JURNAL LITEK : Jurnal Listrik Telekomunikasi Elektronika, Vol. 19, No. 1, Maret 2022, pp. 8~12
pISSN: 1693-8097; eISSN: 2549-8762

ANALISIS NETWORK SECURITY PADA LAYANAN WIFI INDIHOME TERHADAP SERANGAN DENIAL OF SERVICE (DOS)

Ahmad Yusuf Faiz Azmi[1], Jafaruddin Gusti A G[2], Eka Wahyudi[3]

[1,2,3]Fakultas Teknik Telekomunikasi dan Elektro, Institut Teknologi Telkom Purwokerto
Email: 18101002@ittelkom-pwt.ac.id[1], jafaruddin@ittelkom-pwt.ac.id[2], ekawahyudi@ittelkom-pwt.ac.id[3]

Abstrak – Teknologi yang semakin pesat diiringi dengan peningkatan peradaban manusia menyebabkan persaingan yang ketat. Indihome merupakan salah satu produk layanan dari Telkom Group berupa paket layanan yang terpadu dalam satu paket *triple play* meliputi layanan komunikasi, data, dan *entertainment* seperti telepon rumah dan internet (*Internet on Fiber atau High Speed Internet*). Namun disisi lain, terdapat *hacker* yang bertujuan untuk merusak akses koneksi antara pengguna hingga mengalami *down* atau tidak dapat diakses. Teknik serangan *hacker* untuk menyerang wifi korban hingga menjadi *down* adalah dengan menggunakan teknik penyerangan *Denial of Service* (DOS). Sehingga ketika pengguna menyambungkan lagi koneksinya dengan *wifi* pasti akan diputuskan lagi. Hal ini dapat membahayakan kepada keamanan lalu lintas data para pengguna jaringan *wifi*. Tujuan dari penelitian ini adalah memberikan solusi dengan cara meningkatkan keamanan jaringan dari serangan DoS. Pengamanan ditingkatkan dengan cara meng-*update* keamanan jaringan dari *router*. Hasil dari penelitian ini adalah jaringan aman dari gangguan ancaman DoS *attack* dengan menggunakan metode *deauth attack* dari *software* Kali Linux.

Kata-kata kunci: Denial of Service (DOS), Wifi, Indihome, Kali Linux

Abstract – Technology that is growing rapidly accompanied by an increase in human civilization causes intense competition. Indihome is one of the service products from the Telkom Group in the form of an integrated service package in one triple play package covering communication, data, and entertainment services such as phone and internet (Internet on Fiber or High Internet Speed). But on the other hand, there are hackers who aim to damage the connection access between the user until it is down or inaccessible. Hacker attack technique to attack the victim's wifi until it becomes down is to use Denial of Service (DOS) attack techniques. So that when the user reconnects the connection with wifi, it will definitely be disconnected again. This can endanger the security of data traffic for wifi network users. The purpose of this research is to provide a solution by increasing network security from DoS attacks. Security is increased by updating the network security of the router. The result of this research is a secure network from DoS attack threats by using the deauth attack method from the Kali Linux software.

Key words: Denial of Service (DOS), Wifi, Indihome, Kali Linux

I. PENDAHULUAN

Perkembangan teknologi jaringan komputer memudahkan orang untuk memenuhi kebutuhan informasi. Salah satu teknologi yang berkembang pesat adalah teknologi media transmisi nirkabel atau *wireless* [1]. Media transmisi nirkabel merupakan sebuah gelombang radio yang dapat dipancarkan ke semua tempat area yang dapat dijangkau oleh gelombang radio tersebut. Namun beberapa vendor telah menyediakan fitur-fitur yang dapat memudahkan pengguna maupun administrator jaringan untuk menggunakannya, sehingga sering ditemukan pengguna jaringan menggunakan konfigurasi default dari vendor. Oleh karena itu, para *hacker* telah melakukan aksinya untuk menguji kemampuannya. Mereka dapat terhubung dalam satu jaringan yang sama dan mengambil data pengguna lainnya secara ilegal [2].

