ANALISIS DAN MONITORING SNIFFING PAKET DATA JARINGAN LOKAL BPS SUMSEL DENGAN NETWORK ANALYZER WIRESHARK

[1]Abdul Majid, [2]Timur Dali Purwanto
[1]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma, reymajid30@gmail.com
[2]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma, timur.dali.purwanto@binadarma.ac.id

Abstract *- Currently advances in information technology are developing very rapidly, which causes information security issues to become important. The process of tapping information (sniffing) on computer networks is becoming increasingly commonplace, both for positive and reverse purposes. Information Security, namely all efforts to protect information, against unauthorized access or modification of data and information that may occur on storage media or during data transmission. In this study, the sniffing process was used to obtain information such as browser access, username and password. The sniffing process is carried out using the Wireshark software. Wireshark software performs the capturing process of data on the Wireless interface, then observes the capture results containing POST data containing username and password as well as browser activity that passes through the HTTP protocol. From the results of the research conducted, it was found that using Wireshark could perform tapping or sniffing of data passing on a computer network.*

Keywords: Information Security, Sniffing, Wireshark.

Abstrak - Saat ini kemajuan teknologi informasi berkembang sangat cepat, yang bisa membua isu keamanan informasi menjadi sangat penting. Proses penyadapan data informasi (Sniffing) pada jaringan komputer menjadi semakin biasa dilakukan, baik untuk kegunaan yang bersifat positif maupun yang bersifat sebaliknya. Keamanan Informasi yaitu segala usaha perlindungan informasi, terhadap akses atau modifikasi data dan informasi yang tidak sah yang dapat terjadi pada media penyimpanan atau pada saat transmisi data. Dalam penelitian ini, proses sniffing yang digunakan untuk mendapatkan informasi seperti akses browser username dan password. Proses sniffing dilakukan menggunakan perangkat lunak Wireshark. Software Wireshark melakukan proses capturing data pada interface Wireless, lalu mengamati hasil capture-an yang berisikan data POST yang berisi username dan password serta aktivitas browser yang melewati Protokol HTTP. Dari hasil penelitian yang dilakukan didapatkan bahwa dengan menggunakan Wireshark dapat melakukan penyadapan atau pengendusan data yang lewat pada jaringan komputer.

Kata kunci: Keamanan Informasi, Sniffing, Wireshark.

1. Pendahuluan

Didalam jaringan terdapat banyak jenis paket data, masing-masing mempunyai fungsi berbeda serta saling berkaitan. Dan ada juga sebuah paket data yang mengandung informasi seperti kata sandi, alamat suatu web, username, dan banyak lagi [1]. Packet header terdapat macam informasi tentang protokol itu (informasi mengenai jenis, sumber, tujuan). Jenis Data yang akan ditransmisi disebut dengan data payload, dan juga paket trailer yang bersifat opsional. Dan untuk mengetahui packet data pada suatu jaringan dibutuhkan apikasi monitoring yang bekerja secara real time, untuk tujuan mendapatkan informasi lalu menganalisa

paket data yang melintas di Badan Pusat Statistik Provinsi Sumatera Selatan hal ini dilakukan untuk mengetahui aktivitas penggunaan jaringan tentang apa saja yang dilakukan pengguna jaringan yang terhubung ke internet disana.

Wireshark ini merupakan perangkat lunak dan termasuk salah satu protokol analisis yang disebut dengan protokol aplikasi analisis atau paket *sniffer* jaringan. Wireshark bisa digunakan sebagai bahan acuan untuk memperbaiki masalah jaringan dengan cara melihat hasil capturing pada network interface nya, analisa, penggembangan aplikasi dan protokol, serta keperluan pembelajaran. Aplikasi ini menggunakan sistem capture, maksudnya kita dapat menentukan apa-apa saja yang kita butuhkan dalam memonitoring jaringan. Semua proses yang terjadi akan tercapture secara langsung, sehingga dari situ hanya perlu melanjutkan dengan cara memonitoring jaringan dengan wireshark. Dengan menggunakan software ini kita bisa mengcapture packet data yang berkeliaran pada jaringan yang sedang dimonitoring

2. Tinjauan Pustaka

2.1 Monitoring

Monitoring Jaringan Komputer merupakan suatu proses pengumpulan serta melakukan analisis terhadap data pada suatu lalu lintas sebuah jaringan untuk tujuan memaksimalkan seluruh sumber daya yang dimiliki Jaringan Komputer. Monitoring jaringan ini merupakan bagian dari suatu manajemen jaringan [2].

