebenarnya yang bisa dipakai sampai 5 Mbps.
2. *802.11a*
   Saat standar 802.11b sedang dikembangkan, IEEE membuat ekstensi untuk standar 802.11 yang dinamakan 802.11a. Standar ini diciptakan pada saat yang bersamaan dengan standar 802.11b. Standar ini sudah mendukung bandwidth data mencapai 54 Mbps dan menggunakan frekuensi 5 GHz (semakin tinggi frekuensi maka semakin pendek jangkauan sinyal). Dikarenakan berjalan pada frekuensi yang bebeda dengan standar 802.11b, kedua teknologi ini tidak kompatible satu sama lain. Beberapa vendor menawarkan perangkat jaringan hybrid 802.11a/b. Namun perangkat tersebut hanya dapat menjalankan satu standar pada satu waktu
3. *802.11g*
   802.11g dapat dikatakan standar yang dikeluarkan terlambat oleh IEE karena hingga Juni 2003 masih belum di sah kan. Biarpun terlambat, 802.11g sekarang menjadi standar protokol jaringan nirkabel de facto karena sekarang, pada hakekatnya dipakai disemua laptop dan kebanyakan alat-alat lainnya. 802.11g memakai ISM band yang sama dengan 802.11b, tetapi memakai modulasi yang bernama Orthogonal Frequency Division Multiplexing (OFDM). Standar ini punya kecepatan maximum data 54Mbps (dengan throughput yang bisa dipakai sebesar 22 Mbps).
4. *802.11n*
   Dengan IEEE 802.11n maka lebar pita (bandwidth) dapat ditingkatkan dari 54 Mbit/s menjadi 600 Mbit/s. Lebar channel juga meningkat dari sebelumnya 20 Mhz menjadi 40 Mhz. Pada IEEE 802.11n ini ditambahkan dukungan terhadap MIMO (Multiple Input Multiple Output). dan frame aggregation. IEEE 802.11n dapat mencapai kecepatan 72 Mbit/s dengan pada single channel 20 MHz dengan satu antena. Kecepatan 72 Mbit/s ini share untuk semua workstation dan share untuk upload dan download. IEEE 802.11n dapat mencapai kecepatan 150Mbit/s dengan pada dua channel 20 MHz dengan satu antena. Penggunaan dua channel 20 MHz ini disebut 40 MHz mode. Penggunaan 40 MHz mode dengan 4 antena bisa menghasilkan 4x150Mb/s atau bandwidth 600 Mb/s. IEEE 802.11n dapat berjalan pada frekuensi 2,4 GHz atau 5 GHz. Pada frekuensi 2,4 GHz ada kemungkinan interferensi dengan peralatan lain seperti microwave dan bluetooth.
5. *802.11ac*
   Merupakan generasi terbaru dari standar Wifi yang populer digunakan. Memanfaatkan teknologi wireless dual band mendukung koneksi secara bersamaan pada frekuensi 2,4 GHz dan 5 GHz. Menawarkan kompabilitas dengan standar 802.11b/g/n serta mendukung bandwidth mencapai 1300Mbps pada frekuensi 5 GHz ditambah 450Mbps pada frekuensi 2,4 GHz.
6. *802.11ax*
   Standar ini merupakan generasi terbaru yang disebut dengna Wi-Fi 6. Kehadiran generasi ini membawa performa yang lebih baik dari versi terdahulu, Wi-Fi 5 (802.11ac), yang saat ini masih banyak digunakan di sejumlah perangkat. Wi-Fi Alliance mengklaim Wi-Fi 6 mempunyai kemampuan data rate 9,6 Gbps, 40 persen lebih kencang ketimbang Wi-Fi 5 yang hanya mampu mencapai 6,9 Gbps untuk pengguna tunggal. Hal ini dikarenakan Wi-Fi 6 menggunakan 1024-Quadrature Amplitude Modulation (1024 QAM) dan

peningkatan frekuensi hingga 160 MHz yang membuat perangkat dapat menangkap sinyal dengan lebih luas[6].

