ANALISIS METODE FLUXION MENGGUNAKAN WI-FI DEAUTHER UNTUK UJI KEAMANAN WPA2 PADA PERANGKAT ROUTER WIRELESS TOTOLINK N300RT

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Untuk Memperoleh
Gelar Sarjana TeknikPada Fakultas Teknik
Universitas Islam Riau

OLEH :

RAFITA MANDASARI
143510130

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS ISLAM RIAU

PEKANBARU

2021

LEMBAR PENGESAHAN PEMBIMBING SKRIPSI

Nama : Rafita Mandasari

Npm : 143510130

Fakultas : Teknik

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata 1 (S1)

Judul Skrisi : Analisis Metode Fluxion Menggunakan Wi-Fi Deauther Untuk Uji Keamanan Wpa2 Pada Perangkat Router Wireless Totolink N300RT".

Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam skripsi ini telah dipelajari dan dinilai relatif telah memenuhi ketentuan-ketentuan dan kriteria-kriteria dalam penulisan metode ilmiah. Oleh karena itu, skripsi ini layak di setujui untuk disidangkan dalam ujian komprehenshif.

Pekanbaru, 10 Februari 2021

Disahkan Oleh

Ketua Prodi Teknik Informatika	Dosen Pembimbing
Dr. Apri Siswanto S.Kom., M.Kom	Dr. Apri Siswanto S.Kom., M.Kom

LEMBAR PENGESAHAN

TIM PENGUJI UJIAN SKRIPSI

Nama : Rafita Mandasari

NPM : 143510130

Fakultas : Teknik

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata 1 (S1)

Judul Skrisi : Analisis Metode Fluxion Menggunakan Wi-Fi Deauther Untuk Uji Keamanan WPA2 Pada Perangkat Router Wireless Totolink N300RT".

Skripsi Ini Secara Keseluruhan Dinilai Telah Memenuhi Ketentuan-Ketentuan Dan Kaidah-Kaidah Dalam Penulisan Penelitian Ilmiah Serta Telah Di Uji Dan Dapat Di Pertahankan Di Tahap Penguji. Oleh Karena Itu, Tim Penguji Ujian Skripsi Fekultas Teknik Universitas Islam Riau Menyatakan Bahwa Mahasiswa Yang Bersangkutan Dinyatakan **Telah Lulus Mengikuti Ujian Komprehenship Tanggal 17 Desember 2021** Dan Setujui Serta Di Terima Untuk Memenuhi Salah Satu Syarat Guna Memperoleh Gelar Serjana Strata Satu Bidang Ilmu **Teknik Informatika**.

Pekanbaru, 17 Desembar 2021

Tim Penguji

1. Dr. Ir. Evizal Abdul Kadir, M. Eng Sebagai Tim Penguji I (.....)
2. Rizdqi Akbar Ramadhan, S.Kom., M.Kom., CHFI Sebagai Tim Penguji II (.....)

Disahkan oleh

Ketua prodi teknik informatika	dosen pembimbing
Dr. Apri siswanto S.Kom., M.kom	Dr. Apri siswanto S.Kom., M.kom

LEMBAR PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini:

Nama	: Rafita Mandasari
Tempat/Tgl Lahir	: Subarak, 25 Maret 1996
Alamat	: Subarak

Adalah mahasiswa Universitas Islam Riau yang terdaftar pada:

Fakultas	: Teknik
Jurusan	: Teknik Informatika
Program Studi	: Teknik Informatika
Jenjang Pendidikan	: Strata-1 (S1)

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis adalah benar dan asli hasil dari penelitian yang telah saya lakukan dengan judul **"Analisis Metode Fluxion Menggunakan Wi-Fi Deauther Untuk Uji Keamanan Wpa2 Pada Perangkat Router Wireless Totolink N300RT"**. Apabila dikemudian hari ada yang merasa dirugikan dan atau menuntut karena penelitian ini menggunakan sebagian hasil tulisan atau karya orang lain tanpa mencantumkan nama penulis yang bersangkutan, atau terbukti karya ilmiah ini **bukan** karya saya sendiri atau **plagiat** hasil karya orang lain, maka saya bersedia menerima sanksi sesuai dengan peraturan perundangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya untuk dapat digunakan sebagaimana mestinya.

Pekanbaru, 17 Desember 2021

Yang membuat pernyataan,

Rafita Mandasari

LEMBAR IDENTITAS PENULIS

Nama	: Rafita Mandasari
NPM	: 143510130
Tempat/Tanggal Lahir	: Subarak, 25 Maret 1996
Alamat Nama Orang Tua	: Subarak
Nama Ayah	: Amril Mukminin
Nama Ibu	: Marlinda
No.HP/Telp	: -
Fakultas	: Teknik
Program Studi	: Teknik Informatika
Masuk Th.Ajaran	: 2014
Keluar Th. Ajaran	: 2022
Judul Penelitian	: Analisis Metode Fluxion Menggunakan Wi-Fi Deauther Untuk Uji Keamanan Wpa2 Pada Perangkat Router Wireless Totolink N300RT

Pekanbaru, 4 Februari 2022

Rafita Mandasari

HALAMAN PERSEMBAHAN

Assalamu'alaikum Warahmatullahi Wabarakatu..

Alhamdulillah puji syukur penulis ucapkan kepada Allah SWT atas segala rahmat dan karunia-Nya yang telah diberikan kepada penulis sehingga dapat menyelesaikan tugas akhir dengan judul **"Analisis Metode Fluxion Menggunakan Wi-Fi Deauther Untuk Uji Keamanan Wpa2 Pada Perangkat Router Wireless Totolink N300RT".**

Skripsi ini disusun untuk memenuhi persyaratan mencapai derajat strata-1 (S1) di program studi Teknik Informatika Fakultas Teknik Universitas Islam Riau. Penulis menyadari bahwa tanpa bantuan dari pihak-pihak lain, usaha yang penulis lakukan dalam menyelesaikan skripsi ini tidak akan membuahkan hasil yang berarti. Dalam kesempatan ini penulis ucapkan terima kasih kepada :

1. Allah SWT, karena hanya dengan izin dan karunia-Nya maka skripsi ini dapat selesai tepat pada waktunya. Segala puji bagi Allah yang maha mengabulkan segala doa.
2. Orang tua tercinta yakni ayah amril mukminin dan omak tercinta Marlinda beserta saudara penulis Almarhum Rafiqo Rahmad, Nur Elisa, Tito Handiko, Ratna Mandasari, Ziad Abdul Aziz, Serta Abang Ipar Tia Febri, Dan Keponakan Anasya Safa Humaira yang tak henti-hentinya selalau mensuport penulis dan membantu dalam segi materi dan moril serta do'a-do'anya sehingga penulis dapat menyelesaikan penulisan skripsi ini.
3. Bapak Dr. Apri SiswantoS.kom.,M.Kom selaku Dosen Pembimbing atas bimbingan serta support dan motivasi yang diberikan.

4. Segenap Dosen Teknik Informatika Universitas Islam Riau yang telah memberikan ilmu, pendidikan, dan pengetahuan kepada penulis selama duduk dibangku kuliah.
5. Teman-teman fillah Penulis dari club Al-walid Archery, UKM panahan UIR, FSI teknik UIR, UKMI al-kahfi UIR yang telah support penulis hingga saat ini.
6. Teman-teman Penulis di TI UIR, khususnya Sumayyah Tsabitul Haq , Ronaldi Poetra, Agung Surya Ramadhan, Septiyani Yendriki, M. Luthfy, Eryanto Agusriadi, Restu Singgih, Brama Putra Andika, Muahamad Jurizal, Dwi Ayu Azhari dan teman teman Penulis lainnya yang tidak dapat penulis sebutkan satu persatu.

Pekanbaru, 4 Februari 2022

Rafita Mandasari

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Dengan segala kerendahan hati Penulis haturkan rasa syukur dalam kehadirat Allah SWT,yang telah memberikan limpahan rahmat dan karunia-Nya yang berupa kemampuan, kesehatan dan juga kesempatan kepada Penulis untuk menyelesaikan proposal tugas akhir "Analisis Metode Fluxion Menggunakan Wi-Fi Deuther Untuk Uji Keamanan WPA2 Pada Perangkat Router Wireles Totolink N300RT" ini.

Terimakasih kepada semua pihak yang telah membantu penulis dalam proses pembuatan skripsi ini, karena berkat dan dorongan dari berbagai pihak penulis dapat menyelesaikan skripsi ini, rasa terimakasih penulis ucapkan kepada:

1. Terimakasih kepada Allah subhanahu wata'ala dengan izin nya penulis masih melanjutkan kuliah dan alhamdulillah selesai sampai mendapatkan gelar sebagai sarjana.
2. Kedua orang tua Penulis yang telah memberikan motivasi, nasehat, serta semangat untuk mejalankan dan menyelesaikan tugas akhir.
2. Kepada Bapak Dr. Eng. Muslim, ST.,MT Dekan Fakultas Teknik Universitas Islam Riau.

3. Bapak Dr. Apri Siswanto M.Kom selaku Ketua Program Studi Teknik Informatika Universitas Islam Riau sekaligus sepembimbing yang telah memberikan pengajaran, arahan, dan telah sabar dalam memberikan bimbingan di sela- sela kesibukan beliau.
4. Bapak dan Ibu Dosen UIR yang telah banyak memberikan ilmunya selama penulis menduduki bangku perkuliahan khususnya bagi Bapak dan Ibu Dosen Program Studi Teknik Informatika

Demikian yang dapat saya sampaikan semoga dapat bermanfaat bagi seluruh pembaca. Akhir kata, apabila terdapat kesalahan ketik atau format penulisan yang tidak sesuai pada skripsi ini, dengan rendah hati penulis memohon maaf atas segala kekuarangan.

Wassalamu'alaikum Wr. Wb.

