Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet

Zaky Maula Luthfansa[1], Ulla Delfana Rosiani[2]

[1,2]Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang

[1]zakyluthfansa@gmail.com

[2]rosiani@polinema.ac.id

Abstrak—Perkembangan teknologi informasi saat ini berkembang dengan cepat terutama dalam teknologi internet. Hampir semua perangkat sekarang terhubung dengan koneksi internet. Karena semakin luasnya pengguna internet, maka tingkat keamanan terutama dalam pengiriman data sangat perlu diperhatikan. Ada banyak cara untuk melakukan penyadapan paket data yang terjadi pada jaringan internet salah satunya adalah *sniffing*. *sniffing* adalah salah satu teknik dalam penyadapan komunikasi data, *Sniffing* bisa memonitoring setiap komunikasi data yang terjadi pada jaringan internet baik itu protokol HTTP, TLS, ARP, DNS dan lain-lain. Dalam penelitian ini, teknik *sniffing* akan dilakukan dengan perangkat lunak Wireshark pada komunikasi data berprotokol HTTP. Wireshark akan menangkap informasi dari komunikasi data yang terjadi pada *Wireless*, dan melakukan penyaringan informasi dan hanya fokus kepada informasi komunikasi data berprotkol HTTP. Pada protokol HTTP ini akan menghasilkan data POST yang memuat informasi penting seperti username dan password. Hasil dari penelitian adalah melakukan penyadapan jaringan internet dengan Wireshark dapat mengambil informasi data penting yang mengakibatkan hilangnya salah satu sifat keamanan pada jaringan internet yaitu data privasi.

***Kata Kunci*— Sniffing, Wireshark, Keamanan Data, Internet**

I. PENDAHULUAN

Perkembangan teknologi informasi masa kini sangat pesat terutama pada teknologi internet. Penggunaan teknologi internet hampir digunakan pada setiap perangkat yang ada. Penggunaan internet juga memudahkan komunikasi, akibat kemudahan ini banyak yang lebih memilih untuk saling tukar informasi atau mengirim informasi penting melalui jaringan internet. Namun dibalik kemudahan komunikasi pada internet terdapat permasalahan, salah satu permasalahan tersebut adalah penyadapan atau yang biasa disebut dengan *sniffing*[1].

Teknik *sniffing* bisa sangat berbahaya ketika yang disadap adalah komunikasi data masih berprotokol HTTP, mungkin tidak masalah jika data yang dikomunikasikan itu kurang penting seperti membuat status pada wall facebook karena menyadap data seperti itu tidak terlalu berpengaruh besar. Tapi bagaimana jika data yang dikirimkan adalah data penting seperti username dan password, atau komunikasi untuk kepentingan bisnis yang bersifat rahasia? Tentu hal ini menjadi masalah besar[2].

Dalam penelitian ini, proses *sniffing* akan dilakukan dengan perangkat lunak Wireshark. Dari perangkat lunak Wireshark ini komunikasi data pada jaringan internet bisa dimonitoring dan bisa disadap sehingga bisa mendapatkan infromasi penting.

Banyak yang telah melakukan penelitian dengan teknik *sniffing* ini diantara lain untuk analisis jaringan menggunakan Wireshark, Cain and Abels, Network Miner[3]. Lalu ada juga optimasi keamanan dari MITM[4]. Maka dari peneliti memutuskan untuk membuat *sniffing* pada prokol HTTP guna menjelaskan betapa berbahayanya jika *sniffing* terjadi pada komunikasi jaringan berprtokol HTTP.

II. TINJAUAN PUSTAKA

A. Sniffing

Sniffing adalah aktivitas memonitoring dan menangkap data yang lewat pada jaringan internet.

Teknik *sniffing* ini biasanya dilakukan oleh pihak tidak bertanggung jawab untuk mencuri informasi data penting yang terjadi saat adanya komunikasi data pada jaringan internet[5].

B. HTTP

HTTP adalah dasar komunikasi dari World Wide Web, dimana HTTP ini adalah aturan dalam meminta dan menjawab antara client dan server.

