ANALISIS *FLUXION* SEBAGAI PROGRAM UJI KEAMANAN WPA2 PADA PERANGKAT *WIRELESS*

Hamza Alfan Suri [1], Widyanto[2], Taqrim Ibadi[3]
Dosen Universitas Bina Darma [2,3], Mahasiswa Universitas Bina Darma [1]
Jalan Jenderal Ahmad Yani No.12 Palembang
e-mail : hamzaalfansuri@gmail.com[1], widyanto@mail.binadarma.ac.id[2], taqrimibadi@mail.binadarma.ac.id[3]

Abstract : WPA2 is a development of the newest security feature installed on some wireless devices. The use of security testing program as a fluxion WPA2 to know how high the success or the level of vulnerability that can be achieved, the fluxion itself a bash script which shall work on the linux operating system. Not just melakukkan penetration against security WPA2, in this discussion also complies with the proposed title, namely the analysis of the test program as a fluxion WPA2 security. As for the research methods used namely Action Research several stages that must be dilakukkan in this method, diagnosing, Action Planning, Taking Action, Evaluating, and Specifying Learning. As well as the use of Reverse engineering analysis motode with melakukkan manual analysis by observing the workflow script fluxion. Black Box as the testing method, until the desired result is obtained.

Keywords : analysis, *fluxion,WPA2, Reverse engineering*

Abstrak : *WPA2* merupakan pengembangan dari fitur *security* terbaru yang sudah terpasang pada beberapa perangkat *wireless.* Penggunaan *fluxion* sebagai program uji keamanan *WPA2* untuk mengetahui seberapa tinggi keberhasilan atau tingkat kerentanan yang bisa dicapai, *fluxion* sendiri suatu *script bash shall* yang bekerja pada sistem operasi *linux*. Bukan hanya melakukkan *penetrasi* terhadap keamanan *WPA2*, pada pembahasan ini juga sesuai dengan judul yang diajukan yaitu analisis *fluxion* sebagai program uji keamanan *WPA2*. Adapun metode penelitian yang dipergunakan yaitu *Action Research* beberapa tahapan yang harus dilakukkan pada metode ini, *diagnosing*, *Action Planning*, *Action Taking*, *Evaluating*, dan *Specifying Learning*. Serta penggunaan motode analisis *Reverse engineering* dengan melakukkan analisis manual dengan memperhatikan alur kerja *script fluxion. Black Box* sebagai metode pengujian, hingga didapatkan hasil yang diinginkan.

Kata kunci*: analisis, fluxion,WPA2, Reverse engineering*

1. PENDAHULUAN

1.1. Latar Belakang

Di zaman globalisasi saat ini, kemajuan teknologi komunikasi merupakan faktor yang paling penting terhadap peranan sebagian masyarakat untuk mendapatkan akses informasi. Pemanfaatan jaringan komunikasi berbasis *wireless* (tanpa kabel) ialah salah satu media komunikasi yang berkembang sampai saat ini. Penyediaan fasilitas *wireless* atau *Wi-fi* gratis ditempat umum adalah keuntungan bagi sebagian orang, dalam banyak kasus menurut hasil penyelidikan ahli keamanan komputasi, *Jason W Clarke* berpendapat bahwa saat ini fasilitas *Wi-fi* gratis bagi publik menjadi target utama dalam aksi kejahatan *cyber*, oleh karenanya kita tidak beleh menganggap sebuah keamanan jaringan dengan remeh.

Dikembangkan oleh IEEE (*Institute of Electrical and Electronics Engineers)* dari sebuah organisasi yang mengurusi standarisasi LAN dan MAN pada tahun 1980 bulan 2, bagian ini kemudian dinamakan sebagai 802, maka bagian ini dibagi lagi menjadi beberapa unit kerja yang mengurusi *WLan* (Jasakom, 2007, h8).

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*

dalam membangun suatu proyek pada *github*, menunjukan bahwa *watch* 158, *star* 1,109 dan *fork* 430 dengan *script linset*. Dimana *watch* 58 *star* 258 dan *fork* 138.

Tindakan untuk mendapatkan *password* secara paksa bertentangan dengan, UU ITE pasal 30 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 pasal 46 ayat 3 berupa ancaman pidana penjara paling lama 8 tahun atau denda paling banyak Rp.800.000.000,.

