IMPLEMENTASI WIRELESS IDS (INTRUSION DETECTION SYSTEM) UNTUK MONITORING KEAMANAN JARINGAN BERBASIS KISMET

THE IMPLEMENTATION WIRELESS IDS (INTRUSION DETECTION SYSTEM) FOR NETWORK SECURITY MONITORING BASED ON KISMET

Mohamad Gifar Perkasa [1], Setia Juli Irzal Ismail, M.T [2]

[1]Fakultas Ilmu Terapan, Univesitas Telkom
[2]Fakultas Ilmu Terapan, Universitas Telkom

[1] mohgifarperkasa@gmail.com, [2]jul@tass.telkomuniversity.ac.id,

Abstrak

Banyak pihak yang berusaha memanfaatkan kerentanan dari suatu jaringan WLAN maka dibutuhkan suatu WIDS yang user friendly agar dapat mendeteksi adanya serangan dalam suatu jaringan. Sehingga solusi pada kerentangan jaringan WLAN ini yaitu melakukan pengujian dari sistem Wireless Intrusion Detection System (WIDS) untuk memonitoring suatu jaringan wireless yang berbasis Kismet. Aplikasi Kismet adalah sebuah program komputer yang dibuat untuk membantu sebuah monitoring suatu jaringan, Kismet tersebut yang hasil alert-nya atau output berupa tampilan dan waktu pada penyerangan di lakukan. Kismet mempunyai interface yang dapat menampilkan jaringan apa saja yang berada dalam jangkauannya, client mana saja yang terhubung dengan jaringan tersebut serta alerts atau output yang di hasilkan oleh tools ini sebagai WIDS. Ketika Kismet di jalankan lagi, Kismet akan menyimpan log-nya dalam file yang baru dan hanya berbeda penamaan tanggal dan waktunya saja. Selain itu, dengan Kismet client yang menampilkan alert berupa rooling log di interface nya membuat administrator kesulitan dalam menganalisis jaringannya. Oleh karena itu, dibutuhkan adanya pemakaian interface yang user friendly.

Kata kunci: WLAN, WIDS, Kismet, Kismet Server

Abstract

Many people who try to exploit the vulnerability of a WLAN network then takes a WIDS is user friendly in order to detect an attack in a network. So that a solution on the WLAN network kerentangan this is a test of the system Wireless Intrusion Detection System (WIDS) for monitoring a wireless network based Kismet. Kismet application is a computer program created to help a monitoring network, Kismet is the result of his alert or output of the display and the time of the attack. Kismet has a network interface that can display anything that is within his reach, any client connected to the network as well as alerts or output generated by this tool as WIDS. When Kismet on the run again, Kismet will store its logs in a file that is new and different just naming the date and time only. This makes it difficult to search for alerts administrator or output by AP where you want to view or when an administrator wants to see what happens in the network time ago. Moreover, with Kismet client that displays alerts in the form of rooling log in its interface makes difficulties in analyzing network administrator. Therefore, it is necessary to have the use of a user friendly interface.

***Keywords*: WLAN, WIDS, Kismet, Kismet Server**

1. Pendahuluan

1.1 Latar Belakang

Penggunaan jaringan wireless yang paling popular adalah jaringan WLAN. Jaringan ini banyak digunakan di rumah, di universitas, restoran, perpustakaan dan juga tempat-tempat berkumpul lainnya. Namun, jaringan wireless tidak mempunyai batasan yang jelas dan dengan penggunaan gelombang radio ini dapat membuat pihak tertentu untuk melewati celah keamanan dan memanfaatkannya untuk melakukan hal-hal negatif, seperti pencurian password, dan data-data lainnya yang bersifat rahasia atau pribadi. Oleh karena itu, dibutuhkan suatu sistem deteksi yang disebut Intrusion Detection System (IDS) untuk mengantisipasi bahaya tersebut. Dalam jaringan WLAN, IDS ini disebut Wireless Intrusion Detection System (WIDS). WIDS ini dapat mendeteksi serangan pada frame 802.11 pada layer dua dari model Open Systems Interconnection (OSI). Istilah 802.11 ini adalah standar dalam jaringan WLAN.