Pekanbaru, 14 Desember 2021

Rafita Mandasari
NPM : 143510369

ANALISIS METODE FLUXION MENGGUNAKAN WI-FI DEAUTHER UNTUK UJI KEAMANAN WPA2 PADA PERANGKAT ROUTER WIRELESS TOTOLINK N300RT

ABSTRAK

Rafita Mandasari
Universitas Islam Riau
Teknik Informatika
Email : rafitamnadasari@student.uir.ac.id

Era pandemi covid-19 adalah era yang mana semua orang di haruskan untuk berkegiatan serba internet. Mulai dari masalah kerja, belajar mengajar hingga masalah non formalpun harus menggunakan internet.Setiap rumah kebanyakan telah terpasang Wi-Fi guna untuk mengurangi pengeluaran dana pembelian paket data per orangannya. Walaupun permasalahannya, tetap saja ada user ilegal yang ingin menggunakan Wi-Fi untuk internetan tanpa izin pemiliknya. Maka dari itu untuk mencari tahu permasalahan tersebut dibutuhkan percobaan terhadap salah satu penyebab user ilegal dapat mengakses internet tanpa sepengetahuan pemilik Wi-Fi. Adapun konfigurasi yang akan dibagun adalah :"Analisis Metode Fluxion Menggunakan Wi-Fi Deauther Untuk Uji Keamanan WPA2 Pada Perangkat Router Wireless Totolink N300RT."

Kata kunci : Jaringan Wi-Fi, Keamanan WPA2, Metode Fluxion.

ANALYSIS OF THE FLUXION METHOD USING WI-FI DEAUTHER FOR WPA2 SECURITY TESTS ON TOTOLINK N300RT WIRELESS ROUTER DEVICES

ABSTRACT

Rafita Mandasari
Univercity Islam Riau
Teknik Informatika
Email : rafitamnadasari@student.uir.ac.id

The era of the covid-19 pandemic is an era where everyone is required to do all internet activities. Starting from work problems, teaching and learning to non-formal problems, you have to use the internet. Most homes have Wi-Fi installed in order to reduce spending on purchasing data packages per person. Despite the problem, there are still illegal users who want to use Wi-Fi to surf without the owner's permission. Therefore, to find out the problem, it takes an experiment on one of the causes of illegal users to be able to access the internet without the knowledge of the Wi-Fi owner. The configuration to be built is: "Analysis of the Fluxion Method Using Wi-Fi Deauther for WPA2 Security Tests on Totolink N300RT Wireless Router Devices."

Keywords: Wi-Fi Network, WPA2 Security Test, Fluxion Method.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Pada masa ini, kemajuan teknologi komunikasi merupakan faktor yang paling penting terhadap peranan sebagian masyarakat untuk mendapatkan akses informasi. Apalagi pada masa pandemi yang di awali pada tahun 2019, yang mana semua orang sangat membutuhkan jaringan internet di sebabkan Pemberlakuan Pembatasan Kegiatan Masyarakat (PPKM) yang mengharuskan untuk pelajar, mahasiswa, guru, dosen, pekerja kantoran, dan lain sebagainya untuk beraktifis. Aktifitas nya meliputi : kerjaan kantor, proses belajar mengajarf, dan sebagainya. Tidak hanya kegiatan yang bersifat formal saja, bahkan hampir semua aktifitas di luar rumah telah menggunakan internet.

Tidak menutup kemungkinan banyak rumah yang telah menggunkan Wi-Fi dalam meminimalisi pengeluaran dana untuk pembelian paket internet bulanan per orangannya untuk melakukan aktifitas di internet yang mana bertujuan untuk memenuhi kebutuhan hidup PPKM berlangsung. Dengan adanya Wi-Fi banyak orang dapat melakukan aktifitas di internet dengan gratis tanpa membeli paket data per orangannya. Di karenakan bahwa *Wireless Fidelity* (Wi-Fi) adalah standar untuk komunikasi Wireless jarak pendek, terutama digunakan oleh computer dan perangkat seluler. *Wireless* atau Wi-Fi adalah jaringan yang menghubungkan telekomunikasi perangkat satu dengan yang lainnya tanpa menggunakan media

kabel sebagai media penghantarnya. Sebagai gantinya, jaringan nirkabel yang digunakan adalah media transmisi untuk mengantarkan gelombang elektromagnetik. Apabila jaringan komputer membutuhkan kabel jaringan seperti kabel optic, fiber, dan UTP, jaringan nirkabel wireless hanya memanfaatkan gelombang elektromagnetik untuk mengirimkan sinyal dari perangkat satu ke perangkat yang lainnya. Salah satu keunggulan menggunakan jaringan wireless adalah kemudahan pemasangan. Jenis-jenis peralatan yang menggunakan Wireless, seperti Wireless LAN, telepon genggam, telepon cordless, satelit televisi, perangkat komputer dan laptop, remote control, hingga GPS yang berfungsi sebagai navigasi. (https://www.pinhome.id/kamus-istilah-properti/wireless/).

Tetapi walaupun Wi-Fi sangat mudah di gunakan, pastinya ada orang-orang yang masih ingin mengakses Wi-Fi dengan ilegal guna untuk akses internet tanpa memasang Wi-Fi di tempatnya. Mengakses internet dengan memutus dan mengirimkan SSID (nama Wi-Fi) palsu agar dapat terhubung pada Wi-Fi yg di tuju . Evil Twin adalah Service Set Identifier (SSID) palsu yang meniru jaringan Wi-Fi asli . Tiruan ini benar-benar sangat mirip dengan SSID aslinya. Mulai dari nama, kekuatan sinyal, hingga frekuensinya. Pengguna bisa saja menyambungkan perangkatnya ke Wi-Fi Evil Twin ini karena mengira itu adalah Wi-Fi yang asli. Evil Twin ini bekerja dengan menggunakan teknik penyerangan bernama *man-in-the-middle* (MITM). Teknik ini memungkinkan pembuat Evil Twin untuk menyuntikkan *Malware* atau *Backdoor*.

Salah satu praktek Evil Twin terpopuler kepada perangkat pengguna tanpa terdeteksi sama sekali. Malware tersebut lalu bisa digunakan untuk berbagai macam hal sesuai keinginan penyerang. adalah pengguna diarahkan ke halaman login palsu. Entah itu login media sosial, login email, atau sekedar login untuk menggunakan Wi-Fi tersebut. Pengguna yang tak tahu mengira bahwa itu adalah kolom login normal dan mengisi username serta password mereka tanpa rasa curiga. Walaupun faktanya, mereka baru saja menyerahkan informasi penting kepada *hacker* secara sukarela. Seiring berkembangnya teknik untuk menyerang keamanan *Wireless,* diantaranya *brute force*. *Deltaxflux* mengembangkan sebuah program diberi nama *fluxion* untuk mendapatkan *password wireless* tanpa menggunakan teknik *brute force* seperti pada umumnya yang mana Fluxion adalah sistem keamanan dan alat penelitian rekayasa sosial, yang mana bertujuan untuk membuat rekayasa sosial untuk mengambil kunci WPA2 pada titik akses tersebut.

Berdasarkan permasalahan tersebut, maka muncul pemikiran untuk mengajukan penelitian dengan judul **Analisis Metode Fluxion Menggunakan Wi-Fi Deauther Untuk Uji Keamanan WPA2 Pada Perangkat Router Wireless Totolink N300RT.**

1.2 Identifikasi Masalah

Adapun Identifikasi masalah pada penelitan ini adalah *Service Set Identifier* (SSID) yang sama, sehingga susah membedakan mana *Service Set Identifier* (SSID) yang palsu ataupun yang asli, sehingga pengguna Wi-Fi akan tetap masuk pada

salah satunya, jika pengguna memilih *Service Set Identifier* (SSID) palsu, maka pengguna akan terlebih dahulu di masukkan ke halaman login *Service Set Identifier* (SSID) palsu sehingga password yang di masukkan pengguna terbaca oleh peretas dari *Service Set Identifier* (SSID) palsu tersebut.

1.3 Rumusan Masalah

Berdasarkan uraian diatas, maka penelitian merumuskan masalah

1. Bagaimana cara membedakan SSID palsu yang mirip dengan nama SSID asli?
2. Bagaimana cara Wi-Fi deauther memutus jaringan dan perangkat Wi-Fi deuther akan membaca sandi dari target?
3. Apakah metode fluxion cukup efektif dilakukan pada perangkat *Wireless* yang terpasang keamanan WPA2?

1.4 Batasan Masalah

Agar terarahnya penelitian ini, maka penulis memberikan batasan yakni hanya terdapat pada perangkat *HandPhone* (HP) yang terhubung pada perangkat Wi-Fi.

1.5 Tujuan

Adapun tujuan dari uji keamanan WPA2 ini adalah untuk :

1. Mengetahui jika ada user ilegal yang ingin masuk.
2. Mengetahui solusi jika ada penyusup yang akan masuk ke wifi

1.6 Manfaat Penelitian

Adapun manfaat dari penelitan ini adalah

1. Memberikan informasi tentang SSID palsu yang dapat mengambil password dari Wi-Fi yang sedang di gunakan
2. Mengetahui ciri-ciri jaringan SSID palsu yang akan masuk ke perangkat *Handphone* (HP)

BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Berdasarkan penelitian yang dilakukan oleh Baihaqi, Yeni yanti dan Zulfan (2018) dengan judul "Implementasi Sistem Keamanan WPA2 Pada Jaringan Wi-Fi". Teknologi jaringan wireless saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi. Komputer, notebook, PDA, telepon seluler (handphone) dan periferal lainnya mendominasi pemakaian teknologi jaringan wireless. Penggunaan teknologi jaringan wireless yang di implementasikan dalam suatu jaringan lokal sering dinamakan WLAN (Wireless Local Area Network).

Teknologi jaringan wireless memanfaatkan frekuensi tinggi untuk menghantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang di gunakan oleh user maupun oleh operator yang memberikan layanan komunikasi. Pada pengujian ini, User Attack melakukan penetrasi terhadap user dengan cara mencari IP Address user yang terkoneksi pada jaringan Wi-Fi menggunakan tool Fluxion yang telah di install di Kali Linux, Lalu User Attack Menginjeksi paket dengan melakukan Deauthentication Attack, sehingga data yang dibutuhkan yaitu enkripsi key dan handshake data dapat diambil dengan cepat dan mengurangi waktu yang

dibutuhkan untuk melakukan cracking, setelah di dapatkan data handshake, User Attack melakukan cracking WPA2 dengan menggunakan Fluxion untuk mengetahui Password WPA2-PSK melalui user yang terhubung ke jaringan Wi-Fi. Dalam melakukan Password Attack, User Attack hanya membutuhkan user yang terkoneksi ke jaringan Wi-Fi tersebut. Berdasarkan hasil penelitian ini, maka dapat disimpulkan bahwa untuk mengetahui password WPA2-PSK penyerang memerlukan user yang terkoneksi ke jaringan Wi-Fi dengan menggunakan tool Fluxion.