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. Berdasarkan permasalahan tersebut, maka muncul pemikiran untuk mengajukan penelitian dengan judul **"Analisis *Fluxion* Sebagai Program Uji Keamanan WPA2 pada Perangkat *Wireless*".**

1.2. Rumusan Masalah

Berdasarkan uraian diatas, maka peneliti akan merumuskan masalah " Bagaimana cara kerja program *fluxion* mengambil *password* pada keamanan WPA2" dan "Apakah program *fluxion* cukup efektif dilakukan pada perangkat *wireless* yang terpasang keamanan WPA2, dalam hal ini *tethering android, mifi andromax* dan *modem TP-LINK*"

1.3. Tujuan Penelitian

Adapun tujuan dari penelitian ini untuk mengetahui seberapa tinggi keberhasilan program *fluxion* dalam mendapatkan *password* yang menggunakan keamanan perangkat *wireless* WPA2.

2. METODOLOGI PENELITIAN

2.1. Objek Penelitian

Penelitian dilakukkan pada 3 perangkat wireless, yaitu tethering android, mifi andromax, dan modem TP-LINK yang menggunakan keamanan WPA2 dimulai pada bulan November hingga Desember 2016.

2.2. 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 dilakukkan 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 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.*

2.3. Metode Pengumpulan Data

Pengumpulan data merupakan prosedur yang sistematis dan standar untuk memperoleh data yang diperlukan. Selalu ada hubungan antara metode mengumpulkan data dengan masalah penelitian yang ingin dipecahkan. Antara lain dilakukan dengan cara :

a. Observasi, melakukan pengamatan secara tidak langsung ke objek penelitian berupa sebuah *program.*
b. Studi Pustaka, metode yang di lakukan dengan cara mencari bahan yang mendukung dalam pendefinisian permasalahan melalui buku-buku,*browsing internet* serta dokumen yang terkait.

2.4. Alat dan Bahan

a. Peralatan penelitian

Satu unit Laptop dengan spesifikasi :

1. *Operasi System Windows 8.1* dan *Kali Linux*
2. *Processor Intel® i*3-3210u 1.80 GHz
3. *RAM 4 GB*
4. *Hardisk 300 GB*

Satu unit *Smartphone Samsung GT-S6310 dengan Operasi Sistem Android*

Satu unit Mini Router smartfren andromax M3Y

Satu unit Modem Router TP-LINK TD-W8951ND

b. Bahan Penelitian

Data *fluxion-master*

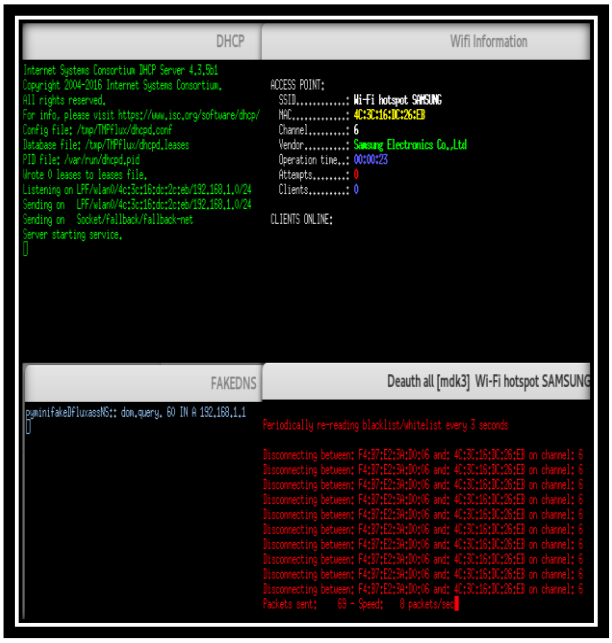
3. HASIL DAN ANALISIS

3.1. *Tethering Android*

Pada *pembahasan ini* tethering yang menggunakan Android v 4.1.2 dengan device handphone SAMSUNG GT-S6310. Terlihat pada gambar 4.1 merupakan tampilan Wifi Portable pada Android. Dan fasilitas configure portable Wi-fi android berupa Network SSID, Security dan Password.

