Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet

Zaky Maula Luthfansa¹, Ulla Delfana Rosiani²

^{1,2}Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang

¹zakyluthfansa@gmail.com

²rosiani@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 permintan 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 instrumentinstrumen 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 u

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. Pertamatama, 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.

Start capturing pack	[−] X C Q = + Ξ ∓ ± <mark>−</mark> Ξ Q Q Q (*)	1
W	elcome to Wireshark	
Ca	pture	
u	sing this filter: 🕌 Enter a capture filter	All interfaces shown •
	Local Area Connection* 10 Local Area Connection* 9 Local Area Connection* 8 Billetooth Network Connection Ethemet 4 Local Res Connection 2	
	Ucal Area Connection* 2 Wi-Fi Local Area Connection* 1 Adapter for loopback traffic capture	

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 :

R Hend	and the second se	8 9 + + 1 1						
	a display filler «Cat-	4					C	3 -
No.	Time	Source	Destination	Protocol	Length Info			-
_	471-155.698522	192,168,1.5	57,109,124,111	TEP	54 63455 +	443 IF	IN, AL	KI-
	472 155, 716245	204.79.197.208	192.168-1.5	TCP	1566 [TEP Ou	t-of-or	der] 4	43
							iss∎11	
	475 155.721350	192.168.1.5	204.79.197.200	itP	16 TCP Du	р аск 4	69#2]	634
	476 155,736066	52,109,124,113	192.168.1.5	TCP	60 443 - 6	3455 [F	IN, AC	XI (
	477 155.736134	192.168.1.5	52.109.124.113	TCP	54 63455 +	443 (A	CK] Se	q=61
	478 155,861935	52.98.66.98	192.168.1.5	TLSv1.2	812 Applica	tion Da	ta	
	479 155.861994	192.168.1.5	52.98.66.98	TCP	54 63457 +	443 [A	KK] Se	q=1
	480 155.862073	52.98.66.98	192.168.1.5	TL5v1.2	92 Applica	tion Da	ta	728
	481 155.862093	192.168.1.5	52.98.66.98	TCP	54 63457 +	443 [A	KK] Se	q=11
c)
0000		ff c0 2e 25 a7 60	59 00 05 00 01	. * 1				
2008	ff ff ff ff ff ff af 81 81 82 c8	ff c0 2c 25 a7 60 5a 9f 9b eb b0 00	59 00 06 00 01 00 08 08 f1 42	. * `i ·	8			
N000 N028	ff ff ff ff ff ff ff af 81 01 02 c6 58 00 69 00 09	ff c0 2e 25 a7 60 5a 9f 9b eb b0 00 00 00 00 00 00 00 00	59 00 06 00 01 00 00 01 42 00 00 09 01 42	. % 1 Z	8			
5000 1010 1020	ff ff ff ff ff ff af 81 01 02 c8 80 00 00 00 00 00	ff c0 2e 25 a7 60 5a 97 9b eb b0 00 90 60 60 00 60 00 00 60 00 00 00 00	69 00 06 00 01 00 00 01 1 42 00 00 08 00 00 X	z. % '1.	8			
10000 10000 10000 10000	ff ff ff ff ff ff ff af 81 01 02 c8 58 00 00 00 00 00 00 00 00 00	ff c0 2e 25 a7 60 5a 9f 9b eb 80 80 80 80 60 80 80 80 80 80 80 80 80 80 80	59 00 05 00 01 00 00 00 11 42 00 00 08 00 09 X 00	z. \$-1- z	8			
: 2000 2018 2010 2010	ff ff ff ff ff ff af 81 01 02 c8 58 00 00 00 00 00 00 00 00 00	ff c0 2e 25 a7 60 5a 9f 9b eb b0 80 60 86 60 80 80 80 80 80 80 80 80 80	69 00 06 00 01 00 00 06 13 42 00 00 08 08 00 00 X	, \$ 'i Z	8			
	ff ff ff ff ff ff ff af 81 01 02 06 09 00 00 00 00 00 00	ff c0 2e 25 a7 60 5a 9f 9b eb b0 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60	59 00 06 00 01 00 00 06 11 42 00 00 06 00 00 X	, \$ '1 Z	8			
2000 0010 0010 0020 0020	ff ff ff ff ff ff af 81 01 02 c8 58 00 00 00 00 00 00 00 00 00 00	ff c0 Ze Z5 a7 60 5a 95 9b eb b0 00 00 00 00 00 00 00 00 00 00 00 00 00	69 00 06 00 01 00 00 00 13 42 00 00 00 00 00 X 00	z. * 1.	8			
100000 100000 100000	ff ff ff ff ff ff af 81 81 02 68 58 00 60 00 60 00 00 00 00 00 00 00	ff c0 2e 25 a7 60 5a 9f 9b, eb b0 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60	59 00 06 00 01 50 00 09 11 42 50 00 09 00 09 X 50	z. * 'i.	- 8 8			
1000H 1000H 10120 10120	ff ff ff ff ff ff ff af 81 01 02 C8 58 00 00 00 00 00 00 00 00 00 00	ff c0 2e 25 a7 60 5a 9f 9b eb b0 60 00 80 60 80 80 60 00 80 60 80 80 80 80	59 00 06 00 01 00 00 06 13 42 00 00 06 06 00 00 X 00	., % 'i. Z	8			
	ff ff ff ff ff ff af 81 91 92 60 88 90 90 90 90 90 90 90 90 90 90	ff c0 2e 25 a7 60 5a 9f 9b eb b0 80 00 6e 80 00 00 00 00 00 00 00 00 00 00 00 00	59 00 05 00 01 00 00 00 f1 42 00 00 00 00 00 00 X	, \$ '1 Z				

