p-ISSN : 2406-7733
e-ISSN : 2597-9922

ANALISIS *SNIFFING* PADA *PASSWORD* DAN *USERNAME* MENGGUNAKAN *NETWORK ANALYZER*

Salsa Dila Apriliyana[1], Sutarti[2]
Program Studi Sistem Komputer, Fakultas Teknologi Informasi
Universitas Serang Raya
Jalan Raya Serang-Cilegon KM. 10, Serang, Banten
E-mail: salsadila1992@gmail.com[1], sutarti86@gmail.com[2]

Abstrak - Pada era globalisasi saat ini, teknologi memainkan peran penting dalam kehidupan manusia. Keamanan jaringan menjadi sangat penting dan harus diperhatikan, membuat celah bagi pelaku kejahatan untuk melakukan aksinya seperti kejahatan *sniffing*. *Sniffing* merupakan bentuk pencurian yang dilakukan untuk mengambil data pengguna secara ilegal maupun mendapatkan informasi sensitif seperti kata sandi dan data pribadi. Pelaku *sniffing* melakukan aksinya dengan membuka salah satu situs *website* yang teridentifikasi masih menggunakan protokol HTTP. Penelitian ini bertujuan untuk melakukan proses *sniffing* pada *password* dan *username* dengan menggunakan metode *Network Analyzer*. Penelitian dilakukan menggunakan *Wireshark* untuk mengambil data berupa *file capture* melalui jaringan *Wi-Fi* saat melakukan kejahatan *sniffing* kemudian *Wireshark* menyaring data yang tertangkap seperti informasi singkat tentang paket, jumlah data yang didapat. Hasil dari penelitian ini, diperoleh informasi TCP *Stream* (tcp.stream) berupa *username* dan *password* pada situs *website* yang masih menggunakan protokol HTTP, serta protokol HTTPS untuk mencegah terjadinya serangan *sniffing*.

Kata Kunci : *Network Analyzer, Password* dan *Username, Website, Sniffing, Wireshark*

I PENDAHULUAN

Pada era globalisasi saat ini, teknologi memainkan peran penting dalam kehidupan manusia. Kemajuan zaman telah mengubah semua aspek kehidupan mansuia, termasuk teknologi, sosial, dan budaya (Majid & Purwanto, 2021). Keamanan jaringan menjadi sangat penting dan harus diperhatikan, karena jaringan yang terhubung ke internet, baik LAN maupun *Wireless,* pada dasarnya tidak aman dan selalu dapat dieksploitasi oleh pencuri. Sistem keamanan jaringan yang terhubung ke internet harus dirancang dan dipahami dengan baik untuk melindungi sumber daya jaringan dan mengurangi serangan otomatis. Ini karena saat data dikirim melalui beberapa terminal hingga sampai tujuan, memberikan kesempatan kepada orang lain yang tidak bertanggung jawab untuk menyadap atau mengubah data, bahkan mencuri data (Kurniawan, 2021).

Saat data dikirim dari *client* ke server atau sebaliknya, tindakan *sniffing* dapat terjadi. Menurut (Anendya, 2022) *sniffing* merupakan salah satu bentuk *cybercrime* yang dilakukan menggunakan jaringan internet dengan tujuan mengambil data pengguna secara ilegal untuk mendapatkan informasi sensitif seperti kata sandi dan data pribadi. Tindak kejahatan ini dapat terjadi ketika sedang terhubung dengan jaringan yang bersifat *public*, kemudian melakukan proses transfer data baik dari *client* server ke pengguna maupun sebaliknya. Di situlah *sniffing* bekerja menggunakan alat untuk menangkap paket data yang dikirimkan menggunakan bantuan *tools.*

Penelitian ini dilakukan untuk menganalisis terjadinya serangan terkait *sniffing* untuk mendapatkan informasi pribadi berupa *username* dan *password* pada salah satu *website* yang teridentifikasi masih menggunakan protokol HTTP. Menggunakan metode *Network Analyzer* dikarenakan *sniffing* biasanya melakukan serangan melalui jaringan *wireless*. Oleh karena itu, metode *Network Analyzer* dapat digunakan untuk menganalisis terjadinya serangan *sniffing* untuk mendapatkan informasi pribadi berupa *username* dan *password* yang terjadi saat penyerangan. Banyak alat yang digunakan untuk melakukan serangan *sniffing, Wireshark* adalah salah satunya.

Menurut (Saputro, 2022) *Wireshark* adalah sebuah aplikasi *capture* paket data berbasis *open-source* yang berguna untuk memindai dan menangkap trafik data pada jaringan internet dengan menghasilkan informasi data bukti kejahatan melalui jaringan komputer.

Penelitian ini bertujuan untuk melakukan analisis terhadap suatu kejahatan *sniffing* yang telah terjadi dengan menggunakan metode *Network Analyzer* dimana hasil yang didapat dari penelitian ini dapat mengungkapkan informasi TCP *Stream* (tcp.stream) berupa *username* dan *password* pada situs *website* yang masih menggunakan protokol HTTP, serta protokol HTTPS untuk mencegah terjadinya serangan *sniffing*.

Berdasarkan permasalahan tersebut, maka penelitian ini tertarik untuk mengangkat penelitian dengan judul "Analisis *Sniffing* Pada *Password* dan *Username* Menggunakan *Network Analyzer*" untuk dapat mengetahui penyerangan terkait *sniffing* berupa data informasi pribadi.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

II. KAJIAN PUSTAKA

2.1 Tinjauan Penelitian

Keamanan pada sebuah web harus selalu di update karena cepat atau lambat keamanan tersebut dapat ditemukan celahnya oleh para *hacker* yang ingin mencuri informasi pada web tersebut (Hae, 2021). Tujuan dari jurnal tersebut adalah untuk mencegah pencurian data terjadi maka keamanan pada sebuah web perlu ditingkatkan dengan metode eksperimen untuk menganalisis tingkat keamanan pada protocol web tersebut dengan cara melakukan *sniffing* pada salah satu web milik Universitas Kristen Satya Wacana. Hasil yang didapat jurnal tesebut adalah mendapatkan hasil tools yang cukup baik dalam melakukan peretasan pada sebuah web, dimana protokol dari web yang semulanya harusnya HTTPS berhasil diturunkan menjadi HTTP.

Peneliti terdahulu kedua yang dilakukan oleh (Kurnia, 2019) dengan permasalahan yang dibahas pada jurnal tersebut adalah kelemahan dari jaringan *wifi* dan *LAN* di universitas Pembangunan Panca Budi Medan. Tujuan dari jurnal tersebut adalah untuk mengamankan *server* sebuah instansi dari serangan *hacker* yang kerap sekali mencari kesempatan untuk mengetahui aktivitas suatu jaringan dengan metode eksperimen untuk menganalisis pemanfaatan *Bettercap* sebagai teknik *sniffing* pada kelemahan suatu jaringan *wifi*. Hasil yang didapat jurnal tersebut adalah mendapatkan hasil beberapa *host* yang menjadi target *sniffing,* diketahui mengakses beberapa url sosial media dan *page login url* lainnya. Akses *username* dan *password* di record ketika aplikasi Bettercap melakukan fitur *sniffer* disetiap hostnya.

Peneliti terdahulu ketiga yang dilakukan oleh Permasalahan yang dibahas pada jurnal tersebut adalah pencurian data-data perusahaan, data-data konsumen, dan data-data *password*. Tujuan dari jurnal tersebut untuk melakukan serangan *sniffing* pada jaringan *WiFi* dan mengetahui tingkat kesulitan dari kegiatan *sniffing* pada suatu jaringan *wifi* dengan metode eksperimen untuk menganalisis ancaman *sniffing* pada jaringan *WiFi* yang memiliki kelemahan dibidang keamanan. Hasil yang didapat jurnal tersebut adalah mendapatkan hasil aplikasi *Cain and Abel* mampu membaca lalu lintas jaringan dan menembus di jaringan *WiFi* PT.Stepa Wirausaha Adiguna.