Sebuah jaringan Wi-Fi biasanya menggunakan suatu mode keamanan yang berfungsi untuk mengamankan jaringan dari orang orang yang tidak bertanggung jawab. Beberapa keamanan Wi-Fi yang diketahui adalah[7] :

1. WEP (Wired Equivalent Privacy)
   Ini merupakan tipe keamanan jaringan wireless yang pertama kali digunakan untuk enkripsi Wi-Fi. Wired Equivalent Privacy (WEP) bekerja menggunakan kunci yang dimasukkan oleh administrator ke access point. Antara kunci yang diberikan access point ke klien dengan yang dimasukkan klien untuk otentifikasi ke access point, keduanya harus sama. Idealnya, standar yang digunakan WEP adalah 802.11b. Namun, karena merupakan tipe keamanan jaringan wireless pertama, sistem keamanannya bisa dikatakan masih lemah. Namun, WEP tetap dipilih banyak orang karena sudah memenuhi standar 802.11b yang mencakup exportable, reasonably strong, reasonably strong, self-synchronizing, optional, dan cpmputationally efficient.
2. WPA (Wi-Fi Protected Access)
   WPA Diciptakan untuk melengkapi keamanan pada WEP, Wi-Fi Protected Access (WPA) menerapkan kunci keamanan statik dengan memanfaatkan Temporal Key Integrity Protocol (TKIP). Memiliki kemampuan untuk berubah secara dinamis, protokol TKIP menggunakan kunci utama sebagai starting point yang berubah secara reguler. Dengan begini, tidak ada kunci enkripsi yang bisa digunakan dua kali. Umumnya, WPA hadir dalam dua tipe, yaitu WPA biasa dan WPA2. Karena merupakan pembaruan dari WEP, WPA biasanya masih menggunakan enkripsi yang sama dengan WEP, yaitu RC4. Sedangkan, standar yang digunakan oleh keamanan jaringan wireless satu ini adalah 802.11i.
3. WPA2
   WPA2 merupakan keamanan jaringan wireless hasil upgrade dari WPA biasa. WPA2 terbagi lagi menjadi dua jenis, yaitu WPA2 personal dan WPA2 enterprise. Disebut juga dengan WPA2 Pre-Shared Key (PSK), WPA2 personal ditujukan untuk pengguna jaringan kecil, misalnya penggunaan jaringan Wi-Fi di rumah. Sayangnya, kelemahan WPA2 PSK justru seringnya disebabkan oleh administratornya sendiri. Masih banyak orang menggunakan password Wi-Fi yang mudah ditebak dan diretas, misalnya angka 1-5 atau tanggal lahir. Sedangkan, WPA2 enterprise ditujukan untuk jaringan yang cenderung lebih besar, contohnya perusahaan. Karena sifatnya ini, penggunaan WPA2 enterprise biasanya mengharuskan pengguna untuk memakai akun yang sudah terintegrasi oleh sistem perusahaan.

Rancangan jaringan yang akan dibangun terdiri dari 1 (satu) unit wireless router, dan 2 (dua) unit laptop. Semua perangkat terhubung satu sama lain. Wireless Router yang digunakan untuk simulasi pengujian kali ini menggunakan mode WISP (Wireless Internet Service Provider). Mode ini dapat menerima sekaligus memancarkan sinyal Wi-Fi untuk digunakan perangkat dibawah nya.Dalam melakukan pengujian keamanan jaringan wireless, ada beberapa macam serangan yang dapat dilakukan, salah satu nya yaitu bruteforce. Serangan bruteforce dilakukan dengan memasukan berbagai macam kemungkinan. Penyerang juga terlebih dahulu capturing dari traffic yang telah di targetkan dengan melakukan handshaking ke user atau pengguna dari suatu access point. Adapun perangkat lunak yang digunakan dalam simulasi pengujian kali ini sebagai berikut.

