ANALISIS KEAMANAN JARINGAN PADA WIRELESS HOME ROUTER TERHADAP SERANGAN WIRELESS 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

HALAMAN PENGESAHAN

DAFTAR ISI

BAB 1

PENDAHULUAN

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"

1.2 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.

1.3 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.

1.4 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.

1.5 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. Konsep Jaringan Wireless

Jaringan *wireless* merupakan salah satu model yang digunakan dalam jaringan komputer yang menghubungkan sekumpulan komputer dengan menggunakan media udara atau gelombang elegtromagnetik sebagai jalur lintas dari data komunikasi. Konsep dari jaringan *wireless* mirip dengan jaringan *Local Area Network (LAN),* perbedaannya hanyalah media yang digunakan untuk jalur lintas data.

Penggunaan jaringan *wireless* tentunya akan lebih meningkatkan mobilitas karena tidak memerlukan kabel agar perangkat dapat terhubung ke dalam jaringan. Pengguna dapat dengan leluasa menggunakan perangkatnya untuk berkomunikasi dalam jaringan tanpa harus menambah biaya untuk menggunakan kabel yang lebih panjang.

Protokol yang digunakan dalam jaringan *wireless* didasari pada IEEE 802.11. Ada tingkatan protokol 802.11 yang digunakan sesuai dengan kegunaannya. Terdapat 3 standard yang biasa digunakan yaitu 802.11b, 802.11g, dan 802.11n. Ketiga jenis ini bekerja pada frekuensi 2.4 GHz dan dapat digunakan sekaligus dalam satu protokol 802.11b/g/n.

2.2.2. Komponen Jaringan Wireless

Dalam jaringan wireless dibutuhkan beberapa komponen yang saling berkaitan agar sebuah jaringan dapat berjalan, antara lain:

a) Access Point

Access Point berfungsi sebagai konverter sinyal radio menjadi sinyal digital yang akan diteruskan ke perangkat WLAN lain. Dengan kata lain access point digunakan untuk menghubungkan perangkat ke *Internet Service Provider (ISP)* agar dapat terhubung dalam jaringan.

b) Wireless LAN Interface

Alat ini digunakan perangkat untuk dapat terhubung ke Access Point. Di beberapa laptop sudah terdapat WLAN Interface Card di dalamnya. Namun juga ada perangkat yang belum terdapat WLAN interface dan dapat menggunakan Wireless Adapter USB.

2.2.3 Jenis Keamanan Jaringan Wireless

Dalam jaringan wireless data dikirim dan diterima melalui gelombang udara. Oleh karena itu sebuah data akan sangat rentan dibaca oleh *attacker,* karena data dikirim bebas melalui udara tanpa adanya keamanan tertentu. Ada beberapa tipe keamanan yang dapat diterapkan dalam konfigurasinya, yaitu:

a) Open System Authentication

Tipe keamanan ini mengijinkan perangkat dapat menggunakan jaringan secara bebas tanpa perlu adanya autentikasi secara khusus.

b) Wired Equivalent Privacy (WEP)

Original 802.11 menggunakan enkripsi Rivest Chiper 4 (RC4) dengan *static key* dan kunci tidak pernah berubah ketika melakukan pertukaran paket, sehingga akan lebih mudah diretas.

c) Wi-Fi Protected Access (WPA-PSK)

WPA masih menggunakan standard WEP, namun dalam proses enkripsi menggunakan algoritma Temporal Key Integrity Protocol (TKIP). Algoritma ini mengubah kunci pada setiap paket, sehingga akan lebih sulit untuk diretas.

d) Wi-Fi Protected Access 2 (WPA2-PSK)

WPA2 menjadi standar saat ini untuk mengamankan jaringan *wireless.* Algoritma enkripsi yang digunakan adalah Advanced Encryption Standard (AES).

Jenis WPA/WPA2 terdapat dua tipe yaitu personal dan enterprise. WPA/WPA2-Enterprise digunakan pada Remote Authentication Dial-In User Service (RADIUS) untuk autentikasi pada jaringan wireless yang menggunakan protokol 802.1X pada server. Sedangkan pada penelitian ini akan fokus pada WPA/WPA2-Personal yang digunakan pada *home* atau *small office network* yang menggunakan Pre-Shared Key (PSK) untuk autentikasi password antara *client* dan *wireless router.*

2.2.4 Wireless Home Router

Pengguna rumahan biasanya menggunakan wireless home router untuk menghubungkan ke jaringan *wireless*. Perangkat *end-device* ini di dalamnya sudah terdapat komponen-komponen yang diperlukan untuk terbentuknya jaringan *wireles*. Proses pengalamatan, *routing, switching, authentication, Quality of Services (QoS), Mac Filtering, dll* sudah ada dalam perangkat kecil ini. Karena satu perangkat ini bekerja sebagai *Access Point, Switch,* dan *Router*, yang umumnya ketiga perangkat tersebut bekerja secara terpisah di masing-masing perangkatnya.

