

Analisis Sniffing Password Menggunakan Aplikasi Cain Dan Abel Pada Jaringan Wifi Universitas Semarang

Susanto¹, Basworo Ardi Pramono², Sri Handayani³

¹ Program Studi Teknik Infomatika, Universitas Semarang

Jl. Soekarno Hatta Semarang, (024) 6702757, e-mail: susanto@usm.ac.id

² Program Studi Teknik Infomatika, Universitas Semarang

Jl. Soekarno Hatta Semarang, (024) 6702757, e-mail: basworo@usm.ac.id

³ Program Studi Teknik Infomatika, Universitas Semarang

Jl. Soekarno Hatta Semarang, (024) 6702757, e-mail: sri@usm.ac.id

ARTICLE INFO

Article history:

Received 23 July 2018

Received in revised form 30 July 2018

Accepted 3 Agustus 2018

Available online 17 Agustus 2018

ABSTRAK

Jaringan wifi sangat rentan terhadap ancaman serangan, karena komunikasi yang terjadi bersifat terbuka. Jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat dieksploitasi oleh para hacker. Pada saat data dikirim melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan pada user lain yang tidak bertanggung jawab untuk menyadap atau mengubah data, bahkan sampai mencuri data tersebut. Khususnya ancaman serangan dari *sniffing*. Aktivitas *sniffing*, yaitu penyadapan data di jaringan komputer dengan cara membelokkan data, merupakan aktivitas yang mudah dilakukan oleh para hacker. Aktivitas ini biasanya disalahgunakan oleh orang yang tidak bertanggung jawab untuk mencuri informasi penting dari korbannya. Hal demikian terjadi karena kurangnya pengamanan yang tepat maupun ketidaktahuan masyarakat awam. Analisa Sniffing pada jaringan wifi universitas semarang membahas penggunaan Aplikasi *Cain and Abel*, yang digunakan untuk mengintai lalu lintas pada jaringan wifi USM, aplikasi *Cain and Abel* ini melakukan *sniffing* yang merekam seluruh aktivitas yang terjadi pada jaringan. Penulis melakukan penelitian ini bertujuan untuk memberikan pengetahuan dasar dari penggunaan Aplikasi *Cain and Abel* pada jaringan wifi USM dan cara menghindari tindak kejahatan ini.

Keywords: wifi, sniffing, usm.

1. Pendahuluan

1.1 Latar Belakang

Pada saat ini kemajuan dan perkembangan teknologi sangat berkembang pesat. Keamanan jaringan menjadi sangat penting dan harus diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat dieksploitasi oleh para hacker, baik jaringan LAN maupun Wireless. Pada saat data dikirim melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada user lain yang tidak bertanggung jawab untuk menyadap atau mengubah data, bahkan sampai mencuri 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 maupun cracker. Beberapa aksi sniffing lebih menakutkan lagi, biasanya cracker melakukan sniffing ditempat rawan,

misalnya seorang user melakukan sniffing di universitas tempat belajar, atau seorang cracker melakukan sniffing untuk mencuri password email, bahkan mencuri data transaksi melalui kartu kredit maupun hal lainnya. Pada kenyataannya, masih sedikit solusi yang tepat untuk mendeteksi maupun untuk mencegah aktivitas sniffing ini. Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai serangan tetapi tidak mengambil tindakan lebih lanjut [1].

Saat ini Universitas Semarang telah menerapkan jaringan computer kabel maupun nirkabel sebagai media pertukaran data atau informasi pelayanan umum maupun akademik dan informasi penting lainnya. Universitas Semarang juga memiliki jaringan wifi yang tidak menutup kemungkinan terjadinya serangan pada jaringan tersebut. Sedikit celah dapat dimanfaatkan oleh para hacker dan cracker untuk menembus suatu jaringan. Oleh karena itu peneliti merasa perlu untuk meneliti dan menganalisis serangan packet data sniffing. Berdasarkan uraian diatas, penulis tertarik untuk mempelajari cara untuk mengetahui tingkat keamanan jaringan tersebut. Oleh karena itu, penulis mengambil bahan mengenai keamanan jaringan internet untuk judul “Analisis Sniffing Password Menggunakan Aplikasi Cain Dan Abel Pada Jaringan Wifi Universitas Semarang”.

1.2 Batasan Masalah

Adapun batasan masalah yang dapat diambil dari rumusan masalah di atas yaitu objek Analisa jaringan dilakukan pada Fakultas TIK, Fakultas Psikologi, Fakultas Ekonomi dan Pascasarjana.