1. aircrack-ng – Untuk Crack WEP dan WPA dengan menggunakan Dictionary attack keys.
2. airmon-ng – Menempatkan jaringan WiFi pada monitoring mode.
3. aireplay-ng – Berguna untuk melakukan packet injector
4. airodump-ng – Berguna untuk melakukan packet sniffing. Ditempatkan pada lalu lintas data PCAP atau IVS files dan menunjukkan informasi tentang jaringan.

Aircrack-ng adalah berbagai kumpulan aplikasi yang berguna untuk menilai dan mengukur tingkat keamanan pada jaringan WiFi. Aircrack bekerja pada jaringan WiFi yang mendukung monitoring mode dan bisa mendeteksi trafik jaringan dari 802.11a, 802.11b and 802.11g. Aircrack-ng berfokus pada keamanan WIFI yang berbeda[11]:

1. Pemantauan: Packet capture dan ekspor data ke file teks untuk diproses lebih lanjut oleh aplikasi pihak ketiga.
2. Menyerang: Serangan ulang, deauthentication, membuat akses point palsu dan melalui via injeksi paket.
3. Pengujian: Memeriksa kartu WiFi dan kemampuan driver (capture and injection).
4. Cracking: Cracking pada WEP dan WPA PSK (WPA 1 dan 2).

Skenario yang digunakan dalam simulasi penyerangkan dengan menyerang diantara lalu lintas dari access point dan target. Kemudian mengumpulkan atau capturing packet data yang telah di monitor dari pergerakan traffic dari access point dan target hingga terasa cukup. Packet tersebut yang telah di kumpulkan akan digunakan untuk melakukan pencarian kata sandi atau password dari wordlist yang berisi kemungkinan kata sandi yang ada. Wordlist yang disediakan memiliki kriteriakata – kata yang berbeda, sehingga akan terlihat perbedaan waktu dalam mendapatkan kata yang dicari. Beberapa kriteria yang disiapkan, sebagai berikut :

1. Pertama, dengan menggunakan kata sandi yang terbilang lemah, dengan kriteria :
   a. Tanpa symbol
   b. Tanpa huruf kapital
   c. Menggunakan angka diakhir
2. Kedua, dengan menggunakan kata sandi yang terbilang cukup, dengan kriteria :
   a. Tanpa symbol
   b. Dengan huruf capital diawal
   c. Dengan angka diakhir
3. Ketiga, dengan menggunakan kata sangat yang terbilang kuat, dengan kriteria :
   a. Dengan symbol
   b. Dengan huruf capital
   c. Dengan angka diawal / tengah / akhir.

3. HASIL DAN PEMBAHASAN

Pada access point, dikonfigurasikan Wi-Fi menggunakan PC User untuk kemudian yang akan dijadikan target dalam pengujian. Pada user dilakukan implementasi dengan mengakses website untuk melihat kecepatan internet yaitu Ookla Speedtest dan website hi.ru yang rentan untuk dilakukan pengujian pada user.

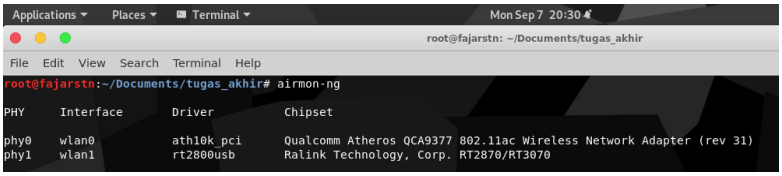
Pengujian dilakukan dengan melakukan serangan Bruteforce, yaitu serangan yang dilakukan dengan mencoba segala kemungkinan kata sandi. Ada beberapa macam metode serangan ini, dan yang akan dipakai dalam simulasi pengujian kali ini adalah metode dictionary attack, yaitu dengan manfaatkan beberapa wordlist yang berisi kata – kata yang mungkin menjadi kata sandi sebuah jaringan Wi-Fi. Rincian serangan ini seperti tabel 1.