Peneliti terdahulu keempat yang dilakukan oleh (Putra *et al*., 2023). Permasalahan yang dibahas pada jurnal tersebut adalah tidak bisa tercegahnya data yang dikirim bisa di sadap oleh orang yang ada di dalam jaringan itu sendiri. Tujuan dari jurnal tersebut untuk mengamankan serangan packet sniffing pada jaringan komputer menggunakan vpn tunnel dengan metode *Tunneling* untuk memastikan bahwa informasi yang dikirim aman dan tidak bocor ke pihak ketiga, terutama bila informasi tersebut besifat rahasia. Hasil yang didapat jurnal tersebut adalah mendapatkan hasil VPN Tunnel dapat digunakan untuk mengamankan packet sniffing dari serangan dan ancaman jaringan komputer yang tepat.

Peneliti terdahulu kelima yang dilakukan oleh (Wijaya, 2022). Permasalahan yang dibahas pada jurnal tersebut adalah jaringan protokol yang kurang aman dan dapat di sadap. Tujuan dari jurnal tersebut adalah untuk meningkatkan jaringan protokol dan memiliki keamanan yang tinggi dengan metode berbasis protokol 802.1X mendapatkan kode otentikasi klien. Hal yang didapat jurnal tersebut adalah mendapatkan hasil Proses *sniffing* menggunakan aplikasi wireshark berhasil mendapatkan kode otentikasi stasiun pada jaringan *WiFi* berbasis 802.1X. Kode otentikasi dapat digunakan ketika stasiun tidak lagi terhubung ke jaringan *WiFi*.

Peneliti terdahulu keenam yang dilakukan oleh (Umasugi, 2022). Permasalahan yang dibahas pada jurnal tersebut adalah koneksi hotspot yang ada di kampus UMMU dapat saja di ganggu atau di *hack* oleh orang-orang yang tidak bertanggung jawab. Tujuan dari jurnal tersebut adalah untuk mengetahui celah keamanan jaringan *wifi* terhadap ancaman serangan pada Kampus A Universitas Muhammadiyah Maluku Utara dengan metode *black box testing* sehingga proses pengujian berjalan dengan baik. Hasil yang didapat jurnal tersebut adalah mendapatkan hasil penelitian yang dilakukan di kampus UMMU khususnya di kampus A ruangan ICT tentang analisis keamanan jaringan *wifi* terhadap serangan *packet sniffing* yang Dimana keamanan *wifi* masih sangat rentan dan masih butuh keamanan jaringan yang lebih maksimal lagi.

Peneliti terdahulu ketujuh yang dilakukan oleh (Arsalan, 2023). Permasalahan yang dibahas pada jurnal tersebut adalah keamanan jaringan pada PT Akurat Sentra Media sering terjadi dikarenakan terdapat port-port yang terbuka dan pengimplementasian topologi jaringan yang tidak aman dapat menyebabkan pengguna yang tidak valid dapat mengakses dan mengelola jaringan lokal di Perusahaan secara illegal. Tujuan dari jurnal tersebut adalah mengimplementasikan keamanan jaringan *wifi* menggunakan *firewall rule mikrotik* terhadap serangan *packet sniffing* di jaringan *wifi* PT Akurat Sentra Media dengan metode simulasi untuk berbuat seakan-akan ada kejadian pada instansi. Hasil yang didapat jurnal tersebut adalah mendapatkan hasil *Firewall rule* berhasil melakukan *action drop* terhadap serangan *arp spoofing* sehingga serangan tersebut dapat diproteksi.

Penelitian terdahulu kedelapan yang dilakukan oleh (Susanto *et al*., 2018). Permasalahan yang dibahas pada jurnal tersebut adalah Universitas Semarang juga memiliki jaringna *wifi* yang tidak menutup kemungkinan terjadinya serangan pada jaringan tersebut. Tujuan dari jurnal tersebut adalah untuk memberikan pengetahuan bagaimana

p-ISSN : 2406-7733
e-ISSN : 2597-9922

melakukan *Sniffing* dalam sebuah jaringan, dan bagaimana cara menghindari tindakan ini dengan metode eksperimen kelompok dibentuk dan dipilih oleh peneliti. Kemudian mencoba mengontrol, mengetahui apa yang terjadi pada setiap kelompok, mengontrol faktor lain yang relevan, dan pada akhirnya melihat atau mengukur dampak dari penelitian. Hasil yang didapat jurnal tersebut adalah mendapatkan hasil *software Cain and Abel* mampu membaca lalu lintas jaringan dan menembus hampir semua wifi di USM. Melakukan *sniffing* dengan *cain and abel* dapat dilakukan dengan mudah tanpa perlu mempelajari ilmu hacker.

Penelitian terdahulu kesembilan yang dilakukan oleh (Fatimah *et al*., 2022). Permasalahan yang dibahas pada jurnal tersebut adalah Universitas PGRI Sumatera Barat memiliki *wifi* yang tidak menutup kemungkinan terjadinya serangan pada jaringan tersebut. Tujuan dari jurnal tersebut adalah untuk mengetahui keamanan jaringan *wifi* terhadap serangan *Packet Sniffing* di Universitas PGRI Sumatera Barat dengan metode deskriptif salah satu metode penelitian yang bertujuan untuk menjelaskan suatu kejadian, penelitian ini dilakukan dengan cara menguji dan menganalisis hasil pengujian pada keamanan jaringan menggunakan aplikasi *Wireshark* dan *Ettercap*. Hasil yang didapat jurnal tersebut adalah mendapatkan hasil sistem keamanan jaringan *wi-fi* pada Gedung A1, Gedung B1, Gedung D1 di Universitas PGRI Sumatera Barat sudah baik. Pada saat dilakukan *scan for hosts* tidak ditemukan *IP* dari laptop korban penyerangan *packet sniffing*.

Penelitian terdahulu kesepuluh yang dilakukan oleh (Kurniawan, 2021)dengan judul *Analisis Keamanan Fasilitas Jaringan (Wi-Fi) Terhadap Serangan Packet Sniffing Pada Protocol HTTP dan HTTPS*. Permasalahan yang dibahas pada jurnal tersebut adalah penggunaan aplikasi *Burpsuite* dan *Wireshark* dalam melakukan simulasi penyerangan. Tujuan dari jurnal tersebut adalah untuk menguji cara kerja protocol yang menggunakan *Secure Socket Layer (SSL)* data dilindungi sebelum dikirim ketujuan maupun sebelum menggunakan *Secure Socket Layer (SSL)* yang pengiriman datanya dalam bentuk *plaint-text* tanpa perlindungan lebih dengan metode deskriptif untuk menjelaskan suatu kejadian. Hasil yang didapat jurnal tersebut adalah mendapatkan hasil dapat melakukan monitoring aktifitas yang dilakukan pengguna menggunakan tools pihak ketiga oleh *network analyzer.*

2.2 Dasar Teori

Keamanan Jaringan

Keamanan jaringan adalah praktik dan prosedur yang dilakukan untuk melindungi jaringan komputer dari ancaman dan serangan yang merusak, seperti virus, *malware*, *hacker*, dan peretasan data. Tujuan utama dari keamanan jaringan komputer adalah untuk melindungi data sensitif dan informasi rahasia dari kebocoran atau akses yang tidak sah (Valencia, 2022). Keamanan jaringan komputer mencakup sejumlah langkah dan teknologi untuk mencegah, mengidentifikasi, dan merespon ancaman keamanan.

Network Analyzer

Program komputer yang disebut *Network Analyzer* atau penganalisis jaringan, juga dikenal sebagai penganalisis protokol jaringan atau penganalisis paket, berfungsi untuk pemecah masalah, pemantauan keamanan, dan tugas manajemen jaringan, seperti memeriksa konfigurasi *firewall* (Hussein, 2022). *Network Analyzer* memberi informasi tentang kinerja jaringan. Dapat menunjukkan pemanfaatan jaringan, bingkai yang rusak, dan frekuensi tabrakan data. Penganalisis jaringan dapat diatur untuk menampilkan alarm saat kondisi tertentu terjadi, seperti saat perangkat baru terhubung ke jaringan. Digunakan untuk mengumpulkan dan mengevaluasi informasi. Dapat memberi tahu tentang tingkat maksimum di mana suatu sistem dapat menerima data tanpa kehilangan data.