Client HTTP biasanya memulai permintaan menggunakan TCP/IP ke port tertentu dalam membuat hubungan. Setelah itu, server HTTP akan mendengarkan perminttan tersebut dan menunggu cluent untuk mengirim permintaan seperti "GET / HTTP/1.1 ".

Begitu menerima kode permintaan, maka server akan merespon dengan jawaban seperti ”200 OK”, lalu menerima permintaan dan mengirim data yang dibutuhkan ke client[6].

C. Wireshark

Wireshark merupakan tools yang bertujuan untuk menganalisa paket data yang ada pada jaringan internet. Wireshark juga termasuk Network Packet Analyzer yang fungsinya untuk menangkap semua data informasi yang ada saat komunikasi data di jaringan internet dan menampilkan informasi data tersebut sedetail mungkin.

Wireshark juga tools yang fleksibel dalam artian Wireshark bisa memerika data baik itu yang terjadi pada jaringan internet kabel maupun wireless[1].

D. Internet

Internet adalah jaringan komputer yang terhubung satu sama lain untuk keperluan komunikasi dan informasi. Komputer dalam jaringan internet dapat digunakan di mana saja di Indonesia atau bahkan di seluruh negeri. Internet juga secara umum diartikan sebagai jaringan komputer di seluruh dunia yang memuat informasi, dan sebagai sarana komunikasi data berupa suara, gambar, video dan teks Informasi ini disediakan oleh operator atau pemilik jaringan komputer atau oleh pemilik informasi yang mempercayakan informasi

tersebut kepada penyedia layanan Internet. Meskipun Internet didefinisikan dari sudut pandang ilmiah, Internet adalah perpustakaan besar dengan jutaan (miliar) informasi atau data, informasi atau data tersebut dapat berupa teks, grafik, audio, atau animasi. Bentuk lainnya bisa berupa media elektronik.[6].

III. METODOLOGI PENELITIAN

Metode deskriptif adalah metode yang tepat dalam penenelitian ini. Metode penelitian deskriptif adalah salah satu metode yang sering digunakan dalam penelitian yang hasilnya ada penjelasan dalam suatu kejadian.

Untuk metode pengumpulan data yang mendukung penelitian ini adalah sebagai berikut:

A. Metode Kepustakaan

Metode keupstakaan adalah metode dalam mencari, mengumpulkan, serta menganalisa sumber data untuk diolah. Sumber data bisa melalui buku, jurnal, e-book, dan modul yang berhubungan dengan penelitian ini[7].

B. Metode Observasi

Metode ini perlu berkoordinasi pada bagian IT untuk dilakukan pengamatan dan penganalisaan pada informasi atau data yang berhubungan dengan penelitian.

Jadi hal ini nantinya akan memudahkan proses dokumentasi.

C. Metode Analsis Data

Analisis data adalah pencarian sistematis dan penggabungan data yang diperoleh dari beberapa kegiatan (yaitu wawancara, catatan lapangan, dan materi lainnya) sehingga mudah dipahami dan semua informasi ini dapat dikomunikasikan kepada orang lain.

Analisis data dimulai dengan menganalisis sistem keamanan jaringan di situs. Dan melakukan pengujian penetrasi jaringan nirkabel. Dengan cara ini, kelebihan dan kekurangan sistem keamanan jaringan dapat dilihat dari lokasi jaringan. Dengan cara ini dapat menemukan permasalahan yang terjadi dan dapat menyelesaikan permasalahan yang sedang terjadi.

Tahapan penelitian selanjutnya adalah analisis, analisis pendahuluan menginformasikan data yang akan dikumpulkan kemudian. Setelah peneliti menyelesaikan pengumpulan data, langkah selanjutnya adalah menganalisis data yang telah diperoleh. Metode ini merupakan upaya untuk menemukan, mengembangkan dan menguji kebenaran suatu ilmu agar karya ilmiah (dari penelitian) dapat menggunakan metode ilmiah untuk mencapai tujuan yang diinginkan secara akurat dan terarah. Padahal metode penelitian adalah strategi umum untuk mengumpulkan dan menganalisis data yang dibutuhkan untuk memecahkan masalah saat ini.