Masuk tahap penyerangan, disini terlihat ada empat jendela yang berbeda yang menunjukan fungsi masing-masing, jendela requests DHCP dan DNS sedang memonitoring aktivitas korban, sedangkan pada 2 jendela yang lainnya menunjukan status laporan yang didapat pada Wifi Information dan pada jendela mdk3 sedang

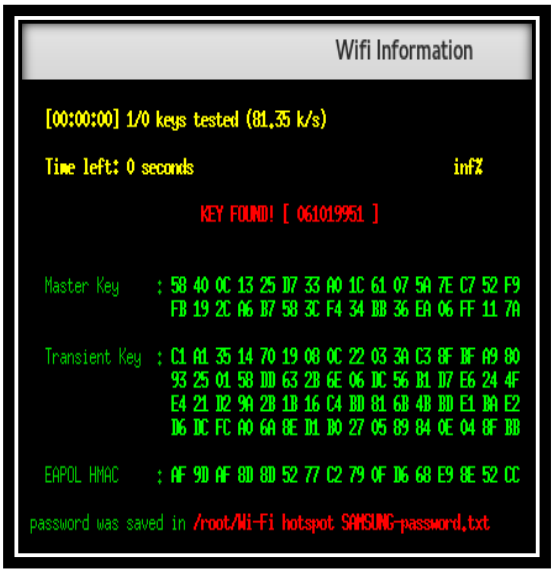
membanjiri paket kepada korban yang sedang login dijaringan tersebut.



Sesaat script tersebut langsung bekerja, tanpa pengetahuan korban sinyal hotspot yang digunakannya akan melemah dan terputus karena paket yang dikirim terlalu banyak, disaat seperti itu mereka akan mendapatkan pemberitahuan harus login ulang ke jaringan. Dengan terhubungnya korban pada hotspot tiruan yang sudah direkayasa mengarahkan untuk memasuki ulang kata sandi wireless tersebut pada halaman login yang terlihat pada gambar 3.1.

Gambar 3.1 Halaman Login.

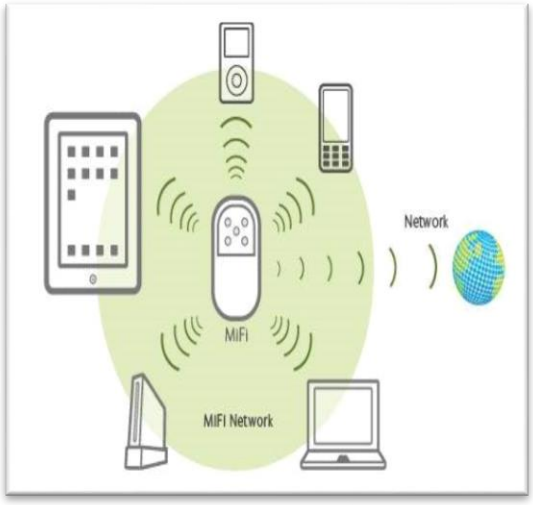
Tak butuh waktu lama, ketika korban telah memasukkan password yang benar maka jendela Wifi Information akan menunjukan password yang diinput oleh korban. Dan terlihat pada gambar 4.13 memberi informasi bahwa password telah ditemukan.



Gambar 3.2 Password ditemukan

3.2. *Mifi Andromax*

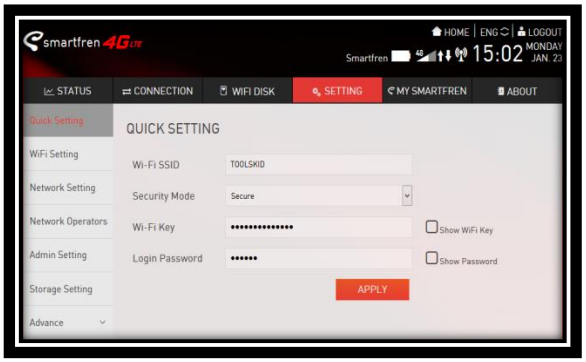
Dikutip dari ngelag.com. *MiFi* merupakan nama yang diberikan pada sebuah perangkat *wireless router* yang berperan sebagai *WiFi Hotspot* **.** *MiFi* ini merupakan kependekan dari *Mobile Wi-FI* . Di Indonesia belakangan ini nama *MiFi* sering kita lihat pada beberapa iklan contohnya *smartfren* .



