Analisis keamanan jarinGAN PADA WIRELESS HOME ROUTER TERHADAP SERANGAN ... untuk meningkatkan keamanan

Skripsi diajukan untuk memenuhi salah satu syarat memperoleh gelar

Sarjana Komputer

Program Studi Teknik Informatika

Oleh

Deny Lukman Syarif

4611419046

Jurusan ilmu komputer

fakultas matematika dan ilmu pengetahuan alam

universitas negeri semarang

2022

Abstrak

daftar isi

Halaman Judul i

Abstrak ii

Daftar Isi iii

Bab 1. Pendahuluan 1

1.1. Latar Belakang 1

1.2. Identifikasi Masalah 2

BAB 1

PENDAHULUAN

1. 1.1. Latar Belakang

Jaringan *wireless* adalah sebuah jaringan nirkabel yang tidak membutuhkan media fisik seperti kabel untuk bertukar informasi dari *device* satu ke yang lain. Semua *wireless devices* beroperasi pada gelombang elektromagnetik sebagai medium/perantaranya. Dengan adanya koneksi tanpa harus terhubung menggukan kabel, jaringan *wireless* sangat memberikan manfaat dalam segi mobilitas yang tinggi dan mengurangi biaya penggunaan. Akan tetapi dalam segi keamaan pada jaringan *wireless* lebih rentan adanya serangan daripada jaringan *wired.* Karena pada jaringan *wireless* hanya menggunakan gelombang elektromagnetik tanpa harus memerlukan *peripheral* seperti kabel untuk bisa tersambung ke jaringan. Sedangkan pada jaringan *wired* harus memerlukan kabel agar bisa tersambung ke dalam jaringan.

Sebuah pertukaran informasi atau data melalui jaringan antara perangkat melalui tahapan *encapsulation* di setiap layer yang nantinya akan dibawa dari perangkat satu ke yang lainnya. Pada saat proses data sedang ditransmit, sebuah paket data dapat saja diubah atau dicuri di tengah perjalanan menuju *destination* oleh *hacker.* Dengan adanya kemajuan teknologi sekarang ini, banyak sekali *tools* yang sudah ada dan dapat digunakan oleh *hacker.* Bahkan orang awam pun yang tidak mempunyai skill atau pengetahuan di bidang *security* pun bisa menggunakannya. Dilihat dari perkembangan *tools* dari tahun 1985-2015 semakin kesini *tools* kecanggihan semakin meningkat dibandingkan pengetahuan secara teknikal untuk dapat menggunakannya.

*Wireless hacking tools* dapat dengan mudahnya dicari di internet dan diinstall pada sistem operasi seperti Aircrack-ng yang dapat digunakan untuk mendeteksi kelemahan keamanan. Dengan *tools* ini dapat digunakan untuk *monitoring*, *cracking*, *attacking,* dan *testing.* Kegunaan-kegunaan ini dapat digunakan dalam dua sisi untuk mengetahui celah keamanan dan untuk meningkatkan keamanannya, tapi dapat juga digunakan untuk memanfaatkan celah keamanan tersebut untuk hal-hal yang tidak seharusnya.

*Wireless home router* di dalamnya sudah terdapat *access point, switch,* dan *router.* Semua proses dari pemberian IP ke perangkat, proses *routing* ke internet, proses *switching*, mengatur *Quality of Services,* dll semua dilakukan pada satu perangkat yaitu *Wireless home router.* Dengan adanya serangan terhadap *Wireless Home Router* melalui *monitoring* proses komunikasi dalam jaringan menggunakan *tools* yang ada, *hacker* dapat melakukan berbagai serangan ke jaringan tersebut jika keamanan pada *Wireless Home Router* tidak diperhatikan.

Berdasarkan uraian di atas, penulis tertarik untuk mempelajari cara untuk mengamankan suatu jaringan.Oleh karena itu, penulis mengambil bahan mengenai keamanan jaringan internet untuk judul skripsi “Analisis Keamanan Jaringan Pada Wireless Home Router Terhadap Serangan ... untuk Meningkatkan Keamanan”

1. 1.2. Identifikasi Masalah
2. 1.3. Rumusan Masalah

Berdasarkan latar belakang masalah dan hubungan pemilihan judul tersebut, maka penulis merumuskan inti permasalahan yaitu menganalisis keamanan dari jaringan *wirelesss home router* yang biasanya digunakan di perumahan-perumahan tanpa pengetahuan di bidang jaringan.

