Vicko Bhayyu / 09011181520036 / SK5C / Jaringan Komputer

PCAP (Packet Capture) didalam jaringan computer mengandung API (Application programming Interface) untuk mencatat traffic jaringan. Pada sistem UNIX mengimplementasikan pcap didalam libpcap library, sedangkan windows menggunakan sebuah port pada libpcap yang dikenal dengan WinPcap.

Software monitoring dapat menggunakan libpcap dan/atau WinPcap untuk mencatat packet yang berjalan pada network,untuk transmisi packet pada network di link layer, dan juga mendapatkan list dari antarmuka jaringan.

PCAP api ditulis dalam bahasa C, dan bahasa lain seperti Java, .NET, dan bahasa scripting.

Analisis PCAP menggunakan bantuan website <https://packettotal.com> dan browser Google Chrome.

Untuk mendapatkan file PCAP menggunakan program WireShark 2.4.0 pada Sistem Operasi Windows 10

* PCAP gbf.wiki (51.255.106.73) (Web page)



Gambar 1. Hasil analisis pcap pada website packettotal.com

Pada web page (dalam hal ini dengan alamat web gbf.wiki) mendapatkan hasil sebagai berikut :

1. Dalam 2 menit melakukan browsing pada alamat gbf.wiki didapati sebanyak 16 kali menggunakan protocol UDP dan 15 kali menggunakan protocol TCP
2. Pada Destination IP, terdapat 9 kali koneksi yg terhubung pada 239.255.255.250 yakni merupakan IPv4 site-local address SSDP (Simple Service Discovery Protocol). SSDP merupakan protocol jaringan berbasis Internet Protocol Suite untuk iklan dan penemuan layanan jaringan dan informasi keberadaan. SSDP digunakan untuk protocol UPnP (Universal Plug and Play) karena provider internet yang digunakan menggunakan FO yg tersambung ke perangkat router, juga terdapat IP address 51.255.106.73 yang merupakan IP Address dari web page tersebut. Dan banyak IP Address yang saya tidak kenali.
3. Koneksi dari IP Source yakni 192.168.5.13 merupakan IP local yang saya gunakan, 192.168.5.1, 192.168.5.3 merupakan perangkat lain yang terhubung pada jaringan internet yang sama.
* PCAP indoxxi.net (Online Video Streaming)



Gambar 2. Hasil analisis indoxxi.net

1. Dalam melakukan browsing, tercatat 60 kali menggunakan protocol TCP dan 10 kali menggunakan protocol UDP.
2. SSL juga tercatat sebagai service yang paling banyak digunakan yakni sebanyak 47 kali.
3. SSDP, dan 104.27.100.39 juga tercatat sebagai destination IP yang paling banyak tercatat

Dari kedua analisis PCAP diatas, terdapat perbedaan pada web page dan online video streaming page, yakni :

1. Web page menggunakan protocol UDP untuk menampilkan kontennya, dan web online video streaming menggunakan protocol TCP untuk menampilkan kontennya.
2. Koneksi yang tercatat pada online video streaming jauh lebih banyak dibanding web page dalam waktu yang singkat.
3. Baik web page, dan online video streaming sama-sama menggunakan protocol SSDP.

Referensi :

Bhayyu, Vicko. 2017. Capture Web Browsing dan Online Streaming. (online) <http://edocs.ilkom.unsri.ac.id/id/eprint/1482> . Diakses pada tanggal 5 September 2017.

WIKIPEDIA. 2017. PCAP. (online) <https://en.wikipedia.org/wiki/Pcap> . Diakses pada tanggal 5 September 2017.

WIKIPEDIA. 2017. Simple Service Discovery Protocol. (onine) <https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol> . Diakses pada tanggal 5 September 2017.

WIKIPEDIA . User Datagram Protocol. (online) <https://id.wikipedia.org/wiki/User_Datagram_Protocol> . Diakses pada tanggal 5 September 2017.