Gambar 3.3 Diagram Cara Kerja Mifi

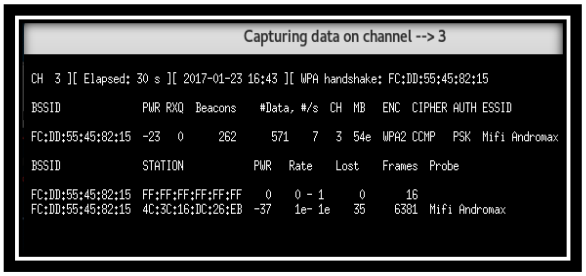
MiFi juga sangat cocok digunakan pada sebuah rumah dengan pengguna internet yang banyak namun tidak ingin menggunakan layanan internet dari provider internet kabel seperti Telkom Indihome misalnya . Karena pengguna MiFi hanya tinggal memasang sebuah kartu sim dan berlangganan layanan internet , bisa bulanan , harian atau hanya ketika diperlukan saja.

Berikut tampilan *device mifi andromax* sebagai objek percobaan uji keamanan WPA2.



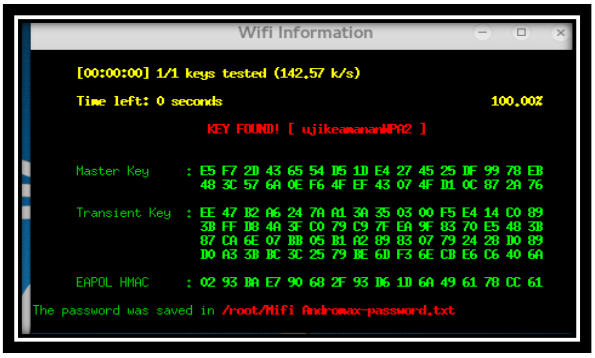
Gambar 3.4 *Device mifi andromax*

Selesai *scanning*, pada tahap selanjutnya proses penggunaan metode-metode penyerangan *script fluxion* sama seperti yang dilakukkan pada skenario *tethering android*, masuk ke tahap mencari sebuah *handshake* ternyata *script fluxion* masih bisa menangkap *handshake* dari *Mobile Wi-Fi* tersebut, terlihat pada gambar 3.5 terdapatnya sebuah MAC yang tertera pada jendela *Capturing data on channel*, yang berarti *script fluxion* dapat bekerja dengan baik.



Gambar 3.5 *Scanning Handshake*

Ketika korban pengguna *wifi* tersebut memasukkan *password* yang benar maka jendela *wifi information* akan menampilkan *password* nya.



Gambar 3.6 *Password* ditemukan.

3.3. *Access Point Tp-Link*

Pada jaringan wireless mode *infrastruktur*, Access Point (AP) bertindak sebagai tokoh utama untuk melayani pertukaran data dalam jaringan. Kartini (2014). Access Point merupakan sebuah perangkat dari jaringan yang berisi *transceiver* dan juga antena yang berfungsi untuk transmisi dan menerima kiriman sinyal dan dari clients remote. Adanya access points (AP) clients wireless tersebut bisa dengan mudah dan cepat untuk menghubungkan pada jaringan LAN kabel dengan cara wireless atau tanpa kabel. Atau bisa juga dikatakan sebagai alat yang memiliki fungsi untuk menyambungkan peralatan wireless pada sebuah jaringan berkabel (wired network) memakai wifi, bluetooth. Wireless Access Point dipakai untuk menghasilkan jaringan WLAN (Wireless Local Area Network) atau juga untuk memperbesar jumlah cakupan jaringan wifi yang telah ada.

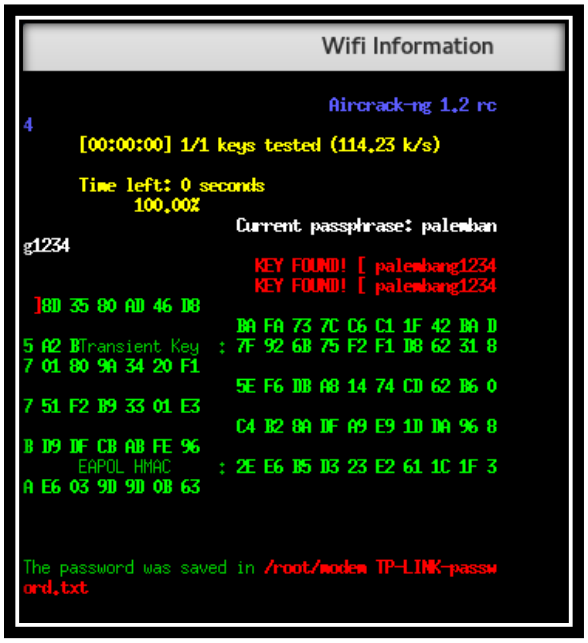
Skenario penyerangan yang terakhir menggunakan perangkat Access Point merk TP-LINK. Dimana pada perangkat tersebut juga memiliki sistem keamanan WPA2, pada gambar 3.7 menampilkan *device* setup pada TP-LINK.

