 ISSN: 1411-3201

ANALISIS KEAMANAN JARINGAN WIRELESS YANG MENGGUNAKAN CAPTIVE PORTAL (STUDI KASUS : WARNET FORTRAN)

Bangkit Kurnia Ari Setyawan, Melwin Syafrizal

STMIK AMIKOM Yogyakarta
email : melwin@amikom.ac.id

Abstract

Nowadays the utilization of wireless-based technology has been developed, whether it's for the usage of education or for benefit of commercial needs. FORTRAN internet cafe is one of internet shops utilizing this technology. However behind the popularity of this technology there some fragility that needs to be fixed. The fragility of the technology is that it's susceptible of assaults from attackers, it can be caused by the overly opened communication. Plated protection is needed in order to minimize the possibility of assaults.

FORTRAN internet cafe has been attempted to minimize the weakness of the technology by using capital portal (Open System Authentication). Authentication of this method is happening when the users accessing the internet for the first time. However, this method can't guarantee that the wireless network is safe from the attackers' assaults. Therefore it is necessary to do some trials to know and find the chances of the safety for this technology.

The trials that are done are MAC Address Spoofing and Man in the Middle Attack, where the MAC Address Spoofing is the one that's successful. This shown that there is still possibility of safety for the wireless system at FORTRAN Internet Café, which is using MAC Address Spoofing. It is needed an added system to handle the existence of safety possibility. DecaffeinatID software as one of simple IDS (Intrusion Detection Server) kinds and User Isolation Method to prevent the clients to communicate with each other.

Keywords:
Wireless, Security, Captive portal, wireless weakness

Pendahuluan

Pemanfaatan teknologi berbasis wireless pada saat ini sudah semakin banyak, baik digunakan untuk pendidikan maupun untuk komersil. Warnet Fortran merupakan salah satu warnet yang memanfaatkan teknologi ini. Namun di balik kepopuleran teknologi ini terdapat kelemahan yang harus di benahi. Kelemahan teknologi ini sangat rentan terhadap serangan yang dilakukan oleh attacker, itu dapat terjadi karena komunikasi yang berlangsung sangat terbuka. Diperlukan pengamanan yang berlapis agar dapat meminimalkan serang tersebut.

Warnet Fortran pun sudah berupaya untuk meminimalkan kelemahan teknologi tersebut, yaitu dengan captive portal (Open System Authentication). Authentication pada metode ini terjadi pada saat user/pengguna melakukan pengaksesan internet untuk pertama kali. Metode ini pun belum biasa di jadikan pedoman bahwa jaringan wireless aman dari serangan attacker. Maka dari itu diperlukan percobaan untuk mengetahui celah keamanan yang masih ada, sehingga dapat mencegah terjadinya kerugian pada Warnet Fortran, serta dapat digunakan untuk meningkatkan kualitas sistem wireless pada Warnet Fortran.

Tinjauan Pustaka

Tinjauan pustaka ini mengambil permasalahan keamanan jaringan wireless, lebih detailnya yaitu keamanan jaringan wireless yang menggunakan captive portal. Referensi yang digunakan penulis salah satunya dari skripsi dengan judul "Analisis Keamanan Wireless di Universitas Muhammadiyah Surakarta", ditulis oleh Hendri Noviyanto, Universitas Muhammadiyah Surakarta tahun 2012.

Referensi tersebut digunakan karena terdapat kemiripan dari permasalahan yang di bahas yaitu kelemahaan sistem jaringan wireless. Tetapi terdapat perbedaan disini difokuskan untuk membahas kelemahaan captive portal dan cara meningkatkan keamanannya sedangkan pada referensi membahas semua sistem keamanan jaringan wireless(WEP, WPA, Captive portal), sehingga kurang fokus terhadap peningkatan sistem keamanannya..

