ISSN : 1978-6603

JURNAL Ilmiah SAINTIKOM Sains dan Komputer

ANALISIS CELAH KEAMANAN PROTOCOL TCP/IP

*M.Syaifuddin[#1], Beni Andika[#2], Rico Imanta Ginting[#3]
[#1,2,3] Program Studi Sistem Informasi, STMIK Triguna Dharma
E-Mail : [#1]msyaifuddins@gmail.com

Abstrak

Jaringan komputer merupakan fasilitator yang bisa gunakan untuk berkomunikasi antar komputer, baik itu dalam sekala besar maupun kecil. Dengan jaringan komputer ini pengguna sangat terbantu. Sebelum pengguna melakukan komunikasi, pengguna diminta melakukan *login* dengan memasukan *username* dan *password* terhadapa suatu halaman web. Kombinasi *Username* dan *password* biasanya disebut *account*. *Account* menjadi hal yang berharga, karena dengan memasukan *account* dengan benar, pengguna bisa masuk dan menggunakan laman web tersebut. Dikarenakan *account* sangatlah penting dalam hal komunikasi ataupun masuk ke laman web, maka tidak jarang *account* ini dicuri oleh sebagian orang.

Pencurian *account* bisa dilakukan dengan beberapa teknik, diantaranya adalah *sniffing*. *Sniffing* ini memanfaatkan kelemahan yang ada di protocol tcp/ip, dimana protocol ini yang digunakan untuk komunikasi antar komputer.

Kata Kunci : Komunikasi data, Sniffing, Protocol TCP/IP

Abstract

Computer network is a facilitator that can use to communicate between computers, both in large and small scale. With this computer network the user is very helpful. Before the user communicates, the user is prompted to login by entering username and password to a web page.

Combination Username and password are usually called accounts. The account becomes a valuable thing, because by entering the account correctly, the user can login and use the web page. Since account is very important in terms of communication or entry to web pages, it is not uncommon this account was stolen by some people. Account theft can be done with several techniques, such as sniffing.
This sniffing takes advantage of the weaknesses that exist in the tcp / ip protocol, where this protocol is used for communication between computers.

Keywords : *Data communications, Sniffing, TCP / IP protocol*

I. PENDAHULUAN

1. Latar Belakang

Perkembangan teknologi khususnya internet (*interconnection- networking*) sangat pesat dan signifikan dalam kehidupan saat sekarang ini. Itu disebabkan karena internet mudah untuk diakses dan digunakannya, serta kecepatan dalam pengiriman data kepada pihak lain. Selain kecepatan dan kemudahan yang ada pada internet, di internet juga banyak yang bisa dilakukan oleh pengguna, seperti melakukan *browsing* dan *chatting.* Maka tidak heran jika internet begitu cepat berkembang dan diminati oleh masyarakat luas.

Tetapi perkembangan internet yang ada masih banyak pengguna yang tidak menyadari bahkan tidak tahu bahwa di dalam melakukan kegiatannya di internet, seperti ketika saat sedang melakukan *chatting* atau mengirim *e-mail* kepada pihak lain, kegiatan itu sangat rentan terhadap kejahatan dunia maya, atau dalam bahasa lainnya disebut *cybercrime.* C*ybercrime* yang dimaksud disini adalah mencuri data atau informasi penting dari korban tanpa sepengetahuan dan seizinnya. Tentu saja hal itu sangat berbahaya dan merugikan bagi pengguna yang mengalaminya. Semua itu bisa terjadi biasanya disebabkan oleh kurangnya pemahaman atau ketidak tahuan pengguna dalam menggunakan internet dengan aman dari *cybercrime*.

Salah satu kejahatan dari *cybercrime* itu adalah *sniffing*. S*niffing* bisa diartikan sebagai ”pengendus atau penyadapan paket data” yang lewat dan berlalu lalang di *TCP/IP* pada jaringan komputer dan umumnya menggunakan kabel sebagai media transmisi, seperti jaringan yang berbasis *Local Area Network* (LAN).

Aktivitas *sniffing* itu terbagi kedalam dua kelompok, yakni *sniffing passive* dan *sniffing active*. *Sniffing passive,* yaitu suatu teknik dimana pelaku melakukan penyadapan data tanpa merubah paket data yang ada. Disini pelaku hanya memerlukan program *sniffer* yang akan merubah *Ethernet Card* korban agar dapat melihat dan mencatat semua data yang dilaluinya. Sedangkan *sniffing active* adalah suatu kegiatan memodifikasi *Address Resolution Protocol* (ARP) cache, sehingga data dari komputer korban ke komputer pelaku. ARP adalah sebuah *protocol* dalam *TCP/IP protocol suite* yang bertanggung jawab dalam melakukan *resolusi* alamat *IP* kedalam alamat *Media Access Control* (MAC Address). Pada *sniffing active* biasanya pelaku melakukan pengiriman paket yang akan mempengaruhi alur data korban.