Namun para *hacker* telah melancarkan aksinya di tempat umum seperti cafe, mall, dan warung. Karena dari sebagian pengguna rata-rata tidak peduli dengan keamanan komunikasi data di tempat *public*, maka dari itu *hacker* dapat melakukan uji coba ilegal ini melalui jaringan *wireless* yang terhubung ke *hacker* [3]. Dibanding dengan menggunakan jaringan kabel atau LAN, jaringan *wireless* lebih rentan dan mudah masuk kedalam jaringan *wireless* yang tersedia. Cukup dengan mendapatkan password *wifi* sudah dapat terhubung ke jaringan yang ditarget oleh *hacker* [4].

Penelitian ini dilakukan dalam 3 tahap. Tahap pertama menggunakan *software* dari Kali linux. *Software* tersebut memiliki berbagai macam *tools hacking* yang tersedia. Tahap kedua menggunakan tools *airodump-ng*, fungsinya untuk mengetahui keberadaan target *wifi* melalui *Basic Service Set Identifier* (BSSID), *Mac Address* dan *frame channel* yang akan diserang. Tahap terakhir, *wifi* target dapat diserang dengan ancaman *Denial of Service* (DoS), yaitu dengan cara menggunakan *tools aireplay-ng deauth*. Dari serangan ini akan mengakibatkan pengguna terputus dengan *wifi* yang sudah disambung. Jika pengguna menyambungkan

lagi koneksinya dengan *wifi* pasti akan diputuskan lagi. Hal ini dapat membahayakan keamanan lalu lintas data para pengguna jaringan *wifi* sehingga diperlukan peningkatan keamanan yang baik untuk dapat mencegah atau menangani serangan DoS.

II. METODOLOGI

A. Tahapan Penelitian

Dalam perencanaan keamanan jaringan pada *wifi* indihome, maka diperlukan beberapa proses pengerjaan agar penelitian dapat berjalan dengan baik. Proses pengerjaan seperti diperlihatkan pada Gambar 1.

Gbr. 1 Flow Chart Penelitian

Penelitian dilakukan dalam beberapa tahapan proses pengerjaan, yaitu:

1. Mengidentifikasi masalah dengan cara studi literatur dan pengamatan yang berhubungan dengan penelitian, yaitu bagaimana mengamankan jaringan *wifi*.
2. Mengumpulkan informasi terkait konfigurasi jaringan *wireless* yang terpasang di area target, yang meliputi tempat, BSSID, dan *Mac Address* yang digunakan.
3. Menyiapkan *hardware* dan *software* yang akan digunakan untuk penelitian.
4. Melakukan sebuah percobaan penyerangan DoS dengan metode penyerangan *deauthentication*.
5. Menganalisa hasil data penyerangan untuk mengetahui tingkat keamanan yang diterapkan dalam jaringan yang terpasang, serta solusi yang akan diterapkan.

B. Ilustrasi Sistem yang Berjalan

Ilustrasi sistem yang berjalan seperti diperlihatkan pada Gambar 2. Sistem keamanan jaringan yang digunakan masih kurang efektif dan efisien dalam mensimulasikan tingkat keamanan pada jaringan internet. Pada sistem keamanan masih terdapat celah yang dapat disusupi oleh pihak-pihak yang tidak memiliki wewenang.

Gbr. 2 Ilustrasi Sistem yang Berjalan

C. Analisis Sistem yang diterapkan

Analisis sistem yang diterapkan yaitu mengidentifikasi dari celah keamanan jaringan pada *wifi* indihome dengan *tools aireplay-ng. Deauthentication attack* untuk mengaudit keamanan jaringan dan memblokir lalu lintas jaringan yang diakui sebagai ancaman dalam jaringan internet serta melakukan beberapa pengecekan terhadap kesalahan pada bagian dari media, *wireless*, dan media koneksinya.

D. Pengaturan Konfigurasi Sistem

Pada pengaturan sistem yang telah dibuat dari topologi dengan menggunakan satu buah pc sebagai pengguna, satu buah *router* akses jaringan *wifi* yang telah disediakan oleh indihome, dan satu buah laptop sebagai *attacker*.