Teknologi analisis data merupakan langkah yang sangat menentukan, karena hasil analisis tersebut akan mengarah pada kesimpulan dari hasil penelitian. Analisis data dapat diselesaikan melalui tahapan berikut:

1. Perancanaan

   Pada tahap ini peneliti membuat instrument-instrumen yang digunakan untuk penelitian.

2. Pelaksanaan

   Pada tahap ini peneliti melaksanan pembelajaran pada sampel penelitian.

3. Evaluasi

   Pada tahap ini peneliti menganalisan dan mengolah data yang telah dikumpulkan dengan metode yang telah ditentukan sebelumnya.

4. Penyusunan Laporan

   Pada tahap ini peneliti menyusun dan melaporkan hasil-hasil penelitian.

D. Metode Percobaan

Salah satu metode penelitian adalah dengan melakukan eksperimen. Untuk dapat melakukan percobaan yang baik, maka perlu dilakukan. Pertama-tama, kita harus memahami segala sesuatu yang berkaitan dengan komponen eksperimen, baik yang berkaitan dengan jenis variabel, sifat eksperimen, karakteristik, tujuan, kondisi eksperimen, prosedur penelitian eksperimen, dan bentuk desain penelitian eksperimen.

Lakukan studi eksperimental untuk menemukan apa yang terjadi pada perawatan yang diinginkan peneliti. Selain itu, metode eksperimental juga digunakan untuk menemukan efek perlakuan tertentu dalam kondisi terkontrol. Proses penelitian eksperimental meliputi:

a) Adanya permasalahan yang perlu diteliti.
b) Pemilihan subjek yang cukup untuk dibagi dalam kelompok percobaan dan kelompok kontrol.
c) Pembuatan atau pengembangan instrument.
d) Pemilihan untuk desain penelitian.
e) Mengeksekusi prosedur.
f) Melakukan analisis data.
g) Menyimpulkan.

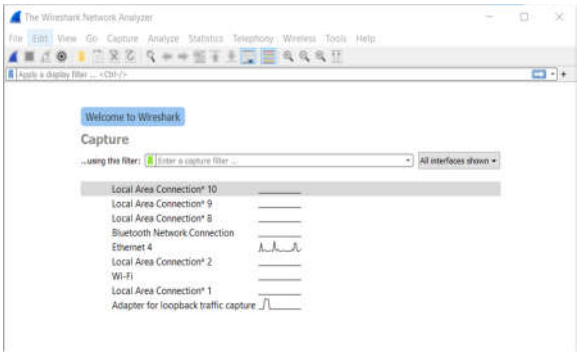
IV. PEMBAHASAN DAN HASIL

Objek dari penelitian adalah proses *sniffing* yang digunakan untuk memonitoring dan menangkap data pada jaringan internet, dan menampilkan informasi yang penting.

Sniffing bisa dikatakan sangat berbahaya jika pengguna tidak menyadari mengisikan data penting pada website yang masih berprotokol HTTP dalam komunikasi datanya.

Pada percobaan ini peneliti akan melakukan *sniffing* menggunakan perangkat lunak Wireshark untuk mendapatkan informasi penting seperti username dan password pada jaringan internet. Berikut ini adalah langkah-langkah untuk melakukan sniffing pada perangkat lunak Wireshark:

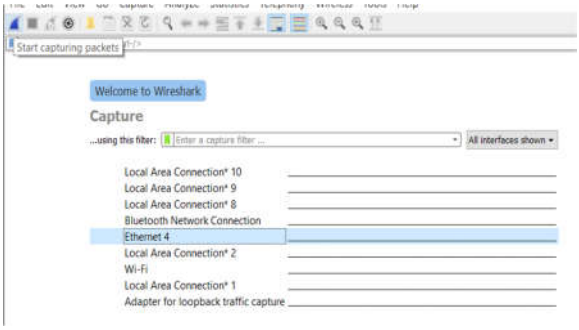
A. Menentukan jalur internet mana yang akan disniffing



Gbr. 1 Menentukan jalur *sniffing*

Pada Gbr 1. Bisa dilihat bahwa ada beberapa *interfaces* yang tertulis pada perangkat lunak Wireshark, *interfaces* ini merupakan daftar jalur yang tersedia pada perangkat untuk menghubungkan perangkat ke jaringan internet.