Landasan Teori

1. Internet

Internet adalah metode untuk menghubungkan berbagai computer ke dalam satu jaringan global,melalui protokol yang disebut Transmission Control Protocol/Internet Protocol (TCP/IP)

2. Wireless LAN

 ISSN: 1411-3201

Wireless atau wireless network merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya
Unit kerja yang paling menarik tentu saja unit kerja 802.11 yaitu unit kerja yang mengurusi wireless LAN. Unit kerja ini sendiri masih dibagi-bagi lagi menjadi unit yang "benar-benar kerja" sekarang namun tidak lagi dengan tanda titik dan angka namun dengan huruf a,b,c sehingga menjadi unit 802.11a, 802.11b, 802.11g, dan seterusnya.(Sto.2007:9) 1

a. Standar 802.11

Standar pertama yang menggunakan frequency hopping spread spectrum (FHSS) dan direct sequence spread spectrum (DHSS) yang beroperasi pada pita 2.4 GHz dengan data rate hingga 2 Mbps.

b. Standar 802.11a

Standar ini beroperasi pada pita 5 GHz dengan menggunakan orthogonal frequency division multiplexing (OFDM) serta data rate hingga 54 Mbps.

c. Standar 802.11b

IEEE 802.11b merupakan pengembangan dari standar IEEE 802.11 yang asli,yang bertujuan untuk meningkatkan kecepatan hingga 5.5 Mb/s atau 11 Mb/s tapi tetap menggunakan frekuensi prakteknya, kecepatan maksimum yang dapat diraih oleh standar IEEE 802.11b mencapai 5.9 Mb/s pada protokol TCP, dan 7.1 Mb/s pada protokol UDP.

d. Standar 802.11g

IEEE 802.11g adalah sebuah standar jaringan nirkabel yang bekerja pada frekuensi 2,45 GHz. 802.11g yang dipublikasikan pada bulan Juni 2003 mampu mencapai kecepatan hingga 54 Mb/s pada pita frekuensi 2.45 GHz, sama seperti halnya IEEE 802.11 biasa dan IEEE 802.11b.

e. Standar 802.11n

IEEE 802.11b merupakan pengembangan dari standar IEEE 802.11 yang asli,yang bertujuan untuk meningkatkan kecepatan hingga 5.5 Mb/s atau 11 Mb/s tapi tetap menggunakan frekuensi prakteknya, kecepatan maksimum yang dapat diraih oleh standar IEEE 802.11b mencapai 5.9 Mb/s pada protokol TCP, dan 7.1 Mb/s pada protokol UDP

3. Keamanan Wireless LAN

Standarisasi awal keamanan wireless 802.11 ini menentukan bahwa untuk bisa bergabung ke dalam jaringan AP, host harus diperbolehkan mengirim dan menerima data melalui AP, dan untuk melalukakn itu terdapat 2 pintu yang harus dilalui yaitu Authentication dan Association. (Sto.2007:89) 2 Standarisasi 802.11 menggunakan 2 jenis authentication.

a. Shared Key Authentication

Shared Key Authentication mengharuskan client untuk mengetahui lebih dahulu kode rahasia (passphare key) sebelum mengijinkan terkoneksi dengan AP.

b. Open System Authentication

Open system authentication ini, dapat dikatakan tidak ada authentication yang terjadi karena client bisa langsung terkoneksi dengan AP (Access point). Setelah client melalui proses open system authentication dan Association, client sudah diperbolehkan mengirim data melalui AP namun data yang dikirim tidak tidak serta merta dilanjutkan oleh AP kedalam jaringannya. Salah satu contoh sistem yang menggunakan metode Open system authentication yaitu Captive Portal.
Captive Portal adalah suatu teknik autentikasi dan pengamanan data yang lewat dari network internal ke network eksternal. Captive Portal sebenarnya merupakan mesin router atau gateway yang memproteksi atau tidak mengizinkan adanya trafik, hingga user melakukan registrasi.
Captive portal juga mempunyai potensi untuk mengijinkan kita untuk melakukan berbagai hal secara aman melalui SSL, IPSec, dan mengset rule quality of service (QoS) per user, tapi tetap mempertahankan jaringan yang sifatnya terbuka di infrastruktur WiFi.

4. Lapisan Protokol TCP/IP

TCP/IP adalah sekumpulan protokol yang didesain untuk melakukan fungsi-fungsi komunikasi data pada Wide Area Network (WAN). TCP/IP terdiri atas sekumpulan protokol yang masing-masing bertanggung jawab atas bagian-bagian tertentu dari komunikasi data. Protokol yang satu tidak perlu mengetahui cara kerja protokol yang lain, sepanjang ia masih bisa saling mengirim dan menerima data.

Metode Penelitian

Jaringan wireless warnet Fortran menggunakan topologi BSS/Infrastruktur dan menggunakan router mikrotik 5.24. Proses login layanan wireless di warnet Fortran ini yaitu dengan memasukkan username dan password. Sistem ini merupakan sistem dengan konsep captive portal.