Gambar 3.7 *Divice setup* TP-LINK

Singkatnya terlihat pada gambar 3.8 menjelaskan proses penyerangan sedang dijalankan dimana jendela Wifi Information memperlihatkan Vendor : TP-LINK TECHNOLOGIES CO.,LTD,

Dan ketika korban dari pengguna *wifi* telah memasukkan *password* yang benar, maka pada jendela *wifi information* akan

menampilkan *password* yang telah diinput oleh korban, terlihat seperti gambar 4.25 dibawah ini.

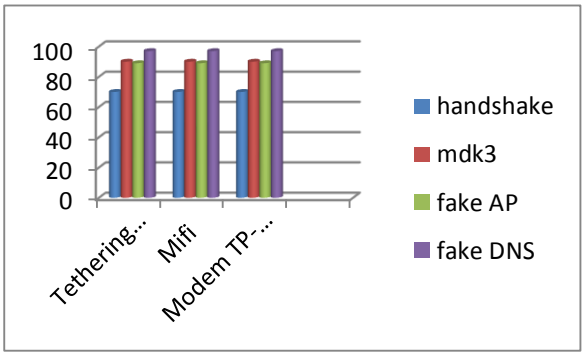


Gambar 3.8 *Password* ditemukan

3.4. Grafik Tingkat Keberhasilan *Script Fluxion*

Terlihat pada table grafik 4.1 dibawah ini menjelaskan bahwa penyerangan *script fluxion* terhadap 3 *device* yang berbeda dengan penggunaan 4 teknik metode penyerangan mampu membuat *script fluxion* berjalan dengan baik.

pada metode *handshake* tingkat keberhasilan yang didapat sebesar 69%, karena 31% yang tersisa membuat *handshake* tidak didapatkan jika disuatu jaringan tersebut tidak terdapat user yang sedang login. *Mdk3* menempati tingkat 88% karena metode penyerangan ini dilakukkan ketika proses *handshake* telah didapatkan. *fake AP* dan *fake dns* kedua teknik penyerangan ini berfokus pada penjebakan user untuk memasukkan ulang *password* asli. Dari ke empat penyerangan tersebut tingkat keberhasilan tidak akan mencapai 100% karena jika user yang terdapat dalam jaringan yang ingin diretas memahami tanda-tanda adanya *social engineering.*



Gambar 3.9. Tingkat keberhasilan *script fluxion*

3.5. Pemahaman Kerja *Script Fluxion*

Analisis terhadap *script fluxion*, analisis dilakukan secara manual dengan memperhatikan alur kerja. Proses kerja *script fluxion* secara garis besar dimulai dari

a. Pemindaian Jaringan
b. Mencari *handshake*, proses tidak akan berhasil jika *handshake* tidak ditemukan,

jadi perlunya sebuah *handshake* untuk memverifikasi *password*

c. Menggunakan *WEB interface* sebagai teknik social engineering
d. Menjalankan proses *Access Point* palsu yang menyamai aslinya
e. Mengaktifkan proses *MDK3,* berfungsi memutuskan semua koneksi penguna yang terhubung dalam jaringan tersebut sehingga membuat mereka untuk terhubung ke jaringan *access point* palsu dan memasukkan *password*
f. Server DNS palsu dijalankan untuk merekam semua permintaan DNS dan memperlihatkan aktivitas yang dilakukkan mereka pada jaringan AP palsu
g. Captive portal berfungsi dalam melayani sebuah halaman, untuk mendorong pengguna memasukkan *password*
h. Setiap *password* yang dimasukkan oleh korban akan diverifikasi dengan *handshake* yang didapat sebelumnya, dan proses akan berakhir secara otomatis jika *password* yang benar telah dimasukkan.