Terlihat di Gbr 1. terdapat seperti garis yang terdapat pada Elektrodiagram. Jika terdapat gelombang pada garis itu maka bisa dipastikan terdapat aktifitas disana. Maksud dari aktifitas yaitu pada *interfaces* tersebut sedang dilakukan komunikasi data pada jaringan internet. Jadi pastikan menggunakan *interfaces* yang tepat sebelum mulai memonitoring menggunakan perangkat lunak Wireshark.

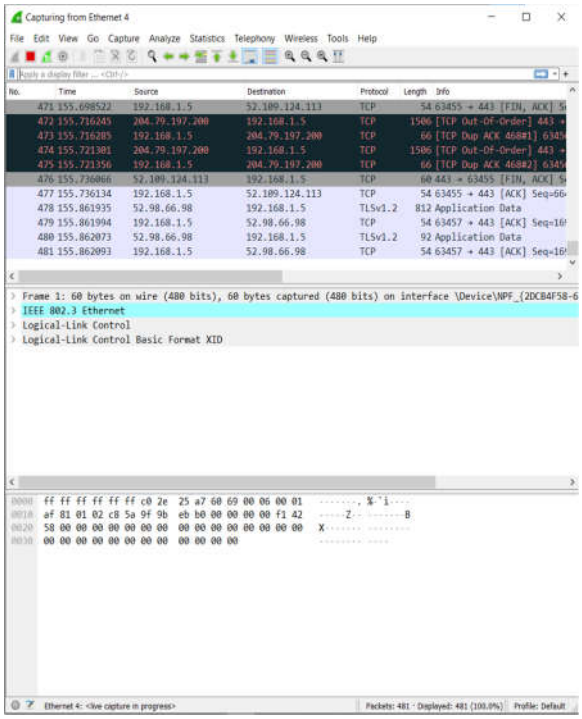


Gbr. 2 Start capturing packets

Setelah menentukan *interfaces* yang tepat, maka klik tombol dengan ikon seperti sirip hiu dengan keterangan "Start capturing packets". Setelah diklik maka proses *sniffing* pada *interfaces* yang dipilih segera dilakukan.

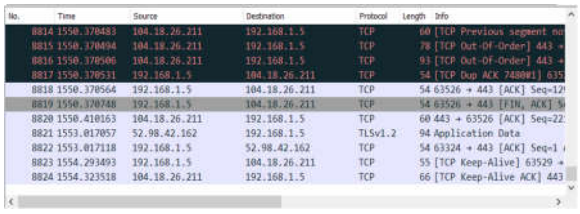
B. Memulai *sniffing*

Pada tampilan awal saat memulai *sniffing* terdapat 3 jendela yang ditampilkan, jendela itu antara lain adalah jendela *packet list,* jendela *packet details*, dan juga jendela *packet bytes*. Masing-masing jendela tersebut menampilkan informasi yang berbeda. Tampilan awal dari Wireshark saat memulai *sniffing* adalah sebagai berikut :



Gbr. 3 Tampilan awal saat *sniffing*

Untuk jendela paling atas lihat Gbr. 4, merupakan jendela *packet list*.

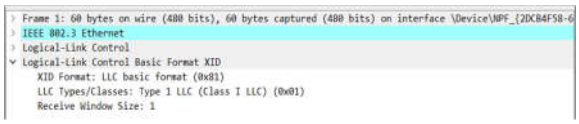


Gbr. 4 Jendela *packet list*

Jendela packet list merupakan jendela yang menampilkan hasil tangkapan paket data pada jaringan internet dalam format tabel yang ditampilkan dalam baris atau *row*.

Setiap baris akan memuat informasi dari paket data diantara sumber packet (*source*), destinasi (*destination*) protokol (*protocol*), panjang packet (*length*), dan informasi dari paket data.

Untuk jendela yang tengah lihat Gbr. 5, merupakan jendela *packet details*.