1. Alat Penelitian

a. Kebutuhan Perangkat Keras

Penelitian ini membutuhkan 2 buah laptop, 1 buah berfungsi sebagai client resmi atau target dan satu lagi sebagai penyerang/attacker. Spesifikasi laptop yang akan digunakan dapat dilihat pada tabel berikut

Tabel 1 Spesifikasi Laptop Penyerang

 ISSN: 1411-3201

Prosesor	Intel (R) core (TM) i5 CPU M450 @ 2.40 GHz
Memori	4096 MB
VGA	Intel (R) HD Graphics
Hard Disk	500 GB
Wireless Adapter	Realtek RTL8191SE

Tabel 2 Spesifikasi Laptop Target

Prosesor	Intel (R) Pentium (R) CPU B950 @ 2.10 GHz
Memori	6144 MB
VGA	Intel (R) HD Graphics
Hard Disk	500 GB
Wireless Adapter	Atheros AR9002WB-1NG

b. Kebutuhan Perangkat Lunak

Perangkat lunak adalah bagian yang penting dalam melakukan penelitian ini. Perangkat Lunak yang dipakai dalam penelitian ini bias didapat secara gratis dari internet. Perangkat Lunak yang digunakan antara lain:

1) Sistem Operasi GNU/Linux Backtrack 5 R2 kernel 3.2.6
2) Wireshark
3) Netdiscover
4) Macchanger

2. Analisis

a. Survei dan Pengambilan Data

Survey di lapangan digunakan untuk melihat keadaan dan kondisi wireless, serta mengambil data yang akan digunakan untuk analisa. Tahap selanjutnya adalah simulasi dan analisis keadaan dan kondisi wireless.
Simulasi yang akan dilakukan berupa kegiatan pencarian Mac Address (MAC Address Spoofing), Man In The middle Attack untuk mendapatkan informasi mengenai username dan password.

b. Teknis Serangan

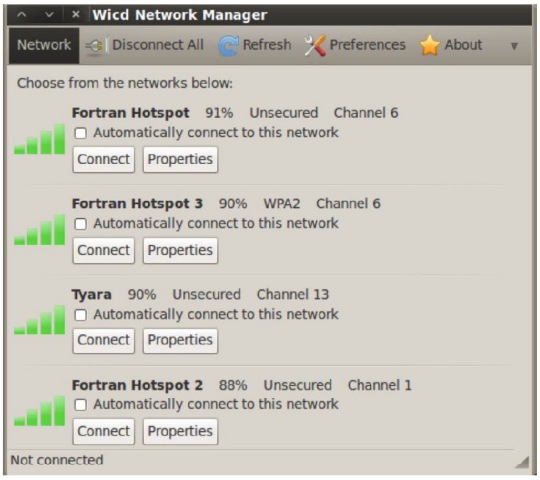
1) Device penyerang mulai mencari koneksi dengan Access point yang menjadi target
2) Device peyerang melakukan koneksi dengan Access point tanpa melakukan pengaksesan internet
3) Device penyerang mulai menjalankan program untuk mencari informasi client resmi (target)
4) Penyerang kemudian melakukan percobaan dengan menggunakan informasi yang diperoleh dari penyadapan informasi yang telah dilakukan
5) Penyerang mulai melakukan perubahan dengan informasi yang didapat, setelah berhasil melakukan perubahan, penyerang melakukan koneksi internet dengan Access point menggunakan identitas yang telah diubah sesuai dengan identitas client resmi