Implementasi ini dilakukan dengan menggunakan tools Wireless IDS. Tools yang digunakan adalah Kismet. Kismet mempunyai interface yang dapat menampilkan jaringan apa saja yang berada dalam jangkauannya, client mana saja yang terhubung dengan jaringan tersebut serta alert yang dihasilkan oleh tools ini sebagai WIDS. Kismet mempunyai program Kismet drone yang ditempatkan ke sensor yang berupa Wireless Router, Kismet server yang mengolah data-data yang dikumpulkan Kismet drone, dan Kismet client yang menampilkan data-data yang telah diolah oelh Kismet server. Kismet server dan Kismet client umumnya ditempatkan pada PC. Hal ini dikarenakan memori Wireless Router yang terbatas.

Kismet masih menyimpan datanya berupa log file yang disimpan sepanjang Kismet itu dijalankan. Ketika Kismet dijalanakan lagi, Kismet akan menyimpan log-nya dalam file yang baru dan hanya berbeda penamaan tanggal dan waktunya saja. Hal ini membuat administrator sulit dalam mencari alert berdasarkan AP mana yang ingin dilihat ataupun pada saat administrator ingin melihat apa yang terjadi di jaringannya waktu lalu. Selain itu, dengan Kismet client yang menampilkan alert berupa rooling log di interface nya membuat administrator kesulitan dalam menganalisis jaringannya. Oleh karena itu, dibutuhkan adanya pemakaian interface yang user friendly. Aplikasi Kismet adalah sebuah program komputer yang dibuat untuk membantu sebuah monitoring suatu jaringan.

1.2 Rumusan Masalah

1. Bagaimana mengimplementasikan Wireless Intrusion Detection System (WIDS) pada jaringan Wireless Local Area Network (WLAN) yang dapat mendeteksi adanya serangan dalam jaringan tersebut ?
2. Bagaimana melakukan pengujian konfigurasi kismet dalam memonitoring serangan jaringan wireless?

1.3 Tujuan

Tujuan yang ingin di capai dalam pelaksanaan proyek akhir ini adalah untuk mengimplementasikan sebuah aplikasi Wireless Intrusion Detection System (WIDS) untuk mendeteksi adanya serangan yang terjadi di jaringan wireless. Dari tujuan umum tersebut, dapat dilihat kembali menjadi beberapa tujuan khusus sebagai berikut :

1. Mengimplemetasikan Wireless Intrusion Detection System (WIDS) pada jaringan Wireless Local Area Network (WLAN) yang dapat mendeteksi adanya serangan dalam jaringan tersebut.
2. Melakukan pengujian agar dapat memonitoring suatu jaringan wireless yang terdeteksi adanya serangan

1.4 Batasan Masalah

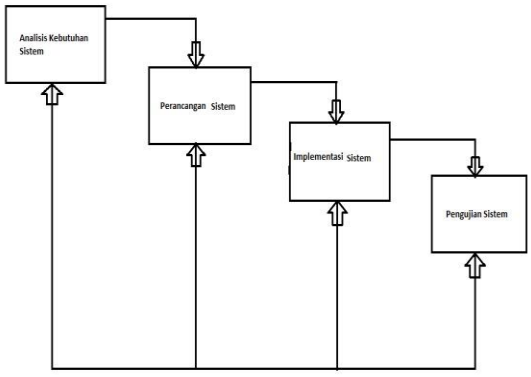
Batasan masalah dalam proyek akhir ini adalah sebagai berikut :

1. Mengimplemetasikan sebuah system WIDS dengan menggunakan tools Kismet yang memiliki fungsi unuk melakukan deteksi terhadap serangan dan memberikan alerting pada jaringan infrastruktur WLAN.
2. Pengujian serangan yang dilakukan menggunakan aircrack-ng dan metode Dos.
3. Tidak membahas tentang penanganan serangan.