2.2 Macam- macam Monitoring Jaringan

Monitoring jaringan dibagi menjadi dua bagian diantaranya [3]:

1) Connection Monitoring

Monitoring jaringan teknik ini melakukan dengan cara menguji koneksi seperti test cmd Ping diantara monitoring station dan perangkat target yang tujuan jika sambungan putus maka bisa dilakukan perbaikan diperbaiki.

2) Traffic Monitoring

Teknik ini merupakan teknik yang menggunakan paket aktual yang akan kemuadian menghasilkan laporan dari traffic jaringan tersebut.

2.3 Wireshark

Wireshark merupakan suatu software yang ditujukan penganalisaan paket data suatu jaringan [4]. Wireshark juga Network analyzer yang berfungsi menangkap paket-paket jaringan pada protokol HTTP, DHCP, DNS, ICMP dan lainnya, wireshark berguna untuk menampilkan informasi hasil capturing dipaket tersebut sedetail mungkin.

2.4 Fungsi Wireshark

1) Menganalisa jaringan.
2) Merekam paket data atau informasi jaringan yang terlihat.
3) Penganalisis informasi yang ada dengan cara melakukan sniffing paket data.
4) Membaca data secara langsung dari Ethernet, wireless LAN.
5) Menganalisis transmisi data pada jaringan, dan proses koneksi dan transmisi diantara computer [5].

2.5 Fitur-fitur Wireshark

1) Capturing paket secara langsung dari inteface jaringan.
2) Menampilkan informasi protokol yang sangat rinci.
3) Open dan Save data paket yang diambil.
4) Impor dan Ekspor paket data dari dan ke banyak program capture lainnya.
5) Pencarian untuk paket pada banyak kriteria [6].

2.6 Protokol HTTP

HTTP merupakan suatu protokol yang bertugas meminta atau menjawab request antara client dan server. Sebuh client HTTP seperti web browser, biasanya dimulai permintaan dengan membuat hubungan TCP/IP ke port tertentu di tuan rumah yang jauh (biasanya port 80) [1].

3. Metodologi Penelitian

3.1 Metode Pengumpulan Data

Disini ini yang digunakan penulis untuk mendapatkan data guna mendukung penulisan ini seperti berikut :

1) Metode Pengamatan *(Observation)*

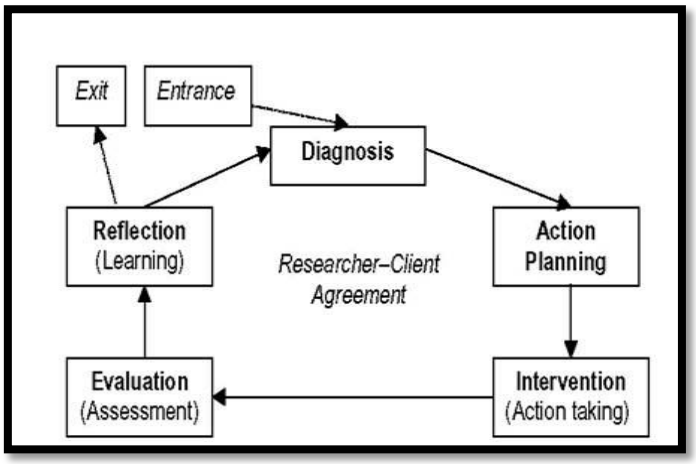
Pada metode ini penulis melakukan pengumpulan data secara langsung dengan melakukan pengamatan situasi ataupun kondisi kegiatan guna mendapatkan informasi di Badan Pusat Statistik Provinsi Sumatera Selatan untuk menjadikan pembahasan pada penelitian nanti.