c. Percobaan

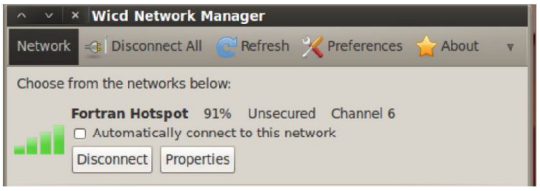
Gambar 1 Halaman Login Hotspot

Mac Address Spoofing

1) Konek ke Access Point Target



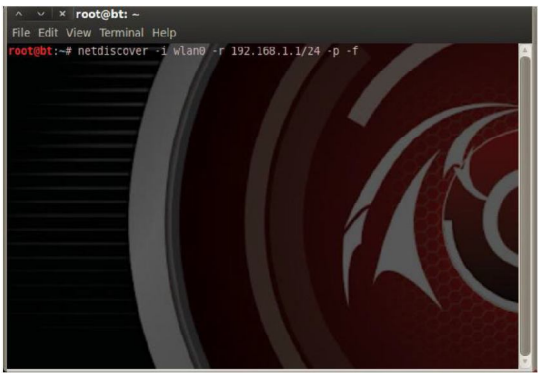
Gambar 2 Access Point Yang Tersedia



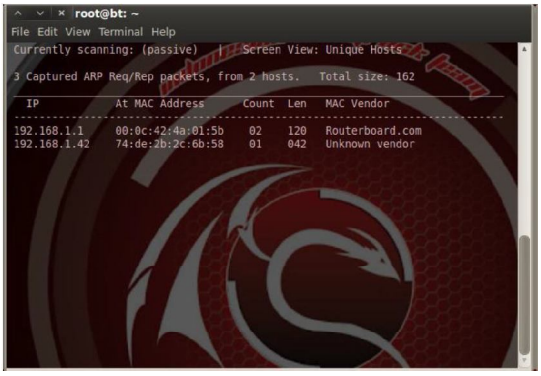
Gambar 3 Koneksi ke Access Point Target

2) Scanning user yang telah terkoneksi

 ISSN: 1411-3201



Gambar 4 Netdiscover Untuk Scanning User Yang Aktif

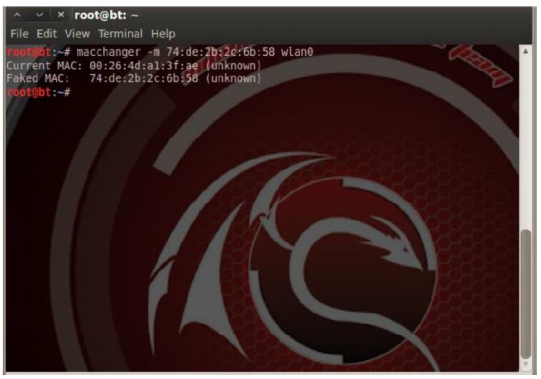


Gambar 5 User Aktif Beserta MAC Address

3) Matikan wifi

Gambar 6 Matikan Wi-Fi

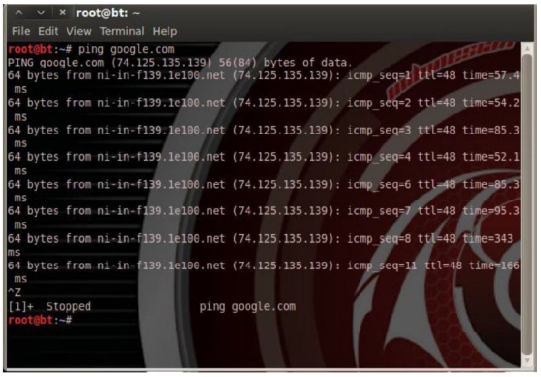
4) Ubah MAC Address



Gambar 7 Macchanger

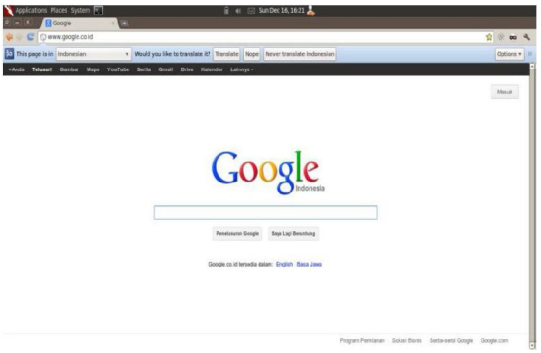
5) Konek kembali dengan Access point target, lakukan pengaksesan internet:

- Pengecekan koneksi internet di Command line dengan perintah ping ke alamat suatu situs