1.6 Metode Pengerjaan

Dalam melaksanakan implementasi ini, metode metode yang akan diterapkan adalah sebagai berikut :

1. Studi Literatur dan pustaka
   Melakukan berbagai diskusi pembahasan dengan dosen pembimbing serta dari pustaka yang mendukung dalam pengerjaan implementasi ini.
2. Pendefinisian masalah dan kebutuhan system.
3. Analisis dan perancangan system, yang meliputi tahapan terstruktur sebagai berikut :
   a) Perancangan system Wireless Intrusion Detection System (WIDS).
   b) Implementasi
4. Implementasi perancangan perangkat lunak, system yang akan diimplementasikan adalah Wireless Intrusion Detection System (WIDS), yaitu system yang dapat mendeteksi adanya serangan yang masuk ke dalam jaringan Wireless Local Area Network (WLAN).
5. Evaluasi system, melakukan uji coba dan evaluasi yang akan diimplementasikan.
6. Mengambil kesimpulan, pengujian WIDS yang dapat disimpulkan dari hasil log yang ada.



Gambar 1.1 Skema Pengerjaan Sistem

2. Tinjauan Pustaka

2.1 Wireless Local Area Network (WLAN)

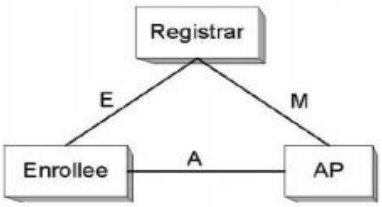
Jaringan ini bisa diakses melalui jaringan kabel maupun nirkabel (wireless). Jaringan kabel dapat membatasi pengguna dalam mengakses internet, namun dengan jaringan wireless, pengguna dapat bebas bergerak dengan jangkauan batas area untuk mengaksesnya. Jenis jaringan yang memakai jaringan wireless ini adalah Wireless Local Area Network (WLAN).

2.2 Wifi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) sebelumnya disebut Wi-Fi Simple Config yaitu program sertifikasi opsional yang dikembangkan oleh Aliansi Wi-Fi, dirancang untuk memudahkan mengatur pengaktifan jaringan keamanan Wi-Fi di rumah dan lingkungan kantor kecil. Wi-Fi Protected Setup mendukung metode (menekan tombol atau memasukkan PIN ke dalam aplikasi sejenis panduan) yang lebih diketahui bagi kebanyakan konsumen untuk mengkonfigurasi jaringan dan memungkinkan keamanan. Mengapa Wi-Fi Protected Setup dibutuhkan? Pengaturan Wi-Fi Protected memiliki fitur keamanan canggih yang disediakan oleh WPA dan WPA2 (Wi-Fi Protected Access), namun beberapa pengguna menemukan fitur tersebut sulit untuk dikonfigurasi dengan benar. Akibatnya, banyak konsumen meninggalkan jaringan Wi-Fi mereka sebagian atau seluruhnya tanpa keamanan. Wi-Fi Protected Setup memberikan konsumen cara standar untuk lebih mudah mengatur Wi-Fi Protected Setup untuk Wireless Local Area Network (WLAN), dan untuk mengaktifkan fitur keamanan. Perangkat tambahan dapat dengan mudah ditambahkan ke jaringan dikemudian waktu. Dengan teknologi Wi-Fi menghubungkan berbagai perangkat, termasuk PC, ponsel dan konsumen elektronik secara sederhana, standar, pengenalan untuk konfigurasi jaringan dan pemberdayaan keamanan yang lebih penting daripada sebelumnya. Konsumen
Wi-Fi akan dapat memilih dari berbagai jenis produk dan merek mengetahui bahwa ada metode sederhana untuk menambahkan perangkat ini ke jaringan mereka.