TABEL 1. Rincian Serangan Bruteforce

Target MAC	D8:32:14:5E:49:A0
Target SSID	target_wifi
Security Mode	WPA2
Tools	airmon-ng, airodump-ng, aireplay-ng, aircrack-ng

Langkah pertama adalah mengatur NIC ke status monitor mode. Perintah yang digunakan untuk melihat NIC yang tersedia adalah

```
root@fajarstn$ airmon-ng
```

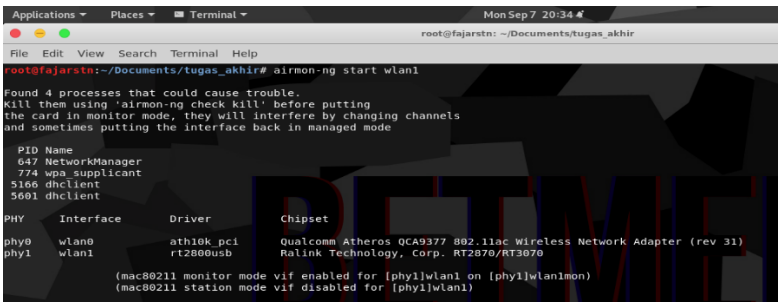


GAMBAR 1. NIC yang tersedia

Disini akan digunakan NIC yang memiliki interface wlan1 dengan chipset Ralink Tech, Corp

Kemudian, mengubah mode untuk wlan1 dari manged mode menjadi monitor mode. Perintah yang digunakan adalah

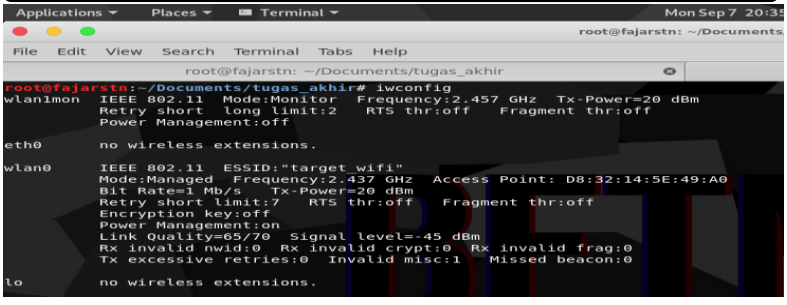
```
root@fajarstn$ airmon-ng start wlan1
```



GAMBAR 2. Merubah wlan1 ke monitor mode

Wlan1 akan berganti nama menjadi wlan1mon, yang menandakan jika perubahan dari managed mode ke monitor mode telah dilakukan. Untuk melakukan pengecekan interface, digunakan perintah

```
root@fajarstn$ iwconfig
```

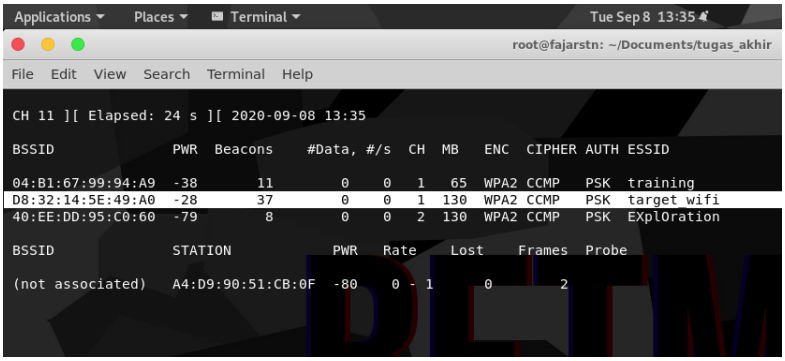


GAMBAR 3. Wlan1 menjadi wlan1mon

Langkah selanjutnya adalah melihat SSID yang tersedia disekitar dengan menggunakan tools airodump-ng perintah

```
root@fajarstn$ airodump-ng wlan1mon
```

Kemudian akan terbuka jendela yang menampilkan informasi tentang SSID yang tersedia