2) Studi Pustaka

Penulis pun melakukan pengambilan data dengan cara membaca dari buku-buku diperpustakaan, jurnal atau pun modul dan situs-situs informasi lain yang ada di internet yang berhubungan dengan penelitian dan pembahasan yaitu tentang *monitoring dan analisis* packet data dengan *wireshark*. Hal ini berguna agar peneliti mendapat banyak referensi untuk keperluan penelitian.

3.2 Metode Penelitian

Pada penelitian ini penulis menggunakan sebuah metode action research yang dibagi beberapa tahapan yaitu .



Gambar 1. Siklus Action Research

1) Melakukan Diagnosa (*Diagnosing*)
2) Membuat rencana tindakan (*Action planning*)
3) Melakukan tindakan (Action Tacking)
4) Melakukan evaluasi (*evaluating)*
5) Pembelajaran *(learning)*

4. Hasil dan Pembahasan

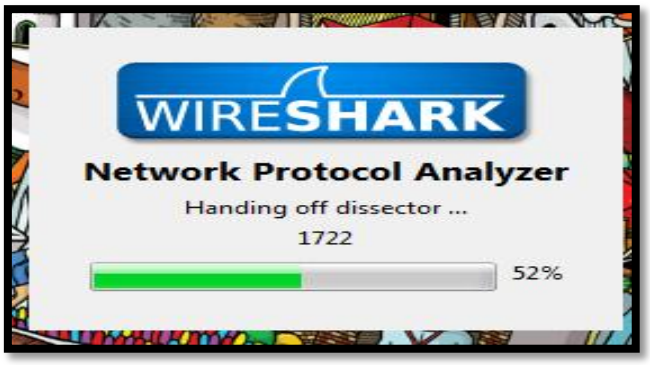
4.1 Persiapan Proses Capturing Wireshark

Dalam percobaan ini penulis melakukan *sniffing* dengan Wireshark untuk dapat informasi mengenai aktivitas jaringan pada protokol http seperti Memantau akses browser yang

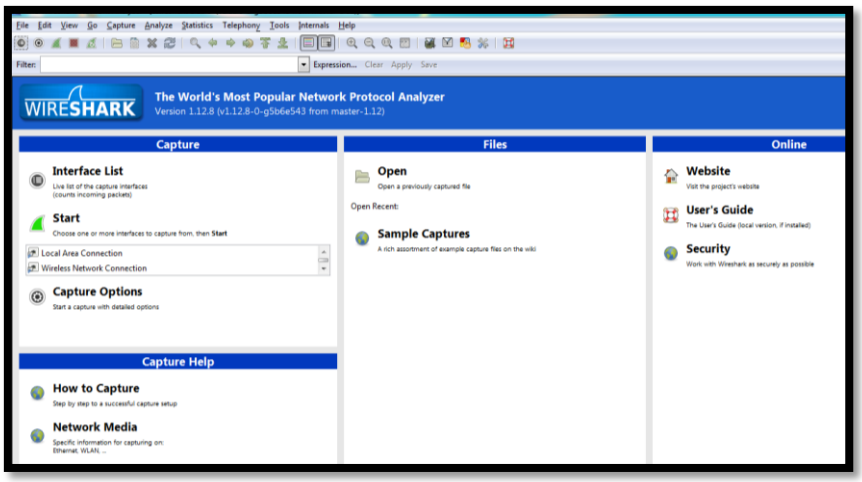
dijalankan menggunakan wireshark dan mencoba memonitor nya dan situs-situs yang dikunjungi. Berikut ini langkah untuk melakukan Capture pada Aplikasi Wireshark

1) Buka wireshark

Setelah itu akan muncul Splash Screen dari Aplikasi Wireshark yang lagi me-load komponen yang diperlukan memonitoring akses browser yang sedang dibuka menggunakan wireshark dan memonitor jaringan.