2.3 Cara Kerja WPS

Ada dua pendekatan utama untuk setup jaringan dalam Wi - Fi Protected Setup yaitu push- button dan memasukkan PIN. Memasukkan PIN adalah wajib di semua perangkat Wi-Fi Protected Setup, sedangkan tombol push adalah opsional (tambahan) dan mungkin juga dapat ditemukan di beberapa perangkat . Memasukkan PIN di semua jaringan Wi-Fi Protected Setup, PIN yang unik (Personal Identification Number) akan diperlukan setiap perangkat untuk bergabung dengan jaringan. Sebuah label PIN atau stiker dapat ditempatkan pada perangkat atau PIN dinamis dapat dihasilkan dan ditampilkan pada layar perangkat (misalnya layar monitor). PIN digunakan untuk memastikan perangkat yang dimaksud ditambahkan ke jaringan yang sedang diatur dan akan membantu untuk menghindari upaya kesengajaan atau kejahatan untuk menambah perangkat yang tidak diinginkan ke jaringan . Sebuah perangkat terdaftar (seperti Access Point atau Router Wireless , PC All in One, dan perangkat lain) akan mendeteksi ketika perangkat Wi-Fi baru berada dalam jangkauan, dan meminta pengguna untuk memasukkan PIN, jika dia ingin menambahkan perangkat baru ke jaringan . Dalam mode ini, jaringan Wi-Fi Protected Setup mengenkripsi data dan mengotentikasi setiap perangkat pada jaringan . Metode memasukkan PIN didukung semua perangkat.



Gambar 2.1 Cara Kerja WPS

2.4 Wireless Intrusion Detection System (WIDS)

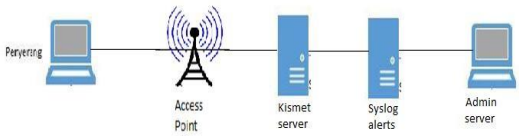
Penggunanaan jaringan wireless berkembang dengan sangat pesat. Dengan adanya jaringan wireless, user dapat lebih mudah dan nyaman menggunakan dan mengakses internet. Penggunaan client tidak terbatas dengan adanya kabel seperti layaknya jaringan kabel. Untuk menjaga jaringan wireless dari hal-hal yang tidak diinginkan, administrator haarus memonitor kejadian-kejadian apa saja yang terjadi di jaringannya dan mendeteksi adanya serangan atau tidak. Untuk melakukannya, administrator harus menginstall sebuah Wireless Intrusion Detection System (WIDS).

2.5 Cara Kerja WIDS

Secara umum, IDS (Intrusion Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan kepada administrator. WIDS membutuhkan sensor untuk mengumpulkan data-data dalam jaringan, server untuk mengolah data yang telah dikumpulkan, dan client untuk menampilkan hasil dari pengolahan data yang telah dikumpulkan. Interface WIDS ditempatkan pada client WIDS.

WIDS dapat mendeteksi serangan pada frame 802.11 pada lapisan dua dari jaringan wireless. Ada tiga tipe frame MAC 802.11 yaitu data frame, control frame, dan management frame. Mayoritas serangan wireless menjadikan management frame sebagai targetnya karena frame ini bertugas untuk melakukan otontekasi, asosiasi, disosiasi, beacon, dan probe request/response. Serangan wireless seperti Man-in-the-Middle (MIM), Rogue Access Point (RAP), war driver, dan Denial-of-service (DoS) yang berjalan pada frame 802.11 dan tidak bisa mendeteksi pada lapisan tiga. IDS pada jaringan nirkabel tidak dapat menerima frame ini, karena management frame tidak dapat diteruskan ke lapisan di atasnya.

WIDS membutuhkan interface khusus. Interface wireless ini harus dioprasikan pada mode monitor, yang dikenal juga sebagai mode RFMON. Mode ini membolehkan perangkat untuk menerima semua lalu lintas yang masuk. Interface yang betugas memonitor harus terus berganti chanel, dikenal dengan channel hopping, yang tersedia pada jaringan tersebut. Beberapa serangan wireless bekerja dengan menggunakan RAP pada channel yang berbeda. Sebagai contoh, serangan MIM menggunakan RAP yang paling sedikit berbeda lima channel dari target AP.