1.3 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan di atas, maka rumusan masalah pada penelitian ini adalah bagaimana keamanan jaringan wifi pada beberapa fakultas di universitas semarang dengan menggunakan metode eksperimen..

1.4 Tujuan Penelitian

Tujuan dari penulisan ini adalah untuk memberikan pengetahuan bagaimana melakukan *Sniffing* dalam sebuah jaringan, dan bagaimana cara menghindari tindakan ini.

1.5 Luaran Penelitian

Luaran dari penelitian ini berupa bahan teori dan modul ajar praktikum.

2. Tinjauan pustaka

2.1 Jaringan Komputer

Jaringan komputer [5] Jaringan Komputer merupakan kumpulan dari perangkat keras dan lunak di dalam suatu sistem yang memiliki aturan tertentu untuk mengatur seluruh anggotanya dalam melakukan aktivitas komunikasi. Satu komputer yang terkoneksi ke jaringan menjadi satu node dari jaringan tersebut. Sedangkan host secara umum diartikan sebagai komputer yang terkoneksi ke jaringan yang dapat memberikan layanan jaringan (network service) [3]. Pertukaran Informasi dan data melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data atau mencetak pada printer yang sama dan bersama-sama menggunakan hardware/software yang terhubung dengan jaringan. Setiap komputer, printer atau periferal yang terhubung dengan jaringan disebut *node* [4]. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node. Jaringan mempunyai beberapa manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri (*stand-alone*), yaitu dalam hal :

1. Jaringan memungkinkan manajemen sumber daya lebih. Pengguna atau *user* dapat saling berbagi printer tunggal dengan kualitas tinggi, dibandingkan memakai printer kualitas rendah di masing-masing meja komputer. Selain itu, lisensi perangkat lunak jaringan dapat lebih murah dibandingkan lisensi *stand-alone* terpisah untuk jumlah pengguna sama.

2. Jaringan membantu mempertahankan informasi agar tetap handal dan *up-to-date*. Sistem penyimpanan data terpusat yang dikelola dengan baik memungkinkan banyak pengguna mengakses data dari berbagai lokasi yang berbeda, dan membatasi akses ke data sewaktu sedang diproses.
3. Jaringan membantu mempercepat proses berbagi data (*data sharing*). Transfer data pada jaringan selalu lebih cepat dibandingkan sarana berbagi data lainnya yang bukan jaringan (*flasdisk, disket, CD*, dan lain sebagainya).
4. Jaringan memungkinkan kelompok kerja berkomunikasi dengan lebih efisien. Surat dan penyampaian pesan elektronik (*email*) merupakan substansi sebagian besar sistem jaringan, disamping sistem penjadwalan, pemantauan proyek, konferensi online dan *groupware*, dimana semuanya membantu tim bekerja lebih produktif.

Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*). Pihak yang meminta layanan disebut klien (*client*) dan yang memberi layanan disebut pelayan (*server*). Arsitektur ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

2.2 Jenis Jenis Jaringan

1. *Local Area Network (LAN)*
Local Area Network (LAN) secara umum adalah jaringan privat yang menghubungkan perkantoran, gedung atau kampus. LAN banyak digunakan untuk menghubungkan komputer pribadi agar dapat saling bertukar informasi [5].
2. *Metropolitan Area Network (MAN)*
Metropolitan Area Network (MAN) adalah jaringan LAN yang luasnya mencakup sebuah kota. Contohnya berupa jaringan televisi yang terdapat di berbagai kota [5].
3. *Wide Area Network (WAN)*
Wide Area Network (WAN) adalah jaringan yang mencakup wilayah geografis yang luas, yaitu antar negara atau benua. Biasanya dalam WAN, *host* dan *subnet* dimiliki dan dioperasikan oleh orang yang berbeda [5].

2.3 Internet protocol (IP)

Merupakan *protocol open system* yang terkenal karena banyak digunakan untuk melakukan hubungan koneksi antar jaringan dan sesuai dengan standar komunikasi LAN maupun WAN. *Internet Protocol* berisi banyak *protocol*, dua *protocol* di antaranya yang paling terkenal yaitu *Internet Protokol (IP)* dan *Transmission Control Protocol (TCP)*.