GAMBAR 4. Target pada hasil airodump-ng

Selanjutnya adalah proses dumpingpada SSID target dengan menggunakan perintah

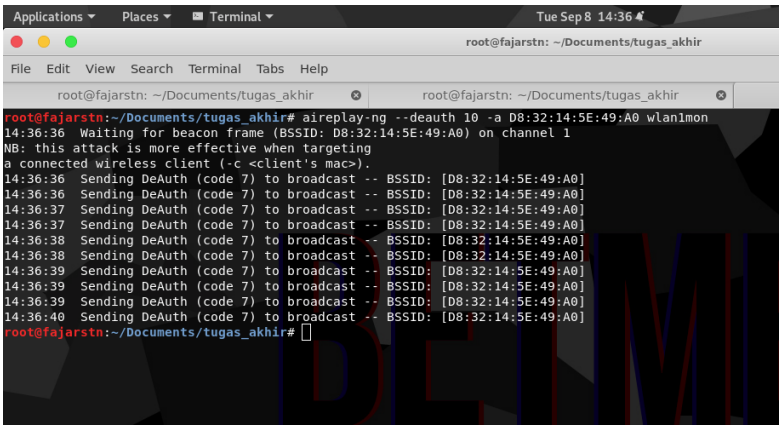
```
root@fajarstn$ airodump-g -c 1 --bssid D8:32:14:5E:49:A0 -w hasil wlan1mon
```

Nomor 1 adalah nomor dari channel SSID target yang terlihat pada gambar 4, sedangkan D8:32:14:5E:49:A0 adalah MAC address access point dari target. Dari proses ini akan menyimpan output file capture yang diberi nama 'hasil' sebagai file yang menyimpan data dari proses capturing traffic SSID target dan akan digunakan untuk melakukan proses cracking password

Proses Selanjutnya deauthentication untuk mendapatkan handshake ke access point target. Proses deauth menggunakan tools aireplay-ng dan menargetkan ke station yang terhubung dengan access point target. Perintah :

```
root@fajarstn$ aireplay-ng --deauth 10 D8:32:14:5E:49:A0 wlan1mon
```

Angka 10 adalah jumlah pesan yang akan di kirimkan ke user.

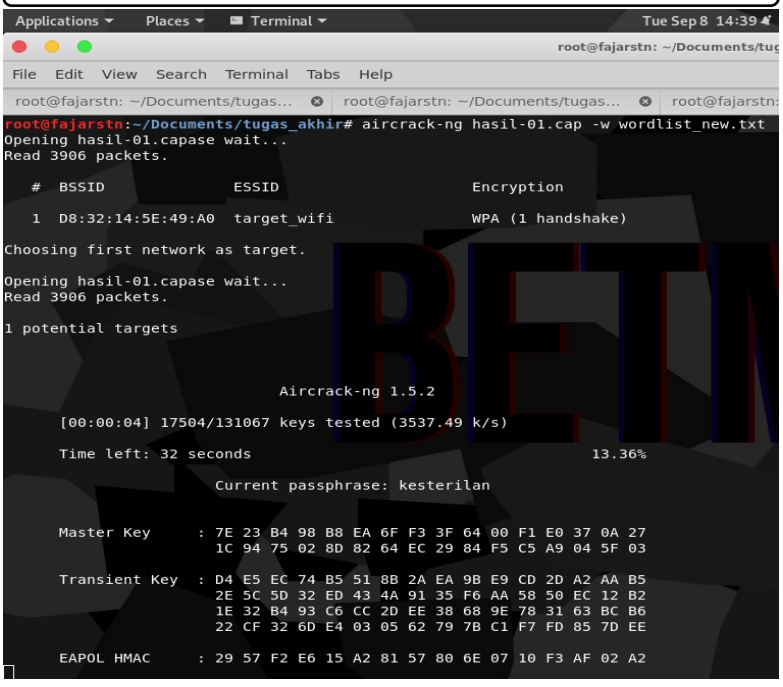


GAMBAR 5. Proses deauth ke user

langkah terakhir, yaitu melakukan cracking password. Setelah sebelum nya disiapkan beberapa wordlist , berisi berbagai macam kata kata yang kemungkinan menjadi kata sandi dari SSID yang menjadi target. Tools yang digunakan adalah aircrack-ng dengan perintah

```
root@fajarstn$ aircrack-ng hasil-01.cap -w wordlist_new.txt
```

