ANALISA UJI KEAMANAN WPA2 MENGGUNAKAN FLUXION PADA PT. ANDAGLOS GLOBAL TEKNOLOGI

PROPOSAL SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Mencapai Gelar
SARJANA KOMPUTER
Jurusan Teknik Informatika

Institut Informatika dan Bisnis darmajaya

Disusun Oleh:

Dwi Nanda Widiatama

NPM.1311010112

FAKULTAS ILMU KOMPUTER

JURUSAN TEKNIK INFORMATIKA

INSTITUT INFORMATIKA DAN BISNIS DARMAJAYA

BANDAR LAMPUNG

2019

PERNYATAAN

Saya yang bertanda tangan dibawah ini, menyatakan bahwa skripsi yang saya buat ini adalah hasil karya saya sendiri, tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi atau karya yang pernah ditulis atau diterbitkan orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka. Karya ini adalah milik saya dan pertanggung jawaban sepenuhnya berada di pundak saya.

Bandar Lampung,17 September 2019

Dwi Nanda Widiatama

NPM 1311010112

HALAMAN PERSETUJUAN

Judul Skripsi	:ANALISA UJI KEAMANAN WPA2 MENGGUNAKAN FLUXION PADA PT. ANDAGLOS GLOBAL TEKNOLOGI
Nama	:**Dwi Nanda Widiatama**
Npm	:1311010112
Jurusan	:Teknik Informatika

Menyetujui :

Pembimbing	Ketua Jurusan Teknik Informatika
Rionaldi Ali S.kom., M.TI	Yuni Arkhiansyah, S.Kom., M.Kom
NIK. 12710212	NIK. 00480802

HALAMAN PENGESAHAN

Pada tanggal 17 September 2019, Ruang G.1.4 telah diselanggarakannya sidang hasil penelitian (skripsi) dengan judul: Analisa Uji Keamanan WPA2 Menggunakan Fluxion Pada PT.Andaglos Global Teknologi. Sebagian persyaratan akademik guna memperoleh gelar Sarjana Komputer, bagi mahasiswa;

Nama Mahasiswa : Dwi Nanda Widiatama

NPM : 1311010112

Program Studi : Teknik Informatika

Dan telah dinyatakan LULUS oleh dewan penguji yang terdiri dari :

Mengesahkan

Nama	Status	TandaTangan
1. **Dr. Suhendro Yusuf Irianto**	**Penguji I**	
2. **Yuni Arkhiansyah.S.Kom.,M.Kom**	**Penguji II**	

Dekan Fakultas Ilmu Komputer IIB Darmajaya

Sriyanto, S.Kom., M.M

NIK. 00210800

BIODATA PENULIS

Nama	: DWI NANDA WIDIATAMA
NPM	: 1311010112
Tempat/Tanggal lahir	: Curup, 29 juli 1994
Agama	: Islam
Suku	: Jawa
Kewarganegaraan	: Indonesia
E-mail	: nandasangpetani@gmail.com
Hp	: 089678970666

RIWAYAT PENDIDIKAN

SD (2001-20007)	:SDN 1 PEKALONGAN
SMP (2007-2010)	:SMPN 2 METRO
SMA (2010-2013)	:SMAN 4 METRO
S1 (2013-2019)	:Teknik Informatika S1 IIB DARMAJAYA Bandar Lampung

Bandar Lampung, 17 September 2019

Dwi Nanda Widiatama

HALAMAN PERSEMBAHAN

Karya ini kupersembahkan kepada :

1. Allah SWT, atas berkat karunia-Nya yang telah diberikan serta pengetahuan yang diturunkan kepada penyusun.
2. Kedua orang tua dan kakak-kakakku yang selalu menyayangi dan mendoakanku dan selalu percaya akan apa yang aku lakukan.
3. Dosen pembimbingku bapak Rionaldi Ali S.Kom., M.TI yang selalu sabar membimbingku dan mengarahkanku sehingga laporan ini dapat diselesaikan.
4. Keluarga besar Teknik Informatika,dan teman- teman yang telah memberikan semangat dan dukungan agar aku terus berjuang untuk menyelesaikan skripsi ini, Terimakasih.
5. Almamaterku tercinta Institut Informatika dan Bisnis (IIB) Darmajaya yang telah mendewasakan dan memberikanku banyak ilmu.

MOTTO

"SEORANG PEMALAS"

"AKAN MENCARI CARA YANG MUDAH"

"UNTUK MENYELESAIKAN"

"PEKERJAAN YANG SULIT"

KERJA CERDAS BUKAN KERJA KERAS

ABSTRAK

ANALISA UJI KEAMANAN WPA2 MENGGUNAKAN FLUXION PADA PT. ANDAGLOS GLOBAL TEKNOLOGI

OLEH

DWI NANDA WIDIATAMA

1311010112

PT.Andaglos Global Teknologi menggunakan layanan provider internet dan di lengkapi fasilitas wifi, lokasi kantor yang terletak di terminal dan berdempetan dengan ruko dan bangunan lainya mengakibatkan jaringan wifi pada PT.Andaglos Global Teknologi dimanfaatkan oleh pengguna secara illegal, Sehingga berdampak pada kecepatan internet yang menurun (lambat), serta informasi dari kariawan PT.Andaglos Global Teknologi mengaku pernah menjadi korban hacking pada social medianya setelah mengakses menggunakan jaringan pada PT.Andaglos global Teknologi

Untuk Membuktikan kebenaran tersebut maka dilakukan uji penetration testing menggunakan *fluxion* pada jaringan PT.Andaglos Global Teknologi dengan metode (*Action Reasearch*) yang mana terdapat beberapa tahapan yaitu *Diagnosing*, *Action Planing*, *Action Taking*, *Evaluating* dan *Specifyng Learning*, untuk membuktikan apakah keamanan jaringan tersebut dapat di tembus.

Uji penetration testing dengan fluxion membuktikan bahwa Keamanan jaringan pada PT. Andaglos Global Teknologi berjalan baik dalam mengamankan kata sandi, namun fluxion terbuki mampu mendapatkan kata sandi dari jaringan tersebut, tidak dengan cara membobol keamanan melainkan dengan cara menipu pengguna jaringan tersebut dengan membuat form login yang sama dengan router yang dipakai PT.Andaglos Global Teknologi , sehingga tanpa sadar pengguna jaringan telah memberikan kata sandi tersebut kepada pengguna fluxion, yang mana mengakibatkan jaringan dapat di akses oleh pengguna secara ilegal.

Kata Kunci: Fluxion, Wireless Hacking, Pentetration Testing.

ABSTRACT

ANALYSIS OF WPA2 SECURITY TEST IN PT. ANDAGLOS GLOBAL TECHNOLOGI USING FLUXION

By:
DWI NANDA WIDIATAMA
1311010112

PT. Andaglos Global Technologi uses internet provider services and is equipped with facilities such as wi-fi. The office is located in the bus terminal and attached to the shop houses and other buildings resulting that the wi-fi network at PT. Andaglos Global Teknologi is used by users illegally, causing a decreased internet speed (slow). Besides, it was found that PT.Andaglos Global Teknologi was claimed to have been a victim of hacking in the social media after accessing the network at PT. Andaglos Global Teknologi.

To prove this, the penetration testing was conducted using fluxion on the PT. Andaglos Global Teknologi network with the method (Action Reasearch) in which there were several stages, namely *Diagnosing*, Action *Planning*, *Action Taking*, *Evaluating* and *Specifying Learning*, to prove whether the network security was translucent.

The penetration testing with Fluxion proved that the network security at PT. Andaglos Global Technologi worked well in securing the passwords, but Fluxion was able to get the passwords from the network, not by breaking into the security but by deceiving the network the users by creating the same login form as the routers used by PT. Andaglos Global Teknologi, so unconsciously the network users gave the password to Fluxion users, which resulted in the network being accessed by users illegally.

Kata Kunci : Fluxion, Penetration Testing, Wireless Hacking

PRAKATA

Puji syukur kepada Allah SWT, karena atas Ridho dan Rahmat-Nya penulis dapat menyelesaikan laporan tugas akhir ini meskipun masih banyak permasalahan dan hambatan yang ikut menyertai. Penulis mohon maaf, jika laporan tugas akhir yang penulis buat masih banyak kekurangan dan kelemahan. Untuk itu penulis berharap kepada seluruh pembaca dapat memberikan saran dan kritik positif yang bersifat membangun demi kesempurnaan tugas akhir yang penulis buat.

Dalam kesempatan ini penulis mengucapkan terimakasih kepada:

1. Bapak Andi Desfiandi, S.E., M.A, Selaku Ketua Yayasan Alfian Husein Institut Informatika dan Bisnis Darmajaya Bandar Lampung.
2. Bapak Ir.Firmansyah YA, MBA., MSc, Selaku Rektor Institut Informatika dan BisnisDarmajaya Bandar Lampung.
3. Bapak Dr. RZ. Abdul Aziz, S.T., M.T, Selaku Wakil Rektor I Bidang Akademik dan Kemahasiswaan, dan Dekan Fakultas Ilmu Komputer Institut Informatika dan Bisnis Darmajaya Bandar Lampung.
4. Bapak Yuni Arkhiansyah, S.Kom., M.Kom, Selaku Ketua Jurusan Teknik Informatika Institut Informatika dan Bisnis Darmajaya Bandar Lampung.
5. Bapak Rionaldi Ali, S.Kom., M.TI, Selaku Dosen Pembimbing yang telah berkenan membimbing dan membantu dalam menyelesaikan skripsi ini.
6. Orang Tua dan Kakak-Kakakku tersayang terimakasih karena telah memberikan semangat, doa dan mencukupi segala keperluan serta mendukungku.
7. Dosen, Staff dan Karyawan Institut Informatika dan Bisnis Darmajaya Bandar Lampung yang telah memberi bantuan baik secara langsung maupun tidak langsung selama saya menjadi mahasiswa.
8. Keluarga Besar PT. Andaglos Global Teknologi Terutama untuk Bapak Budi Sutrisno S.Kom,. M.E yang telah memberikan saran dan membantu memberikan data yang dibutuhkan dalam menyusun skripsi ini.

9. Terimakasih pada sahabatku Samsul Nugroho yang telah menemani dan membantuku dalam menyelesaikan skripsi ini.
10. Terimakasih untuk teman-teman Teknik Informatika dan semua pihak yang tidak dapat saya sebutkan satu persatu, terimakasih atas bantuan dan petunjuknya sehingga saya dapat lebih mudah dalam menyusun skripsi ini.
11. Almamaterku tercinta.

Saya menyadari bahwa skripsi ini masih jauh dari kesempurnaan, baik dalam pembahasan materi maupun dalam penyajiannya, oleh karena itu kritik dan saran yang sifatnya membangun merupakan masukan yang sangat berarti bagi penyempurnaan dimasa yang akan dateng. Semoga skripsi ini bermanfaat dan dapat dijadikan bahan pertimbangan informasi bagi pihak yang berkepentingan.