Pada pengujian SSID palsu melalui user, penyerang membuat sebuah SSID lain yang hampir sama dengan SSID asli, namun yang membedakannya ialah SSID asli memiliki pengamanan WPA2-PSK sedangkan SSID palsu bersifat open. Jadi, user yang tidak teliti dalam menggunakan koneksi jaringan akan terhubung ke SSID palsu, penyerang akan mudah mendapatkan password karena user memasukkan password seperti SSID asli ke dalam sebuah halaman khusus yang telah dibuat oleh tool Wi-Fi Phisher. Dalam tahapan mengetahui password penyerang masih membutuhkan user yang terhubung ke jaringan Wi-Fi, bukan melakukan proses mendapatkan password secara individu.

Berdasarkan penelitian yang dilakukan ole hamza alfan suri , widyanto dan taqrim ibadi (2016) dengan judul "Analisis *Fluxion* Sebagai Program Uji Keamanan WPA2 Pada Perangkat *Wireless*." Dengan menggunakan Dalam rangka menyelesaikan penelitian ini maka digunakan metode penelitian tindakan (*Action Research).* Dalam hal ini tingkat keberhasilan tidak akan mencapai

100% karena jika user yang terdapat dalam jaringan yang ingin diretas memahami tanda- tanda adanya seach engine.

Selanjutnya penelitian yang dilakukan oleh Abraham Yano Suharmanto, Arie S.M Lumenta, Xaverius B.N. Najoan (2018) dengan judul "Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi". Dalam penelitiannya permasalahan yang terjadi yaitu Universitas Sam Ratulangi atau yang dikenal dengan singakatan Unsrat, beralamat Jalan Bahu, Kota Manado, Provinsi Sulawesi Utara. Merupakan lembaga pendidikan tingkat perguruan tinggi dan merupakan Salah Satu Universitas Negeri terbaik Di Sulawesi Utara. Unsrat saat ini telah menyediakan fasilitas jaringan komputer kabel maupun nirkabel atau lebih sering dikenal wireless sebagai sarana untuk pertukaran data, pencarian informasi seperti materi mata kuliah, chatting, Pengisian Kartu Rencana Studi (KRS), penginputan nilai, e-learning atau kuliah jarak jauh dan lain – lain. Fasilitas layanan jaringan komputer tersebut diberikan secara gratis kepada mahasiswa, dosen dan pegawai yang terdaftar di Universitas Sam Ratulangi yang dilaksanakan oleh UPT Teknologi Informasi dan Komunikasi Unsrat Untuk menguji keamanan dari jaringan server UPT Teknologi Informasi dan Komunikasi Unsrat peneliti akan melakukan uji penetrasi jaringan menggunakan metode Action Research terhadap server dan website Unsrat dan kepada user yang aktif terutama yang dalam cakupan penggunaan Wireless dengan batasan – batasan seperti tidak melakukan perusakan terhadap jaringan atau yang dapat merugikan pihak – pihak yang terkait.

Berdasarkan rancangan sistem yang telah dijelaskan sebelumnya maka dihasilkan suatu pengujian terhadap keamanan WPA2-PSK pada jaringan Wi-Fi yaitu dengan menggunakan tahapan untuk mengetahui password melalui pemanfaatan user. Dalam penelitian ini, untuk mengetahui password WPA2- PSK penyerang memerlukan user yang terkoneksi ke jaringan Wi-Fi dengan menggunakan tool Fluxion.

Pada pengujian SSID palsu melalui user, penyerang membuat sebuah SSID lain yang hampir sama dengan SSID asli, namun yang membedakannya ialah SSID asli memiliki pengamanan WPA2-PSK sedangkan SSID palsu bersifat open. Jadi, user yang tidak teliti dalam menggunakan koneksi jaringan akan terhubung ke SSID palsu, penyerang akan mudah mendapatkan password karena user memasukkan password seperti SSID asli ke dalam sebuah halaman khusus yang telah dibuat oleh tool Wi-Fi Phisher. Dalam tahapan mengetahui password penyerang masih membutuhkan user yang terhubung ke jaringan Wi-Fi, bukan melakukan proses mendapatkan password secara individu.

Selanjutnya penelitian yang di lakukan oleh ahmad fajri (2019) dengan judul "Empirical Study On Wi-Fi Performance & Security (Case Study In Depok City)". Sumber utama tingginya pengguna internet di Kota Depok berasal dari pengguna jaringan Wi-Fi pada area perkantoran, hotel, cafe, sekolah, kampus bahkan perumahan. Hal tersebut dikarenakan jaringan Wi-Fi memberikan kemudahan untuk dimanfaatkan sebagai sarana bertukar informasi. Bagaimanapun juga kemudahan

penggunaan jaringan Wi-Fi diikuti dengan ancamana keamanan siber. Sifat broadcast dari Wi-Fi dapat memberikan risiko adanya penyusup yang dapat memperoleh akses yang tidak sah, sehingga menyebabkan data yang dipertukarkan rusak atau bahkan dimodifikasi. Studi empiris pada penelitian ini bertujuan untuk menghasilkan data yang akan diinformasikan kepada para pihak yang berkepentingan untuk mendukung Kota Depok sebagai kota smart city (Detik, 2018), selain itu hasil studi empiris ini juga dapat dimanfaatkan untuk melakukan perbaikan keamanan dan kinerja jaringan Wi-Fi di Kota Depok.

Metode penelitian yang digunakan pada studi empiris ini terdiri atas perancangan tools untuk audit kinerja dan keamanan jaringan Wi-Fi dan wardriving. Wardriving adalah tindakan mencari jaringan Wi-Fi dalam kendaraan bergerak. Kegiatan wardriving bertujuan untuk mengetahui kekurangan dan kelemahan jaringan Wi-Fi pada suatu wilayah tertentu melalui metode pemetaan lokasi. Beberapa informasi yang dapat diperoleh dari hasil kegiatan wardriving, yaitu menemukan access point, mengetahui autentikasi yang digunakan, mengetahui protokol yang digunakan dan mengetahui client-client yang terhubung. Penulis melakukan simulasi wireless scanning dengan cara mengendarai sepeda motor sepanjang jalan Margonda, Depok. Dengan rute dimulai dari perbatasan Kota Depok dengan Jakarta Selatan hingga Depok Mall. Sepanjang perjalanan ditemui gedung-gedung pemerintahan, kampus, sekolah, serta banyak perusahaan-perusahaan yang

bergerak dalam bidang bisnis seperti hotel, mall, dan kafe. Dalam penelitian ini kami menemukan sebanyak 536 jaringan Wi-Fi.

Cara kerja alfa network dalam mengumpulkan data tentang jaringan disekitarnya adalah melalui dua metode yang didefinisikan pada IEEE 802.11. Metode pertama didasarkan pada frame beacon yang secara berkala dikirimkan oleh access point dengan cara broadcast kepada radius disekitarnya. Metode kedua alfa network secara broadcast mengirimkan request frame dan menunggu probe response dariaccess point yang menerima requset. Ketika proses request dan response berhasil dilakukan maka telah terjadi satu siklus shared key authentication. Hasil dari wireless scanning kemudian dipetakan ke dalam google earth. Yaitu dengan cara melakukan network mapping. ***Wi-Fi security*** menginformasikan persentase jaringan Wi-Fi di Kota Depok yang dikelompokan berdasarkan security level yang digunakan yaitu no encryption, WEP, WPA atau WPA2. Berdasarkan hasil persantase tersebut, didapatkan hasil sebanyak 89% sudah menerapkan security WPA/WPA2, 1% menerapkan security WEP, 10% tidak menerapkan security (Wi-Fi bersifat terbuka). Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan Wi-Fi di Kota Depok sudah menerapkan security WPA/WPA2. Dengan kata lain, teknisi ataupun pengguna jaringan Wi-Fi di Kota Depok memiliki kesadaran keamanan informasi yang cukup tinggi. Pengguna Wi-Fi dengan penerapan metode keamanan WEP di Kota Depok sebesar 1%. WEP merupakan protokol enkripsi yang cukup lama. Dan sangat mudah untuk dilakukan carcking password, karena protokol WEP memiliki

beberapa kelemahan dalam hal kunci, initialization vector, data integrity (yang menggunakan algoritma crc32). Pengguna Wi-Fi tanpa menggunakan protokol dan algoritma enkripsi adalah sebesar 10%. Artinya siapa pun dapat mengakses jaringan Wi-Fi tanpa memasukkan password. Penggunaan Wi-Fi tanpa password pada praktiknya akan menimbulkan ancaman seperti pencurian data pribadi, bahaya penyebaran virus, iklan yang mengganggu yang dapat mengandung malicious software dan snooper atau mata-mata.

Sedangkan ***Wi-Fi Performance*** Persentase tertinggi penyebaran Wi-Fi channel di Kota Depok adalah pada channel 1 sebesar 20%, channel 6 sebesar 19% dan channel 11 sebesar 19%. Tingginya penggunaan channel 1, 6 dan 11 pada Kota Depok merepresentasikan bahwa Kota Depok sangat memperhatikan kinerja penggunaan Wi-Fi. Channel 1, 6 dan 11 merupakan channel terbaik karena aman terhadap gangguan interferensi, sehingga kinerja Wi-Fi akan maksimal. Dengan kata lain dapat di simpulkan bahwa Berdasarkan hasil wardriving, Kota Depok dinilai sebagai kota yang sudah sadar akan keamanan informasi khusunya dalam penggunaan Wi-Fi dan siap untuk menghadapi era ekonomi digital karena persentase terbesar yaitu sebesar 89% telah menerapkan keamanan protokol WPA2. Selain itu Wi-Fi di Kota Depok juga memiliki kinerja yang maksimal karena mayoritas channel Wi-Fi yang digunakan bekerja pada channel 1, 6 dan 11 yang aman dari adanya interferensi. Oleh karena itu penilaian keamanan jaringan Wi-Fi di Kota Depok dinilai sudah baik karena sudah sesuai dengan standar IEEE 802.11i yaitu

tentang peningkatan pengamanan pada jaringan Wi-Fi menggunakan WPA2 dan penilaian kinerja jaringan Wi-Fi di Kota Depok juga dinilai sudah baik karena sesuai dengan standar IEEE 802.11b tentang pengaturan channel Wi-Fi yang tidak menimbulkan interferensi.