Kekurangan dari *Network Analyzer* yaitu terkadang secara tidak sengaja, individu dapat membuka *email* spam. Ini dapat memungkinkan penganalisis jaringan yang tidak sah untuk mendapatkan akses ke jaringan. Akibatnya, informasi rahasia dapat digunakan untuk keuntungan pribadi, informasi pribadi karyawan dikompromikan sebagai administrator jaringan dapat melacak semua lalu lintas pengguna (Froehlich, 2021).

Wireshark

Wireshark adalah perangkat lunak yang digunakan untuk melakukan analisis atau monitoring paket data pada jaringan secara *real time*/penuh dan menampilkan hasil analisis paket data tersebut dalam format atau bentuk yang mudah dipahami oleh pengguna. *Wireshark* dapat melakukan paket filtering, paket *color* coding, dan fitur-fitur lain yang dapat melihat secara detail *network traffic* dan inspeksi paket data secara individu. *Wireshark* dapat digunakan pada sistem operasi baik Windows, Mac OS X, maupun Linux (Saputro, 2022). Dengan menggunakan *wireshark*, pengguna dapat melacak masalah jaringan, mengidentifikasi penyebab terjadinya masalah, memeriksa kinerja jaringan, dan memantau aktivitas jaringan secara umum. *Wireshark* mendukung berbagai macam protokol jaringan, termasuk TCP, UDP, HTTP, FTP, DNS, dan banyak lagi (Warni, 2020).

Sniffing

Sniffing adalah salah satu bentuk *cyber crime* yang dilakukan menggunakan jaringan internet dengan tujuan mengambil data pengguna secara ilegal (Anendya, 2022). Tindak kejahatan ini dapat terjadi ketika terhubung dengan jaringan yang

p-ISSN : 2406-7733
e-ISSN : 2597-9922

bersifat *public*, kemudian melakukan proses transfer data baik dari *client* server ke pengguna maupun sebaliknya. Pada proses transfer data tersebut, terjadi aliran data yang bolak-balik dari *client* dan pengguna. Di situlah *sniffing* bekerja, mereka akan menangkap paket-paket data yang dikirimkan menggunakan bantuan *tools*. Setelah itu, *sniffing* akan menangkap dan tersangkut pada komputer korban. Kemudian program berbahaya akan disisipkan guna memperoleh seluruh data korban. Kerja *Sniffing* mulai paket data tersebut terbaca hingga diambil, ada beberapa cara kerja *sniffing* yang dilalui, yakni *collection, conversion, analysis,* hingga pengambilan data (Rahmawati, 2022).

Password

Password (kata sandi) adalah serangkaian karakter yang digunakan untuk mengautentikasi pengguna pada sistem komputer. Salah satu fungsi *password* adalah untuk meningkatkan keamanan dari file, aplikasi, serta jaringan yang ingin dilindungi (Johanna, 2024).

Username

Username dikenal sebagai "nama pengguna" adalah nama pengguna unik yang digunakan oleh pengguna pada platform tertentu. Nama pengguna berfungsi sebagai identitas akun selain *password* untuk *login*, dan juga berfungsi untuk memudahkan pencarian data pengguna (Azqiya, 2023).

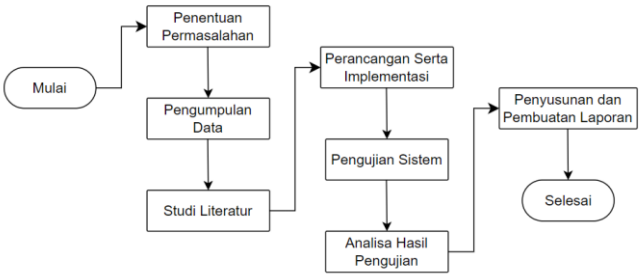
Website

Website pertama di dunia diluncurkan pada tahun 1991 oleh ahli komputer asal Inggris bernama Sir Timothy John "Tim"Berners-Lee. Awalnya, tujuan Tim dalam merancang *website* adalah untuk memfasilitasi pertukaran dan pembaruan informasi antar sesame peneliti di tempat kerjanya (Muhammad, 2023). Itu karena, *website* tersebut hanya dibangun menggunakan HTML (*HyperText Markup Language*). HTML adalah bahasa markup yang hanya mampu menampilkan teks dan gambar yang statis. Baru setelahnya pada tahun 1996, muncul inovasi bernama CSS (*Cascading Style Sheets*). CSS adalah teknologi yang diperkenalkan untuk mempercantik tampilan *website*. Di tahun yang sama, bahasa pemrograman JavaScript dirilis ke *public* sebagai bahasa yang memungkinkan *website* menjadi lebih interaktif dan dinamis. Kemudian pada decade 2000-an, teknologi Flash diluncurkan untuk membuat animasi dan video interaktif pada halaman *web*.

III. METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Untuk mendapatkan data yang akurat serta alur penelitian yang sesuai maka perlu diberi alur yang jelas dalam mendapatkan informasi yang dibutuhkan secara lengkap untuk menunjang akurasi materi serta pembahasan. Berikut tahapan penelitian yang akan dijelaskan:



Gambar 1. Diagram Alur Penelitian

1. Penentuan Permasalahan.
   Kegiatan ini dilakukan untuk landasan atau pondasi dalam mengarahkan pengembangan penelitian.
2. Pengumpulan Data.
   Tahapan ini dilakukan untuk mengumpulkan segala jenis data dan informasi yang dibutuhkan dalam kegiatan *sniffing*.
3. Studi Literatur.
   Tahapan ini dilakukan untuk memperkuat proses penelitian yang akan dilakukan dalam menyelesaikan mencuri data *username* dan *password* yang terjadi saat penyerangan.
4. Perancangan Serta Implementasi.
   Kegiatan ini dilakukan untuk merancang tahapan-tahapan proses dalam penelitian yang dirancang dari berbagai sumber referensi serta teori yang berkaitan dengan penelitian ini.
5. Pengujian Sistem.
   Tahapan ini dilakukan dengan cara menyamakan kinerja *sniffing* dari metode eksperimen serta perangkat komponen pendukung lainnya dengan tahapan-tahapan perintah yang telah dilakukan.
6. Analisa Hasil Pengujian.
   Kegiatan analisis dilakukan dengan mencoba mencuri data *username* dan *password* yang terjadi saat penyerangan menggunakan aplikasi *Wireshark*.
7. Penyusunan dan Pembuatan Laporan.
   Tahapan ini menjelaskan secara detail mengenai masalah yang sedang diteliti, metode yang akan digunakan, hasil penelitian serta penarikan kesimpulan.

3.2 Alat dan Bahan Penelitian

Dalam penelitian ini menggunakan beberapa alat dan bahan. *Hardware* yang diperlukan pada penelitian ini dengan spesifikasi pada Tabel 1.

Tabel 1. Spesifikasi *Hardware*

No.	Bagian Perangkat	Spesifikasi
1.	Tipe	*Laptop*
2.	Prosesor	11th Gen Intel(R) Core (TM) i3-

p-ISSN : 2406-7733
e-ISSN : 2597-9922

No.	Bagian Perangkat	Spesifikasi
		1115G4 @ 3.00GHz 3.00 GHz
3.	Memori	4,00GB RAM
4.	*Storage Drive*	OS (C:) 350GB

Kebutuhan *Software* yang diperlukan untuk penelitian ini antara lain:

1. *Wireshark* dalam penelitian ini, *tool sniffing* berbentuk *software* menggunakan aplikasi *wireshark* versi 4.0.0 untuk mencuri data *username* dan *password* yang dibutuhkan.
2. *Windows* dalam penelitian ini, *Windows* digunakan sebagai sistem operasi pada komputer *server*. *Windows* yang digunakan adalah jenis *Windows11*.
3. *Google Chrome* digunakan untuk membuka link *website* dan melakukan pemeriksaan terhadap link *website* dengan menggunakan *google chrome* versi 120.0.6 (64-bit).

Tabel 2. Spesifikasi *Software*

No.	Bagian Perangkat	Versi	Deskripsi
1.	*Wireshark*	4.0.0	Aplikasi yang digunakan untuk mencuri data *username* dan *password* yang dibutuhkan
2.	*Windows*	*Windows11*	Sistem operasi yang digunakan oleh laptop
3.	*Google Chrome*	120.0.6 (64-bit)	Digunakan untuk membuka dan pemeriksaan terhadap link *website*.