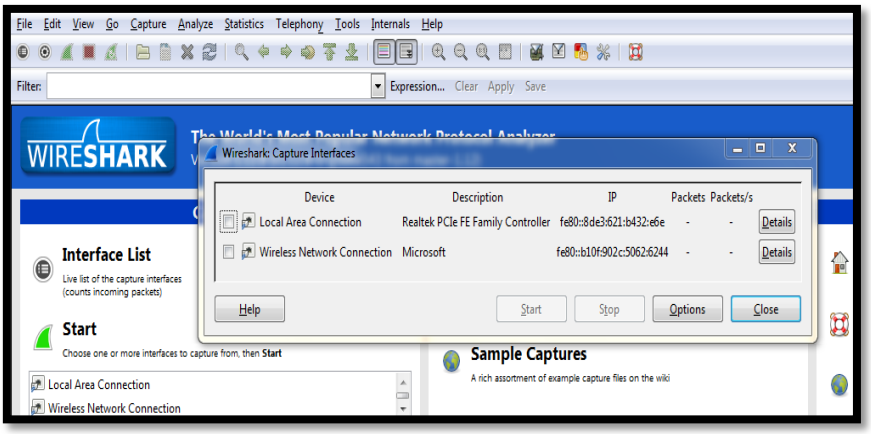


Gambar 2. Tampilan Load Komponen Wireshark



Gambar 3. Tampilan Awal Wireshark

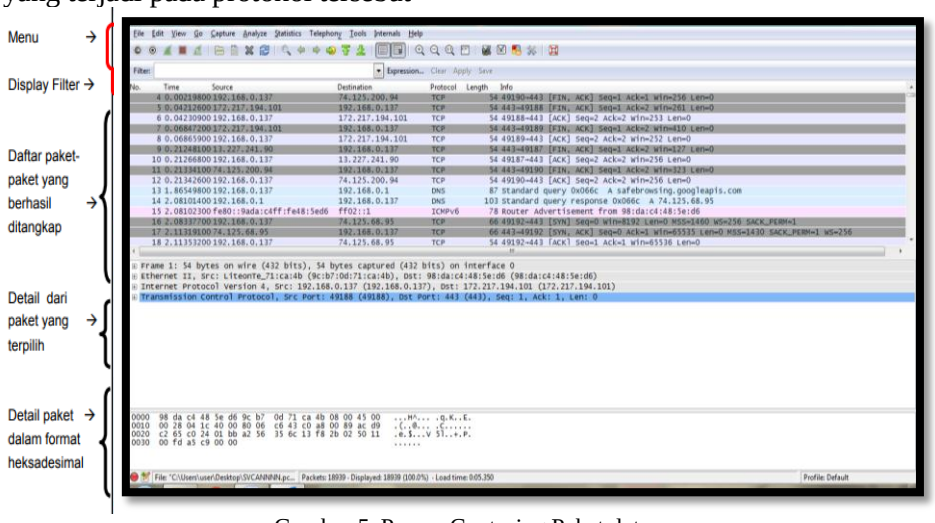
2) Memilih interface yang akan dimonitoring , Wireshark ini bisa membaca data langsung dari network interface Ethernet, 802.11 wireless, dan disini penulis memilih *Interface Wireless* lalu tekan *Start* untuk memulai *Monitoring* & *Sniffing*.



Gambar 4. Memilih Interface

3) Wireshark segera melakukan capture paket-paket didalam suatu jaringan dan akan menampilkannya dengan cepat. Berikut ini merupakan tampilan utama Wireshark ketika sedang meng-capture paket-paket data jaringan.