Bandar Lampung, 17 September 2019

Dwi Nanda Widiatama

1311010112

DAFTAR ISI

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

PT. Andaglos global teknologi adalah sebuah startup yang bergerak di bidang jasa pembuatan aplikasi dan software, yang mana sebagian bersar karyawan nya tidak terfokus pada keamanan jaringan, padahal PT. Andaglos global teknologi menggunakan layanan provider internet dan dilengkapi fasilitas wifi, lokasi kantor yang terletak di terminal berdempetan dengan ruko dan bangunan lainya serta pengetahuan karyawan yang kurang mengenai keamanan jaringan mengakibatkan jaringan wifi pada PT. Andaglos global teknologi dimanfaatkan oleh pengguna secara illegal, sehingga berdampak pada kecepatan bandwitch internet yang menjadi menurun (lemah), serta dari informasi yang di dapat dari salah satu karyawan PT. Andaglos global teknologi mengatakan bahwa dirinya pernah menjadi korban *hacking* pada akun *social* medianya setelah mengakses menggunakan jaringan pada PT. Andaglos global teknologi.

padahal security harus dijaga dengan landasan UU ITE 2008 pasal 15 ayat (1), (2), dan (3) yang berbunyi :

(1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.

(2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.

(3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Metode penetration testing dapat digunakan untuk menjaga keandalan dan keamanan sistemnya melalui serangkaian uji coba keamanan terhadap sistem tersebut, sehingga salah satu cara yang dapat ditempuh untuk memenuhi sarat

berdasarkan UU ITE 2008 adalah dengan melakukan serangkaian uji coba pada sistem tersebut.

Tindakan untuk mendapatkan *password* secara paksa bertentangan dengan, UU ITE jo pasal 46 ayat 3 tahun 2008 yang menyebutkan bahwa, setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan system *elektronik* dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengaman (*cracking, hacking, illegal access)* akan dikenakan hukuman seperti yang tertera pada jo pasal 46 ayat 3 berupa ancaman pidana penjara paling lama 8 tahun atau denda paling banyak Rp.800.000.000,.

1.2 Rumusan Masalah

1. Bagaimana cara menerapkan penetration testing pada sistem PT. Andaglos Global Teknologi
2. Rekomendasi apa saja yang dapat menjadi masukan bagi sistem PT.Andaglos Global Teknologi agar dapat menjaga keamanan sistemnya.

1.3 Ruang Lingkup Penelitian

1. Ruang Lingkup Subjek

   Subjek penelitian ini adalah jaringan wireless pada PT.Andaglos Global Teknologi.
2. Ruang Lingkup Objek

   Objek penelitian ini adalah mengetahui tingkat keberhasilan fluxion dalam mengambil password pada jaringan *(wireless),* pada PT.Andaglos Global Teknologi.
3. Ruang Lingkup Tempat

   Penelitian dilaksanakan di Kantor PT.Andaglos Global Teknologi yang beralamat di Terminal Kemiling Blok R3 No.7, Sumber Rejo, Kemiling, Kota Bandar Lampung.
4. Ruang Lingkup Waktu

Waktu yang ditentukan pada penelitian ini adalah waktu yang didasarkan berdasarkan kebutuhan penelitian yang dilaksanakan pada bulan Desember 2018.

5. Ruang Lingkup Ilmu Penelitian

   Ruang lingkup ilmu penelitian adalah teknik penetration testing terhadap jaringan nirkabel *(wireless).*

6. Batasan Masalah

   Agar ruang lingkup penelitian terarah maka diberi batasan masalah sebagai berikut:

a. Penggunaan aplikasi *Fluxion* untuk menganalisa keamanan jaringan *(wireless)* di PT. Andaglos Global Teknologi
b. Penulis tidak melakukan implementasi peningkatan keamanan jaringan yang sudah ada dan hanya memberikan solusi yang sebaiknya dilakukan untuk mengantisipasi terjadinya serangan seperti yang dilakukan penulis.

1.4 Tujuan Penelitian

1. Menjalankan rangkaian test pada system PT. Andaglos Global Teknologi sehingga dihasilkan rekomendasi atau solusi yang dapat di terapkan pada system PT. Andaglos Global Teknologi.
2. Melakukan pengembangan pada *tool fluxion* dengan penambahan bahasa Indonesia dan penambahan *web interface* pada *directory* fluxion.

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah :

1.5.1 Bagi Perusahaan

1. PT. Andaglos Global Teknologi mampu menjalankan layanan system elektronik dengan baik dan dapat di pertanggung jawabkan sesuai dengan persyaratan seperti dalam UU ITE 2008.
2. PT. Andaglos Global Teknologi memiliki standard dalam memelihara layanan system elektroniknya.

1.5.2 Bagi pengguna

1. Memudahkan pengguuna khususnya yg berada di indonesia untuk melakukan penetration testing dengan fluxion.
2. Memudahkan pengguna dalam menyesuaikan web interface yang dimiliki fluxion dengan merek router yang ada.

1.6 Sistematika Penulisan

Sistematika di dalam penyusunan skripsi adalah sebagai berikut :

BAB I PENDAHULUAN

Bab I merupakan bab pendahuluan yang berisi latar belakang masalah, identifikasi dan perumusan masalah, ruang lingkup penelitian, tujuan penelitian, manfaat penelitian.

BAB II LANDASAN TEORI

Bab II membahas mengenai teori-teori, literatur yang menjadi dasar pembahasan masalah, Ancaman dan Perangkat Lunak Yang digunakan.

BAB III METODE PENELITIAN

Bab III merupakan bab berisikan metode-metode pendekatan penyelesaian masalah yang dinyatakan dalam perumusan masalah seperti jenis analisis kebutuhan non funsional, metode pengumpulan data.

BAB IV ANALISIS

Bab ini menguraikan tentang

1. Hasil Penelitian

2. Analisa atau Pembahasan

BAB V KESIMPULAN DAN SARAN

BAB V merupakan kesimpulan dan saran yang berisi kesimpulan untuk menjawab perumusan masalah dan saran untuk perusahaan demi meningkatan keamanan pada jaringan yang ada di PT.Andaglos Global Teknologi.

DAFTAR PUSTAKA

Berisi daftar buku-buku, jurnal ilmiah, hasil penelitian orang lain, dan bahan-bahan lain yang dijadikan sebagai referensi dalam pembahasan skripsi.

LAMPIRAN

Berisi data yang dapat mendukung atau memperjelas pembahasan atau uraian yang dikemukakan dalam bab-bab sebelumnya. Data-data tersebut dapat berbentuk gambar, tabel, formulir, ataupun flowchart.

BAB II

LANDASAN TEORI

2.1 Konsep Keamanan Jaringan

Pada saat ini issue keamanan jaringan menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker, baik jaringan *LAN* maupun *Wireless*. Pada saat data dikirim akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut. Dalam pembangunan perancangannya, sistem keamanan jaringan yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker*. *Clarke Jason W* (30/3/2015) berpendapat bahwa saat ini fasilitas *Wi-fi* bagi publik menjadi target utama dalam aksi kejahatan *cyber*, oleh karenanya kita tidak beleh menganggap sebuah keamanan jaringan dengan remeh.

Baru-baru ini, forum hacker di dunia maya marak dengan pembahasan tentang sebuah program yang katanya bisa mendapatkan *password wireless* jenis keamanan WPA2 tanpa harus meng-crack algoritma yang digunakan. *Fluxion* adalah sebuah program yang digunakan sebagai alat uji keamanan *wireless* untuk jenis WPA2. Dimana pada program ini mengadopsi dari beberapa teknik yang biasa digunakan untuk mendapatkan sebuah informasi, *Fluxion* berkerja pada sistem operasi *Linux* dan sekarang menjadi populer karena kemudahan penggunaannya, Terbukti dari kepopulerannya di jejaring sosial untuk para developer.

2.2 Ancaman

Pada dasarnya, ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal ke dalam suatu jaringan komputer. Oleh karena itu, harus ditentukan siapa saja yang diperbolehkan mempunyai akses legal ke dalam sistem, dan ancaman-ancaman yang dapat mereka timbulkan. Ada beberapa tujuan yang ingin dicapai oleh penyusup dan, sangat berguna apabila dapat membedakan tujuantujuan tersebut pada saat merencanakan sistem keamanan jaringan komputer. Beberapa tujuan para penyusup adalah:

a. Pada dasarnya hanya ingin tahu sistem dan data yang ada pada suatu jaringan komputer yang dijadikan sasaran. Penyusup yang bertujuan seperti ini sering disebut dengan the curius.

b. Membuat sistem jaringan menjadi down, atau mengubah tampilan situs web. Penyusup yang mempunyai tujuan seperti ini sering disebut sebagai the malicious.

c. Berusaha untuk menggunakan sumber daya di dalam sistem jaringan komputer untuk memperoleh popularitas. Penyusup seperti ini sering disebut sebagai the high-profile intruder.

d. Ingin tahu data apa saja yang ada di dalam jaringan komputer untuk selanjutnya dimanfaatkan untuk mendapatkan uang. Penyusup seperti ini sering disebut sebagai the competition.

2.3 Jenis Serangan Pada Jaringan

1. *Packet Sniffer*

   Packet Sniffing adalah sebuah teknik pencurian data yang dilakukan dengan cara memonitoring atau melakukan analisis terhadap paket data yang ditransmisikan dari komputer *client ke web server*. *Tool* yang biasa digunakan untuk melakukan

teknik packet sniffing ini biasanya adalah *Wireshark dan Netcut. Packet sniffing* ini biasanya dilakukan oleh para hacker atau penyusup yang berbahaya untuk melakukan tindakan yang dilarang seperti mencuri password, dan pengambilan data-data penting lainnya.

Kemudian untuk cara kerja dari packet sniffing dibagi menjadi 3 yaitu collecting, conversion, analysis, dan pencurian data. Untuk penjelasannya adalah sebagai berikut:

2. *Collecting*

   Cara kerja yang pertama dari *packet sniffing* adalah merubah *interface* yang digunakan menjadi "*promicius mode*", dan mulai mengumpulkan atau mengelompokkan semua paket data yang lewat melalui jaringan dalam bentuk *raw binary*.

3. *Conversion*

   Cara kedua adalah mengkonversi atau merubah data yang berbentuk binary kedalam data yang mudah dibaca atau mudah dipahami.

4. *Analysis*

   Cara kerja ketiga adalah dimana betuk data tersebut diklasifikasikan kedalam sebuah blok-blok protocol berdasarkan sumber dari transmisi data tersebut baik berupa tcp, udp dan masih banyak yang lainya.

5. *ARP Spoofing*

   ARP (Address Resolution Protocol) poisoning ini adalah suatu teknik menyerang pada jaringan komputer lokal baik dengan media kabel atau *wireless*, yang memungkinkan penyerang bisa mengendus *frames* data pada jaringan lokal dan atau melakukan modifikasi *traffic* atau bahkan menghentikan *traffic*. *ARP spoofing* merupakan konsep dari serangan penyadapan diantara terhadap dua mesin yang sedang berkomunikasi atau yang disebut dengan *MITM* (*Man in The Middle Attack)*. Prinsip serangan *ARP poisoning* ini memanfaatkan kelemahan pada teknologi jaringan komputer itu sendiri yang menggunakan *arp broadcast*. *ARP* berada pada layer 2, dimana alamat pada layer dua adalah *MAC address*.