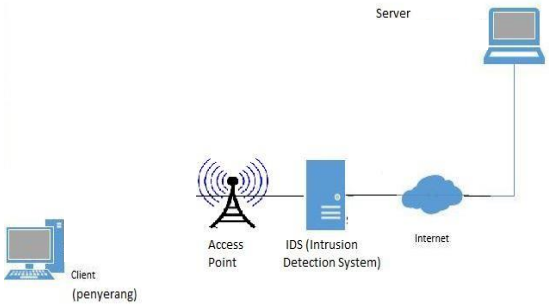


Gambar 2.2 Cara Kerja Kismet WIDS

2.6 Komponen WIDS

Sebelumnya WIDS ini sudah dapat mendeteksi anomali-anomali dan serangan dalam jaringan hanya menggunakan tools Kismet saja, tetapi untuk penyimpanannya, pencarian dan tampilan datanya masih mempunyai kelemahan. Penyimpanan data masih terbatas log pada saat tools Kismet dinyalakan saja dan tidak teroganisir dengan baik sehingga jika ingin mencari data-data yang telah diambil sebelumnya, administrator harus mencarinya secara amnual. Hal ini sangat merepotkan dan memakan waktu karena administrator harus mencari data satu-persatu diantara sekian banyaknya data. Selain itu, tampilan Kismetnya sendiri menggunakan GUI terminal (console) sehingga kurang sesuai jika digunakan sebagai WIDS. Oleh karena itu, untuk mendapatkan WIDS yang sesuai dengan kebutuhan administrator dibutuhkan komponen-komponen sebagai berikut :

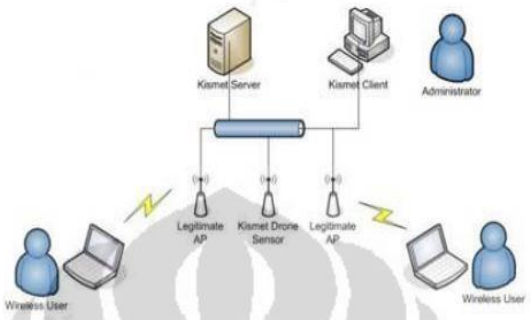
1. Kismet drone : program Kismet yang berfungsi sebagai sensor. Program ini didisain untuk mengubah Kismet menjadi WIDS terdistribusi. Drone menangkap data dan meneruskannya ke Kismet server melalui koneksi kabel. Drone tidak melakukan decoding paket apapun sehingga kebutuhan perangkat kerasnya pun minimal. Kismet drone dijalankan dengan system operasi OpenWRT. Open WRT adalah system operasi open source berbasis Linux yang diperuntukkan untuk perangkat Wireless Router. Kismet drone dapat diunduh dari repository OpenWRT.
2. Kismet server : program Kismet yang berfungsi untuk mengolah paket-paket data yang telah ditangkap Kismet drone. Kismet server merupakan komponen utama dalam sistem WIDS ini. Kismet dapat diunduh dari https://www.kismetwireless.net/code/svn/trunk/.



Gambar 2.3 Desain Jaringan Kismet WIDS

2.7 Kismet WIDS

Kismet merupakan sebuah aplikasi jaringan open source. Kismet mengidentifikasi jaringan dengan cara mengumpulkan paket dan mendeteksi jaringan secara pasif. Aplikasi open source yang menyediakan pengguna dengan 802.11 layer2 jaringan nirkabel sniffer, detektor, dan solusi intrusion detection untuk Linux, BSD, Microsoft Windows dan sistem operasi Mac OS X. Aplikasi ini berjalan di setiap terminal emulator dan fitur client / server arsitektur modular yang mendukung kartu nirkabel yang mencakup baku pemantauan (rfmon) modus. Hal ini pada dasarnya adalah baris perintah 802.11 b / g / n / sniffer lalu lintas jaringan. Ini telah dirancang dari bawah ke atas untuk dapat mengidentifikasi jaringan hanya dengan mendeteksi jaringan bernama standar dan pasif mengumpulkan paket. Hal ini juga dapat mendeteksi tersembunyi Wi-Fi jaringan, dan menemukan jaringan nirkabel non beaconing ada melalui lalu lintas data.