Hasil capturing dibawah belum dilakukan *filtering* protokol http, sehingga semua data terekam dan menyulitkan untuk dilakukan analisis pada protokol *HTTP* untuk memastikan aktivitas yang terjadi pada protokol tersebut

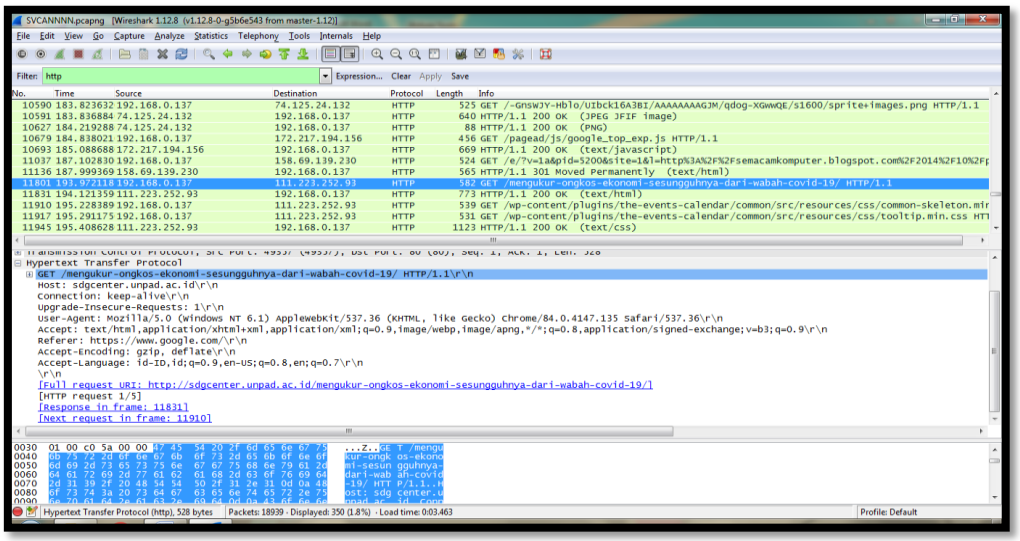


Gambar 5. Proses Capturing Paket data

4.2 Sniffing & Analisis

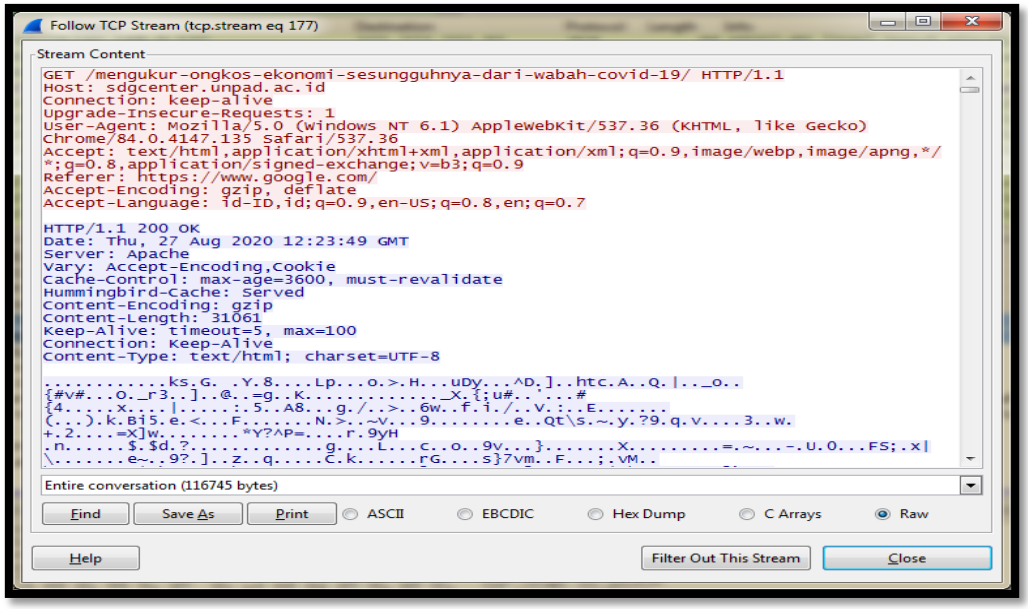
Setelah melakukan Filtering selanjutnya dilakukan analisis paket data yang melewati Protokol HTTP yang berisikan data post atau Get yang terdapat informasi-informasi mengenai aktivitas jaringan yang dilakukan perangkat yang ber alamat IP tersebut.