Misalnya sebuah host (contoh: PC) yang terhubung pada sebuah *LAN* ingin menghubungi *host* lain pada *LAN* tersebut, maka dia membutuhkan inforamsi *MAC address* dari *host* tujuan.

6. *Probe*

   Sebuah probe dapat dikenali dari adanya usaha-usaha yang tidak lazim untuk memperoleh akses ke dalam suatu sistem atau untuk menemukan informasi tentang sistem tersebut. Salah satu contohnya adalah usaha untuk login ke dalam sebuah account yang tidak digunakan. *Probing* ini dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan yang dengan mencoba-coba apakah pintunya terkunci apa tidak.

7. *Scan*

   Scan adalah kegiatan *probe* dalam jumlah yang besar dengan menggunakan *tool* secara otomatis. *Tool* tersebut secara otomatis dapat mengetahui port-port yang terbuka pada host lokal maupun *host remote*, *IP address* yang aktif, bahkan bisa untuk mengetahui sistem operasi yang digunakan pada *host* yang dituju.

8. *Account Compromise*

   Account compromise adalah penggunaan *account* sebuah computer secara ilegal oleh seseorang yang bukan pemilik *acoount* tersebut. *Account compromise* dapat mengakibatkan korban mengalami kehilangan atau kerusakan data. Sebuah insiden *account compromise* dapat berakibat lebih lanjut, yaitu terjadinya insiden *root compromise*, yang dapat menyebabkan kerusakan lebih besar.

9. *Brute Force Attack*

   adalah metode untuk meretas password (password cracking) dengan cara mencoba semua kemungkinan kombinasi yang ada pada “wordlist“. Metode ini dijamin akan berhasil menemukan password yang ingin diretas. Namun, proses untuk meretas password dengan menggunakan metode ini akan memakan banyak waktu.korban, termasuk menjalan kanprogram, mengubah kinerja sistem, dan menyembunyikan jejak penyusupan.

10. *Denial Of Service* (DOS)

Sumber daya jaringan yang berharga antara lain komputer dan *database*, serta pelayanan-pelayanan *(service)* yang disediakan oleh organisasi pemilik jaringan. Kebanyakan user jaringan memanfaatkan pelayanan-pelayanan tersebut agar pekerjaan mereka menjadi efisien. Bila pelayanan ini tidak dapat dipergunakan karena sebab-sebab tertentu, maka tentu saja akann menyebabkan kehilangan produktivitas. Sulit untuk memperkirakan penyebab *denial of service*. Berikut ini adalah contoh penyebab terjadinya *denial of service*:

a. Kemungkinan jaringan menjadi tidak berfungsi karena kebanjiran traffic.

b. Kemungkinan ada virus yang menyebar dan menyebabkan sistem *computer* menjadi lamban atau bahkan lumpuh.

c. Kemungkinan *device* yang melindungi jaringan dirusak.

2.3.1 Serangan yang sering terjadi pada jaringan

1. *Packet Sniffer*
2. *ARP spoffing*
3. B*rute force attack*

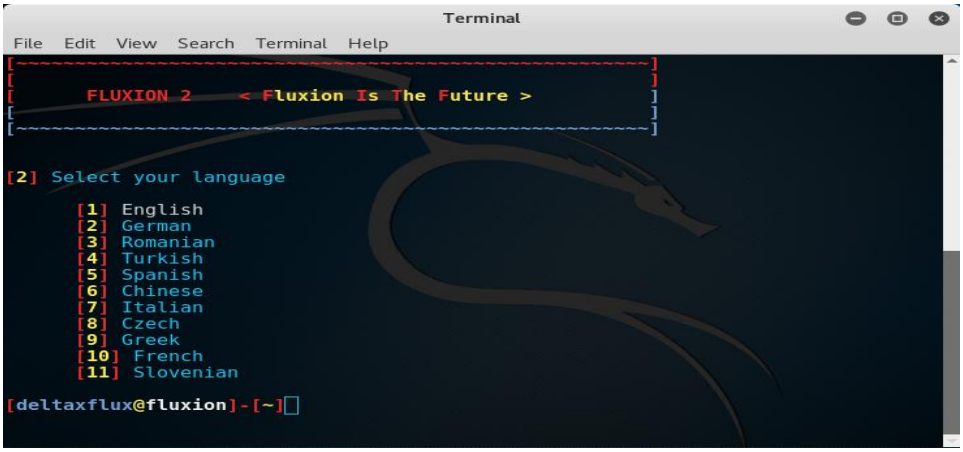
2.4 Perangkat Lunak Yang Digunakan

2.4.1 *Fluxion*

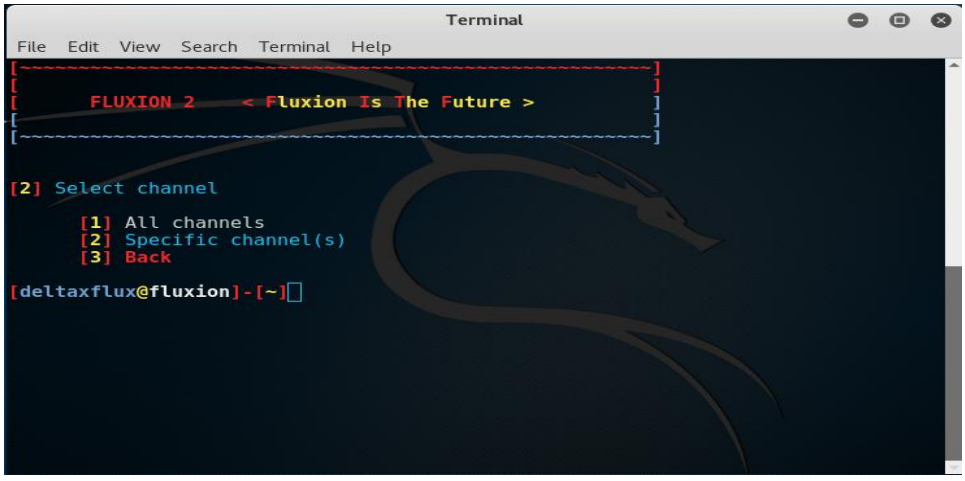
(DO SON 2018) Fluxion adalah alat penelitian audit keamanan dan rekayasa sosial. Ini adalah pengembangan dari linset oleh vk496 dengan harapan yang lebih baik lagi dengan sedikit bug dan lebih banyak fungsi. Skrip mencoba mengambil kunci *WPA2* dari titik akses target dengan menggunakan serangan *(phishing*). atau serngan rekayasa sosial menggunakan titik akses *twin evil* (AP).

Adapun tampilan dan fungsi program fluxion sebagai berikut:

Gambar 2.1 Tampilan awal fluxion



Gambar 2.2 Menampilkan halaman pemilihan Bahasa



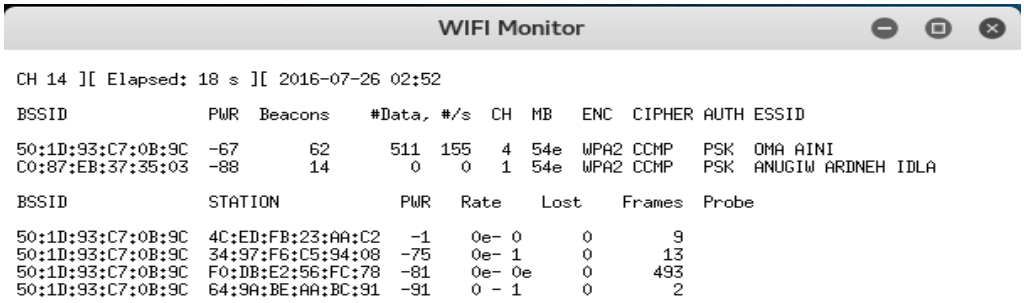
Gambar 2.3 Menampilkan halaman pemilihan channel

1. *All Channels*

   All Channel berfungsi untuk melakukan scan terhadap semua jaringan *(wireless)* yang aktif .

2. *Specific channel (s)*

   Specific Channel berfungsi untuk meilih salah satu dai beberapa jaringan *(wireless)* yang aktif.



Gambar 2.4 Menampilkan *wifi* aktif

2.4.2 Kali Linux

(David Adi Nugroho 2014) Linux adalah salah satu *Operating System* (OS), sama seperti Windows. *Linux* merupakan sistem operasi yang *OPENSOURCE*, artinya *linux* dapat dilihat source codenya, dimodifikasi, dan dikembangkan oleh siapa saja. Asas Linux bermula daripada proses pengembangan *UNIX* yang mana merupakan implementasi bebas dari *POSIX*, *multi-tasking, vitual memory, shared libararies, demand loading, proper memory management,* dan *multi user.*

2.5 Perangkat Keras Yang Digunakan

1. Laptop asus X554L
2. Procecor inter core i5 2.4Ghz
3. RAM 8GB
4. Hardisk 500GB
5. VGA nvidia gforcer 920M 1GB

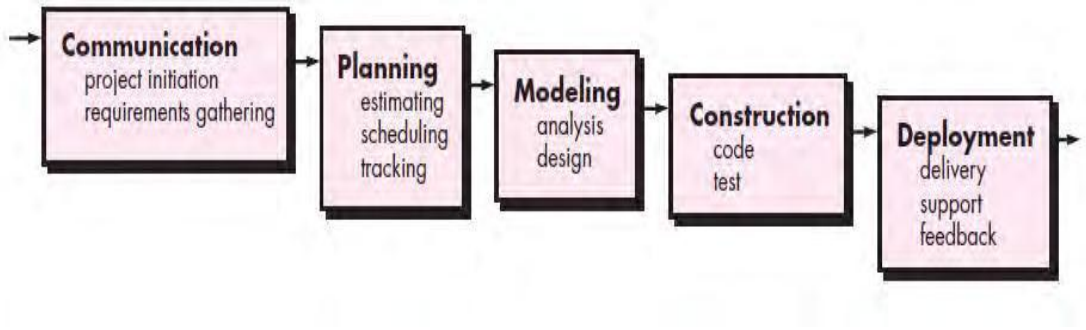
BAB III

METODOLOGI PENELITIAN

3.1 Metode pengembangan sistem

Menurut Pressman (2015:42), model *waterfall* adalah model klasik yang bersifat sistematis, berurutan dalam membangun *software*. Nama model ini sebenarnya adalah *"Linear Sequential Model"*. Model ini sering disebut juga dengan *"classic life cycle"* atau metode waterfall. Model ini termasuk ke dalam model *generic* pada rekayasa perangkat lunak dan pertama kali diperkenalkan oleh Winston Royce sekitar tahun 1970 sehingga sering dianggap kuno, tetapi merupakan model yang paling banyak dipakai dalam *Software Engineering* (SE). Model ini melakukan pendekatan secara sistematis dan berurutan. Disebut dengan *waterfall* karena tahap demi tahap yang dilalui harus menunggu selesainya tahap sebelumnya dan berjalan berurutan.