2.2 Dasar Teori

2.2.1 Wi-Fi

Wi-Fi adalah teknologi jaringan nirkabel yang memungkinkan perangkat seperti komputer (laptop dan desktop), perangkat seluler (ponsel pintar dan perangkat yang dapat dikenakan), dan peralatan lain (printer dan kamera video) untuk berinteraksi dengan Internet. Hal ini memungkinkan perangkat ini - dan banyak lagi - untuk bertukar informasi satu sama lain, menciptakan jaringan.

Konektivitas internet terjadi melalui router nirkabel. Saat Anda mengakses Wi-Fi, Anda terhubung ke perute nirkabel yang memungkinkan perangkat Anda yang kompatibel dengan Wi-Fi untuk berinteraksi dengan Internet. (https://www.cisco.com/c/en/us/products/wireless/what-is-Wi-Fi.html)

2.2.2 Router

Router adalah perangkat jaringan yang meneruskan paket data antar jaringan komputer. Router melakukan fungsi "pengarahan lalu lintas" di Internet. Paket data biasanya diteruskan dari satu router ke lain melalui jaringan yang merupakan internetwork sampai mencapai node tujuan. Sebuah router adalah terhubung ke dua atau lebih jalur data dari jaringan yang berbeda (sebagai lawan dari sakelar jaringan,

yang menghubungkan jalur data dari satu jaringan tunggal). Ketika sebuah paket data masuk pada salah satu jalur, router membaca: Informasi alamat dalam paket untuk menentukan tujuan akhirnya. Kemudian, menggunakan informasi dalam peruteannya tabel atau kebijakan perutean, ia mengarahkan paket ke jaringan berikutnya dalam perjalanannya. Ini menciptakan overlay internetwork. Jenis router yang paling dikenal adalah router rumah dan kantor kecil yang hanya meneruskan data, seperti: halaman web, email, IM, dan video antara komputer rumah dan Internet. Contoh router akan menjadi kabel pemilik atau router DSL, yang terhubung ke Internet melalui ISP. Router yang lebih canggih, seperti router perusahaan, hubungkan bisnis besar atau jaringan ISP hingga router inti yang kuat yang meneruskan data dengan kecepatan tinggi di sepanjang jalur serat optik tulang punggung Internet. Meskipun router biasanya didedikasikan perangkat keras, penggunaan router berbasis perangkat lunak semakin umum. (Ashiqur Rahman1 , Asaduzzaman Noman2 , Zahidul Islam Akash, 2016)

2.2.3 WPA2

WPA2 merupakan level keamanan yang palng tinggi. Enkripsi utama yang digunakan pada WPA2 ini enkripsi AES. AES mempunyai kerumitan yang lebih tinggi daripada RC4 pada WEP sehingga para vendor tidak sekedar upgrade firmware seperti dari WEP ke WPA. Untuk menggunakan WPA2 diperlukan hardware baru yang mampu bekerja dengan lebih cepat dan mendukung perhitungan yang dilakukan oleh WPA2, Sehingga tidak semua adapter

mendukung level keamanan WPA2 ini. Pada security mode WPA2-PSK ada dua pilihan enkripsi pada jenis ini, yaitu TKIP dan AES.

1. TKIP (Temporal Key Integrity Protocol) menggunakan metode enkripsi yang lebih aman dan juga menggunakan MIC (Message Integrity Code) untuk melindungi jaringan dari serangan.
2. AES (Advanced Encryption System) menggunakan enkripsi 128 bit blok data secara simetris. Untuk menggunakan WPA Pre-Shared Key, masukkan password pada WPA Shared Key dengan panjang karakter antara 8 sampai 63. Group Key Renewal Interval diisi dengan nilai default yaitu 3600 seconds.

(Baihaqi, Yeni Yanti, Zulfan , 2017)

Wi-Fi Protected Access versi2 (WPA2) adalah sebuah protokol kriptografi yang berfungsi untuk mengamankan jaringan wireless. WPA2 diperkenalkan oleh Wi-Fi Alliance pada tahun 2004, WPA2 memenuhi persyaratan standar yang ditetapkan oleh IEEE 802.11i. Dalam metode pengamanan WPA2 menggunakan algoritma AES sebagai proses enkripsi dan CBC-MAC sebagai proses enkripsi traffic pada jaringan dan melindungi integritas data. (Ahmad Fajri ,2019)

2.2.4 Deauther

Deauther/ jammer dalam dunia telekomunikasi yaitu sebuah alat yang digunakan untuk memutus hubungan komunikasi perangkat telekomunikasi.

(Eddy Triyono , Imelda Erawati Supono P , Muhammad Nashiruddin, 2015)

Wi-Fi deudher bekerja dengan 2 mode serangan secara bersamaan yaitu memutuskan koneksi device yang terhubung ke accespoint atau router dan juga membuat ssid atau Wi-Fi palsu sebagai captive portal.

2.2.5 Keamanan Jaringan

Keamanan jaringan adalah proses untuk mengidentifikasi dan mencegah pengguna yang tidak sah dari suatu jaringan komputer. Tujuannya tentu saja untuk mengantisipasi resiko ancaman berupa perusakan bagian fisik komputer maupun pencurian data seseorang.

Jenis gangguan dalam jaringan:

Ada beberapa jenis gangguan keamanan jaringan yang perlu Anda ketahui. Berikut daftarnya:

- Hacking: perusakan pada infrastruktur jaringan komputer yang sudah ada.
- Carding: pencurian data terhadap identitas perbankan seseorang. Misalnya pencurian nomor kartu kredit yang dimanfaatkan untuk berbelanja online.
- Deface: perubahan terhadap bentuk atau tampilan website.
- Physing: pemalsuan data resmi.

(https://www.baktikominfo.id/id/informasi/pengetahuan/mengetahui_tentang_sistem_keamanan_jaringan_untuk_proteksi_perangkat_komputer_anda-677)

2.2.6 Fluxion

Fluxion adalah audit keamanan dan alat penelitian rekayasa sosial. Ini adalah remake (pembuatan ulang) dari alat linset oleh vk496 dengan (semoga) lebih sedikit bug dan lebih banyak fungsionalitas. Script mencoba untuk mengambil kunci WPA/WPA2 dari titik akses target melalui serangan rekayasa sosial (phishing). (https://github.com/FluxionNetwork/fluxion)

Cara kerja :

- Pindai jaringan nirkabel target.
- Luncurkan serangan Handshake Snooper.
- Tangkap jabat tangan (diperlukan untuk verifikasi kata sandi).
- Luncurkan serangan Captive Portal.
- Memunculkan AP palsu, meniru titik akses asli.
- Memunculkan server DNS, mengarahkan semua permintaan ke host penyerang yang menjalankan portal tawanan.
- Memunculkan server web, melayani portal tawanan yang meminta pengguna untuk memasukkan kunci WPA/WPA2 mereka.
- Memunculkan jammer, menonaktifkan semua klien dari Acces Poin (AP) asli dan memikat mereka ke Acces Poin (AP) palsu.
- Semua upaya otentikasi di portal tawanan diperiksa terhadap file jabat tangan yang diambil sebelumnya.

- Serangan akan secara otomatis berhenti setelah kunci yang benar telah dikirimkan.
- Kunci akan dicatat dan klien akan diizinkan untuk terhubung kembali ke titik akses target. (https://en.kali.tools/?p=235)

(https://github.com/FluxionNetwork/fluxion)

BAB III

METODOLOGI PENELITIAN

3.1 Peralatan Penelitian

3.1.1 Perangkat penelitian

Disini penulis menggunakan alat dalam upaya menganalisa metode fluxion menggunakan Wi-Fi deauther untuk uji keamanan WPA2 pada perangkat router wireles totolink N300RT, Dalam melancarkan penelitian ini, penulis menggunakan alat untuk mendukung kelancaran dan kesuksesan dalam menganalisa uji coba keamanan WPA2, Penelitian ini menggunakan alat penelitian berupa perangkat keras dan perangkat lunak. Berikut adalah Spesifikasi kebutuhan/ yang di gunakan penulis dalam pembuatan system berupa perangkat ketas (*hardware)* dan perangkat lunak (*software)* :

1. Perangkat Ketas (*Hardware)*

Perangkat keras (*HardwareI*) yang di butuhkan dalam penelitian ini antara lain :

Tabel 3. 1 Table Perangkat Keras (*Hardware*)

No	Nama	Spesifikasi	Fungsi
1	Laptop	• *Prosessor* intel pentium • *Random Acces Memory* (RAM) 2,00 GB • *Monitor* standart • *Keyboart* standart • *Mouse* standart	Media pengantur jalanya tahap-tahan yang akan mengsukseskan penelitian ini, seperti : setting alat, pendeteksi hingga pelancaran penyerangan pada jaringan WPA2 hingga selesai.
2	Wi-Fi Router	Wi-Fi deauther	Alat yang di gunakan untuk menagkap sinyal, memutus dan mengambil password dari taget
3	Handpone	Android	Target penangkap sinyal Wi-Fi
4	Router Wireless	Totolink N300RT	Pemancar sinyal Wi-Fi

2. **Perangkat Lunak (*Software)***

Perangkat lunak (*Software*) yang di butuhkan dalam penelitian ini antara lain :

Tabel 3. 2 Table perangkat lunak (*Software*)

No	Nama	Fungsi
1	Google Crome	pengujian terhadap alat yang di hubungkan menggunakan 3 perangkat yakni : pc, Wi-Fi deuther dan target. Penyettingan perangkat router totolink N300RT

3.1.2 Metode Penelitian

Dalam rangka menyelesaikan penelitian ini maka digunakan metode penelitian tindakan (*Action Research),* Adapun tahapan penelitian yang merupakan bagian dari *action research* ini antara lain :

a. *Diagnosing :* Melakukan *diagnosa* terhadap sistem jaringan *Wireless* keamanan WPA2.

b. *Action Planning :* Melakukan rencana tindakan yang akan dilakukan pada jaringan *Wireless* dengan membuat perancangan dan pengujian sistem keamanan *WPA2*

c. *Action Taking :* Mengimpelementasikan rencana dengan tindakan yang telah dibuat untuk mencari kelemahan sistem jaringan *wireless.*

d. *Evaluating :* Melaksanakan evaluasi hasil analisis dari *program* yang digunakan untuk menemukan *password* pada keamanan sistem *WPA2*, dalam tahap ini yang terlihat adalah terdapat penggabungan jenis serangan apa saja dalam *program fluxion*

e. *Specifying Learning :* review tahalan-tahapan yang telah berkhir dan mempelajari alur fluxion.