Gbr. 3 Tampilan awal saat sniffing

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

No.	Time	Source	Destruction	Protocol	Length	Info	ò
8	814 1558.178483	104.18.26.211	192.168.1.5	TEP	60	[TEP Previous segment not	
		104.18.26.211				[TCP Out-Of-Order] 443 *	
		104.18.26.211				[TCP Dut OF Order] 443 +	
	817 1550, 170511					[TCP Dup ACK 748081] 635	
8	818 1550. 378564	192.168.1.5	104.18.26.211	TCP	54	63526 + 443 [ACK] Seg=12	
8	819 1550. 370748	192.168.1.5	104.18.26.211	TCP	54	63526 + 443 [FIN, ACK] 5	
8	820 1550.410163	104.18.26.211	192.168.1.5	TCP	66	443 + 63526 [ACK] Seg=22:	
8	821 1553.017057	52.98.42.162	192.168.1.5	TLSv1.2	94	Application Data	
8	822 1553.017118	192.168.1.5	52.98.42.162	TCP	- 54	63324 + 443 [ACK] Seg-1 /	
8	823 1554, 293493	192.168.1.5	184.18.26.211	TCP	55	[TCP Keep-Alive] 63529 +	
8	824 1554.323518	104.18.26.211	192.168.1.5	TCP	66	[TCP Keep-Alive ACK] 443	
							v
6						2	

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.

3	Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{2DCB4F58-6 IEEE 002.3 Ethernet
3	Logical-Link Control
×	Logical-Link Control Basic Format XID
	XID Format: LLC basic format (0x01) LLC Types/Classes: Type 1 LLC (Class I LLC) (0x01)
	Receive Window Size: 1
	Chr. 5 Iendela <i>nackat datails</i>

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.

FUEL CARD+++	CAPS Fuelcard online system
Username	1101
Password	
User name or pr	Login +++
The second secon	
1.1.1.1.1.1.	

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.