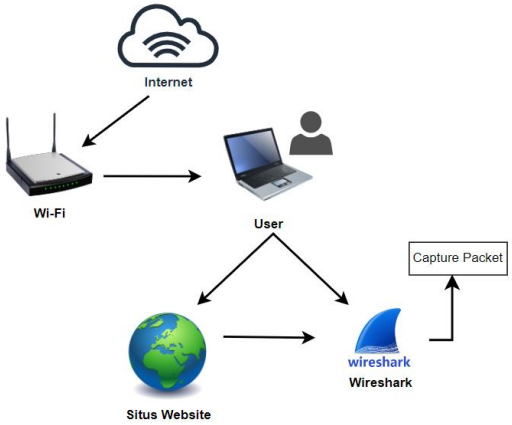
3.3 Data Penelitian

Kumpulan data yang diperoleh dalam penelitian ini merupakan salah satu bentuk kejahatan *cybercrime* yaitu *sniffing* dengan mengambil data pengguna secara illegal untuk mendapatkan informasi sensitif berupa data *username* dan *password* atau data pribadi lainnya yang didapatkan oleh pelaku kemudian dilakukan penyelidikan menggunakan aplikasi *Wireshark*.

3.4 Perancangan Usulan Penelitian

Untuk penelitian ini, perancangan arsitektur jaringan yang akan digunakan harus menghubungkan PC pengguna ke internet. Adapun *software Wireshark* yang digunakan untuk mengambil paket jaringan komputer saat pengguna mengunjungi situs *sniffing*.

Rangkaian yang dilakukan yaitu ketika komputer pengguna terhubung ke internet melalui jaringan *Wi-Fi*, *capture* paket *Wireshark* diaktifkan. Setelah itu, pengguna dapat mengakses tautan yang tercantum pada salah satu situs *website* yang mengarah ke situs *sniffing*, yang kemudian menyimpan data aktifitas jaringan pada *Wireshark*.



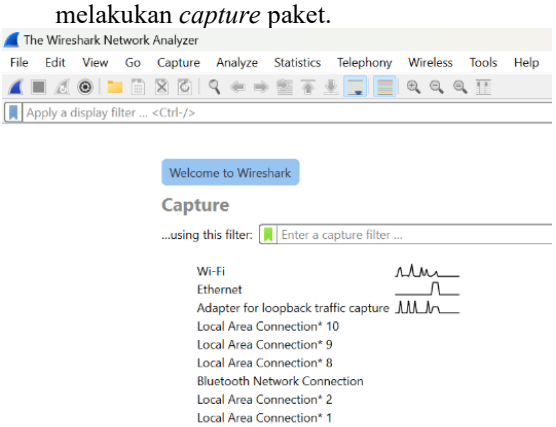
Gambar 2. Rangkaian Alur Analisis

Salah satu kasus *sniffing* yang akan dianalisis adalah *website* yang didapatkan dari *website* acunetix acuart yang teridentifikasi masih menggunakan protokol HTTP, *website* tersebut terdapat informasi pribadi berupa *username* dan *password*, dimana *website* tersebut sangat tidak aman dan ketika pengguna memasukkan data informasi seperti *username* dan *password* maka data tersebut akan tertangkap dan menghasilkan informasi data bukti kejahatan saat terjadi penyerangan *sniffing*.

3.5 Rancangan Pengujian

Pengujian dimulai dengan melakukan *capture* paket jaringan komputer dengan menggunakan *Wireshark*, tahapan yang akan dilakukan yaitu:

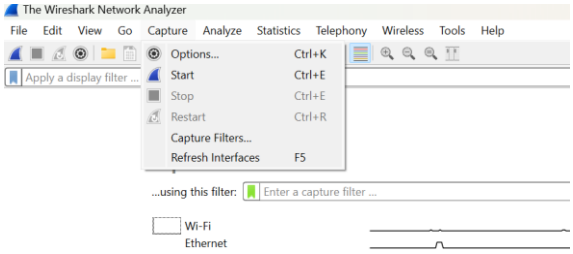
1. Menjalankan aplikasi *Wireshark* untuk melakukan *capture* paket.



Gambar 3. Tampilan *Interface Wireshark*

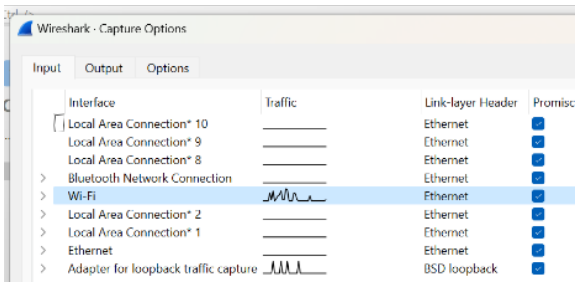
p-ISSN : 2406-7733
e-ISSN : 2597-9922

2. Pilih kolom *Capture* dan klik pilihan *Options* untuk memilih *interface* yang akan dilakukan pengcapturan. Alternatifnya klik dua kali pada pilihan *interface*. Sebelumnya koneksikan laptop dengan jaringan internet terlebih dahulu.



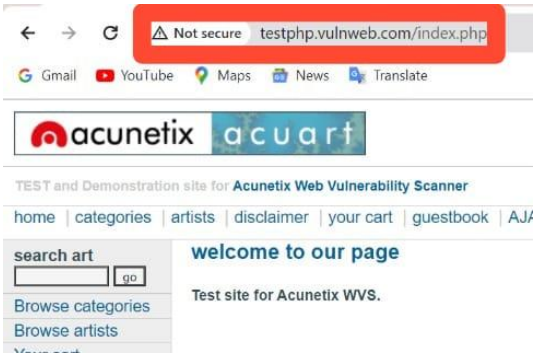
Gambar 4. Pemilihan *Interface*

3. Pilih *interface* yang akan di *capture*. Pada penelitian ini *interface* yang akan dimonitoring yaitu melalui *Wi-Fi*, maka klik bagian *Wi-Fi*. Selanjutnya klik *Start* untuk memulai.



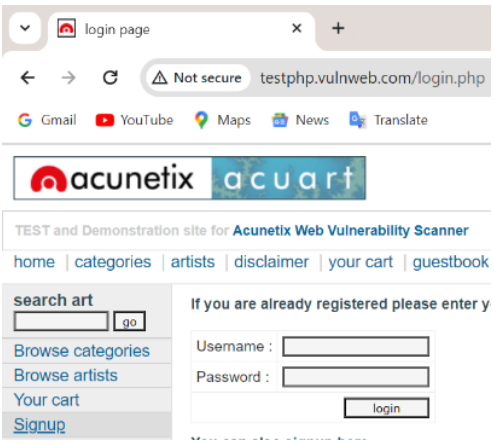
Gambar 5. Pemilihan *Interface Wi-Fi*

4. Disela *Wireshark* berjalan, akses *sniffing* yang ada pada situs *website* Acunetix Acuart. Tampilan awal saat akses situsnya terdapat informasi berupa "welcome to our page Test site for Acunetix WVX".



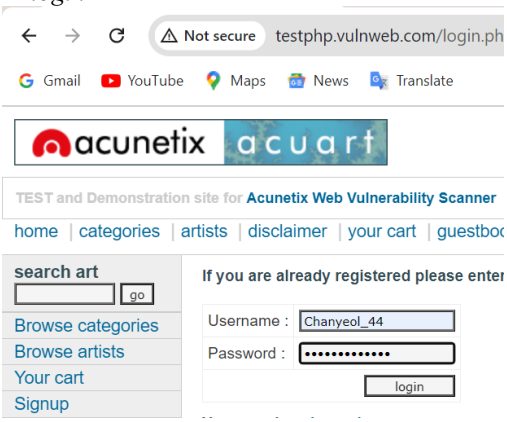
Gambar 6. Tampilan Awal *Website*

5. Selanjutnya saat mengklik pilihan "Signup" yang terletak ada di samping kiri, tampilan yang keluar selanjutnya yaitu permintaan *login* akun Acunetix Acuart yaitu memasukkan *username* dan *password* yang tertaut dengan *website* Acunetix Acuart.