Pada paket *sniffing* juga terdapat istilah S*niffing Promisicuous Mode. Sniffing Promisicuous Mode* adalah suatu cara ataupun teknik yang digunakan dalam penyadapan data dengan cara mengambil seluruh paket data yang di *broadcast* oleh *network adapter driver* dan *protocol stack* meskipun paket itu bukan ditujukan kepadanya.

2. Tinjauan Pustaka

1. Protokol TCP/IP

TCP/IP (*Transmission Control Protocol*/*Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar menukar data dari satu komputer ke komputer lain di dalam jaringan Internet.

TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme *transport* jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (IP *Address*) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di internet. Protokol ini juga bersifat *routable* yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga UNIX) untuk membentuk jaringan yang heterogen.

2. Sniffing

Sniffer paket (arti tekstual: pengendus paket, dapat pula diartikan 'penyadap paket') yang juga dikenal sebagai *Network Analyzers* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak-balik pada jaringan, aplikasi ini menangkap tiap- tiap paket dan kadang-kadang menguraikan isi dari RFC (*Request for Comments*) atau spesifikasi yang lain. Berdasarkan pada struktur jaringan (seperti *hub* atau *switch*), salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu lintas dari salah satu mesin di jaringan. Perangkat pengendali jaringan dapat pula diatur oleh aplikasi penyadap untuk bekerja dalam mode campur- aduk (*promiscuous mode*) untuk "mendengarkan" semuanya (umumnya pada jaringan kabel).

II. MASALAH DAN PEMBAHASAN

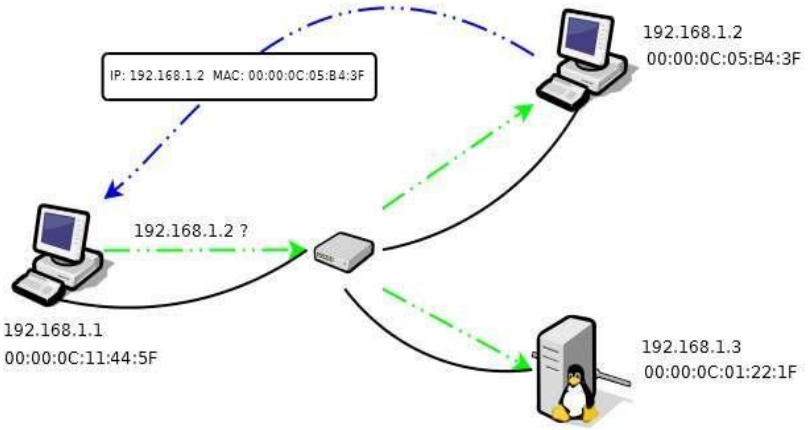
Yang menjadi pembahasan dalam penelitian ini adalah "*bagaimana cara melakukan analisis terhadap celah keamanan protocol TCP/IP*"

Dan pembahasan dari penelitian ini adalah sebagai berikut:

Dasar konsep dari komunikasi jaringan adalah pengiriman data dari sumber ketujuan dan begitu juga sebaliknya. Setiap bentuk komunikasi harus memiliki identifikasi alamat sumber dan tujuan, hal ini dilakukan untuk mengetahui siapa yang mengirim dan siapa yang menerima. Prinsip kerja pada jaringan yang kita ketahui selama ini ketika antar host melakukan komunikasi atau bertukar data, host tersebut menggunakan pengalamatan IP, tapi sebetulnya tidak. Komputer yang melakukan komunikasi atau bertukar data menggunakan alamat MAC. Alasan yang paling mendasar untuk menggunakan alamat IP dari pada MAC adalah, bagi manusia menggunakan alamat IP lebih mudah jika di bandingkan dengan alamat MAC, karena MAC memiliki angka-angka yang lebih banyak jika dibandingkan dengan alamat IP. Disamping angka-angka MAC yang lebih banyak dari pada alamat IP, IP lebih mudah untuk diingat dan angka yang ada lebih tersetruktur dengan baik, maka dari itu dibuatlah sebuah protokol ARP yang berfungsi untuk menterjemahkan/meresolusi alamat IP ke alamat MAC.