he	ф.				(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)
No.	Time	Source	Destination	Protocol	Length Info
	34 1.801786	192.168.1.5	193.110.250.6	HTTP	781 POST / HTTP/1.1 (applic.
	142 2.215105	192,168.1.5	193.110.250.6	HTTP	575 GET /Content/style.css H
	143 2.216767	192.168.1.5	193.110.250.6	HTTP	582 GET /Content/bootstrap.m
	144 2.216982	192,168.1.5	193.110.250.6	HTTP	570 GET /Scripts/jquery-1.4.
	145 2.217152	192,168,1.5	193.110.250.6	HTTP	572 GET /Scripts/jquery.vali
	146 2.217921	192,168.1.5	193.110.250.6	HTTP	574 GET /Scripts/jquery.data
	164 2.496575	193.110.250.6	192.168.1.5	HTTP	257 HTTP/1.1 304 Not Modifier
	165 2.498163	192.168.1.5	193.110.250.6	HTTP	564 GET /Scripts/jquery-ui.j
	166 2.583177	193.110.250.6	192.168.1.5	HTTP	257 HTTP/1.1 304 Not Modifies
	183 2.539561	193,110,250,6	192.168.1.5	HITP	678 HTTP/1.1 200 OK (text/c
-	187 2.763784	193.110.250.6	192,168.1.5	HTTP	1039 HTTP/1.1 200 OK (text/hr
	229 2.833915	193.110.250.6	192.168.1.5	HTTP	258 HTTP/1.1 304 Not Modifier

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,

Destination	Protocol	Length Info
193.110.250.6	HTTP	781 POST / HTTP/1.1 (application/x-www-form-urlencoded)
193.110.250.6	HTTP	575 GET /Content/style.css HTTP/1.1
193.110.250.6	HTTP	582 GET /Content/bootstrap.min.css HTTP/1.1
193.110.250.6	HTTP	570 GET /Scripts/jquery-1.4.4.min.js HTTP/1.1
193.110.250.6	HTTP	572 GET /Scripts/jquery.validate.min.js HTTP/1.1
193.110.250.6	HTTP	574 GET /Scripts/jquery.dataTables.min.js HTTP/1.1
192.168.1.5	HTTP	257 HTTP/1.1 304 Not Modified
193.110.250.6	HTTP	564 GET /Scripts/jquery-ui.js HTTP/1.1
192.168.1.5	HTTP	257 HTTP/1.1 304 Not Modified
192.168.1.5	HTTP	678 HTTP/1.1 200 OK (text/css)
192,168.1.5	HTTP	1039 HTTP/1.1 200 OK (text/html)
192,168,1,5	HTTP	258 HTTP/1.1 384 Not Modified

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.

Wirestark - Follow HTTP Stream	i (topistream eq. 15) - Ethemet 4			-	u	. ^
POST / HTTP/1.1 Host: login.petrolweb.net Connection: keep-alive Content-Length: 29 Cache-Control: wax-age-0 Upg-ade-Insecure-Requests User-Agent: Mozilla/S.0 (87.0.4280.88 Safari/537.3 Origin: http://dogin.petr Content-Type: application Accest: text/fiel_application	: 1 Windows NT 10.9; Win64; x6: 6 Olweb.net //x-waw.fore-urlencoded thon/whal.was.lastication	4) AppleWebKit/537.36 /wnl:g=0.9.image/avif	(KHTML, like (Secko)	Chrom	u U
<pre>iso_iso_iso_iso_iso_iso_iso_iso_iso_iso_</pre>	<pre>ide xchange;vi0;;a0.9 rolweb.net/ flate 0.9;en:U5;an0.8;m;gd=0.7 i04.1007708264; gid=GAI.2; dminHTTP/1.1 200 CK charset=utf=8</pre>	784312068. 1607345046				13
igen: a section is positive in the intervention of the interventin of the intervention of the intervention of the intervent	<pre>seteching;:vi03;qv0.9 robust.net/ Flate 0.9;eru0;qv0.8;ms;qv0.7 do.100770245;_gld=6A1.2; dminHTIP/1.1 200 OK charset=utf=8</pre>	784312868, 1607345846	Show da	fa as A	scil	
response to execution application vision Network (not see the second se	d-exchange;v403;q40.9 rolweb.net/ Hate 0.9env0;q40.8,ms;q40.7 de100720264;_g1d=64.2. dminHTIP/1.1 200 OK charset=utf=8	784312868.1607345846	Stew da	fa as 🙏	SCII Fied 1	ent

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 tereksposnya username dan password yang di masukan saat login tadi, lihat Gbr. 15.

UserName=admin&Password=adminHTTP/1.1 200 OK
Cache-Control: private

Gbr. 15 Tereksposnya 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

 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.