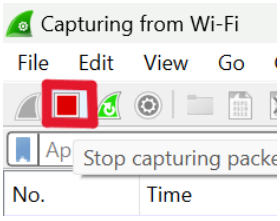
Gambar 7. Tampilan Perintah *Login*

6. Masukkan contoh *username* "Chanyeol_44" dan *password* "12345678". Kemudian klik *login*.



Gambar 8. Tampilan Jika Sudah Dimasukkan *Username* dan *Password*

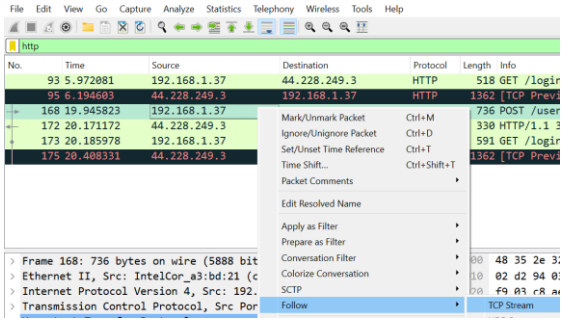
7. Kembali ke program *Wireshark* yang telah dijalankan dengan *interface Wi-Fi*, setelah *Wireshark* melakukan pengcapturan. Kemudian klik tanda yang berwarna merah untuk menyelesaikan *capture* paketnya.



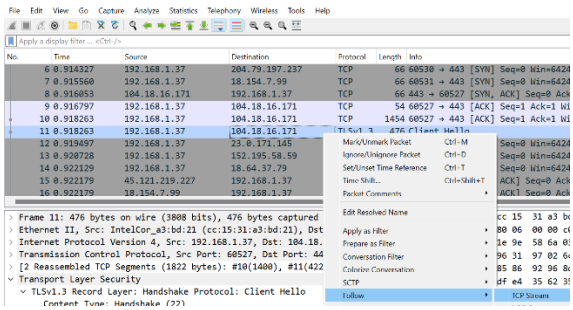
Gambar 9. *Stop Capture*

8. Selanjutnya analisis paket yang difilter melalui protokol HTTP dan protokol HTTPS dengan fitur *Follow TCP Stream*.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

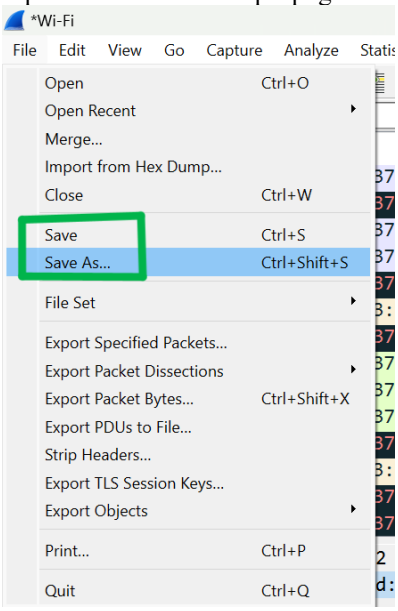


Gambar 10. Tampilan Protokol HTTP Dengan Fitur *Follow TCP Stream*



Gambar 11. Tampilan protokol HTTPS Dengan Fitur *Follow TCP Stream*

9. Kemudian simpan hasil *capture* dengan mengklik pilihan file, dan *Save* atau *Save As*. File yang telah tersimpan pada perangkat komputer berbentuk file *pcapng.



Gambar 12. Penyimpanan Hasil *Capture*

IV HASIL DAN PEMBAHASAN

Hasil Penelitian

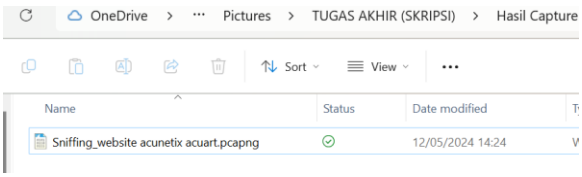
Hasil dari penelitian ini terdapat dua bentuk yaitu hasil pengujian awal melalui tahap proses pengambilan data, serta *sniffing* dan analisis. Adapun hasil pengujian akhir melalui tahap *recovery* hasil analisis yang telah dilakukan.

Hasil Pengujian Awal

Pada pengujian awal dilakukan dengan mengcapture paket data jaringan *Wi-Fi* pada *Wireshark*. Pengujian ini merupakan tahapan dari metode *Network Analyzer* yaitu proses pengambilan data terkait kasus *sniffing*, kemudian proses *sniffing* dan analisis untuk mengamati data hasil *capture*.

A. Pengambilan data

Hasil dari proses pengambilan data didapatkan data yang disimpan dengan nama file (Sniffing_website acunetix acuart.pcapng) yang berisi informasi *capture* paket data mengenai aktifitas yang melintas pada jaringan *Wi-Fi* dan protokol HTTP saat memantau akses *website* yang sedang berjalan. Proses pengambilan data dilakukan dengan membuat jadwal dalam menganalisis paket data jaringan, dilakukan pada tanggal 12 Mei 2024 dengan file *type* berbentuk *Wireshark capture* file.



Gambar 13. Pengambilan Data

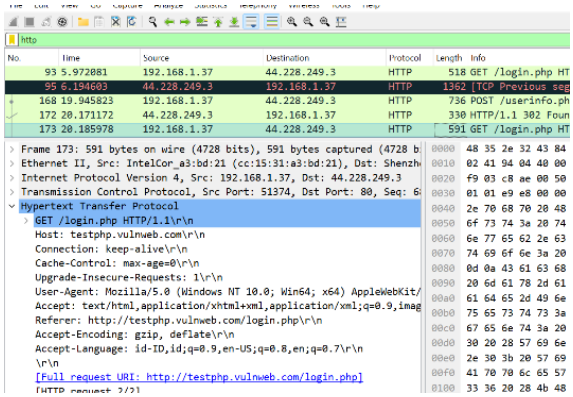
B. Sniffing dan Analisis

Setelah data penelitian terkumpul melalui proses pengumpulan data dengan hasil *capture* paket jaringan komputer pada *Wireshark*. Selanjutnya proses *sniffing* yang akan dilakukan yaitu menganalisis mengenai informasi yang telah ditemukan melalui hasil *capture* paket tersebut. Adapun informasi yang ditemukan yaitu:

1. *Sniffing website* yang diakses dalam *Wireshark*

Paket data dari sebuah *website* yang telah diakses akan ter*capture* dan sudah dilakukan *filtering*. Selanjutnya pilih paket yang mengirimkan suatu pesan GET. Lalu lihat paketnya, maka bisa terlihat *website* yang sedang diakses. Pilih contoh satu dalam protokol HTTP. Dalam box http terlihat permintaan source dan destination Src 192.168.1.37 Dst 44.228.249.3 HTTP591GET/login.php HTTP/1.1. Bisa dianalisis yakni user-agent yang dipakai yaitu Mozilla/5.0 (Windows NT 10.0) browser yang digunakan Chrome/124.0.0.0 Safari/537.36\r\n. Dan Referer yang dituju yaitu Referer: http://testphp.vulnweb.com/login.php\r\n. Dan Host: testphp.vulnweb.com\r\n, selain itu dapat diketahui date yaitu pada Date: Sun, 12 May 2024 07:08:11 GMT dan Full Request Get URI: http://testphp.vulnweb.com/login.php disitu bisa dilihat bahwa adanya aktivitas yang sedang dilakukan dan sedang mengakses laman *web* tersebut dan post diartikan client mengirim data ke suatu *server*.

p-ISSN : 2406-7733
e-ISSN : 2597-9922



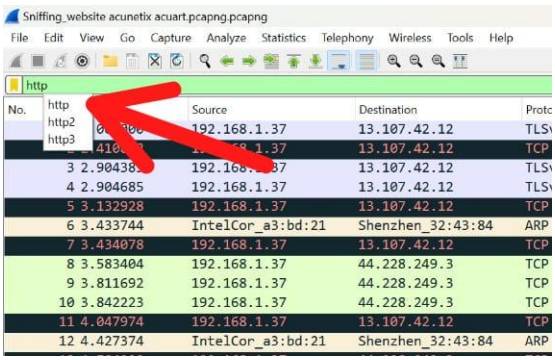
Gambar 14. *Website* yang Diakses dalam *Wireshark*

Gambar 15. Fitur *Follow 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.

