Mengindetifikasi Paket Data Jaringan Menggunakan Wireshark

Kiki Nur Fitria
kikiinur@gmail.com
http://kikiiblablabla.blogspot.com

Lisensi Dokumen:
Copyright © 2003-2007 IlmuKomputer.Com
Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Dalam postingan sebelumnya yang menceritakan tentang Wireshark, tentu kalian sudah mengetahui bahwa salah satu tujuan dari pemakaian software ini yaitu mempermudah kita (admin pada khususnya) untuk memantau atau memonitoing paket paket data yang keluar masuk pada suatu jaringan.

Sebenarnya ada banyak sekali macam macam data pa suatu jaingan itu yang meliputi, ARP, ICMP, DHCP, DNS, IP, TCP, UDP, HTTP, FTP, SMTP, POP, IMAP, WLAN (IEEE 802.11), dan TLS/SSL. Semua itu dapat kita identifikasi melalui Wireshark.

Lalu sebenarnya apa definisi dari paket paket data tersebut, mari kita bahas satu persatu....

1. **ARP,** Address Resolution Protocol adalah protokol untuk mapping dari alamat IP (Internet Protocol) ke alamat fisik MAC (Media Access Control). Misal di suatu jaringan kita ingin mengirim paket ke host A 192.168.1.2, maka pertama kita harus tau sapa yg mempunyai alamat IP tsb. Maka ARP akan membroadcast pertanyaan tsb ke semua host yang ada di jaringan. Sang empunya alamat IP tsb akan menjawab kembali sahutan tsb dengan mengirimkan alamat MACnya. Alamat MAC ini akan disimpan di tabel ARP untuk memudahkan pencarian jika diperlukan pengiriman paket ke tujuan yang sama. Dalam kasus kasus penjelajahan situs internet (misal, www.google.com) maka proses transmisi ARP harus dilakukan terlebih dahulu sebelum proses transmisi HTTP dimulai.
2. **ICMP**, Internet Message Controll Protocol. ICMP merupakan protokol pelengkap dalam IP (Internet Protocol). Sperti halnya IP, ICMP bekerja pada **Network Layer** pada

susunan OSI Layer. ICMP di desain untuk mengontrol pengiriman dan pesan percobaan melewati jaringan IP. Kemampuan untuk memahami ICMP adalah sangat di dibutuhkan untuk setiap perangkat network yang kompatibel dengan IP. Bagaimanapun juga banyak perangkat keamanan seperti firewall memblok atau me-non aktifkan semua bagian dari fungsi ICMP untuk kepentingan keamanan.

3. **DHCP**, Dynamic Configuration Protocol adalah layanan yang secara otomatis memberikan nomor IP kepada komputer yang memintanya. Komputer yang memberikan nomor IP disebut sebagai DHCP server, sedangkan komputer yang meminta nomor IP disebut sebagai DHCP Client. Dengan demikian administrator tidak perlu lagi harus memberikan nomor IP secara manual pada saat konfigurasi TCP/IP, tapi cukup dengan memberikan referensi kepada DHCP Server.
4. **DNS**, Domain Name Server, yaitu server yang digunakan untuk mengetahui IP Address suatu host lewat host name-nya. Dalam dunia internet, komputer berkomunikasi satu sama lain dengan mengenali IP Address-nya. Namun bagi kita tidak mungkin menghafalkan IP address tersebut, manusia lebih mudah menghapalkan kata-kata seperti www.yahoo.com, www.google.com, atau www.facebook.com. DNS berfungsi untuk mengkonversi nama yang bisa terbaca oleh manusia ke dalam IP address host yang bersangkutan untuk dihubungi.
5. **IP**, internet protocol yang berperan dalam pentransmisian paket data dari node ke node. IP mendahului setiap paket data berdasarkan 4 byte (untuk versi IPv4) alamat tujuan (nomor IP). Internet authorities menciptakan range angka untuk organisasi yang berbeda. Organisasi menciptakan grup dengan nomornya untuk departemen. IP bekerja pada mesin gateaway yang memindahkan data dari departemen ke organisasi kemudian ke region dan kemudian ke seluruh dunia.
6. **TCP**, transmission transfer protocol) berperan didalam memperbaiki pengiriman data yang benar dari suatu klien ke server. Data dapat hilang di tengah-tengah jaringan. TCP dapat mendeteksi error atau data yang hilang dan kemudian melakukan transmisi ulang sampai data diterima dengan benar dan lengkap.
7. **UDP**, User Datagram Protocol, adalah TCP yang connectionless. Hal ini berarti bahwa suatu paket yang dikirim melalui jaringan dan mencapai komputer lain tanpa membuat suatu koneksi. Sehingga dalam perjalanan ke tujuan paket dapat hilang karena tidak ada koneksi langsung antara kedua host, jadi UDP sifatnya tidak realibel, tetapi UDP adalah lebih cepat dari pada TCP karena tidak membutuhkan koneksi langsung.
8. **HTTP**, Hypertext Transfer Protocol adalah sistem untuk transmisi dan menerima informasi di Internet. Http berfungsi sebagai permintaan dan prosedur respon yang