Ilustrasi skema jaringan sederhana untuk implementasi uji keamanan WPA2 menggunakan perangkat *router wireless totolink N300RT* metode fluxion menggunakan Wi-Fi deauther. Dalam ilustrasi ini, satu rumah mempunyai 5 anggota keluarga diantaranya : ayah, ibu, abang, kakak dan adek. Rumah mereka memiliki 4 kamar, ruangan kerja, ruang tamu, bagasi, dan dapur. Dalam 1 rumah tersebut

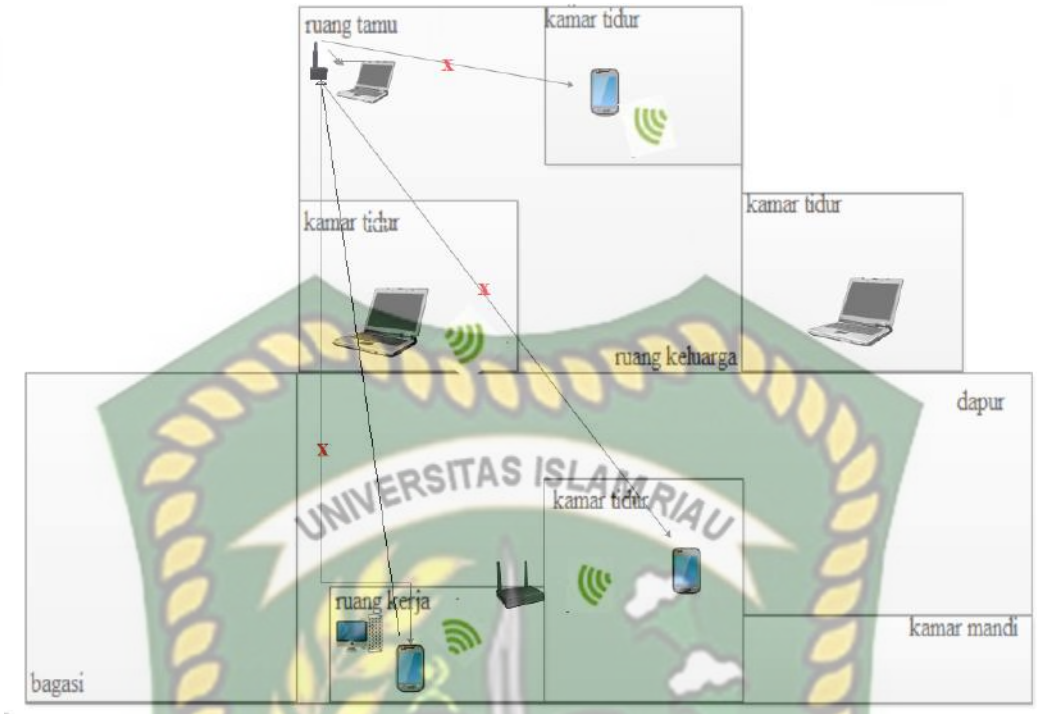
memiliki 1 AP bertujuan untuk menampung acces internet dalam keperluan sehari-hari. Mulai dari pekerjaan, sekolah maupun akses lainnya.

Kemudian salah satu anggota yaitu abang membawa teman-temannya membuat tugas di rumahnya. Kemudian salah satu temannya mencoba mencoba alat yang bernama Wi-Fi deauther yang mana perangkat tersebut di uji cobakan di rumah abang. Setelah perangkat di pasangkan ke laptop, kemudian tes penyerangan tertuju pada perangkat WPA2, pertama handphone mereka di hubungkan pada jaringan Access Poin yang ada di rumah. Kemudian penyerangan di coba, dengan menggunakan laptop dan alat, pertama user akan menetak tombol scan, yang bertujuan untuk memantau Access Poin Yang aktif kemudian mulailah untuk menguji keamanan dari keamanan handphone dengan memutus jaringan semua perangkat yang terhubung pada perangkat Access Poin, kemudian barulah Wi-Fi deauter mengirimkan link untk masuk kembali pada jaringan Wi-Fi yang sama. Setelah login, maka otomatis password yang di masukkan akan masuk pada Wi-Fi deauter, dan akan di baca oleh laptop, dan handphone yg sudah login akan terhubung kembali pada jaringan Access Poin yang asli.

Hal- hal yang harus di perhatikan :

- Banyaknya SSID (Service Set IDentifier merupakan nama dari jaringan)
- Kecepatan akses
- Spesifikasi dan kualitas Access Point dan Perangkat Jaringan

Untuk lebih jelasnya bisa dilihat pada gambar 3.1 :



Gambar 3. 1 Gambar Ilustrasi

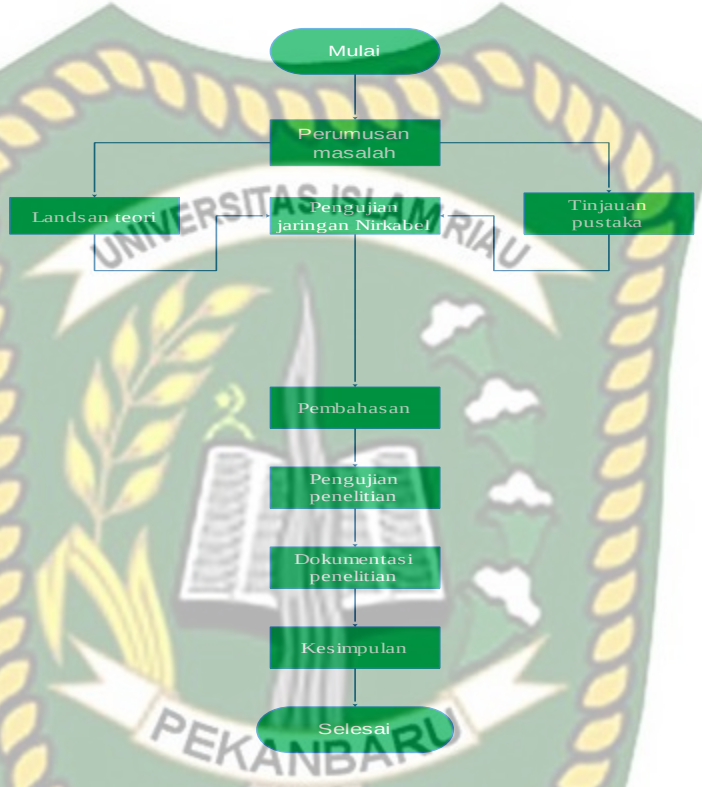
3.1.3 Desain penilitian

1. Gambaran umum penelitian

Dalam hal ini telah di jabarkan diatas bahwa dengan rumusan masalah yang telah tentukan, pengujian keamanan WPA2 juga diambil dari beberapa penelitian sebelumnya yang di rangkum kedalam landasan teori dan tinjauan pustaka. Kemudian untuk memulai penelitian ini dengan, mengujian perangkat nirkabel/ Wi-Fi pastikan ada Wi-Fi yang menyala di sekiran tempat pengujian berlangsung, kemudian jika sudah terdeteksi, masuk ketahap selanjutnya yakni pembahasan, yang mana menguji keamanan WPA2 dengan Wi-Fi deauther dengan metode fluxion pada perangkat router wireless totolink N300RT. Tahapan selanjutnya dokumentasi dalam setiap kegiatan yang di lakukan dalam pengujian, mulai dari setting alat

sampai dengan hasil membobol/ dapat mengambil password Wi-Fi dengan memutus perangkat HP yg terhubung yakni keamanan WPA2. Kemudian hasil dari penelitian ini di masukkan dalam kesimpulan yang berupa laporan.

Untuk lebih jelasnya bisa dilihat pada gambar 3.2 :

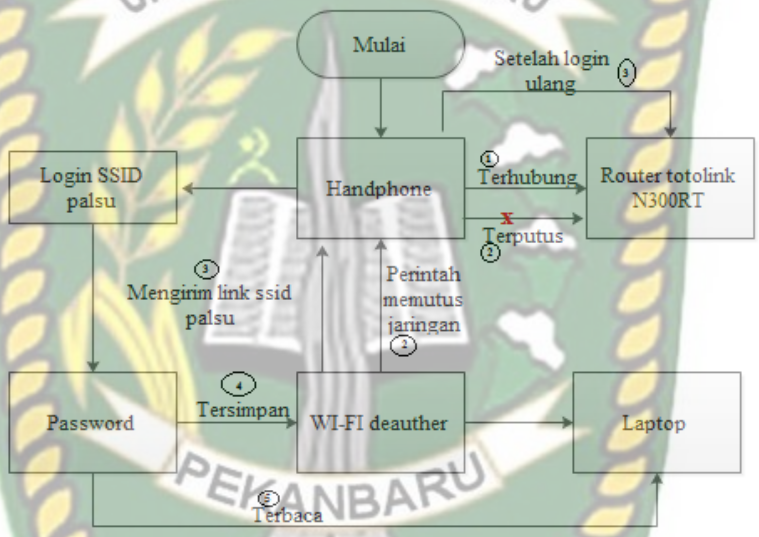


Gambar 3. 2 Alur Gambaran Umum Penelitian

2. Alur penelitian

Tahapan untuk melakukan uji keamanan pada WPA2 ini di mulai dari penyediaan sebuah handphone untuk target dan sebuah router totolink N300RT yang berfungsi untuk pemancal sinyal. Kemudian aktifkan keduanya dan pastikan handphone terhubung pada router totolink N300RT. Kemudian hubungkan perangkat Wi-Fi deauther dengan laptop menggunakan kabel USB dan Pastikan laptop terhubung pada SSID dari Wi-Fi deauther. Pertama buka google crome, lalu

masukkan IP address dari Wi-Fi deauther pada kolom pencarian kemudian tekan tombol enter, maka akan muncul interface perangkat Wi-Fi deauther. Untuk melihat Access Poin yang aktif tekan tombol scan dan memutus perangkat hp dari jaringan Wi-Fi dengan pilih terlebih dahulu Access Point tujuan, kemudian tekan tombol *start deauth* kemudian perintah untuk target login ulang tekan tekan *start evil twin.* Jika berhasil maka akan muncul nama jaringan atau SSID dan password yang telah di masukkan target.