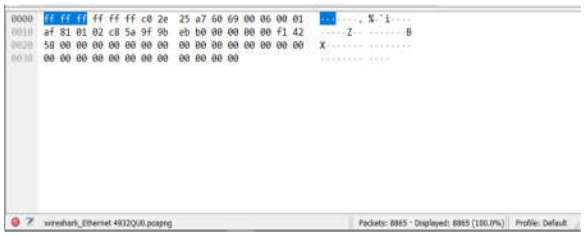


Gbr. 5 Jendela *packet details*

Jendela Gbr. 5 ini berfungsi untuk menampilkan informasi mengenai protokol-protkol dari baris paket data

yang dipilih pada jendela packet list. Data terserbut disajikan secara horizontal dan juga berhirarki.

Untuk jendela yang terletak bawah sendiri lihat Gbr. 6, merupakan jendela *packet bytes*.



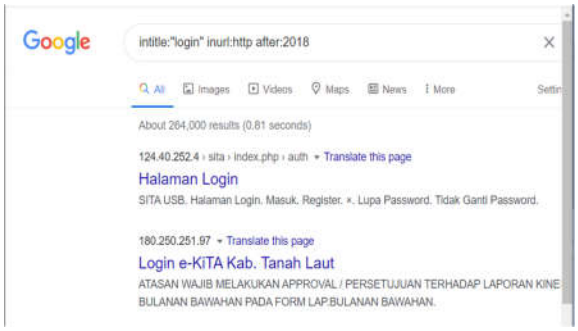
Gbr. 6 Jendela *packet bytes*

Pada jendela Gbr. 6 ini berfungsi untuk menampilkan data raw dari paket data yang diseleksi pada jendela *packet list*. Data raw ditampilkan dalam format hexadecimal dan memuat 16 hexadecimal bytes dan 16 ASCII bytes.

C. Buka website dengan protokol HTTP

Mencari website yang tepat untuk dilakukan percobaan bisa menggunakan mesin pencarian google dengan dengan teknik google dork.

Google dork adalah teknik mencari website dengan digabungkan dengan *filter* untuk mendapat website yang tepat.



Gbr. 7 Penggunaan google dork

Penggunaan google dork bisa dikatakan rumit bahkan mudah tergantung dari jenis penyaringanya. Seperti yang terlihat pada Gbr. 7 disini peneliti menggunakan google dork untuk mencari website dengan ketentuan yang berhubungan dengan login, berprotokol HTTP, dan websitenya dibuat 2018 keatas. Dari sini bisa dilihat banyak sekali website login yang masih menggunakan protokol HTTP dan ini sangat berbahaya jika tidak segera dilakukan upgrade protokol ke HTTPS.

Bahkan masih banyak website pemerintah yang login websitenya masih menggunakan protokol HTTP, seperti website dari siap kerja milik kabupaten Malang, Sistem Informasi Penelitian dan Pengabdian Kepada Masyarakat milik Ristekdikti.

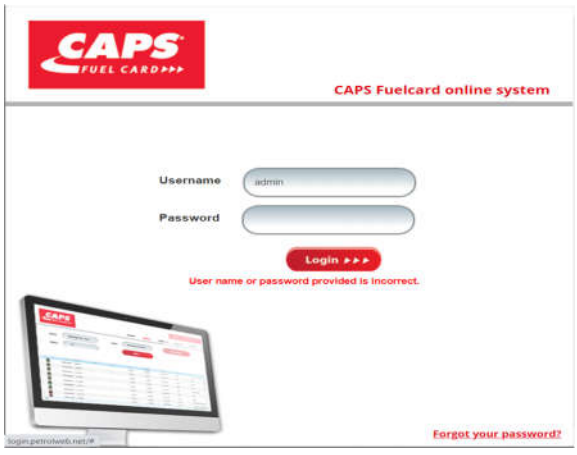
Dalam percobaan penelitian ini, menggunakan website yang sudah mati atau sudah lama tidak terupdate sehingga tidak ada pihak yang dirugikan.