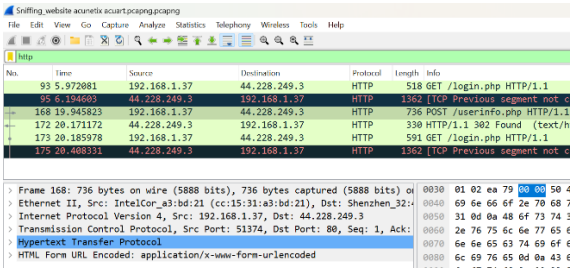
2. *Sniffing Username* dan *Password* yang Melewati Protokol HTTP

Sesudah itu lakukan *capturing* dan *filtering* paket data yang melewati protokol HTTP dengan ketik HTTP pada kolom *display filter*.



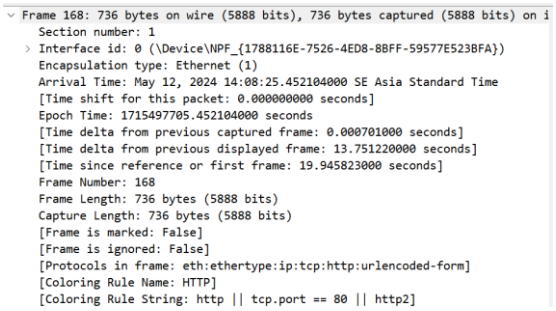
Gambar 16. *Display Filter* dengan HTTP

Banyak data yang terekam menyulitkan untuk dianalisis, maka filter data untuk memudahkan dalam menganalisis protokol. Dengan tampilan seperti diatas sudah dilakukan *filtering* protokol HTTP. Selanjutnya pada gambar 5.5 dilakukan analisis pada paket yang berisi data POST.

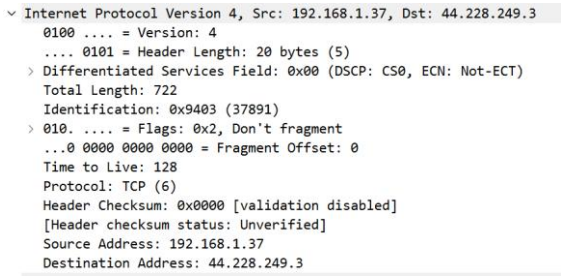


Gambar 17. Paket yang Berisi Data POST

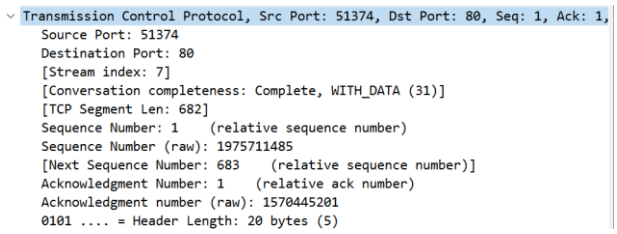
Pada salah satu data POST terdapat informasi seperti alamat IP 192.168.1.37 *source* dan 44.228.249.3 *destination* pada protokol berisi HTTP dan panjang paket 646 *bytes*. Tampilan hasil dari detail paket data seperti *detail* data *Frame*, *Internet Protocol*, *Transmission Control Protocol*, *HyperText Transfer Protocol*, dan fitur *Follow TCP* untuk melihat informasi paket data.



Gambar 18. Paket Data *Frame*



Gambar 19. *Internet Protocol*

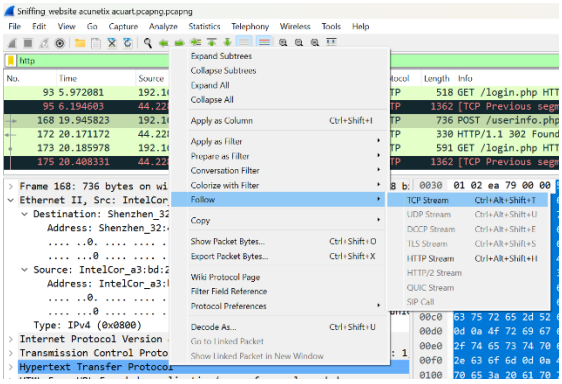


Gambar 20. Detail *Transmission Control Protocol*

p-ISSN : 2406-7733
e-ISSN : 2597-9922

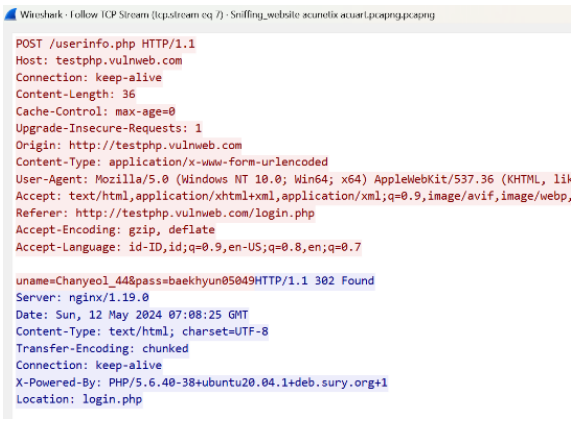
Gambar 21. Detail *HyperText Transfer Protocol*

Pada detail paket data *Transmission Control Protocol* menunjukkan pada *source* menggunakan *port*: 51374, pada *destination* menggunakan *port*: 80. *Website* yang telah diakses dapat diketahui pada detail paket data *hypertext transfer protocol* yaitu *host* : testphp.vulnweb.com, dengan permintaan HTTP POST dengan *user agent* atau keterangan pengguna mengakses dengan *windows* 10, dan *google chrome*. Adapun cara lain untuk mengetahui terkait informasi paket data dengan fitur *follow TCP stream*, dengan klik kanan pada baris paket data kemudian pilih *follow* kemudian pilih *TCP stream*, permintaan akan diproses dan akan menampilkan informasi terkait paket data.



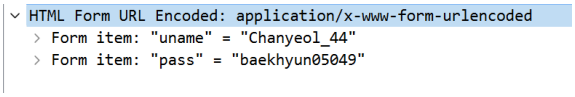
Gambar 22. *Follow TCP Stream*

Informasi terkait detail paket tertera pada perintah *follow* TCP *stream* dari keterangan aktifitas *login*, *host* dari *website* yang diakses, informasi *website* yang diakses, waktu akses, bahasa konten, panjang konten, hingga *username* dan *password*. Informasi yang berwarna merah merupakan perintah dari client, sedangkan informasi berwarna biru berasal dari *server* membalas *client*. Tertera versi HTTP yang dipakai ialah HTTP/1.1, lokasi yang diakses, *host* atau *website* yang sedang dibuka testphp.vulnweb.com, koneksi berjalan atau aktif (*keep-alive*), *username* dan *password* juga tertera.



Gambar 23. Tampilan Hasil *Follow TCP Stream*

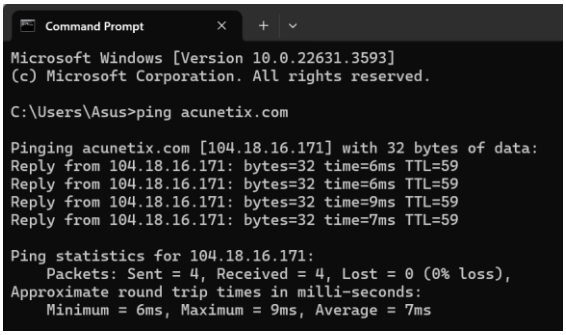
Sniffing informasi terkait *username, password* juga dapat diketahui melalui *HTML from URL Encoded*, terdapat item yang menunjukkan *username* dan *password*. Berikut merupakan gambar *HTML from URL Encoded*.



Gambar 24. *HTML From Encoded*

3. Analisis *Website* Berprotokol HTTPS (*HyperText Transfer Protocol Secure*)

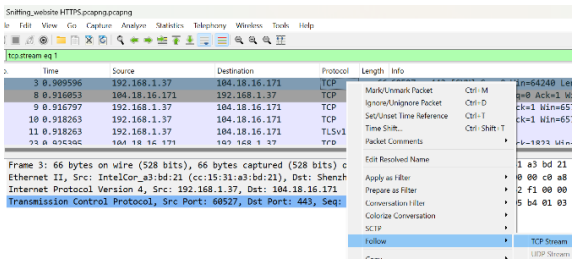
Langkah untuk analisis *website* berprotokol HTTPS yang diakses dengan cara melakukan ping pada *command prompt* guna mendeteksi IP *websitenya*. Dengan cara buka *command prompt* kemudian ketik ping diikuti nama *website* yang akan dituju seperti gambar 25.