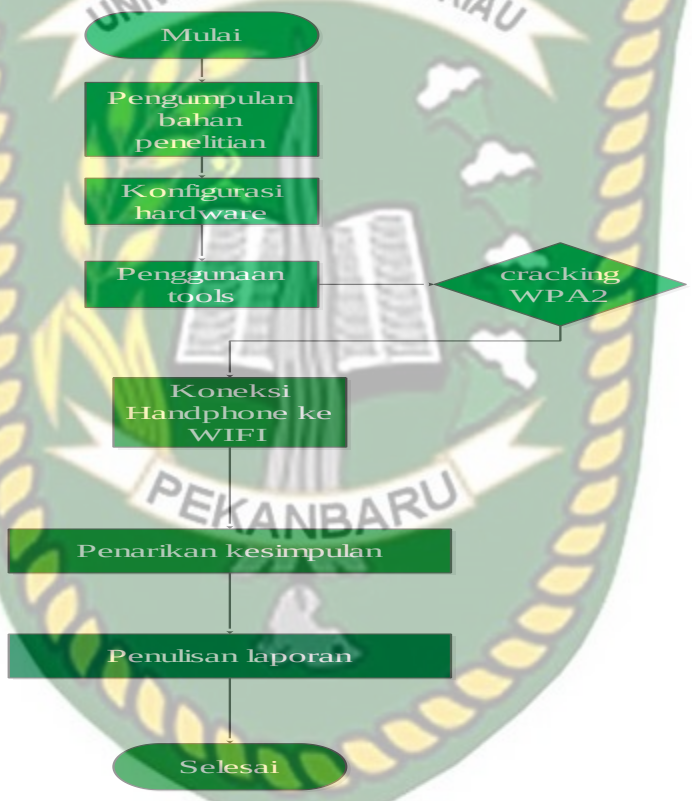


Gambar 3. 3 Gambar alur penelitian uji keamanan WPA2

3. Flowchart IDS (Introduction Detection System)

Dalam IDS ini akan menjelaskan tahap dalam penelitian. Yang mana penelitian ini akan mengumpulkan perangkat yang di butuhkan dalam penelitian ini mulai dari hardware dan software. Kemudian dilanjutkan pada konfigurasi *hardware* yaitu router wireless N3000RT . Kemudian penyerangan yang di lakukan oleh Wi-Fi deauther tahap pertama perangkat hp akan terputus dari SSID asli, kemudian Wi-Fi

deauther mengirimkan link pada perangkat handphone yang telah terputus untuk login ulang, jika client merespon maka target di minta login ulang pada Wi-Fi, jika benar target akan terhubung kembali pada jaringan Wi-Fi asli . secara otomatis password pada Wi-Fi target terdeteksi dan tersimpan pada perangkat router Wi-Fi deauther yang terbaca oleh laptop. Kemudian hasil dari penelitian akan di simpulkan dalam sebuah laporan. Untuk lebih jelasnya bisa dilihat pada gambar 3.3 :



Gambar 3. 4 Gambar Flowchart IDS

3.1.4 Rancangan Sistem

Dalam kelancara sangat di perlukan merancang yang lebih matang, yang mana bertujuan untuk memudahkan dan mengatur alur dalam sebuah sistem dalam penelitian. Di antaranya :

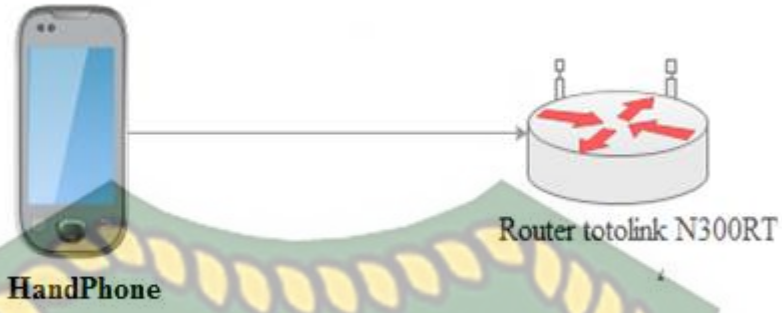
- Setting perangkat

Dalam hal penelitian ini, setting hanya di perlukan untuk perangkat totolink N300RT yang berlaku sebagai contoh dari perangkat router Wi-Fi. Agar memperjelas keterangan di atas, maka penulis akan di jelaskan pada gambar di bawah ini :

Gambar 3. 5 Setting router totolink N300RT

- Menghubungkan perangkat

Pastikan perangkat handpone terhubung dengan Wi-Fi, yang mana router totolink N300RT berpesan sebagai perangkat router totolink .



Gambar 3. 6 Gambar handpone terhubung ke router Wi-Fi totolink N300RT

- Penyerangan pada WPA2

Pada mode penyerangan dari Wi-Fi deauther akan berpatok pada perangkat yang terpasang pada *HandPhone* yang telah terhubung pada Wi-Fi, kemudian Wi-Fi deuther memutus jaringan Wi-Fi pada *HandPhone* yang bertujuan agar *HandPhone* tersebut menyambungkan ulang ke Wi-Fi yg di tuju melalui AP paslu yang terlah di buat, jika *HandPhone* memilih SSID (nama jaringan Wi-Fi) palsu, maka secara otomatis password dari jaringan Wi-Fi tersebut tersimpan pada perangkat Wi-Fi deauther.

Gambar 3. 7 Gambar penyerangan pada WPA2

- Cara kerja perangkat Wi-Fi deauther

Semua SSID akan terdeteksi pada perangkat Wi-Fi deuher dengan menu scan, kemudian pilih salah satu SSID, dikarenakan di penelitian ini menggunakan totolink N300RT, pilih SSID TOTOLINK_N3OORT, kemudian pilih menu start deauth, maka secara otomatis perangkat *HandPhone* akan putus, kemudian pilih menu start evil twin maka perangkat yang terputus di arahkankan ke menu AP palsu yang persis dengan nama AP asli . Jika selesai target akan terhubung kembali ke AP asli dan secara otomatis pula password yang di masukkan tadi akan tersimpan pada Wi-Fi deather. Agar memperjelas keterangan di atas, maka penulis akan di jelaskan pada gambar di bawah ini :

Gambar 3. 8 Gambar alur uji keamanan WPA2 pada perangkat router wireless totolink N300RT

BAB IV
HASIL DAN PEMBAHASAN

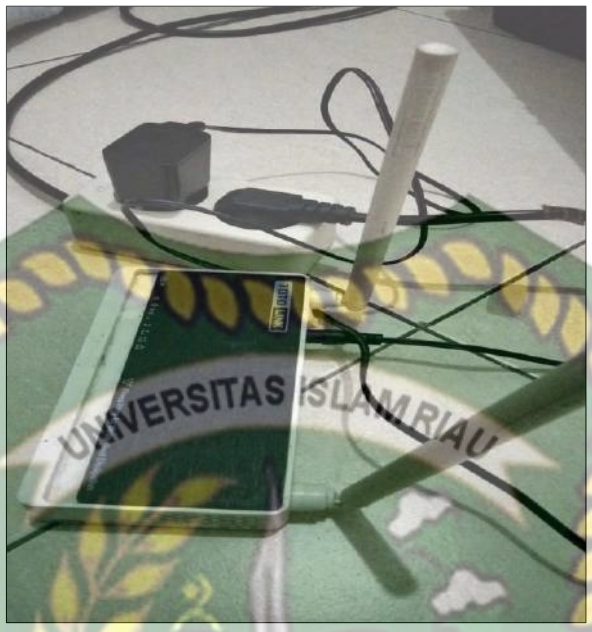
4.1 Hasil Sebelum Konfigurasi

Sebelum melakukan proses konfigurasi penulis akan menjelaskan tahap awal yang harus di lakukan.

1. Pastikan router totolink N300RT tersambung pada daya kemudian tekan tombol powernya, dan pastikan lampunya hidup.

Gambar 4. 1 Gambar setelah tombol power di hidupkan

Maka router akan memproses kemudian lampu akan menyala berwarna kuning yang menandakan router telah siap digunakan.