Gbr. 8 Website yang digunakan untuk percobaan

Bisa dilihat pada website ini terdapat tulisan *Not Secure* disamping alamat website, ini menandakan bahwa website ini tidak berprotokol HTTPS atau setiap komunikasi data yang terjadi pada website ini tidak dienkripsi.

D. Login dan Filter

Setelah menemukan website yang tepat, maka masukan username dan password apa saja lalu lakukan login pada website tersebut.



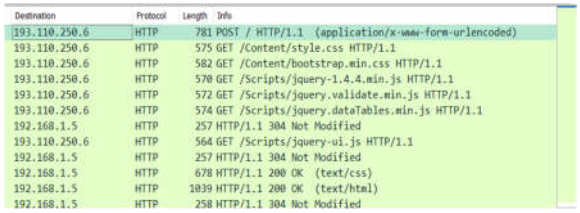
Gbr. 9 Hasil login website

Terlihat pada Gbr. 8 gagal dalam melakukan login, hal ini tidak apa-apa karena sniffing hanya butuh komunikasi data yang terjadi saat tombol login di klik.

Kembali ke perangkat lunak Wireshark, saat melakukan klik tombol login Wireshark sudah merekam komunikasi yang terjadi pada jaringan internet. Sekarang hanya perlu menyaring pada kolom *filter* untuk mendapat protokol HTTP dan ditampilkan pada jendela *packet list* seperti yang dilakukan pada Gbr. 10.

Gbr. 10 *Filter* protkol HTTP

Lalu pada Gbr. 11 bisa dilihat ada beberapa IP di *Destination* dan ada beberapa aksi yang terjadi pada kolom *Info* seperti GET dan POST,



Gbr. 11 *Info* dan *Destination*

IP 193.110.250.6 itu merupakan IP dari Windows Server, berarti disini target webiste mengguakan server dari Windows Server.

Lalu ada beberapa aksi yang terjadi disini antara lain aksi GET dan POST. GET dan POST ini mempunyai fungsi untuk mengirimkan data atau nilai ke halaman lain untuk diproses. Yang membedakan adalah GET digunakan untuk mengambil data dari sumber URL dan POST fungsinya untuk mengirim data dari sumber ke halaman lain untuk diproses[8]. Disini peneliti hanya fokus pada aksi POST yang dilakukan saat login pad website.

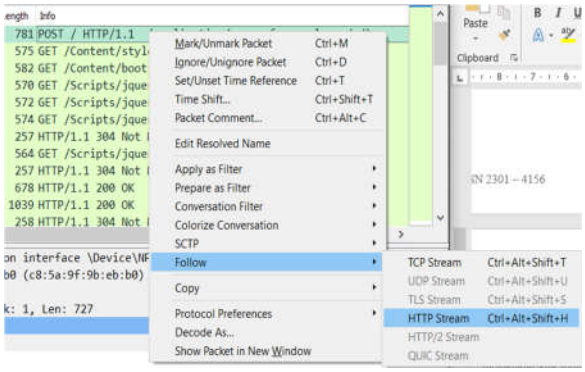
E. Hasil dari sniffing

Setelah menentukan *interfaces,* website, penyaringan protokol, dan aksi maka selanjutnya adalah mencari informasi yang tepat pada kolom *Info*.

Gbr. 12 *Info*

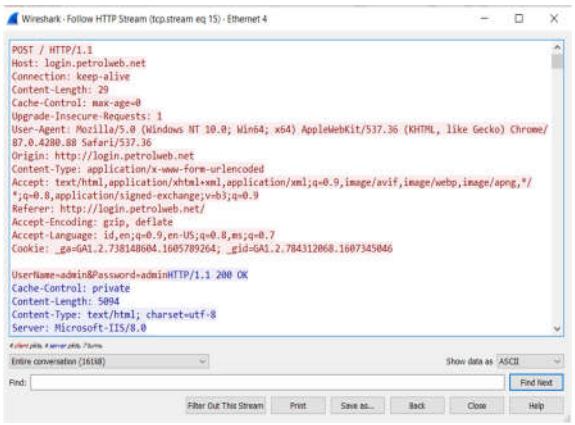
Disini peneliti fokus ke protokol HTTP dengan tujuan Windows Server dengan aksi POST dan HTTP/1.1. HTTP/1.1 ini artinya webserver hanya menerima 1 koneksi untuk tiap object yang akan ditampikan ke website.