Fase-fase dalam *Waterfall Model* menurut referensi Pressman :



Gambar 3.1 Metode Waterfall Menurut Pressman (2015:42)

3.1.1 Communication (Project Initiation & Requirements Gathering)

Sebelum memulai pekerjaan yang bersifat teknis, sangat diperlukan adanya komunikasi dengan *customer* demi memahami dan mencapai tujuan yang ingin dicapai. Hasil dari komunikasi tersebut adalah inisialisasi proyek, seperti menganalisis permasalahan yang dihadapi dan mengumpulkan data-data yang diperlukan, serta membantu mendefinisikan fitur dan fungsi *software*. Pengumpulan data-data tambahan bisa juga diambil dari jurnal, artikel, dan internet.

Pada Tahap ini peneliti melakukan Observasi langsung terhadap program fluxion, observasi ini terfokus pada permasalahan yang menjadi kebutuhan user.

Dijelaskan pada poin **3.2.2.**

3.1.2 Planning (Estimating, Scheduling, Tracking)

Adalah tahapan perencanaan yang menjelaskan tentang estimasi tugas-tugas teknis yang akan dilakukan, sumber daya yang diperlukan dalam membuat sistem, produk kerja yang ingin dihasilkan.

3.1.3 Modeling (Analysis & Design)

Tahapan ini adalah tahap perancangan dan permodelan arsitektur sistem yang berfokus pada perancangan struktur data, arsitektur *software*, tampilan *interface*, dan algoritma program. Tujuannya untuk lebih memahami gambaran besar dari apa yang akan dikerjakan.

Pada tahap ini peneliti tidak melakukan perbahan bentuk design pada fluxion, dikarenakan fluxion adalah program pemanggil yang berbentuk terminal dan berisikan list opsi penggunaan tool.

Sehingga peneliti hanya akan menambah jumblah firtur dan opsi ke dalam program *fluxion*.

3.1.4 Construction (Code & Test)

Tahapan *Construction* ini merupakan proses penerjemahan bentuk desain menjadi kode atau bentuk/bahasa yang dapat dibaca oleh mesin. Setelah pengkodean selesai, dilakukan pengujian terhadap sistem dan juga kode yang sudah dibuat. Tujuannya untuk menemukan kesalahan yang mungkin terjadi untuk nantinya diperbaiki.

Pada tahap ini Peneliti menambahkan file yang dibutuhkan ke dalam directory fluxion, dan menambahkan code program, diantaranya:

1. **echo -e " "$red"["$yelow"10"red"]"$transparent" Indonesia "**

   Yang berfungsi menampilkan list Indonesia pada halaman pemilihan bahasa.

   11) source $WORK_DIR/language/in; break;;

   Yang berfungsi untuk memanggil file berisi bahasa Indonesia di dalam direcrtory fluxion.

2. **echo -e " "$red"["$yelow"10"red"]"$transparent" Huawei "**

   Yang berfungsi menampilkan list web interface

   11) source $WORK_DIR/sites; break;;

   Yang berfungsi memanggil dan menjalankan web interface

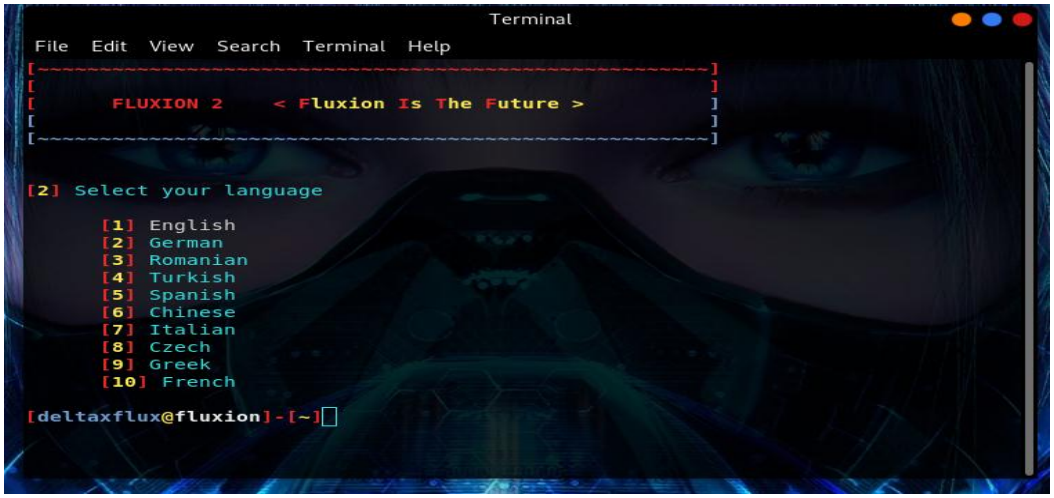
3.1.5 Deployment (Delivery, Support, Feedback)

Tahapan *Deployment* merupakan tahapan implementasi *software* ke *customer*, pemeliharaan *software* secara berkala, perbaikan *software*, evaluasi *software*, dan pengembangan *software* berdasarkan umpan balik yang diberikan agar sistem dapat tetap berjalan dan berkembang sesuai dengan fungsinya.

3.2 Analisis data

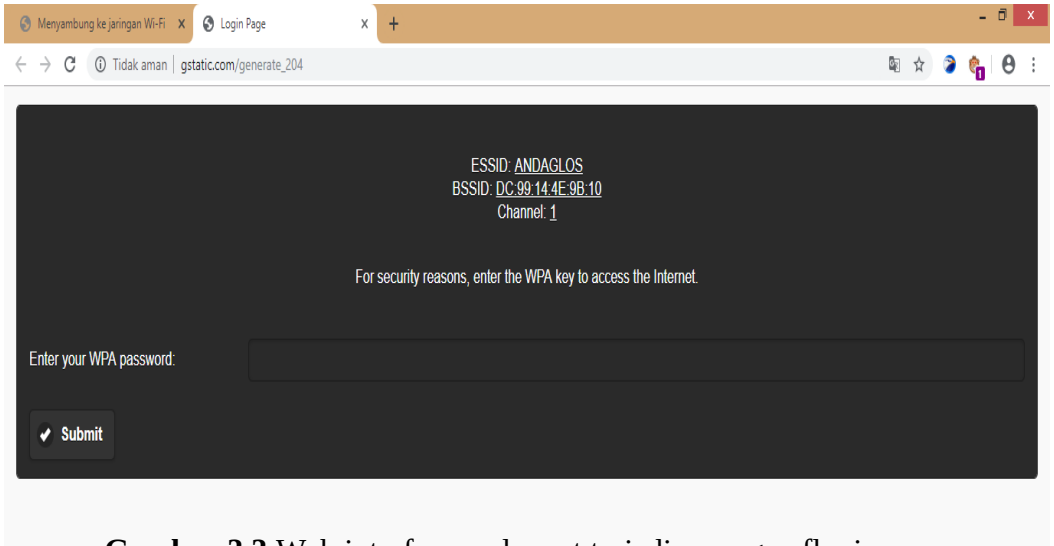
3.2.1 Analisis Fluxion

Berdasarkan hasil observasi, Pada program fluxion tidak terdapat bahasa indonesia pada halaman pemilihan bahasa, Seperti pada gambar 3.2.



Gambar 3.2 halaman pemilihan bahasa pada fluxion

Pada halaman web interface program fluxion hanya memiliki tampilan web yang biasa dan tidak memiliki web interface yang *specific* terhadap *router* yang akan di serang, seperti pada gambar 3.3.



Gambar 3.3 Web interface pada saat terjadi serangan fluxion

3.2.2 Analisis pengguna

Berdasarkan hasil observasi terhadap program *fluxion*, akan lebih baik jika *web interface* pada *fluxion* memiliki beberapa *directory web interface* milik *router* yang di pasarkan di indonesia, karena dapat mengakibatkan kecurigaan pada saat *client* diminta memasukan *password* pada halaman *web*, tetapi web yang ada pada fluxion tampilan *web* nya berbeda dengan *router* yang digunakan.

3.3 Pengumpulan data

Data penelitian merupakan faktor penting yang akan menjadi bahan pertimbangan dalam menentukan metode pengumpulan data. Data merupakan sumber atau bahan yang akan digunakan dalam suatu penelitian. Pengumpulan data terdiri dari :

1. Metode Observasi

   Observasi adalah metode Pengamatan dan pencatatan secara sistematis mengenai objek yang akan di teliti, observasi yag dilakukan oleh peneliti dengan cara pengamatan dan pencatatan mengenai provider yang digunakan, router yang dipakai. dan radius pancaran *wifi* dll.

2. Metode Wawancara

   Wawancara langsung dilakukan pada pimpinan PT. Andaglos Global Teknlogi. Untuk mendapatkan data yang valid.

3. Studi literatur

   Mencari data pengetahuan dan tutorial atau penelitian milik orang lain melalui jurnal dan internet.

3.4 Metode Penetration testing

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

a. Diagnosing

Melakukan *diagnosa* terhadap jaringan *wireless* keamanan WPA2.

b. Action Planning

Melakukan rencana tindakan yang akan dilakukkan pada jaringan *wireless* sebelum melakukan 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 dilihat adalah terdapat penggabungan jenis serangan apa saja dalam *program fluxion.*

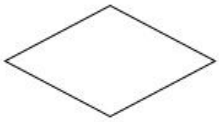
e. Specifying Learning

Melakukan review tahapan-tahapan yang telah berakhir dan mempelajari alur kerja *program fluxion.*

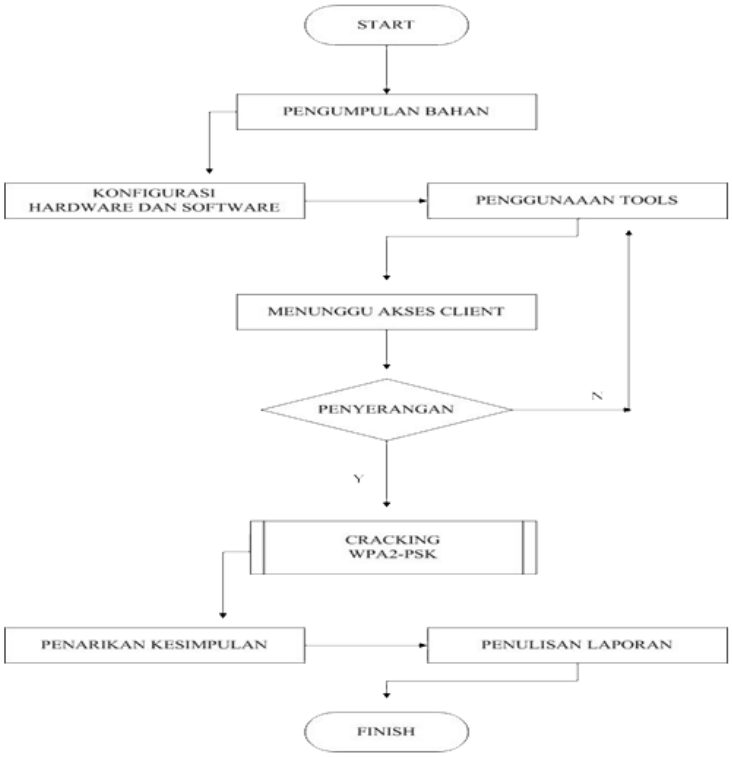
3.5 Flowchart Penetration Testing

Dalam menjaelaskan sebuah permasalahan, alur penelitian disajikan untuk mempermudah pemahaman dalam penelitian tersebut.