Gambar 4. 2 Gambar router ready

2. Pastikan target (Handphone) terhubung pada SSID

Gambar 4. 3 Gambar jaringan Wi-Fi terhubung

4.2 Konfigurasi Router Wireless Totolink N300RT

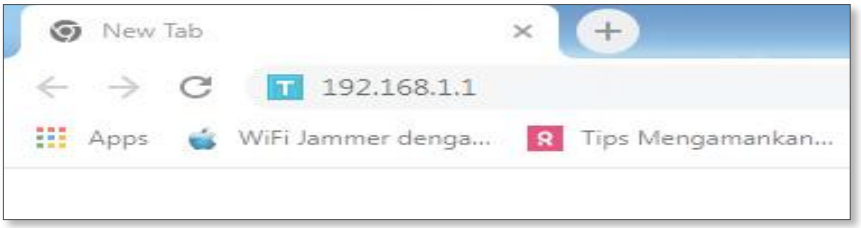
Tahap- tahap yang harus di lakukan saat konfigurasi totolink:

a. Hubungan Wi-Fi totolink pada laptop

Gambar 4. 4 Gambar Wi-Fi totolink N300RT terhubung ke laptop

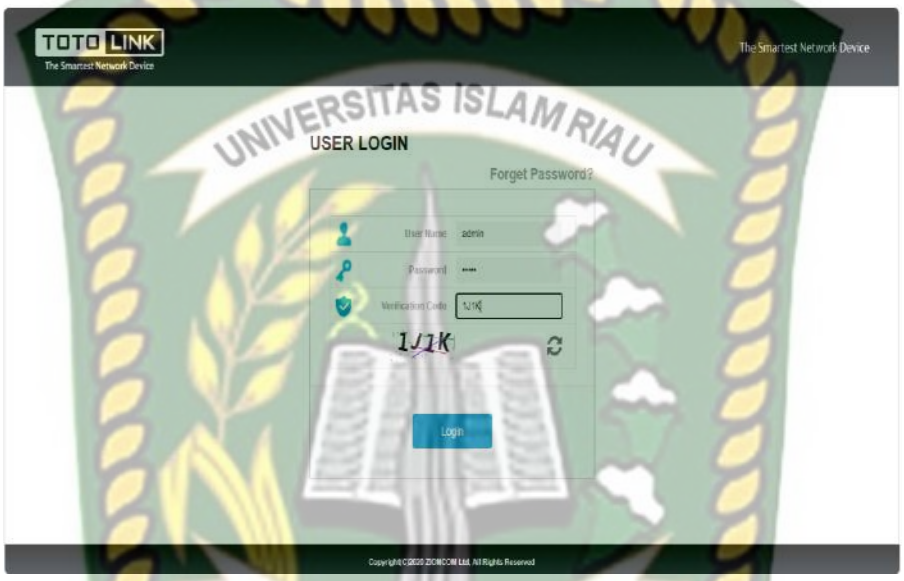
b. Masuk kan IP 192.168.1.1 pada browser

Setelah masukkan IP pada browser kemudian ketak Enter,



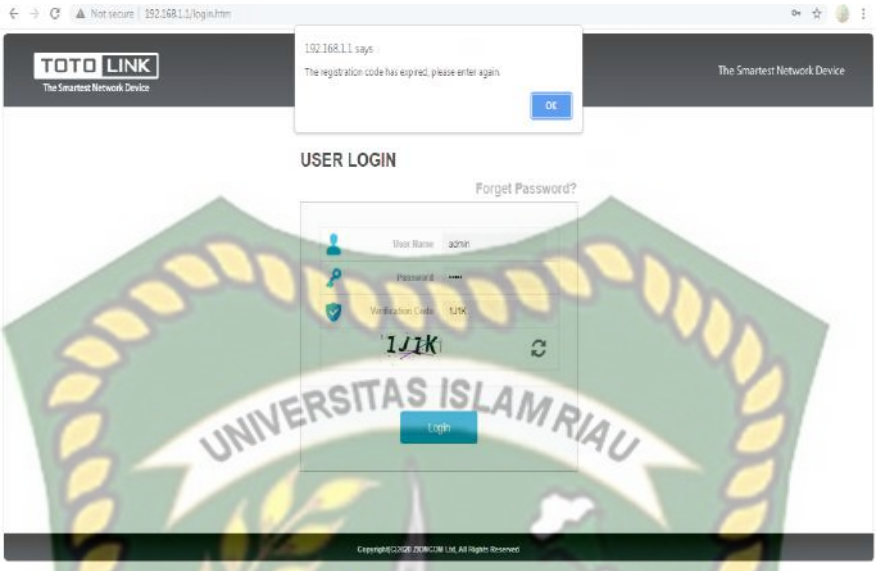
Gambar 4. 5 Gambar IP totolink N300RT

Maka akan muncul form login. Kemudian isi form dengan username : admin, Password : admin, dan isi verification code sesuai kode yang di tampilkan pada layar. Kemudian klik login.



Gambar 4. 6 Gambar Gambar form login

Jika jarak menekan login terlalu lama, maka akan muncul registrasi code kadaluarsa. Dan diminta untuk login ulang.



Gambar 4. 7 Gambar kode Login Kadaluarsa

Kemudian tekan ok pada pada pesan tersebut, maka otomatis akan muncul verifikasi code baru. Kemudian ulang masukkan kode verifikasi yang baru, kemudian tekan ok.

Gambar 4. 8 Gambar Login Verifikasi Baru

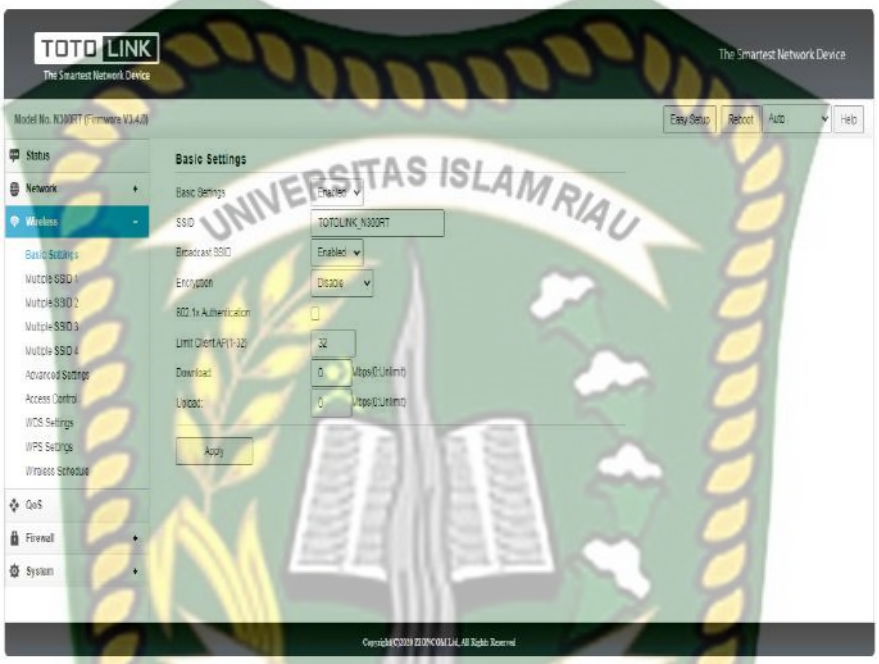
Setelah tekan ok pada form login, maka akan muncul tampilan *Interface* pada totolink N300RT

Gambar 4. 9 Gambar interface totolink

Kemudian untuk konfigurasi, tekan *Advanced* setup pada kanan atas layar, maka akan muncul tampilan setting pada layar.

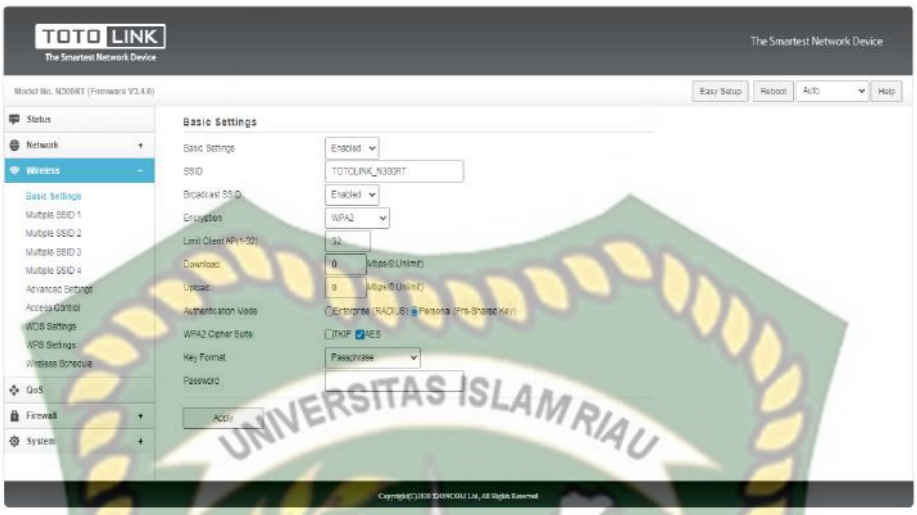
Gambar 4. 10 Gambar Layar Setting Totolink

Kemudian, untuk konfigurasi untuk router totolink N300RT, pilih menu basic setting, lalu konfigurasi menu-menu yang yang perlu di ubah, SSID boleh dengan nama yang kita ingin kan.



Gambar 4. 11 Gambar menu *wireless-basic* setting

Encryption pilih WPA kemudian otomatis mucul field tambahan, Authentication Mode pilih *Personal (Pre-Shared Key)*, WPA2 Cipher Suite pilih *AES*, Key Format pilih *passhrase* dan Password isi sesuai dengan yang pengguna inginkan kemudian klik apply.



Gambar 4. 12 Gambar penyelesaian konfigurasi

Kemudian koneksi jaringan Wi-Fi router totolink N300RT terputus secara otomatis.