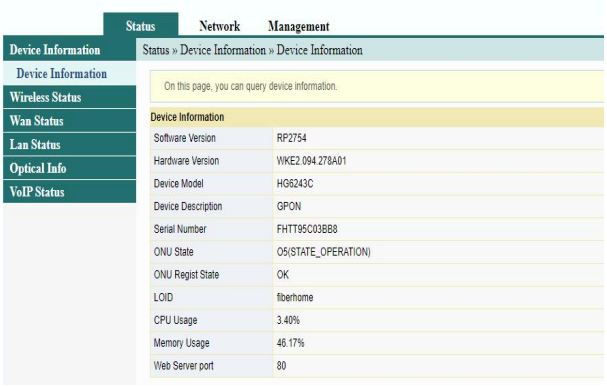
Konfigurasi *router* indihome (*router fiberhome*) dilakukan dengan langkah-langkah sebagai berikut:

1. Login ke *router*

Login ke *router* dilakukan dengan memasukkan IP 192.168.1.1 pada URL *browser*, dan menekan tombol enter pada *keyboard*. Selanjutnya akan tampil halaman *login* seperti pada Gambar 3 dibawah ini. Gunakan *username* "user" dan *password* "user1234".

Gbr. 3 Tampilan Login Awal Web *Router* Fiberhome

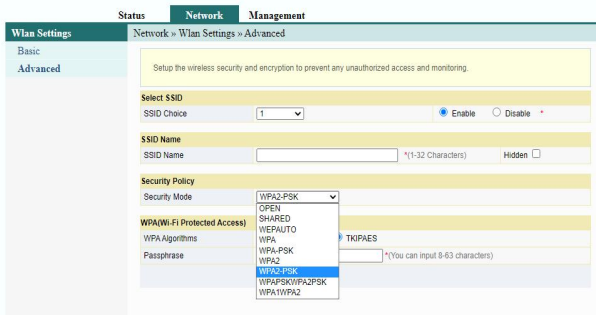
Selanjutnya akan tampil menu awal web *router*, seperti diperlihatkan pada Gambar 4. Pada tampilan tersebut terdapat beberapa menu status yang berfungsi untuk mengetahui info yang ada di dalam *router*, menu *network*, dan menu *management*.



Gbr. 4 Tampilan Menu Awal Masuk Web Router Fiberhome

2. Memilih Menu *Network*

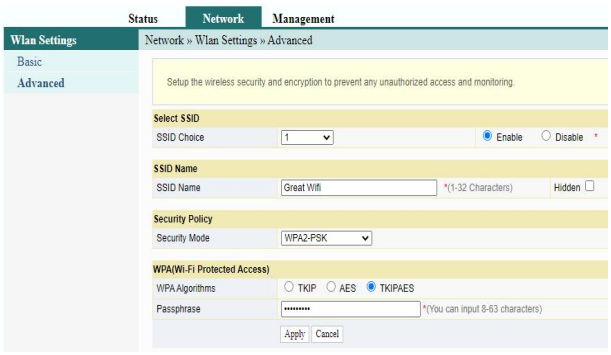
Menu *network* dipilih untuk mengetahui pengaturan *wifi* yang digunakan sebelumnya. Pada Gambar 5 dapat dilihat bahwa masih banyak pengaturan yang masih kosong dan perlu diisi, seperti SSID *name* dan *Security Mode*.



Gbr. 5 Tampilan Jenis Pilihan pada *Security Mode*

3. Mengatur Menu *Network Advanced*

User SSID diisi dengan "*Great Wifi*", *security mode* dipilih WPA2-PSK, WPA *algorithms* dipilih TKIPAES, dan mengisi *passphrase* seperti pada tampilan Gambar 6. Kemudian memilih *apply* supaya sistem memperbarui konfigurasi jaringan.