Gambar 8 Pengecekan dengan CLI

- Pengecekan koneksi internet dengan web browser

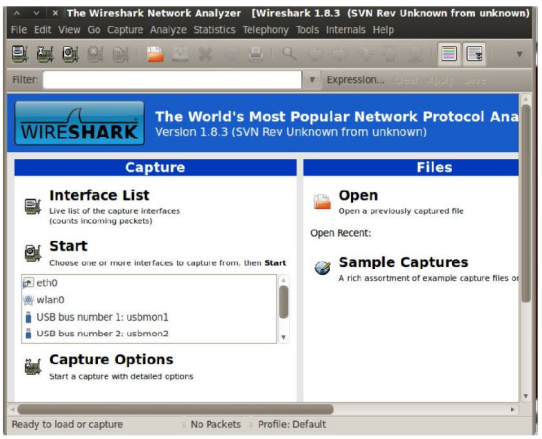


Gambar 9 Pengecekan Koneksi dengan Web Browser

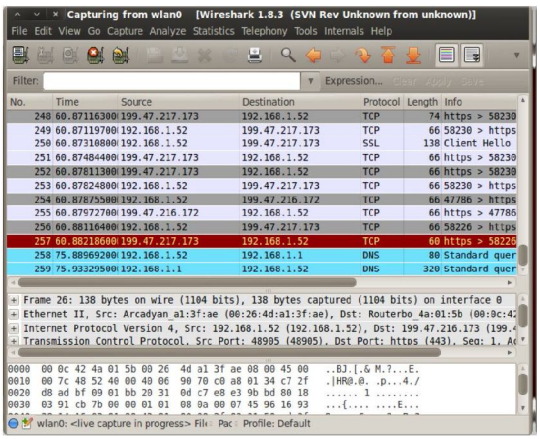
Man in The Middle Attack

1) Jalakan program wireshark

 ISSN: 1411-3201

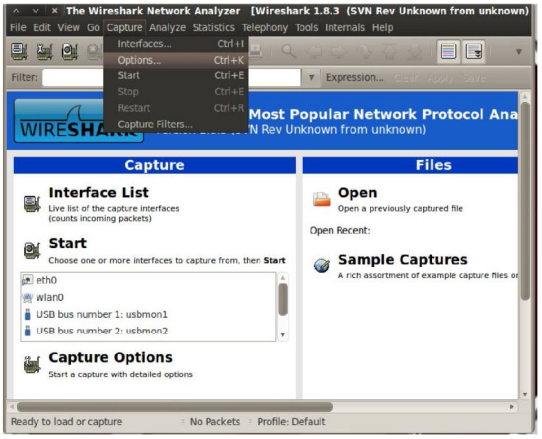


Gambar 10 Wireshark



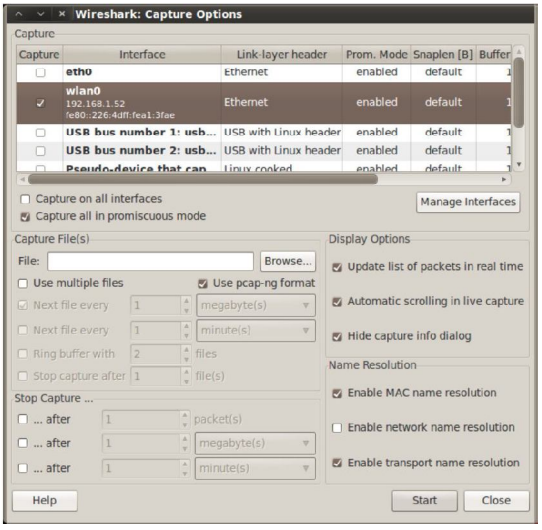
Gambar 13 Proses Sniffing

2) Klik capture lalu pilih option



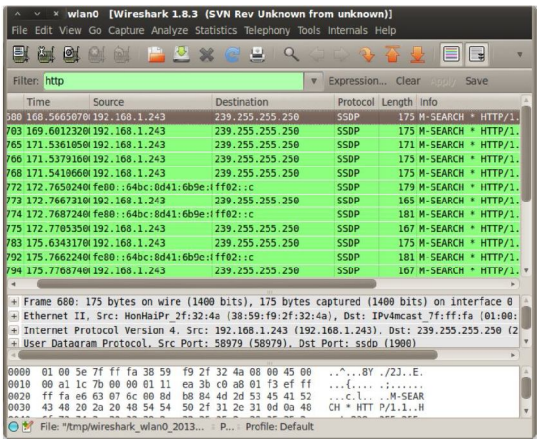
Gambar 11 Memilih Interface

3) Interface yang dipilih adalah Ethernet Card yang menuju ke jaringan



Gambar 12 Interface Yang Tersedia

4) Untuk men-sniffing password, pada kolom filter ketikkan "http" untuk memudahkan pengelompokan data