File 'hasil-01.cap' adalah file hasil dari proses capturing traffic dilangkah 4 dan wordlist_new.txt merupakan file txt yang berisi wordlist atau kata kata yang kemungkinan menjadi kata sandi dari SSID target



GAMBAR 6. Proses cracking password menggunakan aircrack-ng

Pengujian yang dilakukan:

1. *Pemblokiran Akses Internet*
2. *Pembatasan Bandwidth*
3. *Penyadapan (ARP Spoofing / Man In The Middle Attack)*

Dari beberapa pengujian menggunakan metode penetration testing yang dilakukan 3 serangan, yaitu 1 serangan (bruteforce) ke access point dan 2 (hijacking network dan arp spoofing) serangan ke user. Secara keseluruhan, implementasi pengujian dapat dilihat pada tabel 2. Dan Serangan bruteforce yang dilakukan terhadap access point dilakukan dengan 3 kriteria password dengan hasil dapat dilihat pada tabel 3.

TABEL 2. Hasil Pengujian

Serangan	Informasi Yang Diperlukan	Status
Bruteforce	*Wordlist*, *Handshake* user yang terhubung ke access point, Channel dan BSSID dari access point target	Berhasil
Hijacking Network (Pemblokiran internet)	IP Address Target yang terhubung dalam jaringan yang sama dengan penyerang.	Berhasil
Hijacking Network (Pembatasan Bandwidth)	IP Address Target yang terhubung dalam jaringan yang sama dengan penyerang.	Berhasil

TABEL 3. Hasil Serangan Bruteforce

Password	Kriteria	Status (Waktu)
doaibu300	Lemah, tidak menggunakan symbol, tidak menggunakan huruf kapital.	Berhasil (27 Detik)
Doaibu300	Cukup, tidak menggunakan simbol, menggunakan huruf kapital dan angka.	Berhasil (1 Menit 20 Detik)
Doa!&u300	Kuat, menggunakan simbol, huruf kapital, dan angka.	Berhasil (2 Menit 30 Detik)

Dari tabel 3, dapat dilihat perbedaan password yang diberikan berdasarkan kriteria yang telah dimiliki. Perbedaan kriteria yang digunakan berpengaruh besar terhadap kuat atau tidak nya password yang digunakan sehingga perbedaan waktu untuk proses cracking password menjadi lebih lama. Walaupun access point sudah menggunakan mode keamanan WPA2 yang merupakan mode keamanan wireless yang terbaru, ternyata belum cukup aman karena masih bisa di lakukan cracking password terhadap kata sandi yang digunakan.

Keberhasilan penyerangan berdampak besar terhadap user atau klien yang terhubung ke jaringan yang lemah tersebut. Penyerang dapat melakukan serangan lanjutan setelah berada dalam jaringan yang sama dengan user target. Penyerang dapat mencuri data – data sensitif seperti username dan password user yang mengakses suatu website dengan melakukan serangan ARP Spoofing, terlebih jika website yang diakses tidak memiliki protocol keamanan yang kuat.

Penetration Testing yang dilakukan dalam menguji keamanan sebuah jaringan telah berhasil dilakukan dengan sukses nya dalam proses cracking password yang hasilnya password yang digunakan tidak begitu aman. Pengunaan berbagai karakter dalam sebuah kata sandi atau password menjadi sangat penting, dilihat dari rentang waktu yang didapat dalam melakukan Penetration Testing untuk proses cracking password. Lemah nya keamanan yang dimiliki oleh sebuah jaringan Wi-Fi berdampak besar terhadap pengguna yang terhubung dalam jaringan tersebut. Dibuktikan dengan berhasil nya melakukan Penetration Testing dalam mencuri data / informasi sensitive milik user.