Gambar 2.4 Arsitektur Kismet WIDS

.

2.8 Arsitektur Kismet WIDS

Kismet wireless telah dilengkapi dengan Kismet drone yang membuatnya menjadi aplikasi WIDS terdistribusi. Arsitektur Kismet terdiri dari :

1. Kismet drone : mengumpulakn data-data dalam jaringan dan mengirimkannya ke Kismet server.
2. Kismet server : mengolah data yang telah dikumpulkan
3. Kismet client : menampilkan hasil dari pengolahan data yang telah dikumpulkan.

Perangkat-perangkat yang dibutuhkan agar dapat menjalankan Kismet WIDS ini yaitu :

1. Komputer (Kismet server dan Kismet client dapat menggunakan 1 komputer).
2. Wireless adapter (jika ingin menggunakan drone, wireless adapter berada pada Wireless Router, jika tidak ingin menggunakan drone, wireless adapter bisa dari build-in PC atau USB wireless adapter).
3. Wireless Router (dikonfigurasi program Kismet drone).

3. Analisis dan Perancangan

3.1 Gambaran Sistem Saat Ini (Atau Produk)

Secara umum, sistem yang akan diimplementasikan dalam kondisi

prototype dan memonitoring suatu jaringan.

3.2 Analisis Kebutuhan Sistem (Atau Produk)

3.2.1 Spesifikasi dan Kebutuhan Perangkat Keras

Adapun perangkat keras (hardware) yang akan digunakan dalam pengerjaan proyek akhir ini adalah :

a) Perangkat keras yang digunakan
   a. Spesifikasi perangkat keras untuk server
      1. Processor : Intel (R) Corei3 (R) CPU 2.40GHz
      2. Memori : 2GB DDR3
      3. Drive : 500GB Harddisk, 1DVD-RW
      4. Perangkat tambahan : Access Point dan Wireless Card
   b. Spesifikasi perangkat keras untuk client (penyerang)
      1. Processor : Intel Coleron Dual-Core 1.40GHz
      2. Memori :4GB DDR3-SDRAM
      3. Drive : 320GB Harddisk, 1DVD-ROM

3.2.2 Spesifikasi Kebutuhan Perangkat Lunak

Adapun perangkat Lunak (software) yang akan digunakan dalam pengerjaan proyek akhir ini adalah :

a) Sistem Oprasi : Ubuntu 14.04 64 bit
b) Kismet
c) Kismet Drone
d) Kismet Server
e) Air crack-ng
f) Dos
g) Kali Linux

3.3 Perancangan Sistem

Dalam perancangan atau pembuatan sistem keamanan jaringan ini ada beberapa installasi software dan peralatan yang dibutuhkan, antara lain :

A. Acces Point

Acces Point perangkat, seperti router nirkabel / wireless, yang memungkinkan perangkat nirkabel untuk terhubung ke jaringan. Pada access point terdapat router built-in, sementara yang lain harus terhubung ke router untuk menyediakan akses jaringan. Dalam kedua kasus, access point biasanya didesain untuk perangkat lain, seperti jaringan switch atau modem broadband.

B. Kismet

Kismet adalah sebuah program komputer yang dibuat untuk membantu sebuah monitoring suatu detektor jaringan wireless, sniffer, dan sistem pendeteksi penyusup pada komputer. Wireless ialah satu jenis jaringan berdarsarkan media komunikasinya, yang memungkinkan perangkat-perangat didalamnya seperti komputer, hp, dll bisa saling berkomunikasi secara wireless/tanpa kabel.