Gambar 14 Pengelompokan Berdasar Protokol HTTP

Hasil dan Pembahasan

1. Implentasi

2. Pengujian

a. DecaffeinatID

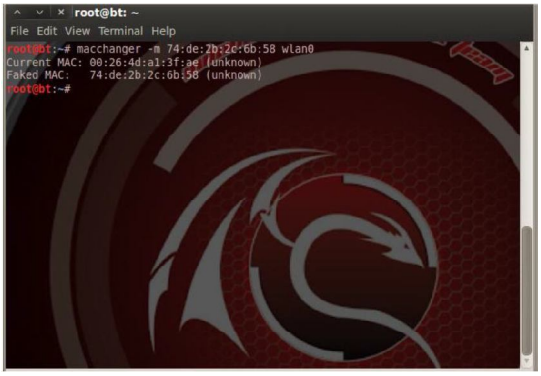
Tujuan Pengujian DecaffeinatID Untuk mengetahui DecaffeinatID bekerja dengan baik yaitu dengan memberikan peringatan kepada administrator saat terjadi MAC Address Spoofing dan mencatat akivitas client. Berikut ini adalah mekanisme pengujian:

1) Penyerang mulai mencari koneksi dengan Access point yang menjadi target
2) penyerang melakukan koneksi dengan Access point tanpa melakukan pengaksesan internet
3) Penyerang mulai melakukan scanning user yang aktif

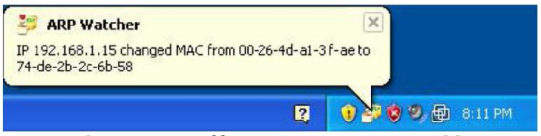
 ISSN: 1411-3201

4) Setelah scanning jaringan dan mendapakan informasi tentang MAC Address seperti pada gambar 4.9
5) Penyerang mulai melakukan perubahan dengan menggunakan informasi yang didapat seperti pada gambar 4.6
6) Saat penyerang melakukan perubahan, DecaffeinatID memberikan peringatan kepada administrator seperti pada gambar 4.7.

Indikator Pengujian DecaffeinatID dapat dilihat dari penyerang mencoba merubah MAC Address dengan MAC Address milik client resmi seperti pada gambar 4.6 maka DecaffeinatID memberikan peringatan kepada administrator seperti pada gambar 4.7.



Gambar 15 Penyerang merubah MAC Address



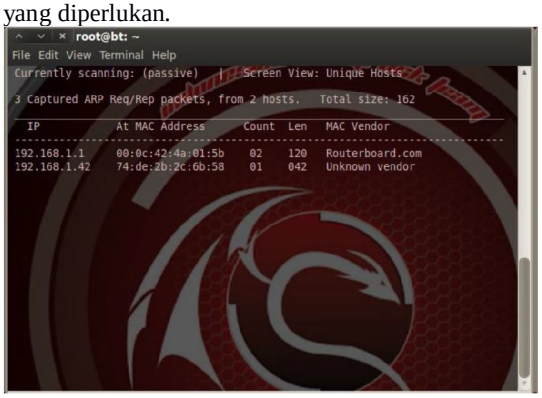
Gambar 16 DecaffeinatID Saat MAC Address Berubah

b. Isolasi User

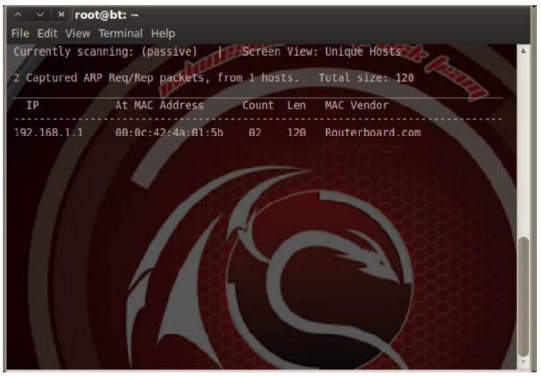
Tujuan pengujian metode isolasi user adalah untuk mengetahui saat terjadinya scanning oleh penyerang, penyerang tidak mendapatkan informasi seperti IP Address dan MAC Address milik client yang lain. Adapaun mekanisme pengujian metode Isolasi User adalah sebagai berikut:

1) penyerang mulai mencari koneksi dengan Access point yang menjadi target
2) penyerang melakukan koneksi dengan Access point tanpa melakukan pengaksesan internet
3) Penyerang mulai melakukan scanning user yang aktif
4) Saat melakukan scanning jaringan penyerang tidak mendapatkan informasi yag di butuhkan seperti pada gambar 4.10

Indikator pengujian metode Isolasi User adalah ketika penyerang mencoba melakukan scanning jaringan untuk mendapatkan informasi seperti pada gambar 4.10 tetapi tidak mendapatkan informasi yang diperlukan.