1) Sniffing situs yang diakes dalam wireshark
   a. Paket data dari sebuah situs yang telah diakses akan tercapture dan sudah di lakukan filtering.
   b. Selanjutnya Pilih paket yang mengirimkan suatu pesan GET. lalu lihat paketnya, maka bisa terlihat situs yang sedang diakses.
   c. Pilih contoh satu dalam protocol HTTP. Dalam box *http* terlihat permintaan source dan destination Src 192.168.0.137 Dst 111.223.252.93 HTTP582GET/mengukur-ongkos-ekonomi-sesungguhnya-dari-wabah-covid-19/ HTTP/1.1.



Gambar 6. sdgcenter.unpad.ac.id

Bisa dianalisis yakni user-agent yang dipakai yaitu Mozilla/5.0 (Windows NT 6.1) browser yang di gunakan Chrome/84.0.4147.135 Safari/537.36\r\n. Dan referer yang dituju yaitu Referer: https://www.google.com/\r\n. dan Host: sdgcenter.unpad.ac.id\r\n , selain itu dapat diketahui date yaitu pada Date: Thu, 27 Aug 2020 12:23:49 GMT dan Full Request Get URI: *http://sdgcenter.unpad.ac.id/mengukur-ongkos-ekonomi-sesungguhnya-dari-wabah-covid-19/* disitu bisa dilihat bahwa adanya aktivitas yang sedang dilakukan dan sedang meng akses laman web tersebut dan post diartikan client mengirim data ke suatu server.



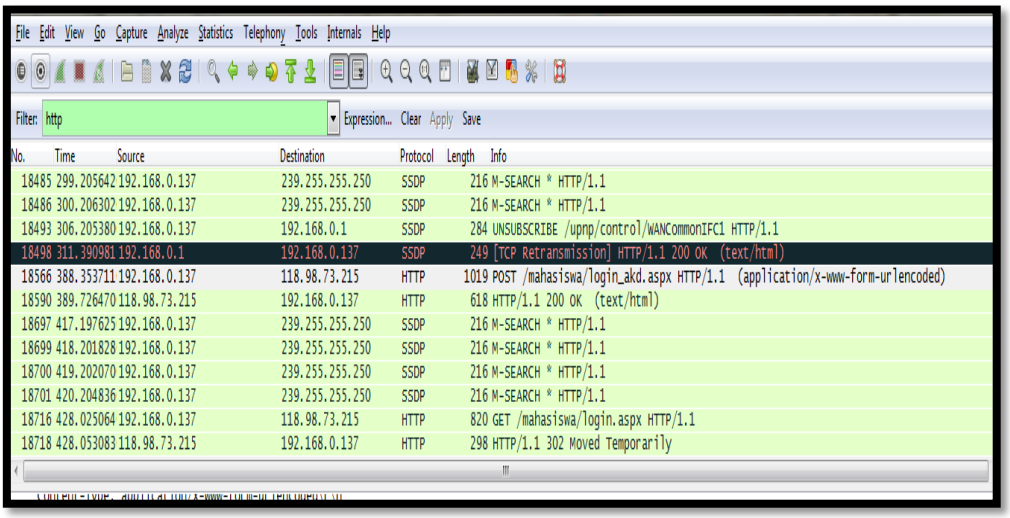
Gambar 7. TCP Stream

Gambar capture TCP Stream wireshark yang dapat menampilkan info Get. Yaitu client melakukan permintaan pada server agar server bisa mengetahui dan menampilkan request client seperti gambar tersebut client melakukan request pada server situs Request Get pada situs