Metode tersebut tersaji dalam (*basic flowchart*) yang terdiri dari:.

SIMBOL ATAU GAMBAR	NAMA	KETERANGAN
	PROSES	Menyatakan kegiatan yang akan ditampilkan dalam diagram alir.
	DECISION	Proses atau Langkah di mana perlu adanya keputusan atau adanya kondisi tertentu. Di titik ini selalu ada dua keluaran untuk melanjutkan aliran kondisi yang berbeda
	PREDEFINED PROCES (SUB PROGRAM)	Digunakan untuk mewakili data masuk atau data keluar
	TERMINATOR	Menunjukkan awal atau akhir sebuah proses.
	GARIS ALIR (FLOW LANE)	Menunjukkan arah aliran proses atau algoritma.

Gambar 3.4 . simbol , nama dan fungsi



Gambar 3.5 . *Basic flow chart* (*Action research*)

Dari *Basic flow chart* yang terlihat pada gambar 3.2 dapat dijelaskan beberapa tahapan – tahapan sebagai berikut:

1. Pengumpulan bahan mencari tutorial – tutorial baik dari internet, buku dan artikel - artikel tentang masalah yang berhubungan dengan keamanan jaringan *wireless*.
2. Menyiapkan *hardware* dan *software* yang dibutuhkan seperti menggunakan terminal *Kali Linux* dan *tool-tool* tambahan lainnya untuk proses penyerangan.
3. Melakukan konfigurasi *tool-tool* yang telah tersedia pada *Kali Linux* ataupun *tool* tambahan lainnya agar proses penyerangan terhadap *client* dapat berjalan dengan baik.
4. Menunggu *user* yang terkoneksi ke internet untuk mendapatkan *handshake* ataupun informasi mengenai SSID, MAC *address*, IP *address*, *Channel* dan lain-lain. Sehingga diperoleh sebuah paket berupa kode enkripsi untuk dipecahkan menjadi *password* WPA2-PSK.
5. *User attack* dapat mengakses jaringan *WiFi* dengan memanfaatkan *handshake* dan paket kode enkripsi yang telah dipecahkan dengan menggunakan *tool-tool* pada Kali Linux, jika *handshake* sulit untuk didapatkan dari *user* itu dikarenakan jaringan *user* lama dalam merespon paket yang dikirim dari *user attack* ataupun *frame* nya yang rendah, sehingga harus mengulangi lagi penggunaan *tool* kepada *user* yang lain.
6. Menarik kesimpulan, untuk memutuskan sebuah kesimpulan yang bisa kita terapkan pada saat proses penyerangan oleh *user attack* terhadap keamanan WPA2-PSK pada jaringan WiFi dilihat dari sisi (*success/fail*).
7. Menulis laporan dari proses-proses penyerangan yang telah dilakukan untuk mendapatkan *password* keamanan WPA-PSK pada jaringan WiFi.

3.6 Kebutuhan perangkat lunak

Untuk melakukan Penetration testing membutuhkan beberapa jenis perangkat lunak, yaitu sebagai berikut:

1. *Kali linux*
2. *Fluxion*
3. *DHCP*
4. *HOSTAPD*
5. *MDK3*
6. *LIGHTTPD*

3.7 Kebutuhan perangkat keras

Untuk menjalankan perangkat lunak diatas membutuhkan perangkat keras dengan spesifikasi yang cukup, adapun spesifikasi minimum perangkat keras untuk menjalankan perangkat lunak diatas adalah :

a. spesifikasi minimal *Prosesor Intel Core i3* atau lebih.
b. RAM *(Random Acces Memory)* 2Gb atau lebih.
c. *Graphics card* 1GB atau lebih.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Penelitian Pengembangan fluxion

Setelah tahap-tahan pengambangan telah dilaksanakan pada program fluxion V.2.1 serta serangkaian uji coba pada bagian yang telah dikembangkan dapat dilihat bahwa *fluxion* sudah memiliki pilihan menu bahasa Indonesia dan *web interface* dari beberapa merek *router* yang beredar di Indonesia dan menjadi *fluxion V.2.1*.

4.2 Tampilan Antar Muka Fluxion V.2.1

Tampilan antar muka dari program *fluxion* yang sudah dikembangkan menjadi seperti berikut :

4.2.1 Tampilan Utama Fluxion V.2.1

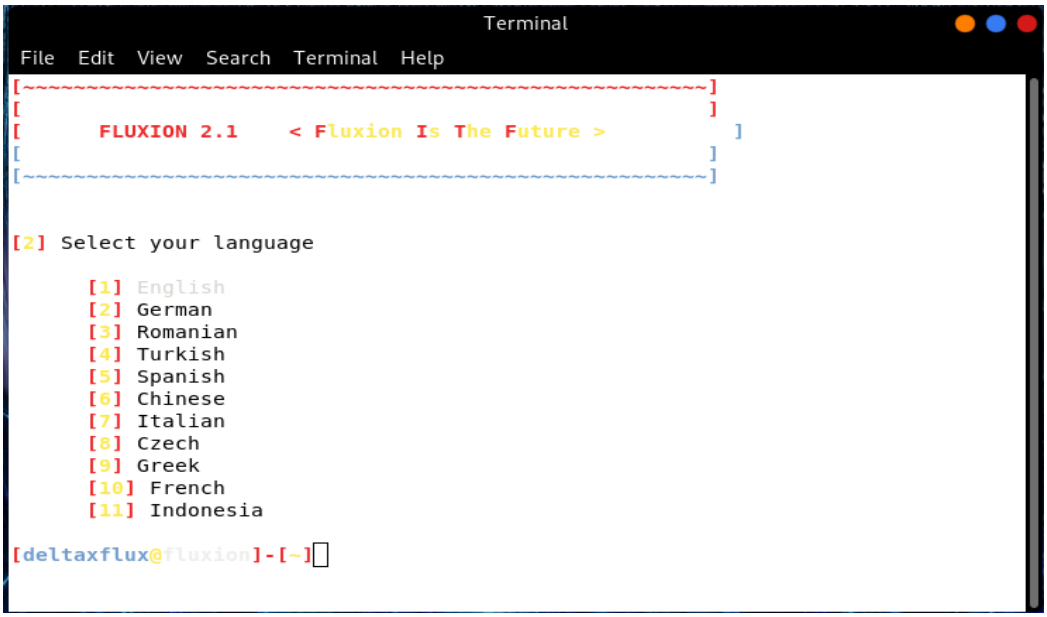
Pada tampilan utama fluxion terlihat nomor versi dan nama pengembang.

Gambar 4.1 tampilan Utama *Fluxion*

4.2.3 Tampilan Pemilihan Bahasa

Pada tampilan halaman pemilihan bahasa pada program *fluxion* dapat dilihat bahwa sudah ada pilihan bahasa Indonesia pada nomor sebelas, yang mana pada versi 2 tidak terdapat bahasa Indonesia.

Pilihan bahasa indonesia berguna untuk memudahkan pengguna baru yang berada di Indonesia untuk memahami perintah-perintah menjalankan *penetration testing* menggunakan *fluxion.*



Gambar 4.2 Tampilan pemilihan bahasa

4.2.3 Tampilan Web Interface

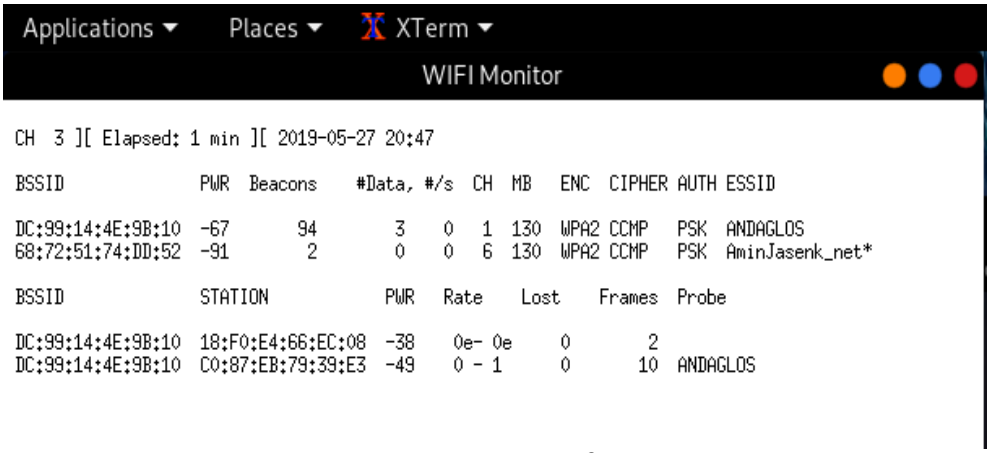
Pada tampilan *web interface* telah di kembangkan yang sebelumnya tidak memiliki spesifikasi atau merek router yang di edarkan atau di gunakan di indonesia, dan setelah dikembangkan kini *fluxion* memiliki web interface yang sesuai dengan rotuer yang beredar di indonesia, salah satunya yaitu *web interface* milik *HUAWEI, seperti pada gambar 4.3.*

Gambar 4.3 Tampilan *web interface router Huawei* pada *fluxion* V.2.1

4.3 Hasil penelitian penetration tesing

4.3.1 Wifi monitor

Analisa system pada PT. Andaglos global teknologi memperlihatkan *power* jaringan yang dipancarkan router dalam radius 20 Meter berada pada angka -67/100 yang mana power dari jaringan tersebut yang dapat diterima oleh *device* atau *pc client* dalam radius 20 meter adalah 33/100 sehingga memiliki kemungkinan gagal yang tinggi ketika dilakukan *penetration testing.*

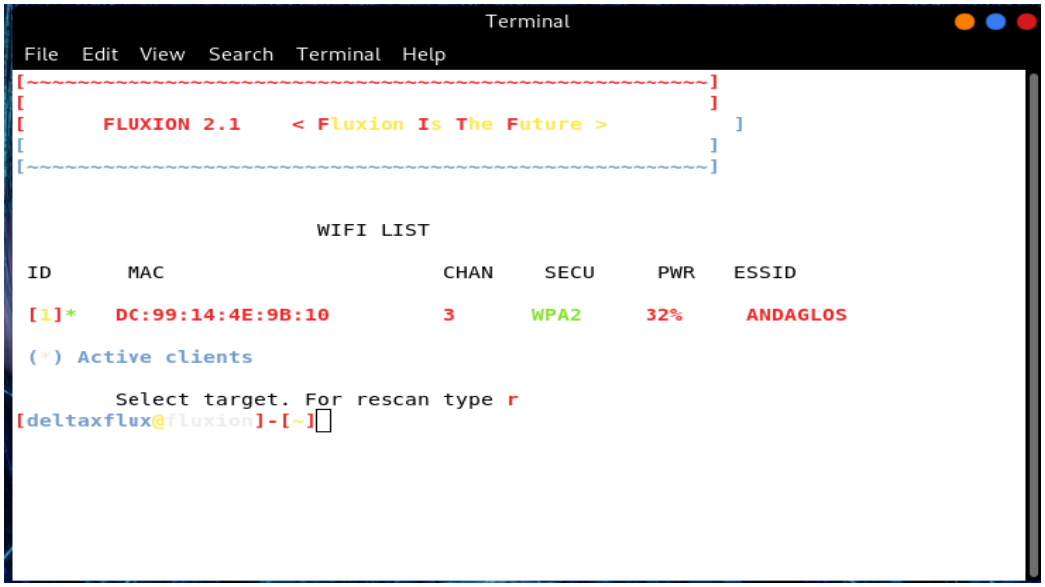


Gambar 4.4 Tampilan *wifi* monitor

4.3.2 Wifi list

Pada tahan ini pemilihan jaringan sangat perlu dilakukan sebelum melakukan *penetration testing*, karena ada beberapa jaringan yang tidak dapat diserang jika jaringan atau system tersebut tidak memenuhi siarat.

