ANALISIS KEAMANAN FASILITAS JARINGAN (*Wi-Fi)* TERHADAP SERANGAN PACKET SNIFFING PADA PROTOCOL HTTP DAN HTTPS

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Teknik Pada Fakultas Teknik
Universitas Islam Riau

OLEH:

REZA KURNIAWAN
163510134

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2021

LEMBAR PENGESAHAN PEMBIMBING SKRIPSI

Nama	: **Reza Kurniawan**
NPM	: 163510134
Fakultas	: Teknik
Program Studi	: Teknik Informatika
Jenjang Pendidikan	: Strata 1 (S1)
Judul Skripsi	: Analisis Keamanan Fasilitas Jaringan (*wi-fi*) Terhadap Serangan Packet Sniffing Pada Protocol Http dan Https.

Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam skripsi ini, telah dipelajari dan dinilai relatif telah memenuhi ketentuan ketentuan dan kriteria-kriteria dalam metode penulisan ilmiah. Oleh karena itu, skripsi ini dinilai layak serta dapat disetujui untuk disidangkan dalam ujian seminar komprehensif.

Pekanbaru, 16 Desember 2020

Disahkan Oleh :	**Disetujui Oleh :**
Ketua Program Studi Teknik Informatika	Pembimbing
Arbi Haza Nasution, B. IT (Hons), M. IT	**Yudhi Arta, ST., M.Kom**

LEMBAR PENGESAHAN

TIM PENGUJI UJIAN SKRIPSI

Nama : Reza Kurniawan
NPM : 163510134
Fakultas : Teknik
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata 1 (S1)
Judul Skripsi : Analisis Keamanan Fasilitas Jaringan (*Wi-Fi*) Terhadap Serangan Packet Sniffing Pada Protocol Http dan Https

Skripsi ini secara keseluruhan dinilai telah memenuhi ketentuan-ketentuan dan kaidah-kaidah dalam penulisan penelitian ilmiah serta telah diuji dan dapat di pertahankan dihadapan tim penguji. Oleh karena itu, Tim Penguji Ujian Skripsi Fakultas Teknik Universitas Islam Riau menyatakan bahwa mahasiswa yang bersangkutan dinyatakan **Telah Lulus Mengikuti Ujian Komprehensif Pada Tanggal 29 Januari 2021** dan disetujui serta diterima untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Strata Satu Bidang Ilmu **Teknik Informatika**.

Pekanbaru, 29 Januari 2021

Tim Penguji

1. Dr. Ir. Evizal Abdul Kadir, M.Eng Sebagai Tim Penguji 1 (……)
2. Apri Siswanto, S.Kom., M.Kom Sebagai Tim Penguji II (……)

Disahkan Oleh :

Ketua Prodi Teknik Informatika	**Dosen Pembimbing**
Arbi Haza Nasution, B. IT (Hons), M. IT	**Yudhi Arta, ST.,M.Kom**

KATA PENGANTAR

بسم الله الرحمن الرحيم

Bismillahirohmannirohhim.

Dengan menyebut nama Allah SWT yang Maha Pengasih lagi Maha Penyayang, Penulis ucapkan puji syukur atas kehadirat-Nya yang telah melimpahkan rahmat, hidayah dan inayahnya kepada kami sehingga penulis dapat menyelesaikan proposal skripsi yang berjudul "Analisis Keamanan Fasilitas Jaringan (*Wi-fi*) Terhadap Serangan Packet Sniffing Pada Protocol HTTP dan HTTPS" ini tepat pada waktunya.

Proposal skripsi ini telah penulis susun dengan maksimal dan mendapatkan bantuan dari berbagai pihak sehingga dapat memperlancar pembuatan proposal skripsi ini. Untuk itu penulis menyampaikan banyak terima kasih kepada semua pihak yang telah berkontribusi dalam pembuatan proposal skripsi ini.

Terlepas dari semua ini, penulis menyadari sepenuhnya bahwa masih ada kekurangan baik dari segi susunan kalimat maupun tata bahasanya. Oleh karena itu dengan tangan terbuka penulis menerima segala saran dan kritik agar penulis dapat menyempurnakan laporan ini.

Akhir kata penulis berharap semoga proposal ini dapat memberikan manfaat, inspirasi dan dapat dipergunakan oleh instansi terkait.