2.4 Mac address (Media Access Control)

Merupakan identifikasi unik pada yang dimiliki oleh setiap perangkat komputer, switch, router, access point dan segala macam perangkat yang memungkinkan dihubungkan kedalam jaringan.

2.5 Sniffer

Yang dikenal dengan *network analyzer* adalah perangkat lunak ataupun perangkat keras yang digunakan untuk menghalangi dan mencatat semua lalu lintas dalam sebuah jaringan. *Sniffer* menangkap seluruh aliran paket data pada jaringan [2].

3. Metode penelitian

3.1 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah :

1. Observasi: Mengamati kebutuhan *user* (pengguna) yang akan menggunakan aplikasi sebagai alat bantu pembelajaran materi pengenalan PC mini dalam mata kuliah mikrokontroler dan robotika

2. Studi Pustaka : Mengumpulan literatur pendukung penelitian, baik dari buku referensi ataupun dari jurnal ilmiah.

3.2 Metode Pengembangan Sistem

Metode yang digunakan pada penelitian ini adalah metode eksperimen. Didalam penelitian eksperimental, peneliti beraksi dari awal dalam hal pembentukan dan pemilihan kelompok, mencoba mengontrol, memutuskan apa yang terjadi pada setiap kelompok, mencoba mengontrol semua faktor lain yang relevan, mengontrol perubahan yang telah ia perkenalkan, dan pada akhir studi mengamati atau mengukur pengaruh atas kelompok-kelompok percobaan . Penelitian ini terdiri atas beberapa tahap, yaitu:

- 1) Tahap Awal (Persiapan):
 - a) Menentukan Objek/Subjek yang akan diteliti,
 - b) Menentukan Variabel Penelitian,
 - c) Membuat desain penelitian,
- 2) Tahap Pelaksanaan:
 - a) Melaksanakan eksperimen/penelitian,
 - b) Mengumpulkan data dari proses eksperimen,
 - c) Menganalisis data,
 - d) Menyusun laporan,
- 3) Tahap Akhir (Kesimpulan).

Pada tahap ini terdapat gambaran mengenai hasil yang dari penelitian.

4. HASIL DAN PEMBAHASAN

4.1 Tahap Awal (Persiapan):

- a) Menentukan Objek/Subjek yang akan diteliti,
Objek yg diteliti adalah wifi USM dan karakter password yang sering digunakan.
- b) Menentukan Variabel Penelitian,
Wifi beberapa fakultas di USM, dan password sia.usm.ac.id
- d) Membuat desain penelitian,
Tim akan melakukan sniffing di beberapa fakultas di USM.

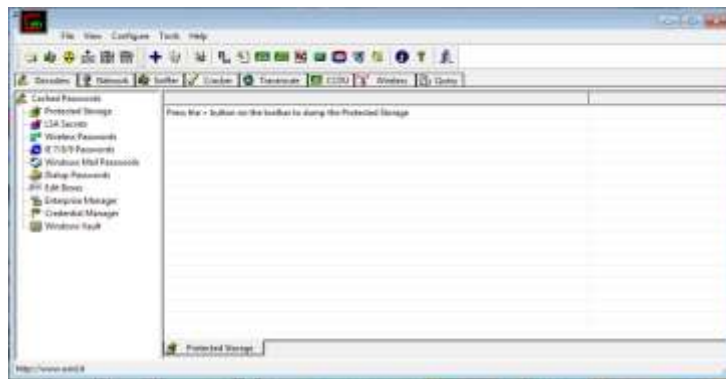
4.2 Tahap Pelaksanaan:

- a) Melaksanakan eksperimen/penelitian,

eksperimen proses sniffing dalam jaringan USM

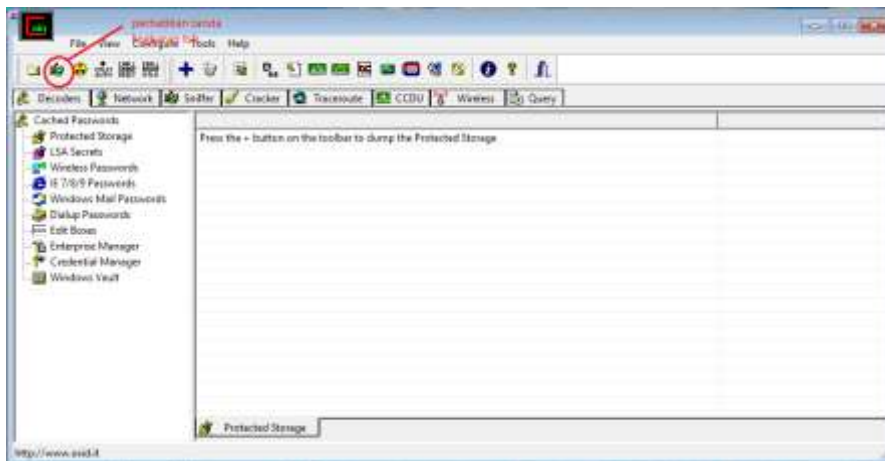
Langkah-langkah:

1. *Download aplikasi Cain and Abel* ,kemudian *install*.
2. Setelah diinstall, buka *aplikasi Cain and Abel* maka akan muncul tampilan seperti dibawah ini.



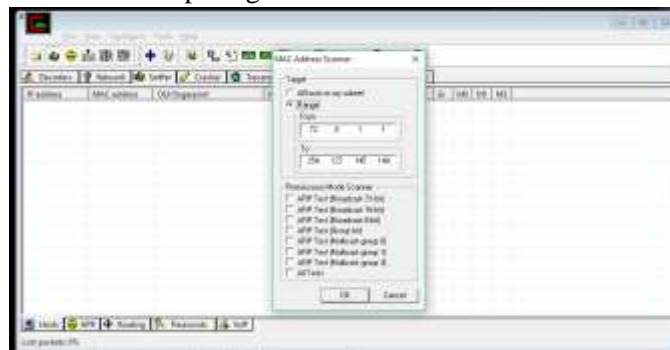
Gambar 1. Tampilan aplikasi *cain and abel*

3. Klik *Start/Stop Sniffer*.



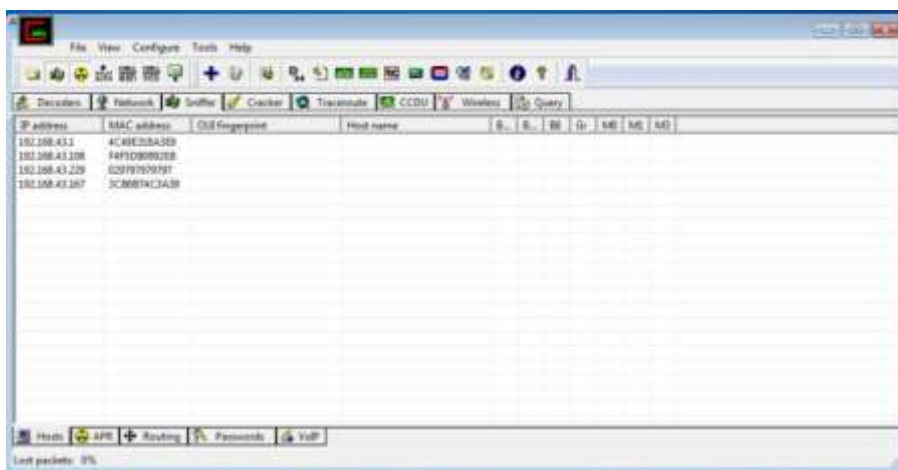
Gambar 2 . Petunjuk *button*

4. Klik kanan *Scan Mac Address* seperti gambar dibawah ini:



Gambar 3 *Scan mac address*

5. Setelah itu klik APR .



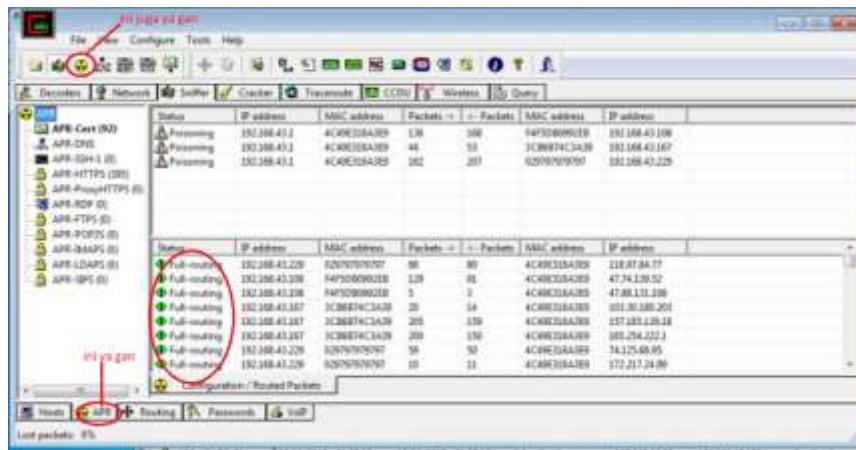
Gambar 4 Petunjuk *button APR*

6. Dibawah ini sedang melakukan proses *sniffing* dapat dilihat beberapa terdeteksi sedang membuka *website* diantaranya facebook,instagram,google dan yahoo.