Gambar 17 Scanning User Sebelum Menerapkan Metode Isolasi User



Gambar 18 Scanning User Setelah Menerapkan Metode Isolasi User

Kesimpulan dan Saran

1. Kesimpulan

1) Sistem keamanan wireless captive portal pada Warnet Fortran pada umumnya sudah cukup baik. Hal ini dibuktikan dengan percobaan metode Man In The Middle Attack tidak didapat informasi penting seperti username dan password utuk mengakses jaringan wireless.
2) Celah keamanan pada sistem wireless Warnet Fortran masih memberikan kemungkinan untuk melakukan kegiatan MAC Address Spoofing, sehingga dibutuhkan konfigurasi atau sistem tambahan untuk mengantisipanya.
3) Sistem atau konfigurasi tambahan yang diperlukan untuk memperbaiki celah keamanan yang ada, diantaranya dengan menggunakan software decaffeinatID sebagai software monitoring dan metode

 ISSN: 1411-3201

isolasi user. DecaffeinatID memberikan peringkatan kepada Administrator saat terjadi MAC Address Spoofing dan metode isolasi user mencegah penyerang pada saat melakukan scanning.

2. Saran

1) Administrator Warnet sebaiknya ikut memperhatikan perkembangan sistem yang ada. Walau pun menggunakan hardware dengan sistem keamanan yang baik dan sudah memproteksi sistem wirelessnya. Administrator harus tetap memperhatikan keamanan yang ada, karena sebaik apapun sistem keamanan pasti masih terdapat celah. Faktor maintenance yang dilakukan administrator untuk menangani celah tersebut sangatlah penting.
2) Penanganan untuk dapat meminimalisir terjadinya serangan MAC Address Spoofing dapat dilakukan dengan memantau aktivitas client yang terhubung ke dalam jaringa untuk mengetahui perubahan yang terjadi, jika ada aktivitas yang dianggap mencurigakan seperti serangan administrator dapat langsung memutus client yang melakukan aktivitas tersebut.
3) Pengecekan jaringan secara berkala diperlukan utuk menghindari terjadinya permasalahan/eror pada jaringan yang bisa mengakibatkan terganggunya kinerja jaringan.

Daftar Pustaka

[18] Fauzan, F. 2012. Perancangan dan Analisis Keamanan Jaringan Terhadap ARP Spoofing pada Hotspot, www.fauzanfadillah.wordpress.com/2012/02/10/, diakses tanggal 4 November 2012.

[19] Noviyanto, H. 2012. Analisis Keamanan Wireless di Universitas Muhammadiyah Surakarta. Skripsi. Surakarta : Fakultas Teknik, Universitas Muhammadiyah Surakarta.

[20] Purbo, Onno. W. 2003.Captive Portal, http://kambing.ui.ac.id/onnopurbo/orari-diklat/teknik/2.4ghz/wifi-advanced/captive-portal-11-2003.doc , diakses tanggal 7 November 2012

[21] Sto. 2007. Wireless Kung Fu : Networking & Hacking. Jasakom.

[22] Wahana Komputer. 2012. Network Hacking dengan Linux Backtrack. Yogyakarta: Andi Offset.

Biodata Penulis

Bangkit Kurnia Ari Setyawan, adalah mahasiswa Jurusan Teknik Informatika Program Strata 1 STMIK AMIKOM Yogyakarta.

Melwin Syafrizal, S.Kom, M.Eng, mempreoleh gelar Sarjana Komputer (S.Kom) dari Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta dan gelar Magister Teknik (M.Eng) dari Program Pasca Sarjana Jurusan Magister Teknik Informatika Universitas Gadjah Mada. Saat ini aktif sebagai dosen di STMIK AMIKOM Yogyakarta dan menjabat sebagai Sekretaris Jurusan Sistem Informasi STMIK AMIKOM Yogyakarta.