2) Sniffing UserName& Password yang Melewati Protokol HTTP

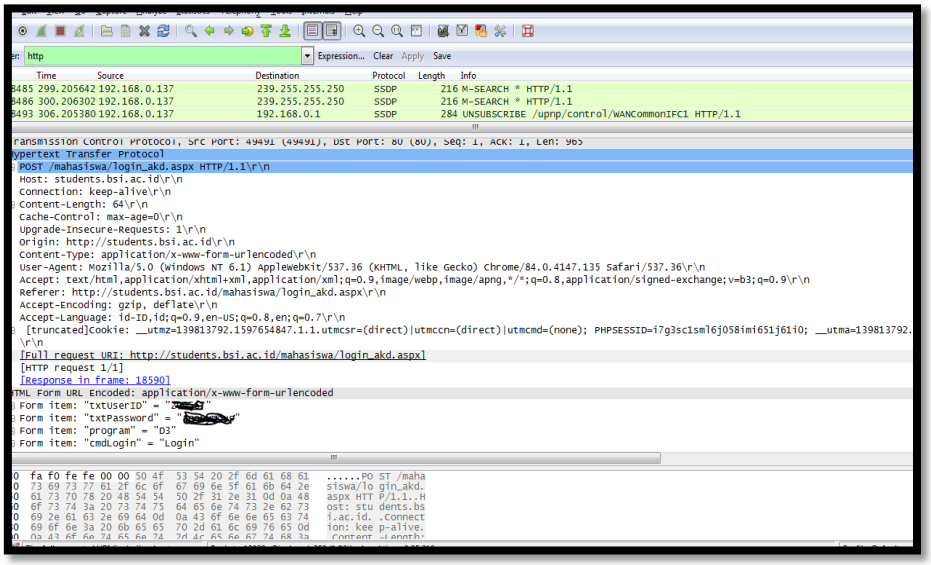
a. Sesudah itu lakukan capturing dan Filtering paket protokol *HTTP*, dan lakukan analisis paket berisikan data POST

Src 192.168.0.137 Dst 118.98.73.215 HTTP Port 1019 POST /mahasiswa/ login_akd.aspx HTTP/1.1



Gambar 8. POST DATA

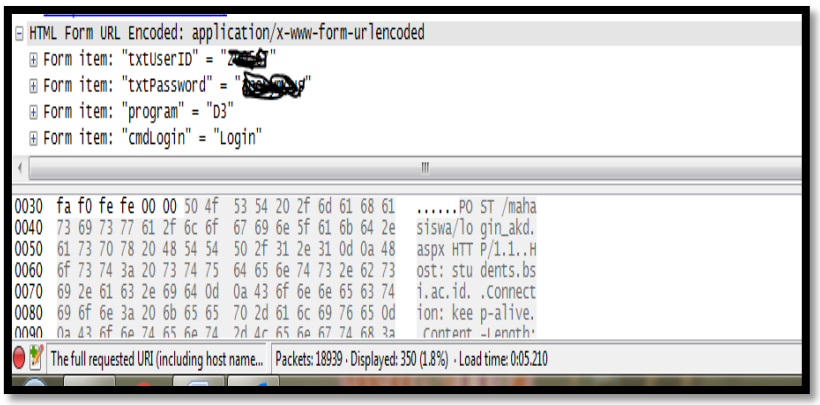
b. Didalam POST itu terdapat beberapa informasi seperti, alamat IP Src 192.168.0.137 dst 118.98.73.215, Port TCP yang dipakai yaitu Source Port: 49491 (49491) dan Port 80 dst, lalu terdapat informasi HTTP yang berisi POST, host, connection, content-length, origin, user-agent, dan yang paling penting HTML form URL yang berisi Username dan Password seperti gambar dibawah



Gambar 9. Box *Hypertex transfer protokol*

3) Analisa Box Hypertext Transfer Protocol (HTTP) :
   a. Server: Apache/2.4.18 (Ubuntu)
      Menampilkan server dari alamat yang diminta oleh destination pada source.
   b. Content Type: application/x-www-form-urlencoded
      Menunjukkan jenis data (isi) yang terdapat pada content type.
   c. Date: Thu, 27 Aug 2020 12:27:03 GMT
      Menunjukkan waktu pengiriman data pada saat komunikasi data.
   d. POST /mahasiswa/login_akd.aspx HTTP/1.1
   e. Host: students.bsi.ac.id Alamat Website yang dituju
   f. Full request URI: http://students.bsi.ac.id/mahasiswa/login_akd.aspx
   g. Kesimpulan: Lapisan Application, aplikasi yang bekerja saat browsing