IP : 192.168.1.1
MACADDRESS : 00-00-0C-67-89-6f

Berikut cara kerja daripada ARP dalam memberikan Packet saat akan berkomunikasi



Gambar 1. Pemberian ARP saat komputer akan berkomunikasi

Sebuah host yang mendukung teknologi TCP/IP akan melakukan komunikasi dengan IP: 192.168.1.2 di dalam satu segmen jaringan, maka host akan mem-*broadcast* paket tersebut kejaringan. Dengan cara mem-*broadcast* paket, maka setiap host yang terhubung kejaringan itu akan mendapatkan paket *request*. Setiap host yang menerima paket *request* akan memeriksa IP *address*-nya. Host yang bukan pemilik IP yang dimaksud akan mengabaikan *request*. sedangkan Host pemilik IP: 192.168.1.2 yang mendapatkan *request* akan menjawab (*replay*) dan memberikan alamat IP berserta alamat MAC-nya.

Dengan didapatkannya alamat IP dan MAC yang dituju oleh pem- *broadcast*, maka keduanya sudah saling terhubung dan bisa melakukan komunikasi baik itu meminta ataupun memberikan data. Alamat MAC yang didapatkan oleh pem-*broadcast* akan disimpan (dihapus dalam waktu/priode tertentu) didalam tabel ARP untuk mempermudah komunikasi dilain waktu.

Dalam sistem kerja dari ARP adalah "kepercayaan" (*trust*), Tentu hal ini merupakan keuntungan sekaligus titik kelemahan dari ARP. Ini didasarkan pada ide bahwa seluruh mesin mau bekerja sama dan setiap respon yang didapat dianggap benar. Cara kerja ARP yang ada dapat dibagi menjadi 2 (dua) jenis, yaitu:

1. ARP *Request*. Pesan ini digunakan untuk meminta MAC address dari suatu IP address. Pesan ini biasanya dibroadcast ke semua host pada jaringan melalui alamat broadcast ethernet
2. ARP *Reply*. Jawaban dari ARP *Request*. Setiap host yang menerima ARP *Request* akan memeriksa *request* tersebut untuk mengetahui apakah dirinya adalah pemilik IP *address* yang ada di dalamnya, jika 'iya' maka harus memberikan jawaban berupa pesan ARP *Reply*

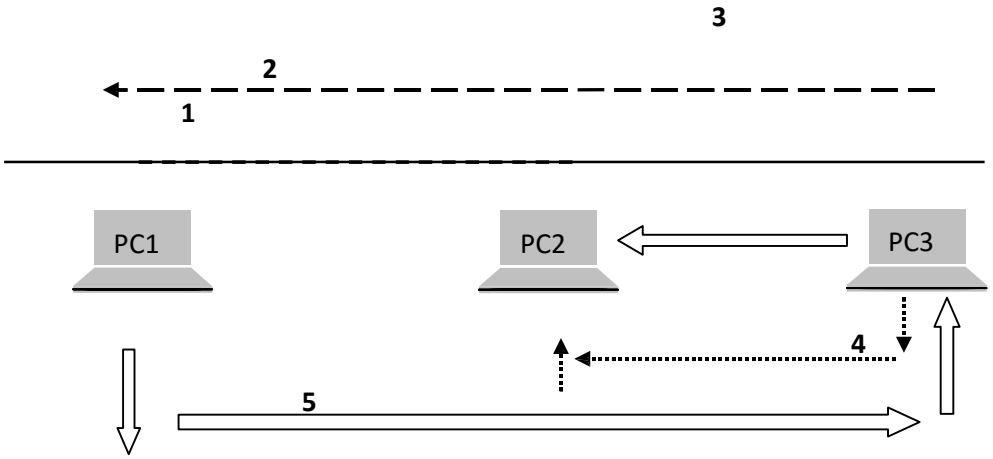
yang salah satu fieldnya mengandung MAC *address* dari IP *address* yang diminta dari host penanya.

3. RARP (*Reverse* ARP) *Request*. Pesan ini meminta IP *address* dari suatu MAC *address*.
4. RARP *Replay*. Pesan ini merupakan jawaban dari ARP *Request*, memberikan IP *address* dariMAC *address* yang berasosiasi.

Dengan cara kerja protokol ARP yang mengirim pesan ARP *request* secara *broadcast* kesemua host, ternyata hal ini menimbulkan celah keamanan bagi protokol TCP/IP.