Siarat utama *fluxion* untuk menyerang ialah harus ada client yang terkoneksi pada jaringan tersebut seperti pada gambar 4.5.



Gambar 4.5 tampilan halaman wifi list

Pada gambar 4.5 terdapat 2 jaringan yang berbeda dan memiliki warna yang berbeda yang dapat menunjukan mana jaringan yang memiliki *client* dan jaringan yang tidak memiliki client.

1. Warna kuning pada *MAC* dan tidak ada nya tanda bintang di sebelah nomor seperti yang terlihat pada gambar 4.5 menunjukan tidak adanya client yang terhubung pada *router*.
2. Warna merah pada *MAC* dan dengan adanya tanda bintang di sebelah nomor seperti gambar 4.5 menunjukan bahwa ada *client* yang terhubung pada *router*.

4.3.3 Attack option

Tahap ini adalah tahap pembuatan *fakeAP* (akses point palsu)

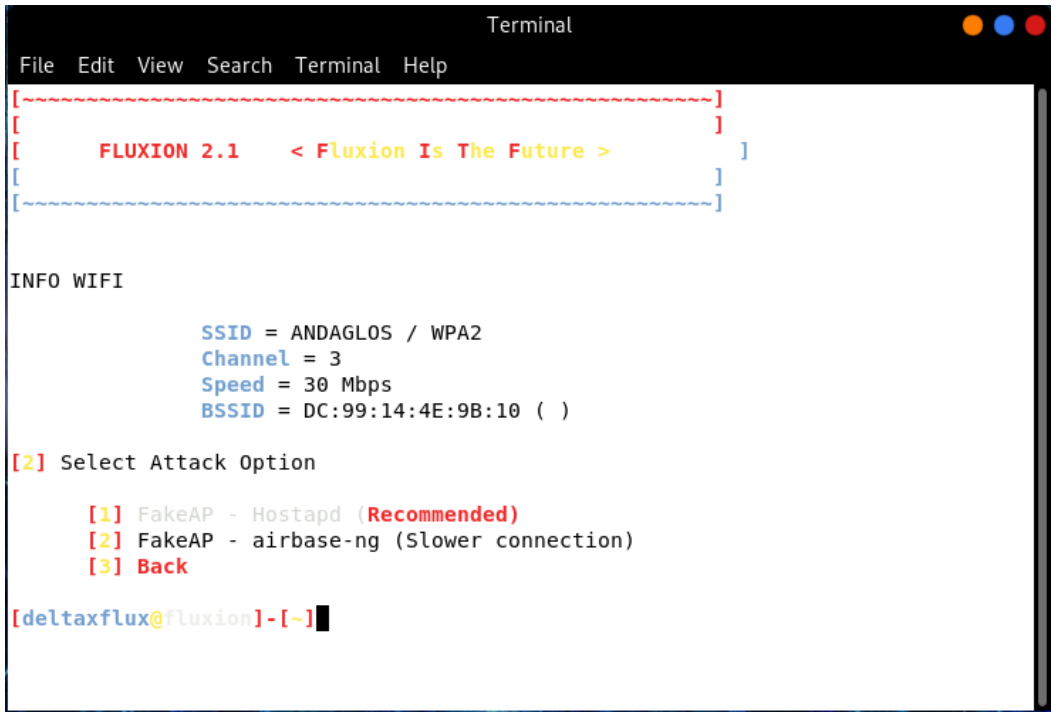
Dan ada dua pilihan di dalam nya yaitu:

1. **Hostapd**

   Hostapd adalah tool yang berfungsi membuat *pc* atau laptop dapat menjadi akses point, *hostapd* direkomendasikan untuk jaringan yang memiliki *power* bagus atau standar, tingkat keberhasilan menggunakan *tool* ini sangat tinggi pada saat menjalankan *fluxion.*

2. **Airbase-ng**

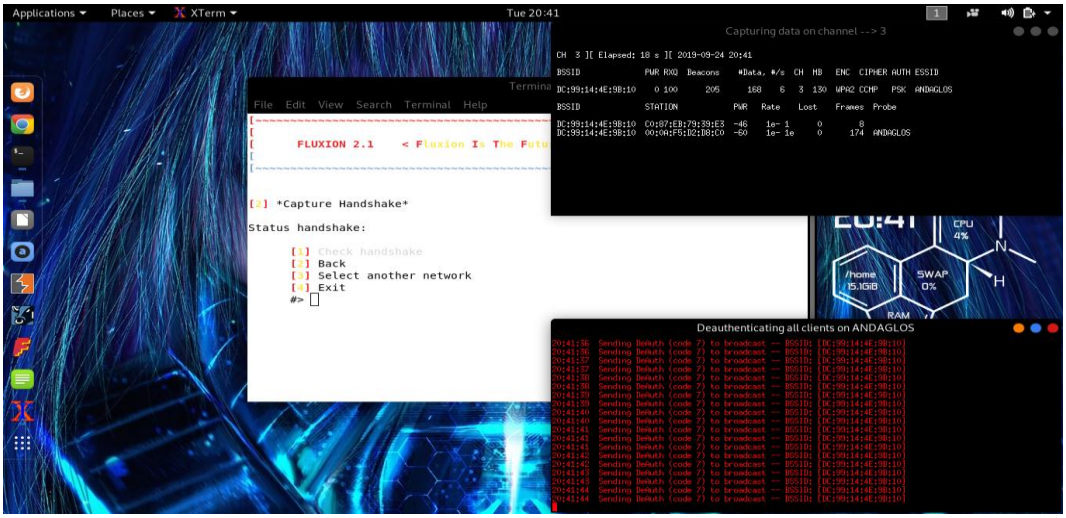
   Airbase-ng adalah sebuah *tool* yang serupa dengan *hostapd* hanya saja *airbase-ng* memiliki kemungkinan gagal yang sangat tinggi pada saat di jalankan di *fluxion* dan hanya dapat bekerja apa bila power dari jaringan lemah, Jadi penggunaan *airbase-ng* tidak direkomendasikan pada saat melakukan *penetration testing* menggunakan *fluxion.*



Gambar 4.6 Tampilan halaman *Attack option*

4.3.4 Capture handshake

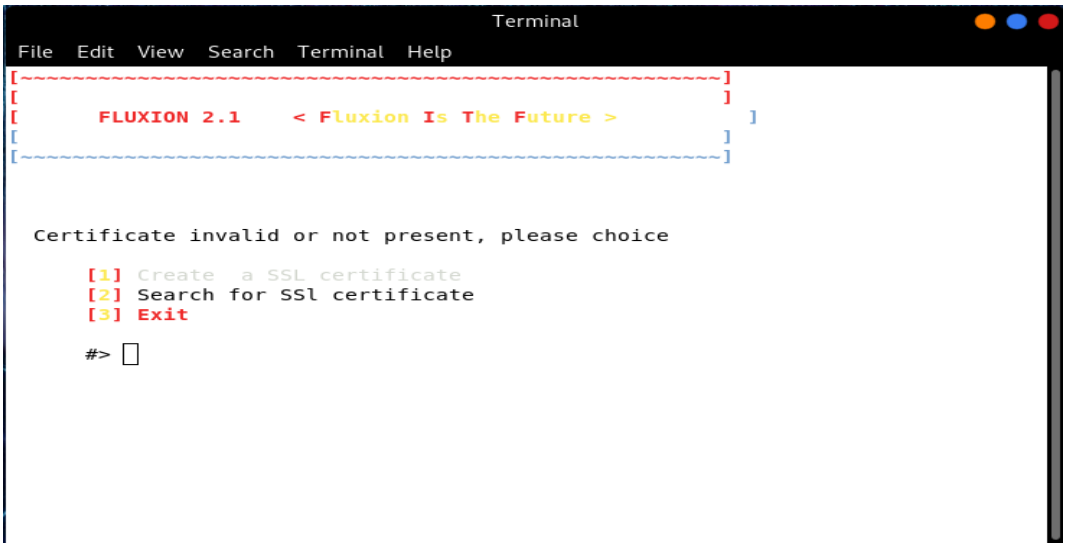
Capture handshake adalah proses yang terjadi ketika komputer akan berkomunikasi dengan perangkat asing untuk menetapkan peraturan untuk dapat saling berkomunikasi. ketika komputer berkomunikasi dengan perangkat lain seperti *printer*, *modem*, atau *server* jaringan.



Gambar 4.7 Tampilan halaman *capture handshake*

4.3.5 Certificate SSL

Halaman ini adalah halaman pembuatan *certificate SSL* yang berfungsi untuk mengamankan transmisi data dengan aman melalui *web*.