Gbr. 6 Tampilan Menu *Network Advanced*

WPA2-PSK (Wi-Fi *Protected Access* II) dipilih karena *wifi* tersebut akan diimplementasikan untuk jaringan publik. Protokol WPA2 lebih aman jika dibandingkan dengan WPA dan WEP. Untuk itu keamanan WPA2 menjadi lebih *recommended* digunakan untuk umum. Enkripsi menggunakan TKIPAES lalu pada pengisian *passphrase* diisi dengan minimal kata kunci adalah 8 karakter, yang terdiri dari huruf dan angka yang cukup layak dan cukup kuat digunakan sebagai *password*. Setelah itu, ketika jaringan router sudah selesai dikonfigurasi, jaringan akan dipakai sebagai pengujian untuk penyerangan DoS *Attack*.

III. HASIL DAN PEMBAHASAN

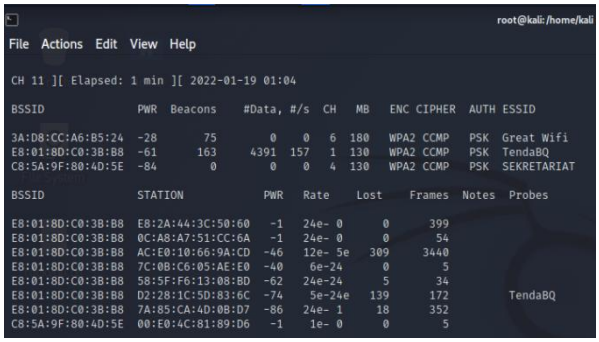
A. Hasil

Analisis dibagi menjadi dua tahap, yaitu mengidentifikasi jaringan *wifi* target menggunakan *airodump-ng*, dan proses peretasan DoS pada *wifi* target menggunakan *tools aireplay-ng deauthentication*.

1. Mengidentifikasi *Wifi*

Pada metode *filtering* target *wifi* dilakukan untuk mengetahui parameter yang diambil dari BSSID, *Frame Channel*, enkripsi, dan SSID yang ada pada indihome. Identifikasi pada jaringan *wifi* menggunakan *tools airodump-ng*. Analisis dilakukan untuk melakukan uji coba penyadapan jaringan guna mendapatkan koneksi dari jaringan *wifi* yang ada. Dari hasil identifikasi *wifi*, diketahui bahwa *wifi* yang telah diretas menggunakan metode *deauth attack.* Dengan demikian, pada *wifi* tersebut lalu lintasnya menjadi tidak aman dan terganggu.

Pada Gambar 7 dapat dilihat bahwa semua jaringan *wifi* area sekitar telah ditampilkan. Pada tampilan tersebut terdapat 3 *wifi* sekaligus, dan mendapatkan berbagai informasi dari BSSID, enkripsi serta *frame channel* yang digunakan. Langkah selanjutnya adalah fokus terhadap satu target, yaitu dari BSSID "*Great Wifi*" yang akan di-*capture.*



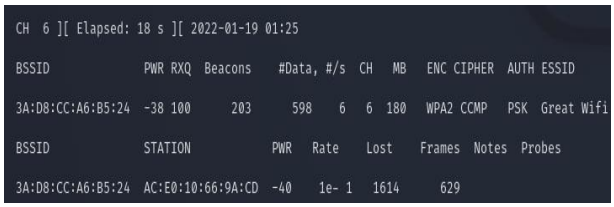
Gbr.7 Tampilan Hasil *Filtering Wifi* pada *Tools Airodump-ng*

2. *Capturing Wifi* Target

Capturing wifi target dilakukan dengan menjalankan *software* Kali linux serta menggunakan *tools airodump-ng* untuk menampilkan informasi tentang keberadaan

wifi target dengan lengkap, yaitu informasi BSSID, *Frame Channel*, enkripsi, dan SSID yang digunakan.

Capturing wifi target menggunakan data *script wifi* target, yaitu dari SSID "*Great Wifi*". Berikut isi penjelasan perintah dari *script*-nya: "airodump-ng [nama tools] -c6 [sebuah nomor channel] -w [nama file capturing] -d bssid [nomor bssid wifi target] wlan0 [port wlan interface yang digunakan]". Hasil *capturing wifi* target seperti diperlihatkan pada Gambar 8.