Pekanbaru, 29 Januari 2021

Penulis

DAFTAR ISI

Hal

DAFTAR TABEL

Hal

DAFTAR LAMPIRAN

Hal

REZA KURNIAWAN
Program Studi Teknik Informatika Fakultas Teknik
Universitas Islam Riau
Email : rezakurniawan@student.uir.ac.id

ABSTRAK

Didalam sebuah jaringan komputer banyak sekali paket data yang berlalu lalang pada kabel jaringan, baik itu paket data yang mangandung informasi-informasi penting yang bersifat pribadi yaitu username dan password, alamat dari sebuah situs, ip address user dan sebagainya. Pada umumnya setiap jaringan yang terhubung melalui internet tingkat keamanannya masih rendah dan tidak selalu aman masih dapat diekploitasi oleh para *hacker*. Dengan adanya masalah yang terjadi saat ini maka dengan melakukan analisis terhadap keamanan website terhadap serangan *packet sniffing* yang mana pada *packet sniffing* dapat menyadap komunikasi antara *web browser* dan *server* tanpa diketahui target. Serta untuk mengetahui bagaimana tingkat keamanan dari protokol-protokol pertukaran data *(Hypertext Transfer Protocol*) HTTP dan (*Hypertext Transfer Protocol Secure*) HTTPS.Dari hasil analisis kemanan website terhadap protokol jaringan antara HTTP dan HTTPS terhadap serangan *packet sniffing* yaitu dapat melakukan monitoring aktifitas yang dilakukan pengguna menggunakan *tools* pihak ketiga oleh *network analyzer* dengan tujuan untuk mengontrol pengawasan terhadap pengguna sehingga *administrator* dapat memantau pertukaran data yang terjadi antara *web browser* dengan *server* yang mencurigakan.

Kata Kunci: Tingkat Keamanan, Protocol HTTP dan HTTPS, *Packet Sniffing*

REZA KURNIAWAN
Program Studi Teknik Informatika Fakultas Teknik
Universitas Islam Riau
Email : rezakurniawan@student.uir.ac.id

ABSTRACT

In a computer network there are lots of data packets passing by on network cables, both data packets that contain important personal information, namely username and password, address of a site, user IP address and so on. In general, every network connected via the internet has a low level of security and is not always safe and can still be exploited by hackers.With the current problem, by analyzing the website security against packet sniffing attacks, packet sniffing can intercept communications between web browsers and servers without the target knowing. As well as to find out how the security level of data exchange protocols (*Hypertext Transfer Protocol*) HTTP and (*Hypertext Transfer Protocol Secure*) HTTPS.From the results of the website security analysis of the network protocols between HTTP and HTTPS against packet sniffing attacks, which is to monitor user activities using third-party tools by network analyzers with the aim of controlling surveillance of users so that administrators can monitor data exchange that occurs between web browsers and suspicious server.

Keywords: Security Level, HTTP and HTTPS Protocols, Packet Sniffing

BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer bukanlah sesuatu yang baru saat ini, hampir disetiap tempat banyak terdapat jaringan komputer untuk memperlancar arus informasi pada tempat tersebut. Didalam sebuah jaringan komputer banyak sekali paket data yang berlalu lalang pada kabel jaringan, baik itu paket data yang mangandung informasi-informasi penting yang bersifat pribadi yaitu username dan password, alamat dari sebuah situs, ip address user dan sebagainya. Pada umumnya setiap jaringan yang terhubung melalui internet tingkat keamanannya masih rendah dan tidak selalu aman masih dapat diekploitasi oleh para *hacker*. Dalam pembangunan sebuah perancangan system keamanan jaringan *wi-fi* yang telah terhubung ke internet haruslah diteliti dan dipelajari sehingga dapat dipahami oleh pengguna agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh seorang *hacker* yang tidak bertanggung jawab.

Dengan Meningkatnya kejahatan yang terjadi melalui lalu lintas jaringan yang bersifat bolak-balik, maka telah banyak pada saat ini sebuah web browser menggunakan lalu lintas jaringan yang terenkripsi. Setiap web browser membutuhkan sebuah protocol dalam melakukan transaksi pertukaran data. Protocol HTTPS dengan tingkat keamanan yang dilengkapi protocol keamanan tambahan yaitu *Secure Socket Layer (SSL)* atau *Transport Layer Security (TLS).* Pada *Secure Socket Layer (SSL)* berguna untuk mengenkripsi proses-proses

autentifikasi yang terjadi pada web browser. Sedangkan *Transport Layer Security (TLS)* untuk mengamankan HTTP menjadi HTTPS.

Pada saat ini telah banyak terdapat beberapa teknik penyerangan terhadap sistem keamanan jaringan yaitu memaksa masuk dengan menyerang database password, mengirim paket data dalam jumlah yang sangat besar terhadap suatu server, serangan kemanan jaringan dalam bentuk *smurf attack*, serangan jaringan dengan *Ping of death*, Serangan dengan *Stream Attack*, Serangan dengan *Spoofing*, Serangan dengan *Man In the middle*, Serangan dengan *Sniffer*, serangan dengan *cracker*, dan serangan dengan *Spamming*.