Gambar 4.8 Tampilan halaman *create sertificate SSL*

4.3.6 Web interface

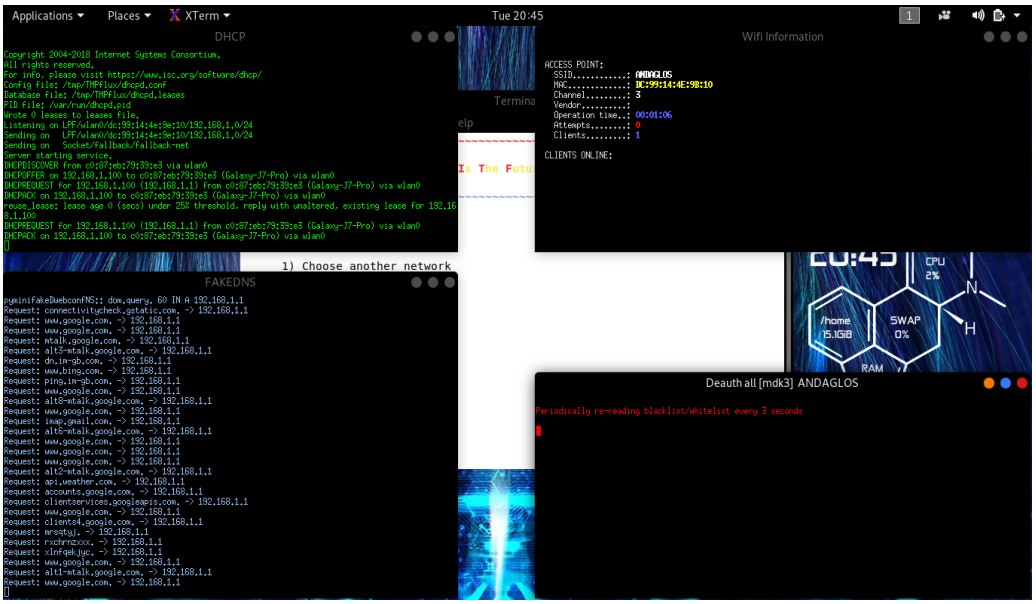
Tahap ini adalah tahap pembuatan *web interface* yang nantinya akan digunakan untuk menjebak *client* agar memasukan password pada halaman *web* tersebut.

Gambar 4.9 Tampilan halaman pilihan *web interface*

4.3.7 Menjalankan web interface

Tahap ini adalah tahap terakhir dari program *fluxion*, yaitu tahap menjalankan web interface dan monitor akan menampilan empat jendela terminal yaitu:

1. *DHCP* yang berfungsi memberikan ip kepada *client* agar dapat tersambung dengan *web interface* palsu yang telah kita buat.
2. *Fake DNS* berfungsi sebagai *database* untuk menyimpan *ip client* sehingga dapat terhubung pada *web interface* palsu.
3. *Deauth all (MDK3)* berfungsi untuk memutuskan client dari *router* dengan cara mengirim paket sebanyak- banyak nya sehingga client terputus dari *router.*
4. *Wifi information* berfungsi untuk melihat apakah ada *client* aktif yang mengakses *web interface* palsu tersebut.

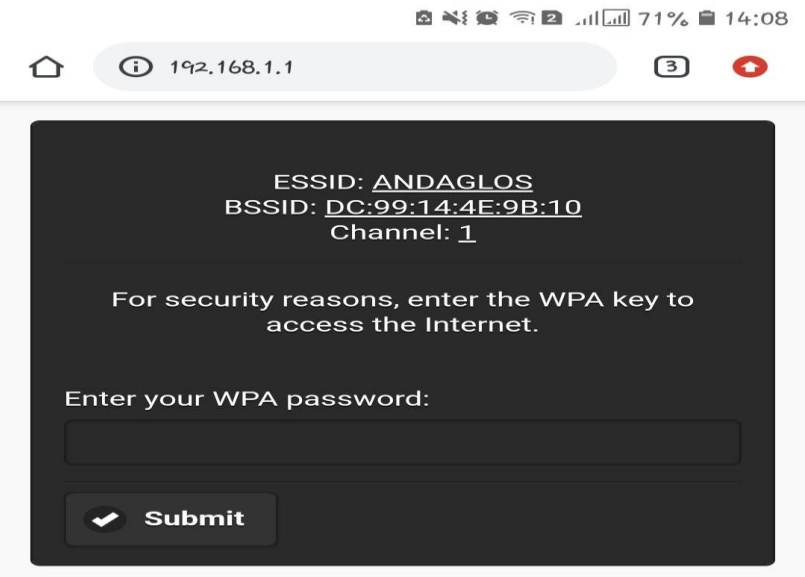


Gambar 4.10 Tampilan menjalankan *web interface (evil twin)*

4.3.8 Tampilan pada client

Pada tahap ini pada *device client* akan menampilkan dua opsi jaringan yaitu jaringan asli dan jaringan palsu, yang mana *client* tidak bisa tersambung pada jaringan asli dan di arahkan ke jaringan palsu.

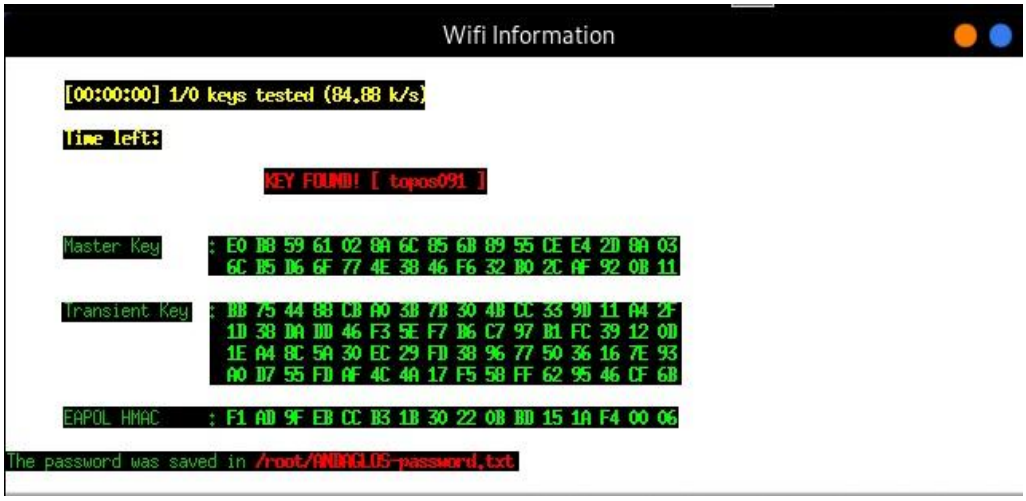
Gambar 4.11 Tampilan jaringan palsu *fluxion*



Gambar 4.12 Tampilan pada *client* yang masuk jaringan palsu

4.3.9 Mendapatkan password

Tahap ini adalah tahap dimana *client* sudah memasukan *password* pada *web interface* palsu.



Gambar 4.13 Tampilan *Password* telah berhasil di dapatkan

4.4 Kelebihan dan kekurangan fluxion

Adapun kelebihan dan kekurangan pada program fluxion yaitu sebagai berikut:

Kelebihan program fluxion adalah sebagai berikut:

1. *Fluxion* sangat mudah digunakan untuk melakukan *penetration testing.*
2. *Fluxion* memiliki tingkat keberhasilan yang tinggi dalam mendapatkan *password wifi* di bandingkan dengan program lainya.
3. *Fluxion* tidak membutuhkan waktu yang lama untuk mendapatkan *password.*
4. *Fluxio*n V.2.1 memiliki beberapa *web interface* yang sama dengan beberapa router yang digunakan di Indonesia.

Kekurangan program fluxion adalah sebagai berikut:

1. *Fluxion* tidak bisa menembus keamanan *wpa2* atau *router* secara langsung.
2. *Fluxion* tidak bisa mendapatkan *password* jika di jaringan tersebut tidak memiliki *client* aktif yang sedang menggunakan jaringan tersebut.
3. *Fluxion* tidak memiliki *web interface* yang lengkap untuk melakukan penetration testing. Hanya memiliki *web interface* biasa tanpa merek.

BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

5.1.1 Program fluxion

Program *fluxion* terbukti sangat efisien digunakan sebagai *tools penetration testing*, oleh sebab itu pada saat ini *fluxion* menjadi primadona bagi para pengembang untuk melakukan *penetration tesing*, maka dari itu dapat di ambil kesimpulan:

1. Cara kerja program *fluxion* untuk mendapatkan *password* adalah dengan metode penetration testing (evil twin).
2. Program *fluxion* terbukti dapat digunakan untuk melakukan *penetration testing* pada jaringan yang kuat dan lemah.
3. *Fluxion* terbukti mampu digunakan untuk *tools penetration testing* dan terbukti dapat mendapatkan *password* keamanan *wpa2* pada jaringan *wifi*.

5.1.2 Sistem PT.Andaglos Global Tenologi

Sistem keamanan jaringan PT.Andaglos Global Teknologi tidak mengatasi masalah atau memiliki celah dalam keamanan perangkat nya, namum kurang nya pengetahuan karyawan tentang keamanan jaringan membuat sistem tersebut sangat mungkin dapat di masuki oleh pengguna yang memanfaatkan program fluxion, maka dari itu dapat di ambil kesimpulan:

1. Pegawai atau karyawan PT. Andaglos Global Teknologi tidak mengetahui ketika sistem mereka telah diserang menggunakan program *fluxion.*
2. Pegawai atau Karyawan PT.Andaglos Global teknologi tidak mengetahui apabila ada *client* ilegal yang telah masuk ke dalam jaringan *router* mereka.
3. PT.Andaglos Global teknologi hanya menggunakan susunan jaringan standar pemasangan dan tidak menambahkan perangkat apapun seperti mikrotik atau membuat gateway untuk keamanan jaringanya.

5.2 Saran

5.2.1 Program fluxion

Saran untuk program *fluxion* yang telah dikembangan menjadi fluxion V.2.1 adalah:

1. Program *fluxion V.2.1* harus menambahkan *web interface* milik berbagai merek *router* yang ada di Indonesia suapaya lebih lengkap dan lebih memudahkan pengguna *fluxion.* Melakukan *penetration tesing* sesuai dengan *router* target.
2. Program *fluxion* mungkin dapat dikembangkan lagi sehingga dapat di tambah kan *tools* penetration lain di *directory* nya sehingga memiliki banyak pilihan untuk penyerangan.

5.2.2 Sistem PT.Andaglos Global Teknologi

Saran untuk PT.Andaglos Gobal Teknologi setelah dilakukan penetration testing pada sistem nya adaah:

1. Membuka *port* jaringan sesuai dengan jumlah karyawan yang dipekerjakan.
2. *Restart router* apabila menemukan bahwa jaringan device terputus sendiri dari router, terlihat dua nama jaringan yang sama pada *device* mereka.
3. Membiarkan pengguna *fluxion* masuk dan menambahkan *MAC address device* yang digunakan oleh penyerang ke dalam *blacklist,* sehingga *device* tersebut tidak akan bisa terkoneksi ke *router* PT.Andaglos Global Teknologi di kemudian hari.
4. Membuat gateway user password untuk masuk ke dalam system jaringan PT.Andaglos Global teknologi.