Gbr. 8 Tampilan Isi *Capturing Wifi* Target

Hasil *capturing wifi* target dapat digunakan untuk memonitor informasi dari *wifi* target. Mac *address* perangkat yang terhubung ke AP target akan ditampilkan. Dari informasi SSID "*Great Wifi*" terlihat bahwa ada 1 *client* yang terhubung dengan AP. Langkah selanjutnya adalah menjalankan *tools aireplay-ng deauth* yang berdampak pada *client* atau *user* dapat gagal terhubung.

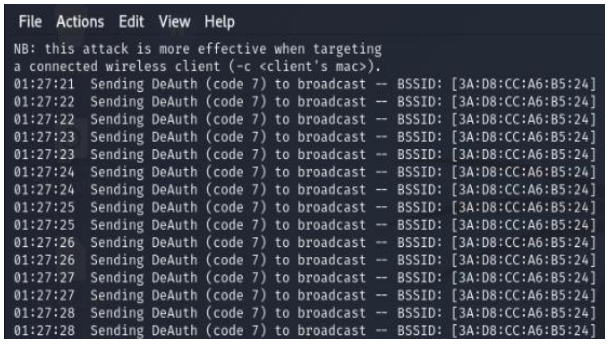
3. DoS *Attack Deauthentication*

Jaringan *wifi* dapat mengalami serangan DoS yang menargetkan *client* dan *wifi* target. Serangan semacam ini dapat dilakukan dengan mengirimkan paket serangan *deauthentication* terus menerus.

Penjelasan dari script di atas adalah sebagai berikut:

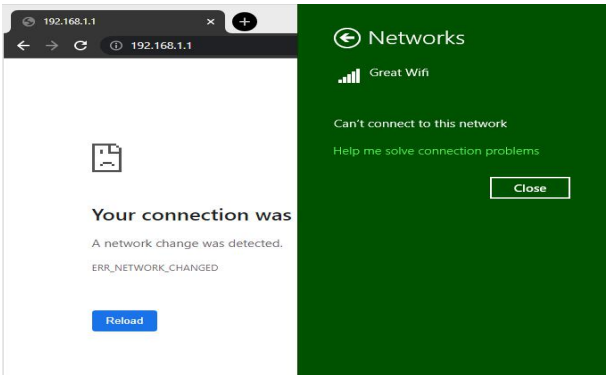
a. *aireplay-ng* : Nama *tools* yang digunakan pada terminal.
b. *–deauth* : Sebuah metode penyerangan.
c. 0 : berarti serangan *deauthentication*
d. -d 3A:D8:CC:A6:B5:24 : Nomor BSSID *wifi* target yang akan diserang
e. wlan0 : Port kartu jaringan *wireless* lan yang digunakan.

Gambar 9 adalah tampilan *output script* dari "aireplay-ng --deauth 0 -a 3A:D8:CC:A6:B5:24 wlan0.



Gbr. 9 Tampilan Paket Serangan DoS

Pada Gambar 9 dapat dilihat bahwa penyerangan DoS dengan metode *deauth attack* behasil diluncurkan. Angka "01:27:21 – 01:27:29" adalah waktu peluncuran paket serangan DoS, sedangkan untuk *output* "Sending DeAuth to broadcast BSSID : [3A:D8:CC:A6:B5:24]" adalah peluncuran paket DoS pada BSSID *wifi* target. Hasil penyerangan ini menyebabkan *client* atau *user* yang terhubung *wifi* otomatis juga disconnected, seperti diperlihatkan pada Gambar 10.