Gambar 25. Tampilan *Command Prompt*

Dapat diketahui setelah melakukan pemanggilan IP dengan CMD didapat alamat IP *website* yaitu 104.18.16.171. *Follow TCP Stream* untuk melihat detail paket HTTPS, dengan langkah yang sama seperti langkah pada *follow* protokol HTTP. Dengan klik kanan pada baris data dengan IP *website* yang telah diketahui pilih *follow* kemudian pilih *TCP stream*.

p-ISSN : 2406-7733
e-ISSN : 2597-9922



Gambar 26. *Follow TCP Stream* Pada Detail Paket HTTPS

Informasi yang ditampilkan berupa sekumpulan kode acak pada jejak pertukaran data yang terjadi di *website*, sulit untuk mengetahui informasi apa saja yang terjadi. Beberapa pada *follow TCP* HTTP semua informasi tertera dengan jelas seperti *host* hingga *username* dan *password*, pada *follow TCP* HTTPS sulit dibaca dan tidak diketahui informasi penting seperti *username* dan *password*.

Gambar 27. Tampilan Hasil *Follow TCP Stream* HTTPS

Hasil Pengujian Akhir

Selanjutnya proses terakhir yang dilakukan yaitu *recovery* dengan menyajikan informasi yang didapatkan dari hasil *sniffing* serta analisis terhadap file Sniffing_website acunetix acuart.pcapng telah selesai dilakukan. Informasi yang didapatkan melalui hasil analisis yaitu terdapat protokol-protokol jaringan yang terlibat saat mengakses *website* Acunetix Acuart. Adapun hasil keseluruhannya ditampilkan dengan tabel 3 dan dapat dilihat pada gambar 26 sampai gambar 27.

Tabel 3. Laporan Hasil *Sniffing* dan Analisis

No.	Paket Data	Hasil
1.	Paket Data Nomor 173	▪ Protokol HTTP Perintah GET ▪ *Host* : testphp.vulnweb.com\r\n ▪ User-Agent : Mozilla/5.0 (Windows NT 10.0) ▪ Browser : Chrome/124.0.0.0 Safari/537.36\r\n ▪ Date : Sun, 12 May 2024 07:08:11 GMT
		▪ Full Request Get URI: *http://testphp.vulnweb.com/login.php*
2.	Paket Data Nomor 168	▪ Protokol HTTP perintah POST ▪ *Host :* testphp.vulnweb.com ▪ *Connection* : keep-alive ▪ *Content-Type :* application/x-www-form-urlencoded ▪ *Location* : login.php ▪ *Username* : Chanyeol_44 ▪ *Password* : baekhyun05049
3.	Paket Data Nomor 3	▪ Protokol HTTPS ▪ Sekumpulan kode acak ▪ Sulit dibaca ▪ Tidak diketahui informasi *Username* dan *Password*

Total HTTP dan HTTPS *packets* yang sudah *dicapture* terlihat pada Tabel 4. Proses *capture* data selama 3 hari dengan memonitor paket data yang melewati salah satu jaringan di sebuah rumah, jaringan yang digunakan cukup lancar saat melakukan *capture* data banyak sekali lalu lintas dan banyak juga data keluar masuk, paket data yang melintas berbagai jenis protokol dan jenis interaksi.

Tabel 4. Total HTTP dan HTTPS *packets*

No.	Hari	HTTP Packets		HTTPS Packets	
		Pagi	Malam	Pagi	Malam
1.	Senin	32941	3003	3703	4831
2.	Selasa	6468	1225	2100	1938
3.	Rabu	9983	5489	2060	3838

Pembahasan Penelitian

Pada penelitian telah dilakukan proses *sniffing* serta analisis yang didapatkan dari *website* Acunetix Acuart. *Website* Acunetix Acuart dengan tautan http://testphp.vulnweb.com/login.php yang teridentifikasi masih menggunakan protokol HTTP merupakan *website* yang dibuat oleh pelaku untuk memanipulasi korban. Dalam pengujian ini metode yang digunakan yaitu *Network Analyzer* dikarenakan penelitian yang dilakukan yaitu menganalisis *sniffing* melalui jaringan. Adapun jaringan yang digunakan dalam penelitian ini yaitu *Wi-Fi*.

Pada pengujian awal yang dilakukan yaitu pengambilan data yang didapatkan dari hasil *capture* paket jaringan komputer pada *Wireshark*. Adapun file yang disimpan dengan nama file (Sniffing_website acunetix acuart.pcapng) berisi informasi *capture* paket data jaringan komputer saat akses *website* acunetix acuart yang dilakukan pada tanggal 12 Mei 2024 dengan file *type* berbentuk *Wireshark capture* file.

Proses *sniffing* yang dilakukan selanjutnya yaitu menganalisis hasil file *capture* Sniffing_website acunetix acuart.pcapng. Pada pengujian ini hanya berfokus terhadap evaluasi

p-ISSN : 2406-7733
e-ISSN : 2597-9922

kasus *sniffing website* acunetix acuart maka analisis yang dilakukan terkait informasi jaringan hanya saat terjadi informasi pada situs *website* saja.

Adapun protokol-protokol yang diamati yaitu protokol HTTP yang berisikan data GET dan POST yang terdapat informasi-informasi mengenai aktivitas jaringan yang dilakukan perangkat yang beralamat IP tersebut. Protokol selanjutnya yaitu HTTPS yang dihasilkan saat pencegahan terjadinya *sniffing*. Informasi yang didapatkan yaitu ketika protokol HTTPS melakukan ping guna untuk mendapatkan IP *websetnya*.

Pada bagian protokol HTTP yang berisi data GET yang dihasilkan pada saat situs *website* diakses dengan menampilkan informasi berupa alamat IP 192.168.1.37 *source* dan 44.228.249.3 *destination*, informasi lainnya berupa Host: testphp.vulnweb.com\r\n, referer yang dituju yaitu Referer: http://testphp.vulnweb.com/login.php\r\n, user-agent yang dipakai yaitu Mozilla/5.0 (Windows NT 10.0) browser yang digunakan Chrome/124.0.0.0 dan Full Request Get URI: *http://testphp.vulnweb.com/login.php* serta menampilkan info GET pada TCP Stream yaitu dimana *client* melakukan permintaan pada server agar server bisa mengetahui dan menampilkan request client.

Selain menganalisis hasil protokol HTTP yang berisi data GET, dilakukan analisis protokol HTTP yang berisi data POST yaitu terdapat informasi seperti alamat IP 192.168.1.37 *source* dan 44.228.249.3 *destination* dan panjang paket 646 *bytes*. *Website* yang telah dapat diketahui pada detail paket data *Hypertext Transfer Protocol* yaitu *host*: testphp.vulnweb.com dengan *user-agent* atau keterangan pengguna mengakses dengan *windows* 10 dan *google chrome* serta informasi paket data dengan fitur *follow* TCP Stream menghasilkan informasi penting berupa *username* dan *password* yang diketahui 'uname=Chanyeol_44 & pass=baekhyun05049HTTP/1.1 302 Found' dan tertera versi HTTP yang dipakai ialah HTTP/1.1.

Setelah melakukan analisis terkait *sniffing* pada *website* acunetix acuart yang dilakukan pada *Wireshark* untuk mengcapture paket data jaringan komputer dengan pemanfaatan jaringan *Wi-Fi* telah memberikan informasi bahwa *website* yang berprotokol HTTP yang berisi data GET dan POST menggunakan alamat IP yaitu192.168.1.37 *source* dan 44.228.249.3 *destination*. Terdapat protokol HTTPS dimana informasi yang ditampilkan berupa sekumpulan kode acak pada jejak pertukaran data yang terjadi di *website*, sulit untuk mengetahui informasi apa saja yang terjadi dikarenakan protokol HTTPS digunakan untuk mengamankan koneksi internet dan mencegah terjadinya serangan *sniffing*.