C. Kismet drone

merupakan program Kismet yang berfungsi sebagai sensor. Program ini didisain untuk mengubah Kismet menjadi WIDS terdistribusi. Drone menangkap data dan meneruskannya ke Kismet server melalui koneksi kabel. Drone tidak melakukan decoding paket apapun sehingga kebutuhan perangkat kerasnya pun minimal. Kismet drone dijalankan dengan system operasi OpenWRT. Open WRT adalah system operasi open source berbasis Linux yang diperuntukkan untuk perangkat Wireless Router. Kismet drone dapat diunduh dari repository OpenWRT.

D. Kismet server

Merupakan program Kismet yang berfungsi untuk mengolah paket-paket data yang telah ditangkap Kismet drone. Kismet server merupakan komponen utama dalam sistem WIDS ini. Kismet dapat diunduh dari

https://www.kismetwireless.net/code/svn/trunk/.

E. Aircrack-ng

Ialah untuk memonitor dan menganalisa jaringan wireless fungsinya untuk mengubah kode-kode file hasil capture dari Airodump menjadi password sebenarnya yang sedang dicari http://gedelumbung.com/menjebol-password-wi-fi-dengan-aircrack/

F. Dos

Didefinisikan sebagai distributed denial of service. Serangan DDoS untuk membuat sumber daya komputer (yaitu - website, aplikasi, e-mail, pesan suara, jaringan) berhenti merespons. Metode serangan dengan mengirimkan paket data ke suatu host.

3.4 Langkah Pengerjaan

1. Konfigurasi Access Point WRT610N Cisco
2. Konfigurasi Kismet yang akan menjadi tools IDS (Intrusion Detection System)
3. Installasi paket Ubuntu 14.04 64 bit

3.5 Pengujian Sistem

1. Penyerangan pertama adalah Dos Attack, penyerangan ini dilakukan dengan cara mengirimkan paket data ICMP secara terus menerus kekomputer target.
2. Penyerangan kedua adalah Aircrack-ng, penyerangan ini dilakukan dengan cara mengirimkan kode-kode hasil file capture dari airodump menjadi password sebenarnya.

Daftar Pustaka

[1] Wright 2003, Januari, Detecting Wireless LAN MAC address Spoofing.

[2] http://www.sans.org/reading_room/whitepapers/honors/wireless-attacks-intrusion-detection-perspective_1681. diakses pada 5 Febuari 2015.

[3] https://www.kismetwireless.net/code/svn/trunk/README,2011. diakses pada 5 Febuari 2015.

[4] Murray 2009, April, An Inexpensive Wireless IDS using Kismet and OpenWRT. SANS. http://www.sans.org/reading_room/whitepapers/detection/inexpensive-wireless-ids-kismet-openwrt_33103.

[5] http://www.dd-wrt.com/wiki/index.php/Kismet_Server/Drone. diakses pada 5 Febuari 2015.

[6] http://sagan.softwink.com. diakses pada 5 Febuari 2015.

[7] http://www.usr.com/download/whitepapers/wireless-wp.pdf. diakses pada 5 Febuari 2015.

[8] https://www.kismetwireless.net/code/svn/trunk/. diakses pada 6 Febuari 2015.

[9] http://www.plimbi.com/article/40502/fungsi-kernel diakses pada 6 Febuari 2015

[11] Viehbock 2011, Desember, Brute Forcing Wi-fi Protected Setup

[12] https://www.kismetwireless.net/code/svn/trunk/. diakses pada 6 Febuari 2015.

[13] http://csrc.nist.gov/publication/nistpubs/800-94/SP800-94.pdf. diakses pada 6 Febuari 2015.

[14] http://gedelumbung.com/menjebol-password-wi-fi-dengan-aircrack/ diakses 6 Febuari 2015