Cara Kerja dari Wireless Home Router ini adalah dengan meng-*advertise beacon* yang berisi *Shared Service set Identifier (SSID)* untuk menginfokan bahwa perangkat ini menyediakan pelayanan wireless. SSID ini biasa

dikenal oleh orang sebagai nama dari WiFi. Lalu perangkat yang mempunyai WLAN NIC akan men-*discover* SSID dan melakukan autentikasi untuk mendapatkan akses ke jaringan lokal dan internet.

2.2.5 Ancaman Keamanan Jaringan Wireless

Kenyamanan penggunaan pada jaringan *wireless* ini yang dapat menghubungkan perangkat ke internet tanpa harus tersambung dengan kabel dan jangkauannya yang cukup luas memang sangat membantu aktivitas dalam berbagai hal. Namun tentu yang namanya teknologi dimana itu merupakan ciptaan manusia, dan tidak mungkin sebuah teknologi dapat berjalan dengan sempurna, pasti tetap ada celah walaupun sedikit saja. Kekurangan ini dapat timbul dari berbagai sisi, seperti dari sistemnya dan konfigurasi oleh pengguna. Celah inilah yang mungkin dimanfaatkan oleh *attacker* untuk menjalankan aksinya. Beberapa serangan yang menjadi ancaman dalam jaringan wireless, antara lain:

a) Traffic Monitoring

Seorang *hacker* ataupun orang biasa dapat dengan mudahnya melakukan serangan ini dengan menggunakan *tools* yang ada di internet seperti Aircrack-ng, AirMagnet dan AiroPeek. Serangan ini bersifat pasif, karena *attacker* tidak perlu melakukan apapun secara fisik terhadap sasaran. Si *attacker* cukup berada di area *wireless* LAN tersebut. *Attacker* dapat memonitor semua transaksi yang berjalan pada jaringan *wireless* tersebut. Jika pada jaringan *wireless* tersebut tidak memerhatikan konfigurasi keamanan data seperti melakukan enkripsi, maka data-data yang bersifat *credential* seperti *username, password, id card,* dan sebagainya dapat dengan mudah didapatkan oleh *attacker.*

b) Unauthorized Access

Sebuah jaringan komputer seperti di rumah merupakan jaringan yang bersifat *private.* Mungkin saja di jaringan tersebut terdapat sebuah server yang digunakan untuk penyimpanan hal-hal terkait pekerjaan. Akan berbahaya jika ada orang lain yang tidak berhak mengakses di jaringan tersebut. Jika ada orang lain yang menggunakan jaringan tanpa sepengetahuan si pemilik, hal ini dapat menimbulkan berbagai macam masalah, misalnya *attacker* membuat authorized access tidak dapat terhubung ke internet, mencuri informasi di server, dan sebagainya. Hal ini tentu berkaitan dengan konfigurasi pada *wireless home router.*

c) Man-in-The-Middle Attack

Penggunaan enkripsi dan autentikasi dapat meningkatkan keamanan pada jaringan wireless. Namun, *smart hacker* masih dapat mencari kelemahan yang ada. Serangan ini menempatkan *attacker* di antara *user* dengan *access point.* Saat user yang sudah terautentikasi melakukan *request* ke *access point, attacker* akan menangkap *frame* tersebut dan mengubah *MAC Address* pada *user* menjadi *MAC Address* si *attacker,* sehingga ketika *access point* me-*replay request* tersebut, *frame* akan diterima oleh *attacker.* Karena *frame* akan dikirim dengan melihat *MAC Address*-nya.

d) Denial of Service

Serangan ini sering dikenal sebagai DoS attack yang mempunyai tujuan untuk membuat sibuk jaringan komputer atau perangkat lain tidak befungsi sebagaimana mestinya. Salah satu serangan dari DoS ini adalah *brute-force* dengan mengirimkan paket yang besar secara terus menerus dan menghabiskan sumber daya pada jaringan sasaran, dan memaksanya untuk *shut-down*. Hal ini dapat dilakukan dengan *tools* pada Aircrack-ng seperti De-Authenticate.

BAB 3

METODE PENELITIAN

3.1 Waktu dan Tempat Penelitian

Penelitian ini akan dilaksanakan pada bulan Agustus 2022 – Desember 2022 di Kecamatan Suruh, Kabupaten Semarang.