Setelah itu lakukan HTTP *Stream* pada info tersebut seperti Gbr. 13



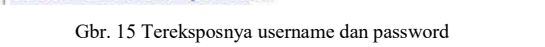
Gbr. 13 Letak HTTP *Stream*

Fungsi HTTP *Stream* ini adalah melihat langsung bagaimana dan apa yang terjadi pada protokol HTTP saat melakukan pengiriman data pada saat login.



Gbr. 14 HTTP *Stream*

Pada Gbr. 14 bisa dilihat jika terdapat blok tulisan warna merah dan warna biru. Hal ini bukan hanya gaya, melainkan terdapat artinya. Untuk tulisan dengan blok merah itu merupakan data yang dikirimkan dari website untuk webserver dan tulisan dengan blok biru itu merupakan respon dari webserver untuk ditampilkan pada website. Di HTTP *Stream* ini, bisa dilihat host dari websitenya, *type-content*, *User-Agent*, dan sebagainya. Data-data tersebut cukup penting karena dari situ bisa diketahui peneliti mengakses website menggunakan Sistem operasi apa dengan arsitektur apa. Dan yang paling penting adalah terekspos nya username dan password yang di masukan saat login tadi, lihat Gbr. 15.



Gbr. 15 Terekspos nya username dan password

Bisa dilihat disana sangat terpampang jelas username dan password yang dimasukan saat login tadi. Inilah mengapa *sniffing* pada komunikasi data pada jaringan internet berprotokol HTTP sangat berbahaya, karena selain mudah dilakukan tapi hasil yang diberikan merupakan data yang terbilang sangat sensitif.

Sniffing pada penelitian ini hanya koneksi antara perangkat peneliti ke webserver, akan lebih berbahaya lagi jika *sniffing* digabungkan dengan teknik lain seperti Man In The Middle (MITM) Attack.

V. KESIMPULAN

Sniffing dengan menggunakan Wireshark pada komunikasi data berprotokol HTTP menghasilkan informasi penting seperti username dan password. Menghindari *sniffing* dapat dilakukan dengan meningkatkan protokol komunikasi data pada jaringan internet menjadi HTTPS.

REFERENSI

[1] M. Ferdy Adriant and Is Mardianto, "Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan," *Semin. Nas. Cendekiawan*, pp. 224–228, 2015.

[2] P. T. Mahmud, "Sniffing Jaringan Menggunakan Wireshark," pp. 5–8, 2020, doi: 10.31219/osf.io/h5wu7.

[3] D. Susianto and A. Rachmawati, "IMPLEMENTASI DAN ANALISIS JARINGAN MENGGUNAKAN WIRESHARK , CAIN AND ABELS , NETWORK MINNER (Studi Kasus : AMIK Dian Cipta Cendikia)," *J. Cendikia*, vol. XVI, pp. 120–125, 2018.

[4] I. Riadi, R. Umar, and I. Busthomi, "Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain," vol. 04, no. June, pp. 15–19, 2020.

[5] E. M. Putra, B. Tujni, and E. S. Negara, "Analisis Kemanan Jaringan Internet (Wifi) dari Serangan Packet Data Sniffing Di Universitas Muhammadiyah Palembang," pp. 1–11.

[6] A. A. Zabar and F. Novianto, "Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux," *Komputa J. Ilm. Komput. dan Inform.*, vol. 4, no. 2, pp. 69–74, 2015, doi: 10.34010/komputa.v4i2.2427.

[7] J. Danandjaja, "Metode Penelitian Kepustakaan," *Antropol. Indones.*, 2014, doi: 10.7454/ai.v0i52.3318.

[8] A. Firdaus, S. Widodo, A. Sutrisman, S. G. F. Nasution, and R. Mardiana, "Rancang Bangun Sistem Informasi Perpustakaan Menggunakan Web Service Pada Jurusan Teknik Komputer Polsri," *J. Inform.*, vol. 5, no. 2407–1730, p. 83, 2019.