DAFTAR PUSTAKA

KEAMANAN JARINGAN WLAN TERHADAP SERANGAN *WIRELESS HACKING* PADA DINAS KOMUNIKASI & INFORMATIKA DIY
Vol 1, No 1 (2017): PROSIDING SENSEI 2017
http://jurnal.unmuhjember.ac.id/index.php/SENSEI17/article/download/844/679

ANALISIS SISTEM KEAMANAN *WIRELESS LOCAL AREA NETWORK* (WLAN) PADA PROSES *TETHERING*
Jom FTEKNIK Volume 5 Edisi 2 Juli s/d Desember 2018
https://jom.unri.ac.id/index.php/JOMFTEKNIK/article/download/21865/21159

Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT.PLN (Persero) Wilayah P2B Area Sorong
Volume 19 No. 3, Desember 2014
https://ejournal.gunadarma.ac.id/index.php/tekno/article/view/1110

ANALISIS MASALAH KEAMANAN JARINGAN WIRELESS KOMPUTER MENGGUNAKAN CAIN
Vol.6 No.1 (2014
http://csrid.potensi-utama.ac.id/index.php/CSRID/article/view/19

SISTEM KEAMANAN JARINGAN NIRKABEL
Majalah Ilmiah INFORMATIKA Vol. 3 No. 2, Mei 2012
http://www.unaki.ac.id/ejournal/indesx-php/majalah-ilmiah-informatika/article/download/68/105

PENGEMBANGAN SISTEM PENGAMAN JARINGAN KOMPUTER BERDASARKAN ANALISIS FORENSIK JARINGAN
(JITEKI) Vol. 3, No. 1, Juni 2017
http://journal.uad.ac.id/index.php/JITEKI/article/download/5665/3539

ANALISIS KEAMANAN JARINGAN NIRKABEL PUBLIK DENGAN RADIUS (STUDI KASUS UNIVERISTAS SATYA NEGARA INDONESIA – FAKULTAS TEKNIK
Vol.13 No 1 Maret 2017
https://lppm.usni.ac.id/jurnal/Jurnal%20Limit-Faizal.pdf

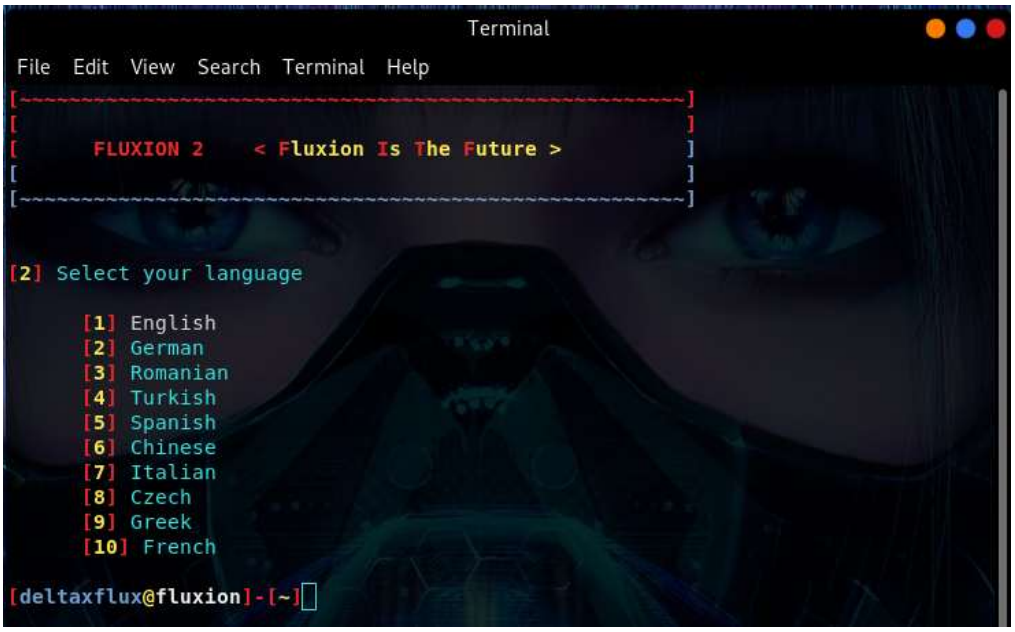
Sistem proteksi Jaringan *WLAN* Terhadap Serangan *Wireless* Hacking
JRECJournal of Electrical and Electronics Vol. 7 No. 1
http://jurnal.unismabekasi.ac.id/index.php/jrec/article/download/1762/1489/

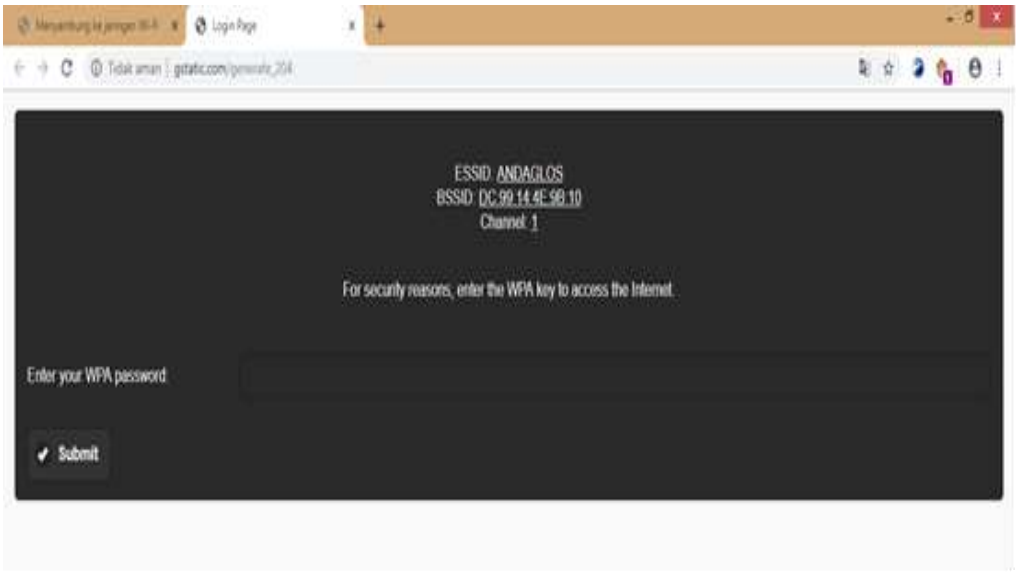
ANALISIS KELEMAHAN CELAH LAPISAN KEAMANAN PADA JARINGANNIRKABEL
Jurnal Ilmiah Media Processor Vol.9 No.1, Februari 2014
http://ejournal.stikom-db.ac.id/index.php/processor/article/download/52/52/

Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas Gadjah Mada)
JNTETI, Vol. 1, No. 1, Mei 2012
http://ejnteti.jteti.ugm.ac.id/index.php/JNTETI/article/download/3/2

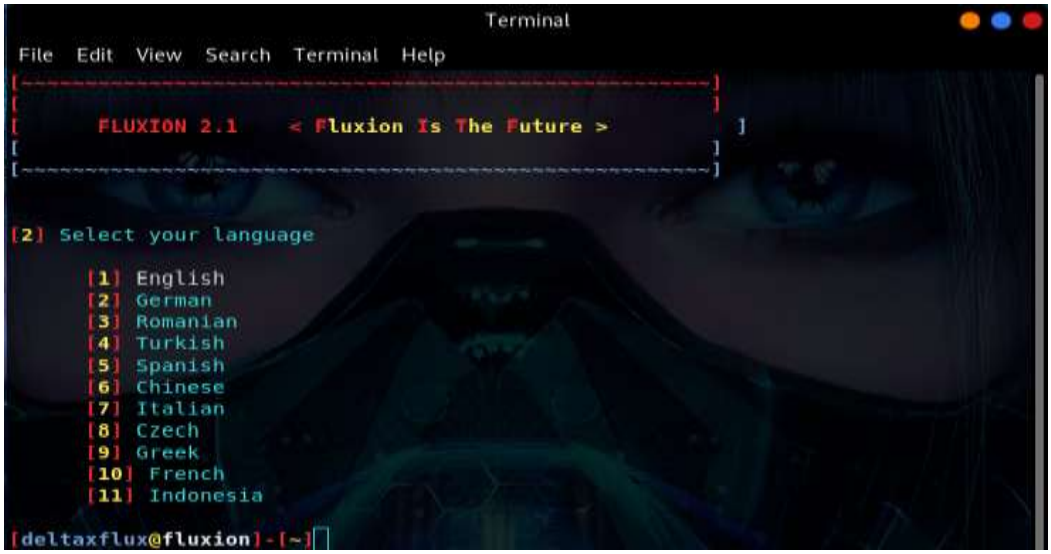
FLUXION WIFI ANALYZER ORIGINAL PACKAGE
https://github.com/FluxionNetwork/fluxion.git

Fluxion sebelum dikembangkan





Fluxion sesudah dikembangkan



Dokumentasi Penelitian di PT. Andaglos Global Teknologi


ASUS

SURAT KEPUTUSAN
REKTOR IIB DARMAJAYA
NOMOR : SK.0201/DMJ/DFIK/BAAK/IV-19
Tentang
Dosen Pembimbing Skripsi
Semester Genap TA.2018/2019
Program Studi S1 Teknik Informatika

REKTOR IIB DARMAJAYA

Memperhatikan :
1. Bahwa dalam rangka usaha peningkatan mutu dan peranan IIB Darmajaya dalam melaksanakan Pendidikan Nasional perlu ditingkatkan kemampuan mahasiswa dalam **Skripsi.**
2. Laporan dan usulan Ketua Program Studi **S1 Teknik Informatika.**

Menimbang :
1. Bahwa untuk mengefektifkan tenaga pengajar dalam Skripsi mahasiswa perlu ditetapkan **Dosen Pembimbing Skripsi.**
2. Bahwa untuk maksud tersebut dipandang perlu menerbitkan Surat Keputusan Rektor.

Mengingat :
1. UU No.20 Tahun 2003 Tentang Sistem Pendidikan Nasional.
2. Peraturan Pemerintah No.60 Tahun 2010 tentang Pendidikan Sekolah Tinggi
6. Surat Keputusan Menteri Pendidikan Nasional Republik Indonesia No.165/D/0/2008 tertanggal 20 Agustus 2008 tentang Perubahan Status STMIK-STIE Darmajaya menjadi Informatics and Business Institute (IBI) Darmajaya
7. STATUTA IBI Darmajaya
8. Surat Ketua Yayasan Pendidikan Alfian Husin No. IM.003/YP-AH/X-08 tentang Persetujuan Perubahan Struktur Organisasi
6. Surat Keputusan Rektor 0383/DMJ/REK/X-08 tentang Struktur Organisasi.

Menetapkan

Pertama : Mengangkat nama-nama seperti tersebut dalam lampiran Surat Keputusan ini sebagai Dosen Pembimbing Skripsi mahasiswa Program Studi S1 Teknik Informatika.

Kedua : Pembimbing Skripsi berkewajiban melaksanakan tugasnya sesuai dengan jadwal yang telahditetapkan.

Ketiga : Pembimbing Skripsi yang ditunjuk akan diberikan honorarium yang besarnya sesuai dengan ketentuan peraturan dan norma penggajian dan honorarium IBI Darmajaya.

Keempat : Surat Keputusan ini berlaku sejak tanggal ditetap kan dan apabila dikemudian hari terdapat kekeliruan dalam keputusan ini, maka keputusan ini akan ditinjau kembali.

Ditetapkan di : Bandar Lampung
Pada tanggal : 22 April 2019
a.n. Rektor IIB Darmajaya,
Dekan Fakultas Ilmu Komputer

Sriyanto, S.Kom., M.M., Ph.D
NIK. 00210800

1. Ketua Jurusan S1 Teknik Informatika
2. Yang bersangkutan
3. Arsip