Copyright © 2003-2007 IlmuKomputer.Com

9. semua agen di Internet mengikuti sehingga informasi dapat cepat, mudah, dan akurat disebarluaskan antara server, yang memegang informasi, dan klien, yang mencoba untuk mengaksesnya. Http umumnya digunakan untuk mengakses halaman html, tetapi sumber daya lain bisa dimanfaatkan juga melalui http.
   Dalam banyak kasus, klien dapat bertukar informasi rahasia dengan server, yang perlu diamankan untuk mencegah akses yang tidak sah. Untuk alasan ini, https, atau http yang aman, dikembangkan oleh Netscape untuk memungkinkan transaksi perusahaan otorisasi dan aman.
10. **FTP**, File Transfer Protokol adalah suatu protokol yang berfungsi untuk tukar-menukar file dalam suatu network yang mensupport TCP/IP protokol. Dua hal penting yang ada dalam FTP adalah FTP server dan FTP Client. FTP server menjalankan software yang digunakan untuk tukar menukar file, yang selalu siap memberian layanan FTP apabila mendapat request dari FTP client. FTP client adalah komputer yang merequest koneksi ke FTP server untuk tujuan tukar menukar file (mengupload atau mendownload file).
11. **SMTP**, Simple Mail Transfer Protocol (SMTP) adalah suatu protokol yang digunakan untuk mengirimkan pesan e-mail antar server, yang bisa dianalogikan sebagai kantor pos. Ketika kita mengirim sebuah e-mail, komputer kita akan mengarahkan e-mail tersebut ke sebuah SMTP server, untuk diteruskan ke mail-server tujuan. Mail-server tujuan ini bisa dianalogikan sebagai kotak pos di pagar depan rumah kita, atau kotak PO BOX di kantor pos. Email-email yang terkirim akan "nongkrong" di tempat tersebut hingga si pemiliknya mengambilnya. Urusan pengambilan e-mail tersebut tergantung kapan di penerima memeriksa account e-mailnya.
12. **POP3**, Post Office Protocol version 3 adalah suatu protokol yang berfungsi untuk menarik atau mengambil email dari server email yang digunakan.
    Untuk menggunakan POP3 bisa dari Microsoft Outlook. biasanya untuk menggunakan POP3 di perlukan settingan:
13. **IMAP**, Internet Message Access Protocol adalah protokol mail yang digunakan untuk mengakses email pada web server remote dari klien lokal. IMAP dan POP3 adalah dua yang paling umum protokol internet mail yang digunakan untuk mengambil email. Kedua protokol yang didukung oleh semua klien email modern dan web server.
14. **WLAN (IEEE 802.11)**,
15. **TLS/SSL**, Protocol SSL dan TLS berjalan pada layer dibawah application protocol seperti HTTP, SMTP and NNTP dan di atas layer TCP transport protocol, yang juga merupakan bagian dari TCP/IP protocol. Selama SSL dan TLS dapat menambahkan keamanan ke protocol apa saja yang menggunakan TCP, keduanya terdapat paling sering pada metode akses HTTPS. HTTPS menyediakan keamanan web-pages untuk

Copyright © 2003-2007 IlmuKomputer.Com

aplikasi seperti pada Electronic commerce. Protocol SSL dan TLS menggunakan cryptography public-key dan sertifikat publik key untuk memastikan identitas dari pihak yang dimaksud. Sejalan dengan peningkatan jumlah client dan server yang dapat mendukung TLS atau SSL alami, dan beberapa masih belum mendukung. Dalam hal ini, pengguna dari server atau client dapat menggunakan produk standalone-SSL seperti halnya Stunnel untuk menyediakan enkripsi SSL.

Demikian penjelasan mengenai definisi singkat mengenai paket paket data yang sering kali kita lihat berlalu lalang pada software monitoring seperti Wireshark. Setelah tau tentang definisi masing-masing paket data, kita bisa mengidentifikasi paket paket yang sering kita lihat di Wieshark.

Biografi Penulis

Kiki Nur Fitria. Menyelesaikan sekolah SMA pada tahun 2009 di SMA 9 Semarang. Sekarang sedang melanjutkan studi di Politeknik Negeri Semarang, mengambil jurusan D4 Teknik Telekomunikasi konsentrasi Jaringan Radio Komputer. Berbagai artikel menarik lain tersedia secara gratis di situs blog *http://kikiiblablabla.blogspot.com*

Copyright © 2003-2007 IlmuKomputer.Com