Gambar 4. 13Gambar tampilan akhir

4.3 Hasil Pengujian Keamanan WPA2 Menggunakan Wi-Fi Deauther

Penelitan ini membahas tentang uji coba keamanan WPA2 yang mana dalam penelitiannya menggunakan alat- alat pendukung seperti di bawah ini:

- Latop Berfungsi sebagai alat penyerang target

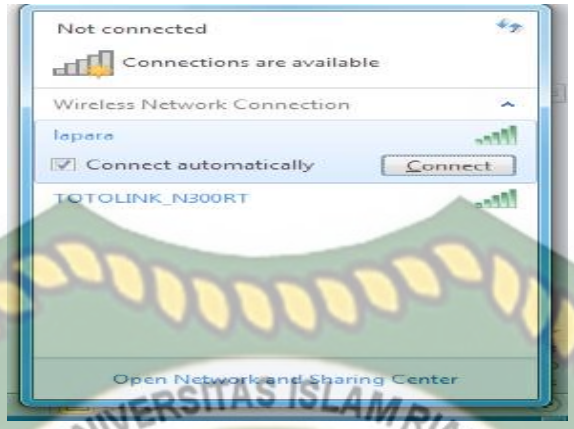
- Kabel USB Berfungsi untuk menyambungkan Wi-Fi deauther ke laptop
- Wi-Fi Deauther Berfungsi sebagai perangkat yang pelacak Wi-Fi yang mana bertugas untuk memutus dan mengambil password Wi-Fi target
- HandPhone Berfungsi sebagai target

Tahap Pengujian Keamanan WPA2 Menggunakan Wi-Fi Deauther:

1. Untuk memulai uji keamanan WPA2, hubungkan Wi-Fi deauther dengan laptop menggunakan kabel USB.

Gambar 4. 14 Gambar WI-FI deauther dengan laptop menggunakan kabel USB

2. Hubungkan jaringan ke SSID Wi-Fi deuther yang bernama lapara pada jendela *Wireless Network connetion,* dengan meng klik SSID lapara, klik connect.



Gambar 4. 15 Gambar jendela *Wireless Network connetion*

Muncul jendela *Connet to network*, masukkan secutity key : *password* , kemudian klik oke. Maka lapara akan terhubung pada laptop.

Gambar 4. 16 Gambar jendela *Connet to network*

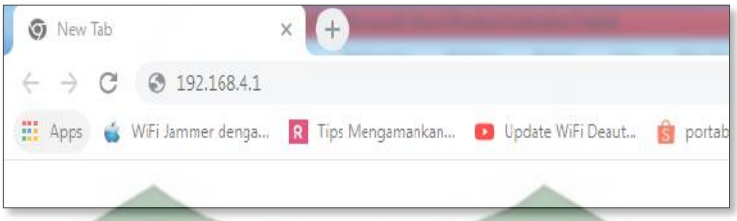
SSID lapara ter koneksi.

Gambar 4. 17Gambar SSID lapara ter koneksi

3. Kemudian, pastikan Handphone terhubung pada SSID router totolink N300RT

Gambar 4. 18 Gambar SSID router totolink N300RT

4. Kembali ke laptop, Masuk ke *browser* kemudian ketik IP 192.186.4.1 lalu tekan Enter



Gambar 4. 19 Gambar jendela *browser*

Kemudian akan muncul *interface* perangkat Wi-Fi deauther, target masih dalam keadaan *default* :

Target

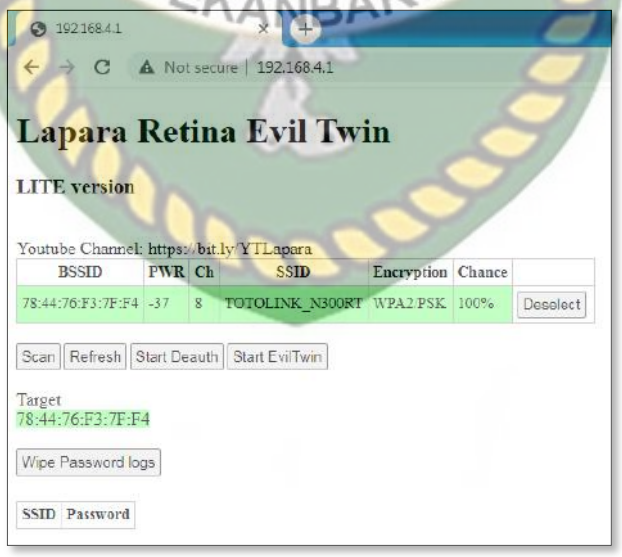
FF:FF:FF:FF:FF:FF

Gambar 4. 20 Gambar interface perangkat Wi-Fi deauther

5. Klik field **SCAN** yang berfungsi untuk melacak Wi-Fi yang aktif

Gambar 4. 21 Gambar hasil tombol *SCAN*

6. Klik **Select** yang berfungsi untuk memili SSID yang akan di pilih. Dalam hal ini klik SSID TOTOLINK_N300RT, maka akan muncul BSSID pada **Target**.



Gambar 4. 22 Gambar field select

7. Klik start **Start deauth** yang berfungsi untuk memutus jaringan Wi-Fi yang tersambung pada perangkat HP (HandPhone)

Gambar 4. 23 Gambar Sart deauth

8. Maka jaringan yang ada di Handphone (HP) akan terputus dan Access Poin dengan nama Wi-Fi (SSID) yang sama akan menjadi ganda.

Gambar 4. 24 Gambar SSID ganda

Klik **Start Evil Twin** berfungsi untuk mengirimkan link SSID palsu dengan meng klik SSID TOTOLINK-N300RT maka akan mucul link SSID palsu maka target di minta untuk mengisi password ulang atau login ulang.

Gambar 4. 25 Gambar Start Evil Twin

Gambar 4. 26 Gambar pengisian password

Setelah mengisi password atau login ulang, maka secara otomatis password yang telah dimasukkan akan terbaca oleh perangkat laptop dan tersimpan pada perngkat Wi-Fi deauther. Dengan cara meng refresh kembali jendela interface pada Wi-Fi deauther, kemudian muncul target yang telah dipilih sebelumnya kemudian SSID dan password yang telah di masukkan oleh target dan walaupun benar jika tertekan double atau lebih maka satu yang terbaca benar,perangkat sistem dari Wi-Fi deauther membutuhkan proses beberapa detik untuk dapat memproses jaringan Wi-Fi target.

Keterangan :

- Merah yang berarti password salah
- Hijau yang berarti password benar

Gambar 4. 27 Gambar Hasil login target

9. Klik Wipe Password Longs yang berfungsi untuk mengapus riwayat password yang telah berhasil di ambil dari perangkat HandPhone target.

Gambar 4. 28 Gambar Wipe Password Logs

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pembahasan yang sudah di di paparkan dalam peneletian ini yang berjudul analisis metode fluxion menggunakan Wi-Fi deauther untuk uji keamanan WPA2 pada perangkat router wireless totolink N300RT, maka dapat disimpulkan sebahai berikut :

1. Pada *script fluxion* proses pengambilah *password* sangat berpengaruh, jika *password* tidak ditemukkan proses kerja *script* tidak akan berhasil, dan pada Wi-Fi minimal mempunyai satu user yang sedang login karena *password* didapatkan oleh user yang sedang melakukkan aktivitas pada jaringan tersebut.
2. Awalan Handphone yang terhubung akan terputus terlebih dahulu. Kemudian a SSID telah menjadi ganda, maka target akan kebingungan dan memilih salah satu dari SSID, jika terpilih SSID palsu maka akan di alihkan lansung dengan login dari SSID palsu dan jika taget login menggunakan SSID asli maka target password target akan terbaca dan target akan masuk ke jaringan awal tanpa target menyadari bahwa SSID yang di masuki itu SSID pals. Namun jika terpilih SSID asli maka akan lansung terhubung pada jaringan awal dan tidak akan terjadi proses login ulang.
3. *Script fluxion* masih menggunakan teknik *social engineering* yang begitu tampak jelas pada bagian ketika korban telah terhubung pada jaringan palsu dan diminta untuk memasukkan ulang *password.*

5.2 Saran

Simulasi yang sedang di bangun ini sangat jauh dari kata sempurna terdapat Kekurangan. Untuk itu sangat di perlukannnya pengembangan lebih lanjut agar Simulasi ini bisa sempurna, adapun saran dari simulasi ini

- Agar bisa lebih baik lagi seperti Penggunaan metode yang tidak menimbulkan kecurigaan pada target.
- Perangkat *wireless* dengan berkeamanan WPA2 yaitu *tethering android, mifi,* dan *access point TP- LINK,* masih mempunyai celah untuk diretas menggunakan *script fluxion* melalui penggabungan beberapa metode penyerangan meliputi penggunaan *fake AP, handshake , mdk3,* dan *fake DNS.*

DAFTAR PUSTAKA

Arsih peni. 2017. Penerapan evil twin detektor dalam pendekatan penggnaggu jaringan nirkabel pada user. Vol 4, No 2

Abraham Yano Suharmanto, Arie S.M Lumenta, Xaverius B.N. Najoan. 2018. Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi. Manado : Jurnal Teknik Informatika Vol 13, No 3, ISSN : 2301-8364

Fajri Ahmad. 2019. Studi Empiris Terhadap Kinerja & Keamanan Wi-Fi (Studi Kasus Di Kota Depok) Vol 6, No. 6, p-ISSN: 2355-7699 e-ISSN: 2528-6579

Https://www.pinhome.id/kamus-istilah-properti/wireless/

Https://www.cisco.com/c/en/us/products/wireless/what-is-Wi-Fi.html

Https://www.baktikominfo.id/id/informasi/pengetahuan/mengetahui_tentang_sistem_keamanan_jaringan_untuk_proteksi_perangkat_komputer_anda-677

Https://www.pinhome.id/kamus-istilah-properti/wireless/

(https://en.kali.tools/?P=235)

Https://www.baktikominfo.id/id/informasi/pengetahuan/mengetahui_tentang_sistem_keamanan_jaringan_untuk_proteksi_perangkat_komputer_anda-677

Rahman1 Ashiqur , Asaduzzaman Noman2 , Zahidul Islam Akash.2016. Cisco Router Configuration with IP. Volume-5, Issue-7, pp-17-22. e-ISSN: 2320-0847 p-ISSN : 2320-0936

Suharmanto Abraham Yano, Arie S.M Lumenta, Xa Verius B.N Najoan. 2018 .Analisa Keamanan Jaringan Wireles Di Universitas Sam Ratulangi. Manado : Jurnal Teknik Informatika Vol 13, No. 3, ISSN : 2301 : 8364

Suri Hamza Alfan , Widyanto, Taqrim Ibadi. 2016. Analisis *Fluxion* SebagaiProgram Uji Keamanan Wpa2 Pada Perangkat *Wireless*. Palembang

Triyono Eddy, Imelda Erawati Supono P , Muhammad Nashiruddin. 2015.Jammer Untuk Dual Band GSM Dan CDMA. JURNAL TELE Volume 13 Nomor 2 Edisi Oktober 2015