a) Box HTML Form URL Encoded: application/x-www-form-urlencoded. Dapat dilihat dalam Box HTML Form terdapat Hasil Sniffing aktivitas perangkat dengan IP 192.168.0.137 yang sedang mengakses sebuah laman website dan yang berisikan Password yang melewati protokol Htpp tersebut ,disitu saya tutup untuk menghindari penyalahgunaan.



Gambar 10. HTML form Data POST

b) Dari percobaan yang penulis lakukan, dapat disimpulkan bahwa Sniffing dapat dilakukan dengan memanfaatkan jaringan lokal, Sniffing dari Username dan Password menggunakan Wireshark telah berhasil mengcapture Aktivitas perangkat yang sedang Login ke sebuah website http://students.bsi.ac.id/mahasiswa/login_akd.aspx. Dengan mendapatkan informasi mengenai aktivitas yang dilakukan seperti login pada sebuah website.
   a. Form item: "txtUserID" = ~~"200567"~~
   b. Form item: "txtPassword" = "~~anonymou"~~
   c. Form item: "program" = "D3"
   d. Form item: "cmdLogin" = "Login"

Percobaan monitoring ini dilakukan sebagai rujukan dan memberikan pengetahuan bagaimana cara melakukan Sniffing paket data dalam sebuah jaringan, yang berguna mengukur tingkat keamanan sebuah jaringan yang dapat dijadikan bahan rujukan oleh seorang Admin suatu jaringan.

5. Kesimpulan

Berdasarkan monitoring dan pembahasan pada penelitian ini, maka didapat kesimpulan sebagai berikut:

1. Dapat mempermudah proses capturing paket data secara langsung pada network interface, dan bisa menampilkan berupa informasi yang detail yang melewati protokol *Http*, mengenai hasil informasi penting yang dan rahasia seperti Mac Addres perangkat pada protokol *Arp* dan juga username dan password serta informasi akses browser pada protokol *Http*, serta dengan wireshark memudahkan proses monitoring yang dilakukan admin jaringan.
2. Wireshark ini hanya cuma bisa melakukan monitoringg jaringan dan tidak bisa melakukan tindakan seperti troubleshout langsung ke interface , tetapi wireshark ini bisa jadi bahan acuan seorang admin untuk memonitoring jaringan dikarenakan tampilan GUI yang memudahkan proses analisis secara real time.
3. Dengan dilakukan monitoring didalam Penulisan ini adalah untuk memberikan pengetahuan cara melakukan pengendusan dalam suatu jaringan, dan dari Penulisan ini diharapkan meningkatkan keamanan suatu jaringan dengan menggunakan aplikasi monitoring wireshark.

Referensi

[1] http://*Pengertian Paket Data-Semacam Komputer|Blog Semacam Ilmu Komputer, Algoritma dan Pemrograman/*. (Diakses pada 20 Juli 2020).
[2] Sofana, 2013. *Membangun Jaringan Komputer : Mudah membuat Jaringan Komputer (Wired & Wireless) untuk pengguna Windows* . Bandung: Grasindo.
[3] http://*ilmukomputer.org/2013/01/28/keunggulan-monitoring-jaringan-dengan-menggunakan-software-wireshark/*. (Diakses pada 14 Agustus 2020).
[4] Kurniawan. 2012. *Panduan Analisis dan Investigasi Paket Data Jaringan Menggunakan Wireshark*. Yogyakarta : Andi Publisher.
[5] M. Ferdy Adriant. 2015. "*implementasi wireshark untuk penyadapan (sniffing) paket data jaringan*". Jurnal Seminar Nasional Cendekiawan , hlm. 224-227.
[6] http:// *id.wikipedia.org/wiki/Wireshark*/ (Diakses pada 31 juli 2020).