Kelebihan *software Wireshark* yang digunakan dalam melakukan analisis terhadap serangan *sniffing website* ini dapat melakukan analisis paket data melalui jaringan saat mengakses *website* yang masih menggunakan protokol HTTP dilakukan secara *real-time* dan informasi yang diberikan disajikan secara detail terlebih *Wireshark* merupakan *software* yang berbasis *open-source*. Tetapi saat *capture* paket, *Wireshark* hanya dapat menganalisis aktifitas jaringan *Wi-Fi* yang beroperasi melalui *device* yang menjalankan *Wireshark* saja walaupun *device* lain terhubung dengan jaringan yang sama.

Analisis terhadap serangan *sniffing* yang dilakukan pada situs *website* telah berhasil menemukan informasi TCP Stream (tcp.stream) berupa *username* dan *password* pada situs *website* yang masih menggunakan protokol HTTP, adapun protokol lain yang dapat mencegah terjadinya *sniffing* yaitu protokol HTTPS yang digunakan untuk mengamankan jaringan internet.

V. PENUTUP

Kesimpulan

Berdasarkan penelitian yang telah dilakukan dengan tercapainya rumusan masalah terkait kasus yang akan diamati sesuai dengan tujuan penelitian maka didapatkan kesimpulan yaitu:

1. Penggunaan *Wireshark* dalam menganalisis penyerangan *sniffing* dapat dilakukan melalui proses *sniffing* pada *password* dan *username* saat mengakses situs *website* yang masih menggunakan protokol HTTP tersebut. Mengenai informasi penting yang didapatkan dari protokol HTTP yang berisi data POST yaitu terdapat informasi paket data dengan fitur *follow* TCP Stream (tcp.stream) menghasilkan informasi berupa *username* dan *password* yang diketahui 'uname=Chanyeol_44 & pass=baekhyun05049' dan masih banyak detail informasi lainnya.
2. Penerapan metode *Network Analyzer* membuktikan bahwa metode ini dapat menganalisis terjadinya pencegahan dari *sniffing* dengan menggunakan protokol HTTPS yang artinya protokol ini telah terenkripsi dan saat dianalisis interaksi detail paket hanya menampilkan kode acak yang sulit dibaca dan diketahui ketika dilakukan *sniffing*. Sebuah *website* yang menggunakan protokol HTTPS yang sudah terenkripsi lebih aman karena dapat meningkatkan tingkat keamanan jaringan dan mengamankan koneksi internet serta informasi pribadi seperti *username*, *password* bahkan sampai detail data tidak dapat diketahui oleh pelaku *sniffing*.

Saran

Berdasarkan hasil kesimpulan yang telah diperoleh, saran yang diberikan yaitu pada penelitian ini *software* yang digunakan hanya *Wireshark* saja sehingga hanya dapat menganalisis aktifitas jaringan *Wi-Fi* yang beroperasi melalui *device* yang menjalankan *Wireshark* saja walaupun *device* lain

p-ISSN : 2406-7733
e-ISSN : 2597-9922

terhubung dengan jaringan yang sama. Untuk penelitian selanjutnya mampu melakukan penelitian dengan menggunakan *tools analyzer* yang berbeda.

DAFTAR PUSTAKA

Abdillah, M. A., Yudhana, A., & Fadil, A. (2020). Sniffing pada jaringan WIFI berbasis protokol 802.1X Menggunakan Aplikasi Wireshark. *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, *4*(1), 1.

Arini, A., Luthfi Arsalan, M., & Teja Sukmana, H. (2024). Keamanan jaringan Wi-Fi TERHADAP Serangan packet sniffing Menggunakan firewall rule (Studi Kasus : Pt. akurat.co). *Cyber Security Dan Forensik Digital*, *6*(2), 30–38.

Arsalan, M. L. (2023). *Keamanan Jaringan Wireless Fidelity (Wi-Fi) Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus: PT Akurat Sentra Media* (Bachelor's thesis, Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta).

Azqiya, D. (2023, January 28). *Penjelasan APA ITU username Dan Alasan Penggunaannya*. Leskompi. https://www.leskompi.com/penjelasan-username/

Fatimah, F., Mary, T., & Pernanda, A. Y. (2022). Analisis Keamanan Jaringan Wi-Fi Terhadap serangan packet sniffing di universitas PGRI Sumatera barat. *JURTEII: Jurnal Teknologi Informasi*, *1*(2), 7–11.

Froehlich, A. (2021, October 11). *What is a network analyzer?*. Networking. https://www.techtarget.com/searchnetworking/definition/network-analyzer.

Hae, Y. (2021). Analisis Keamanan Jaringan Pada web dari serangan sniffing dengan metode Eksperimen. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(4), 2095–2105. https://doi.org/10.35957/jatisi.v8i4.1196.

Hussein, S. (2022, February 19). *Network analysis (analisis jaringan) Dalam Sistem Informasi geografis*. GEOSPASIALIS. https://geospasialis.com/network-analysis/.

Johanna. (2024, February 7). *Mengenal APA ITU Password & Fungsinya Untuk Keamanan*. Blog Dewaweb. https://www.dewaweb.com/blog/apa-itu-password/.

Kurnia, D. (2019, May). Pemanfaatan Bettercap Sebagai Teknik Sniffing Pada Paket Trafik Jaringan Wifi. In *Prosiding Seminar Nasional Teknik UISU (SEMNASTEK)* (Vol. 2, No. 1, pp. 83-85).

Kurniawan, R. (2021). *Analisis Keamanan Fasilitas Jaringan (Wifi) Terhadap Serangan Packet Sniffing Pada Protocol Http Dan Https* (Doctoral dissertation, Universitas Islam Riau).

Mahmud, P. T. (2020, March 28). Sniffing Jaringan Menggunakan Wireshark. Jurnal Jaringan Komputer. https://doi.org/10.31219/osf.io/h5wu7

Purnama, T., Muhyidin, Y., & Singasatia, D. (2023). IMPLEMENTASI intrusion detection system (IDS) snort Sebagai Sistem Keamanan Menggunakan whatsapp Dan Telegram Sebagai media notifikasi. *JURNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI*, *14*(2), 358–369.

Putra, R. E., Jalinusl, N., Islami, R., & Iqbal, M. (2023). Mengamankan Serangan packet sniffing pada JARINGAN komputer menggunakan VPN Tunnel. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer)*, *22*(2), 340.

Rahmawati, A. (2022, June 21). *Sniffing: Pengertian, Jenis, Cara Kerja Dan Contoh*. DosenIT.com. https://dosenit.com/hacking/sniffing

Sahara, R., Abdullah, S., & Saputra, R. (2022, July). Analisis Ancaman Sniffing pada Jaringan WiFi di PT. Stepa Wirausaha Adiguna. In *Prosiding Seminar Nasional Riset Information Science (SENARIS)* (Vol. 4, No. 2, pp. 224-230).

Silalahi, P. R., & Sitohang, S. (2023). Analisis Keamanan Jaringan Pada fasilitas WIFI TERHADAP serangan sniffing di pt duta computer. *Computer and Science Industrial Engineering (COMASIE)*, *9*(8), 30.

Susanto, S., Pramono, B. A., & Handayani, S. (2018). Analisis sniffing password Menggunakan aplikasi Cain Dan Abel Pada Jaringan WIFI Universitas Semarang. *Jurnal Transformatika*, *16*(1), 67.

Umasugi, A. (2022). Analisis Keamanan Jaringan Wi-Fi Terhadap Packet Sniffing Di Kampus A Universitas Muhammadiyah Maluku Utara. *PRODUKTIF: Jurnal Ilmiah Pendidikan Teknologi Informasi*, *6*(2), 597-602.

Valencia, V. N. G. A. P. (2022, March 23). *Sistem Keamanan Jaringan: Pengertian, jenis Dan Tips Keamanannya*. DosenIT.com. https://dosenit.com/software/sistem-keamanan-jaringan

Warni, S. (2020, October 17). *Mengenal Wireshark, Fungsi Dan Cara Kerjanya*. Hosteko Blog. https://hosteko.com/blog/mengenal-wireshark-fungsi-dan-cara-kerjanya

Wijaya, D. P. (2022). Aplikasi Wireshark Untuk Sniffing Jaringan Berbasis Protokol. *Jurnal Teknologi Informasi*, 2(9), 1-10