Untuk mengetahui paket data dan mengontrol pengguna pada jaringan LAN terutama pada saat pengguna terkoneksi dengan jaringan *wi-fi* yang akan mengakses internet menggunakan web browser. Maka dibutuhkan suatu analisis jaringan menggunakan tools pihak ketiga oleh network analyzer dengan tujuan menganalisa jaringan dengan melakukan pengawasan terhadap pengguna sehingga administrator dapat dengan mudah memonitoring aktivitas-aktivitas yang dilakukan oleh pengguna.

Berdasarkan uraian diatas, penulis tertarik untuk mempelajari cara untuk mengamankan suatu jaringan. Oleh karena itu, penulis mengambil bahan mengenai keamanan jaringan internet untuk judul skripsi **"Analisis Keamanan Fasilitas Jaringan (*Wi-fi*) Terhadap Serangan Packet Sniffing Pada Protocol HTTP dan HTTPS".**

1.2 Identifikasi Masalah

Adapun identifikasi masalah yang dapat diambil dari latar belakang tersebut adalah sebagai berikut:

1. Kurangnya pemahaman tentang keamanan data di jaringan komputer oleh network administrator dan pengguna komputer secara umum, khususnya ancaman terhadap pencurian data pada jaringan *wi-fi* seperti username dan password.
2. Kurangnya pemahaman tentang pencegahan bagaimana mengatasi penyadapan terhadap jaringan *wi-fi*.
3. Kurangnya pengawasan terhadap aspek keamanan dalam komunikasi melalui jaringan komputer karena telah banyak aktivitas pertukaran informasi rahasia melalui internet.

1.3 Batasan Masalah

Karena luasnya permasalahan yang ada di dalam penelitian ini, maka penulis membatasinya. Adapun batasan masalah dalam penelitian ini, yaitu:

1. Penggunaan Aplikasi *Burpsuite* dan *Wireshark* dalam melakukan simulasi penyerangan.
2. Penggunaan Aplikasi *Burpsuite* untuk melakukan simulasi penyerangan *man in the middle attack* dan aplikasi *Wireshark* untuk menganalisa packet data antara protocol HTTP dan HTTPS.
3. Pada Serangan ini menggunakan penyerangan lokal yaitu menggunakan koneksi *Ethernet* atau *Wi-fi*.

4. Pada OS (*Operating system*), penulis menggunakan *Kali Linux* dengan *Virtual Box*.
5. Penelitian ini hanya memberikan simulasi bagaimana bentuk penyerangan *sniffing* yang dilakukan oleh penyerang dan mengevaluasi bagaimana perbandingan pada aspek keamanan antara pertukaran data dengan *protocol* HTTP maupun HTTPS. Setelah dianalisa barulah didapat sebuah kesimpulan atau solusi bagaimana mengatasi penyerangan *packet sniffing* seperti yang penulis lakukan.
6. Dalam Penelitian ini *wi-fi* itu hanya sebagai gerbangnya saja, data yang akan dicuri ada pada *website*. Untuk penelitian ini penulis menganalisa *website* dengan *protocol* HTTP dan HTTPS yaitu website jurnal pknstan dan *facebook*.

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah disebutkan, maka permasalahan pada penelitian ini dapat diambil sebuah rumusan masalah yaitu, “Bagaimana bentuk Penyerangan snifing pada web yang di *security* dan web yang tidak di *security* dan bagaimana perbandingan antara 2 kondisi tersebut ?”.

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

1. 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 data nya dalam bentuk *plaint-text* tanpa perlindungan lebih.
2. Berguna untuk solusi bagaimana mengamankan jaringan wi-fi agar menjadi lebih baik.
3. Untuk membandingkan 2 kondisi bagaimana penyerangan terhadap web yang di*secure* dan yang tidak di*secure*.
4. Untuk menguji seberapa jauh keamanan jaringan *wi-fi* yang terkoneksi dengan internet baik yang menggunakan *Secure Socket Layer* (SSL) maupun yang tidak menggunakan *Secure Socket Layer* (SSL).

BAB II

LANDASAN TEORI

2.1 Studi Kepustakaan

Menurut Adzan Abdul Zabar (2015), pada penelitian dengan judul Keamanan HTTP dan HTTPS Berbasis Web Menggunakan Sistem Operasi *Kali Linux* yang menjelaskan bahwa Aspek keamanan dalam komunikasi melalui jaringan komputer menjadi semakin penting terutama karena banyaknya aktivitas pertukaran informasi rahasia melalui Internet. Untuk menghindari penyadapan atau tindak kejahatan lainnya. Oleh karena itu, penelitian ini akan membahas beberapa kelemahan yang ada pada Internet khususnya pada website dengan melakukan perbandingan keamanan antara http dan https.

Perbedaan dengan penelitian yang ingin dilakukan oleh penulis ialah penulis tidak hanya melakukan perbandingan keamanan dari kedua protokol saja melainkan penulis ingin melakukan perbandingan dengan analisa bagaimana sebuah bentuk atau kondisi penyerangan sniffing terhadap protocol yang disecure dan tidak disecure.