1. 1.4. Batasan Masalah

Dalam pembuatan skripsi ini, penulis membatasi masalah yang akan dianalisis yaitu:

1. Penggunaan *tools* Aircrack-ng dan *Wireshark* untuk menganalisa keamanan jaringan di perumahan yang menggunakan jaringan *wireless.*
2. Penulis melakukan analisa serangan ke beberapa *mode security* pada jaringan *wireless* untuk mengetahui perbedaan hasil serangan.
3. Penulis hanya memberikan solusi yang sebaiknya digunakan untuk mengantisipasi terjadinya serangan seperti yang dilakukan penulis.
4. 1.5. Tujuan Penelitian

Tujuan yang hendak dicapai penulis dalam penelitian ini adalah untuk menganalisa keamanan dari jaringan *wireless home router* di perumahan dari serangan dan bagaimana solusi untuk mengantisipasinya.

1. 1.6. Manfaat Penelitian

Penelitian ini bermanfaat untuk, antara lain:

1. Sebagai pengetahuan untuk umum khususnya yang di rumahnya menggunakan jaringan *wireless home router* terhadap bahaya jaringan *wireless* tanpa pengamanan.
2. Sebagai data yang bisa dijadikan referensi dalam konfigurasi *wireless home router* untuk mengamankan jaringan lebih baik.

BAB 2

Tinjauan pustaka

2.1. Telaah Penelitian

Pada penelitian sebelumnya yang berjudul Detection of Wireless Fake Access Points oleh Norbert Lovinger (2020), jaringan *wireless* sudah menjadi bagian dari keseharian yang digunakan untuk melakukan berbagai aktivitas seperti bekerja, menonton hiburan, mencari informasi, dan sebagainya. Namun masih banyak individu yang kurang perhatian dengan keamanan jaringan *wireless* yang digunakannya. Hal ini memicu terjadinya ancaman serangan dengan menjadikan jaringan *wireless* sebagai media untuk melancarkan serangan oleh si *attacker.* Dengan menggunakan *wireless fake access point* jika pengguna kurang berhati-hati saat akan menggunakan jaringan *wireless* akan sangat mudah menjadi korban.

Penelitian lain yang dijadikan referensi adalah penelitian Ryan VanSickle (2019) dengan judul Effectiveness of Tools in Identifying Rogue Access Points on a Wireless Network. Isi dari penelitiannya adalah dengan adanya *wireless access point* yang dengan mudahnya digunakan untuk koneksi ke internet, namun seringkali kurang dalam konfigurasi keamanannya. *Attacker* dapat saja membuat *rogue access point (RAP)* menggunakan perangkat lain untuk mengakali *user* agar terhubung dengan *access point* yang palsu. Dengan adanya *tools* seperti Aircrack-ng, Kismet, dan inSSIDer dapat dengan mudahnya mengidentifikasi mana *access point* yang asli dan yang palsu.

Penelitian lain yang juga dijadikan acuan adalah penelitian Michael Kyei Kissi (2020) dengan judul Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools. Isi dari penelitiannya adalah penggunaan jaringan *wireless* yang tingkat fleksibilitas dan mobilitasnya yang tinggi sudah digunakan di beragam organisasi seperti bandara, restoran, hotel, dan sebagainya. Dengan banyaknya perangkat yang terhubung dengan jaringan *wireless,* komunikasi atau informasi akan dikirim dan diterima melewati sinyal elektromagnetik. Sehingga *attacker* dapat dengan mudahnya untuk melakukan *sniffing* dan *capture data packets*. Pada penelitian ini ditujukan untuk melakukan *testing* untuk melakukan serangan dengan menggunakan Kali Linux dan *Aircrack-ng tools.* Berbeda dengan penelitian sebelumnya, dimana Aircrack-ng digunakan untuk mengidentifikasi *rogue access point (RAP),* di penelitian ini Aircrack-ng digunakan untuk melakukan serangan pada jaringan *wireless.*

2.2. Landasan Teori

2.2.1.

bab 3

metode penelitian

3.1 Waktu dan Tempat Penelitian

Penelitian akan dilaksanakan setelah

daftar Referensi

Aircrack Home Page. 2022. “AIRCRACK-NG”, ([http://aircrackng.com](http://aircrackng.com/))

Kissi, Michael. 2020. Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools. Diakses pada tanggal 5 April 2022

Lovinger, Norbert. 2020. Detection of wireless fake access points. Diakses pada tanggal 4 April 2022

VanSickle, Ryan. 2019. Effectiveness of Tools in Identifying Rogue Access Points on a Wireless Network. Diakses pada tanggal 4 April 2022