Gbr. 10 *Wifi* Disconnected ketika Serangan DoS diluncurkan

B. Pembahasan

Berdasarkan informasi di atas, dapat dilihat bahwa jaringan *wireless router* indihome tersebut masih memiliki kemungkinan untuk diserang menggunakan DoS *attack* menggunakan metode *deauthentication*. Berikut adalah alasannya:

1. *Wireless router* indihome masih menggunakan enkripsi WPA2-PSK. Pada kasus enkripsi ini, ketika sebuah *client* melakukan koneksi ke *wifi,* akan terjadi proses *handshake* dengan melakukan *brute force* (memaksa login secara berulang-ulang) menggunakan sebuah *wordlist*.txt. Di sisi lain, penyerang dapat menerapkan metode *deauthentication*.
2. *Wireless router* indihome menggunakan *fiberhome* seri HG6243C. Untuk jaringan nirkabelnya masih menggunakan protokol tipe *frame* IEEE 802.11n-2009 yang merupakan sebuah perubahan standar jaringan *wireless* 802.11-2.007 IEEE seperti 802.11 b/g. Penggunaan protokol ini masih rawan terkena serangan DoS dan juga masih umum diimplementasikan di *router* saat ini.

Rekomendasi solusi pencegahan dari DOS attack ini adalah adalah sebagai berikut:

1. Meng-*update* Enkripsi ke WPA3-PSK

Enkripsi WPA3-PSK membuat peningkatan keamanan lebih lanjut yang mempersulit pembobolan jaringan dengan menebak kata sandi. Meskipun penyerang mendapatkan kunci enkripsi lalu lintas, sulit untuk menghitung penggunaan lalu lintas data yang dikirimkan dengan WPA3-*Personal*. SAE memberikan manfaat kerahasiaan terkini dan keamanan data yang lebih banyak melalui jaringan terbuka.

WPA3-PSK juga menyediakan bingkai manajemen terlindungi (PMF) untuk menghindari penyadapan dari area publik. Setelah diuji, pemakaian enkripsi WPA3-PSK pada jaringan *wifi* tidak dapat ditembus oleh serangan DoS *deauthentication*.

2. *Update* Jaringan ke 802.11w

Pemakaian protokol 802.11w pada jaringan *wifi* memberikan peningkatan keamanan pada lapisan *Media Access Control* (MAC). Protokol struktur standar ini merupakan sistem untuk mengendalikan integritas data, keaslian dari sisi sumbernya, larangan membuat dan penyalinan yang tidak berwenang, serta kerahasiaan data dan cara perlindungan lainnya.

Standar protokol ini memperkenalkan perlindungan fitur dari bingkai manajemen dan langkah-langkah keamanan tambahan yang memungkinkan menetralisir dari serangan eksternal, seperti mencegah terkena ancaman serangan dari DoS, dan juga sudah memiliki fitur *Wireless Intrusion Prevention System* (WIPS). WIPS dapat membantu melindungi dari ancaman keamanan *wireless* lain yang sepenuhnya berada di luar cakupan 802.11w.

IV. KESIMPULAN

Berdasarkan dari analisis data dan percobaan serangan DoS yang dilakukan, maka dapat diambil kesimpulan bahwa pemakaian *security mode*/enkripsi WPA2-PSK, serta tipe jaringan protokol IEEE 802.11w, masih dapat ditembus oleh DoS *deauthentication*. Sistem keamanan *wifi indihome* tidak dapat ditembus oleh serangan DoS *deauthentication* dengan cara:

1. meng-*update security mode*/enkripsi yang digunakan pada *wifi* indihome, dari WPA2-PSK menjadi WPA3-PSK, dan
2. meng-*update* tipe jaringan yang digunakan, dari protokol IEEE 802.11n ke protokol IEEE 802.11w.

REFERENSI

[1] Sabdho, H. D., & Ulfa, M. (2018). Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing pada Kantor PT. Mora Telematika Indonesia Regional Palembang. *Prosiding Semhavok*, *1*(1), 15-24.

[2] Fauzi, A. R. F., & Suartana, I. M. (2018). Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing dengan Menggunakan IDS. *Jurnal Manajemen Informatika*, *8*(2), 11-17.

[3] Samsumar, L. D., & Gunawan, K. (2017). Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless LAN); Studi Kasus di Kampus STMIK Mataram. *Jurnal Ilmiah Teknologi Infomasi Terapan*, *4*(1), 73-82.

[4] Amarudin, A., & Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo*, *12*(2), 72-75.