Karena setiap host dijaringan yang berada dalam satu *broadcast* domain dapat merespon pesan ARP *broadcast* tersebut, meskipun isi pesan itu bukan ditujukan untuknya. Tidak hanya itu, siapapun di jaringan juga dapat mengirim ARP *request* dengan berpura-pura menjadi salah satu host yang sah, namun dengan alamat fisik (MAC) yang di palsukan. *Malicious* host melakukan hal tersebut dengan cara membuat paket (*crafted packet*) ARP palsu. Celah keamanan ini yang menjadi dasar untuk melakukan *spoofing* ARP dengan cara ARP *cache poisoning* yang bertujuan untuk melakukan *sniffing active*.

Gambar di bawah ini akan ditunjukan bagaimana ARP itu bisa dialihkan ke tempat yang bukan tempat atau bagiannya.



Gambar 2. Pengalihan data di dalam ARP

Keterangan

	IP	MAC
PC1 =	192.168.1.1	00:00:0C:11:44:5F
PC2 =	192.168.1.2	00:00:0C:05:B4:3F
PC3 =	192.168.1.3	04:D1:22:05:FE:FE

Proses kerja dari gambar 2 di atas:

1. PC1 akan melakukan komunikasi dengan PC2, tetapi didalam cache ARP PC1 belum terdapat alamat IP dan MAC paket *request* kejaringan maka seluruh *host* (PC1 dan PC3) mendapatkan paket tersebut. Proses tersebut dapat disimulasikan pada garis lurus no

2. dari PC2. Maka untuk mengetahui alamat IP dan MAC PC2 tujuan (PC2) PC1 melakukan *broadcast request* ke jaringan. Dengan di-broadcast-nya2. PC2 yang merasa paket *request* tersebut untuknya, maka PC2 mengirimkan paket *replay* yang berisi alamat IP dan MAC *Address* ke PC1.
   Proses tersebut dapat digambarkan oleh garis no 2 putus-putus.
3. Paket *broadcast request* yang diterima oleh PC3 dapat dimanfaatkan oleh *malicious* untuk dapat melakukan tindak kejahatan seperti mencuri dengar informasi yang akan dilakukan oleh PC1 dengan PC2, maka PC3 mengirimkan paket *replay* palsu. Paket *replay* palsu tersebut berisi alamat IP PC2 tetapi alamat MAC-nya adalah alamat MAC PC3 (192.168.1.2, 04:D1:22:05:FE:FE). Proses tersebut dapat disimulasikan pada garis no 3 putus-putus.
4. Maka setiap komunikasi yang dilakukan oleh PC1 akan didengar oleh PC3, karena informasi tersebut akan berbelok ke-PC3 sebelum sampai ke- PC2. Walaupun data itu berbelok ke PC3, tetapi PC3 tidak bisa mendapatkan informasi/data penting, karena informasi yang dikirim ke PC1 hanya berhenti di PC3 dan tidak sampai ke-PC2. Untuk bisa mendengarkan komunikasi yang dilakukan oleh PC1 dengan PC2 haruslah PC3 dapat meneruskan informasi/data yang dikirim oleh PC1. Untuk itu PC3 memberikan paket *request* yang berisi alamat IP PC1 dan alamat tetapi alamat MAC-nya adalah alamat MAC PC3 (192.168.1.1, 04:D1:22:05:FE:FE), yang seolah-olah paket tersebut dari PC1. Proses tersebut dapat disimulasikan pada garis no 4 putus-putus.
5. PC3 berhasil melakukan pemberian paket *raplay* palsu ke PC1 dan memberikan paket *request* ke PC2, maka PC3 bisa mendengarkan setiap komunikasi yang dilakukan antara kedua PC (PC1 dan PC2), karena setiap informasi/data yang dikirim dari PC1 akan berbelok ke PC3 dan PC3 akan meneruskan ke PC2. Proses tersebut dapat disimulasikan pada garis no 5 berbentuk garis panah.

III. KESIMPULAN

Dari penelitian yang telah dilakukan, maka dapat disimpulkan bahwa ketika dua komputer sedang melakukan komunikasi ataupun bertukar informasi, maka paket komunikasi tersebut bisa dialihkan ketempat yang berbeda atau ke komputer lain.

DAFTAR PUSTAKA

[1] Jaringan Komputer; Komunikasi Data dan Komputer Edisi 6. William Stallings.

[2] CEH (Certified Ethical Hacker). Jasakom

[3] www.masagunglearning.com