4. Kesimpulan dan Saran

4.1. Kesimpulan

Dari hasil pembahasan uji coba keamanan WPA2 pada perangkat *wireless* didapatkan kesimpulan.

1. Bahwa tiga 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.*
2. Pada *script fluxion* proses pengambilah *handshake* sangat berpengaruh, jika *handshake* tidak ditemukkan proses kerja *script* tidak akan berhasil, dan pada *wifi* minimal mempunyai satu user yang sedang login karena *handshake* didapatkan oleh user yang sedang melakukkan aktivitas pada jaringan tersebut.
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.*

4.2. Saran

Script fluxion ini tidak akan mampu mendapatkan suatu *password* dari jaringan

yang sedang diretas, apabila pengguna *wifi* mengerti akan yang namanya *social engineering*. Terlihat begitu mencurigakan ketika ingin memasukkan ulang *password* pada jaringan palsu tersebut, dimana korban akan diarahkan memasukkan ulang melalui *browser*. Saran pengembangan *script fluxion* pada bagian input *password* supaya tidak begitu mencurigakan ketika korban telah terputus dari jaringan yang asli dan terhubung pada jaringan yang palsu, *script* tersebut langsung menampilkan jendela input ulang *password* tanpa harus melalui *browser*.

Daftar Pustaka

Achmadi, Meizar Didi. (2014). Jurnal: Mengenai Jaringan *Wireless.*

Erlansyah, Deny. (2011). Jurnal: Analisis Keamanan Sistem WPA Radius

Forum Diskusi : *unix.stackexchange.com/questions/299245/installing-packages-in-kali-linux*

Github.com/deltaxflux/fluxion

Jasakom. (2007). Ebook: "Wireless Kung Fu Networking & Hacking", Penerbit Jasakom. Jakarta Barat

John D.Howard. (2013). Ebook: "*An Analysis of security incidents on the internet*"

Kartini (2014). Jurnal : Membangun Jaringan Nirkabel (*Hotspot Area)* dan Manajemen Hotspot dengan "Antamedia *Hostpot Manager*" Sebagai Sarana Komersial Berbasis *Wifi*

Megawati, Christina (2012). Jurnal: Implementasi dan Analisis Unjuk Kerja Sistem Keamanan Jaringan Wireless Berbasis Linux Platform dan DD-WRT Firmware

Nugroho, Agung (2012). Jurnal: Analisis Keamanan Jaringan *Wireless Local Area Network* dengan Access Point Tp-Link

Ngelag.com : Membahas tentang *mifi*

Nurwendah, S. (2012). Jurnal: Analisis Kelakuan *Denial-of-Service attack* (DoS *attack*) pada Jaringan Komputer dengan Pendekatan pada Level Sekuritas.

Rajab, Muis (2010). Jurnal: Analisis dan Perancangan *Wireless* LAN *Security* Menggunakan WPA2-Radius

Rumalutur, Sonny. (2014). Jurnal: Analisis Keamanan Jaringan Wireless LAN (WLAN) pada PT.PLN Sorong. Universitas Gunadarma

Rizal, Yose. (2012). Jurnal: Perancangan Simulasi Man In The Middle Attack pada Algoritma Kriptografi RSA dan Pencegahannya dengan Interlock Protocol.

S, Amri (2015). Universitas Sumatera Utara.

Sonhaji, dkk. 2010. Rekayasa Ulang (*Re-engineering*).

Stallings, William (2005). Ebook: Cryptography and Network Security Principle and Practices, Fourth Edition.

Supriyanto, Aji. (2006). Jurnal: Analisis Kelemahan Keamanan pada Jaringan Wireless. Universitas Stikubank Semarang.

Siti Zaim (2015). Seminar Nasional Informatika 2015 UPN "vereran" Yogyakarta

Sinambela, Josua. (2007). Makalah Seminar: Keamanan Wireless LAN (*Wifi)*

Yogatama, Yustinus. (2015). Jurnal: Analisis Pengaruh Pengamanan WPA dan WPA2 Terhadap Performa Jaringan *Wireless 802.11N*

Zam, Efvy. (2012). Wireless Hacking. Jakarta Selatan: Penerbit Mediakita.