4. KESIMPULAN

Pengujian keamanan jaringan Wi-Fi dengan Penetration Testing berhasil dilakukan. Pengujian serangan terhadap user dengan melancarkan serangan ARP Spoofing dan Hijacking Network berhasil dilakukan. Dari 3 kriteria kata sandi yang digunakan, semuanya berhasil di crack. Ini menandakan kata sandi tersebut belum aman. Pada serangan Hijacking network yaitu melakukan pemblokiran akses internet dan melakukan pembatasan bandwidth, serangan berhasil dilakukan dengan hasil user tidak dapat mengakses internet dan user mengalami penurunan kecepatan internet. Seabiknya Menggunakan tools penetration testing lain seperti airgeddon dengan versi terbaru dan lebih efisien serta tidak memakan waktu yang lama.

REFERENSI

[1] Bayu, I. K., Yamin, M., & Aksara, L. F. (2017). Analisa Keamanan Jaringan WLAN Dengan Metode Penetration Testing (Studi Kasus : Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO). semanTIK, 69-78.

[2] Pujiarto, B., Utami, E., & Sudarmawan. (2013). EVALUASI KEAMANAN WIRELESS LOCAL AREA NETWORK MENGGUNAKAN METODE PENETRATION TESTING (KASUS : UNIVERSITAS MUHAMMADIYAH MAGELANG). Jurnal DASI, 16-20.

[3] Wang, S.-L., Wang, J., & Pan, Z.-P. (2016). Wireless Network Penetration Testing and Security Auditing. EDP Sciences, 5.

[4] Zaim, S. (2015). APAKAH WPA/WPA2 BENAR-BENAR AMAN? DEKRIPSI PAKET DATA TERENKRIPSI PADA WPA/WPA2. Seminar Nasional Informatika (SEMNASIF), 268-276.

[5] Mulyanta, Edi. (2005). Pengenalan Protokol Jaringan Wireless Komputer. Yogyakarta : ANDI OFFSET

[6] Nusanet, A. (2016, 5 6). Standar Protokol Jaringan Wireless IEEE 802.11. NUSANET : https://www.nusa.net.id/blog/article/standar-protokol-jaringan- wireless-ieee-802-11/ [14 Agustus 2020]

[7] Abdullah, Suhendra. (2007). Jaringan Wireless di Dunia Berkembang Edisi ke Dua. Jakarta : Hacker Friendly LLC Media.

[8] Samudro, A. (2020, 1 14). Perbedaan WiFi 6 dan WiFi 6E yang Menjanjika Koneksi Lebih Cepat. TIRTO.ID : https://tirto.id/perbedaan-wifi-6-dan-wifi-6e-yang-menjanjikan-koneksi-lebih-cepat-erPZ [14 Agustus 2020]

[9] Edge-Cyber. (2019, 12 2). Ini Dia 4 Tipe Keamanan Jaringan Wireless yang Mesti Diketahui. E.D.G.E : https://edge-cyber.com/tipe-keamanan-jaringan-wireless [12 Agustus 2020]

[10] Arifin, Zaenal. (2007). Mengenal Jaringan Wireless LAN (WLAN). Pekanbaru : Andi Publisher.

[11] Singh, Hardeep. (2017). Kali Linux Wireless Penetration Testing and Security – From Beginner to a Wifi Penetration Testing Ninja. New Delhi : Rootsh3ll.

[12] Feradhita. (2019, 7 17). Metode Pentest: Black-Box, Grey-Box, dan White-Box Testing. LOGIQUE Blog: https://www.logique.co.id/blog/2019/07/17/metode- pentest/ [14 Agustus 2020]

[13] Anonimity. (2018). Module 16 - Hacking Wireless Network. California : Certified Ethical Hacking.

[14] Purbo, Onno W. (2016). Belajar Attacking. Pekanbaru : Penerbit Andi.

[15] Feradhita. (2020, 2 12). Apa Itu Brute Force? Apa Saja Metode yang Digunakan?. LOGIQUE Blog. https://www.logique.co.id/blog/2020/02/12/apa-itu-brute- force/ [19 Agustus 2020]

[16] Anon. (2018, 2 6). Pengertian Aircrack-ng dan Fungsinya. IMMERSALAB : https://www.immersa-lab.com/pengertian-aircrack-ng-dan-fungsinya.htm [12 Agustus 2020]