3.2 Bahan dan Alat Penelitian

Dalam penelitian ini bahan penelitian berdasarkan dari teori dasar keamanan jaringan wireless yang diambil dari berbagai sumber seperti artikel, jurnal, dan materi Studi Independen di Course Cisco Certification Network Associate (CCNA). Untuk spesifikasi alat yang digunakan pada penelitian ini adalah sebagai berikut:

1. Kebutuhan perangkat keras dan sistem operasi, antara lain:

   a) Laptop HP 14ck0011TU, *Processor dual-core* 1,6 GHz, RAM 8 GB

   b) Notebook Acer Aspire One HAPPY2-N57C, *Processor dual-core* 1,6 GHz, RAM 2 GB (sebagai *client)*

   c) Smartphone VIVO Y55, Android Marshmallow 6.0, RAM 2 GB (sebagai *client)*

   d) TP-LINK Wireless Adapter USB 802.11b/g/n 300 Mbps

   e) Sistem Operasi Windows 7 Ultimate

   f) Sistem Operasi Mabox (Manjaro Openbox) Linux

2. Kebutuhan perangkat lunak.

   a) Software Terminator (sebagai terminal)

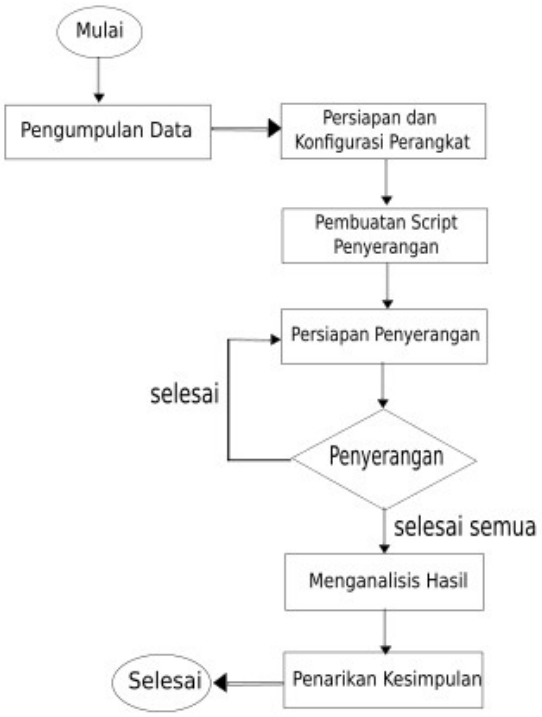
   b) Software VIM (sebagai teks editor)

   c) Tools Aircrack-ng (sebagai alat utama melakukan serangan)

   d) Software Wireshark (untuk melihat hasil monitoring)

3.3 Kerangka Pemikiran dan Flowchart

Dalam menjelaskan sebuah permasalahan kerangka pemikiran atau alur penelitian disajikan dalam bentuk flowchart untuk mempermudah pemahaman dalam penelitian tersebut. Berikut flowchart dari alur penelitian yang akan dilakukan:



Gambar 3.1. Flowchart Alur Penelitian

3.4 Tahapan Instalasi dan Konfigurasi Software

1. Instalasi Terminator pada Mabox Linux

   - Buka Terminal dengan menggunakan Ctrl + T

   - Update package dengan “sudo pacman -Syu”

   - Setelah update selesai, install Terminator dengan “sudo pacman -S terminator”

   - Tunggu hingga proses installasi selesai

2. Instalasi Vim

   - Ketikkan “sudo pacman -S vim”, lalu tekan enter pada terminal

   - Tunggu hingga proses instalasi selesai

3. Instalasi Aircrack-ng

   - Ketikkan “sudo pacman -S aircrack-ng”, lalu tekan enter pada terminal

   - Tunggu hingga proses instalasi selesai

4. Instalasi Wireshark

- Ketikkan “sudo pacman -S wireshark”, lalu tekan enter pada terminal

- Tunggu hingga proses instalasi selesai

DAFTAR REFERENSI

Aircrack Home Page. (2022). AIRCRACK-NG. Diakses pada 6 April 2022, dari http://aircrackng.com

Jaringan Wireless. (2020). Jaringan Wireless : Pengertian, Cara Kerja, Tipe, Kelebihan Dan Kekurangannya. Diakses pada 9 April 2022, dari https://teks.co.id/jaringan-wireless/

Kissi, Michael Kyei & Asante, Michael. (2020). Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools. *International Journal of Computer Applications,* 176(32)*,* 975 – 8887. Diakses pada tanggal 5 April 2022

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

eTutorial.org. 2018. Security Threats. Diakses pada 10 April 2022, dari https://etutorials.org/Networking/wn/Chapter+8.+Wireless+Network+Security+Protecting+Information+Resources/Security+Threats/

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