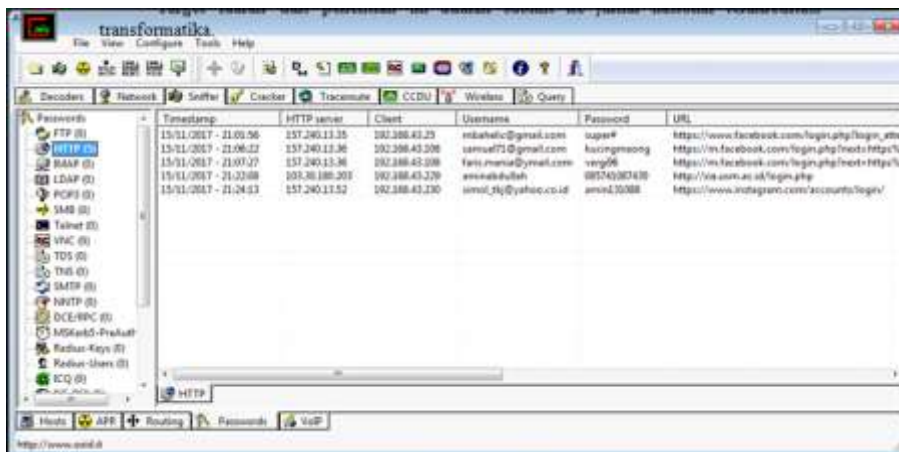
Gambar 5 Proses sniffing.

7. Klik start/stop APR, pastikan status di bawah berwarna hijau (full routing) hal ini memungkinkan untuk proses sniffing berhasil.



Gambar 6 Full Routing

8. Berikut hasil sniffing yang didapatkan



Gambar 7 Hasil Sniffing

- b) Mengumpulkan data dari proses eksperimen,

Tabel 2. Data *Sniffing wifi*

No	User	Password	URL
1	aria	Bi*****	http://journals.usm.ac.id/
2	yogie	P@*****	http://journals.usm.ac.id/index.php/index/login
3	PRODG211	te*****	http://sia.usm.ac.id/login.php
4	btjms_manager	D2*****	http://portal.johnnyandrea.com/
5	saumafarzhabi	89*****	http://sia.usm.ac.id/login.php
6	mbahelic@gmail.com	su*****	https://www.facebook.com/login.php
7	samuel71@gmail.com	ku*****	https://m.facebook.com/login.php
8	faris.mania@ymail.com	ve*****	https://m.facebook.com/login.php
9	aminabdullah	85*****	http://sia.usm.ac.id/login.php
10	simol_tkj@yahoo.co.id	am*****	https://www.instagram.com/accounts/login

c) Menganalisis data,

1. analisa data wifi dari beberapa fakultas
2. analisa data password yang didapatkan

5. Kesimpulan

Kesimpulan yang dapat diambil dari kegiatan penelitian adalah:

1. *Software Cain and Abel* mampu membaca lalu lintas jaringan dan menembus hampir semua wifi di USM.
2. Melakukan *sniffing* dengan *cain and abel* dapat dilakukan dengan mudah tanpa perlu mempelajari ilmu hacker.
3. *Password* yang di deteksi oleh *software* ini masih belum memakai kaidah *password* yang baik dan benar.

DAFTAR PUSTAKA

- [1] Ariyanus. 2007. *Instrusion Detection System*, Andi : Yogyakarta.
- [2] Agus Kurniawan, 2013. *Network Forensics Panduan analisa dan investigasi paket data jaringan menggunakan wireshark*. Penerbit Andi. Yogyakarta.
- [3] P. K. Panwar and D. Kumar, 2012 "Security through SSL," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, pp. 178-184,
- [4] P. Asrodia and V. Sharma, 2013 "Network monitoring and analysis by packet sniffing method," *international Journal of Engineering Trends and Technology (IJETT)*, vol. 4,
- [5] Tanenbaum, A. S. 2003. *Computer Networks*. New Jersey: Pearson Education.