Penelitian Dian Kurnia (2019) dengan judul Pemanfaatan Bettercap Sebagai Teknik Sniffing Pada Paket Traffic Jaringan *Wi-fi* ialah adanya perancangan suatu jaringan *wi-fi public* yang terhubung ke internet melalui modem. Jaringan yang telah dibangun dilakukan analisis traffik jaringan, protocol jaringan dengan teknik-teknik sniffing. Sniffing difokuskan pada pencarian username dan password untuk login web dan mencoba mengetahui lebih paket data keluar masuk ketika *user login*

pada *page login web* dan keseluruhan aktifitas user dalam mengakses url di browser.

Perbedaan keamanan jaringan yang akan penulis kerjakan ialah penyerang melakukan koneksi dengan *Acces point* dengan melakukan suatu koneksi internet dan penyerang mulai melakukan *scanning user* yang aktif.

Penelitian Susanto (2018) tentang Analisis Sniffing Password Menggunakan Aplikasi *Cain dan Abel* Pada Jaringan *Wi-fi* Universitas Semarang ialah Saat ini Universitas Semarang telah menerapkan jaringan computer kabel maupun nirkabel sebagai media pertukaran data atau informasi pelayanan umum maupun akademik dan informasi penting lainnya. Universitas Semarang juga memiliki jaringan *wi-fi* yang tidak menutup kemungkinan terjadinya serangan pada jaringan tersebut. Sedikit celah dapat dimanfaatkan oleh para *hacker* dan *cracker* untuk menembus suatu jaringan. Oleh karena itu peneliti merasa perlu untuk meneliti dan menganalisis serangan *packe*t data *sniffing.*

Perbedaan Serangan jaringan yang penulis kerjakan ialah adanya analisa dalam keamanan jaringan *wireless*. Yang mana jaringan *wireless* hanya sebagai gerbangnya saja dan data yang akan dicuri ada pada web.

2.2 Dasar Teori

2.2.1 Konsep Keamanan Jaringan

Penulis memiliki acuan pada penelitian Noviyanto yang berjudul analisis keamanan *wireless* di universitas Muhammaddiyah Surakarta yaitu pada saat ini suatu keamanan jaringan sangat penting dan patut diperhatikan, terutama untuk

jaringan yang terhubung dengan internet atau *wi-fi* dan memiliki dasar tidak selalu aman dari penyadapan, baik dari jaringan wired LAN maupun *wireless* LAN. Pada pembangunan sebuah sistem keamanan jaringan internet haruslah direncanakan dan dipahami agar dapat melindungi pengguna dan meminimalisir terjadi serangan oleh orang yang tidak bertanggung jawab.

Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Berikut ini akan dibahas mengenai ancaman, kelemahan, dan *policy* keamanan jaringan.

2.2.2 Ancaman

Pada dasarnya, ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal ke dalam suatu jaringan komputer. Oleh karena itu, harus ditentukan siapa saja yang diperbolehkan mempunyai akses legal ke dalam sistem, dan ancaman-ancaman yang dapat mereka timbulkan. Ada beberapa tujuan yang ingin dicapai oleh penyusup dan, sangat berguna apabila dapat membedakan tujuantujuan tersebut pada saat merencanakan sistem keamanan jaringan komputer. Beberapa tujuan para penyusup adalah:

a. Pada dasarnya hanya ingin tahu sistem dan data yang ada pada suatu jaringan komputer yang dijadikan sasaran. Penyusup yang bertujuan seperti ini sering disebut dengan the curius.

b. Membuat sistem jaringan menjadi down, atau mengubah tampilan situs web. Penyusup yang mempunyai tujuan seperti ini sering disebut sebagai the malicious.
c. Berusaha untuk menggunakan sumner daya di dalam sistem jaringan komputer untuk memperoleh popularitas. Penyusup seperti ini sering disebut sebagai the high-profile intruder.
d. Ingin tahu data apa saja yang ada di dalam jaringan komputer untuk selanjutnya dimanfaatkan untuk mendapatkan uang. Penyusup seperti ini sering disebut sebagai the competition.

2.2.3. Kelemahan

Kelemahan menggambarkan seberapa kuat sistem keamanan suatu jaringan komputer terhadap jaringan komputer yang lain, dan kemungkinan bagi seseorang untuk mendapat akses ilegal ke dalamnya.

2.3. Jenis - Jenis Ancaman Keamanan Jaringan

2.3.1 Packet sniffer

Menurut Achmad Rizal Fauzi (2018), *Packet sniffer* ialah suatu teknik pemantauan setiap komunikasi dan transfer data yang lintas pada jaringan dan memonitor semua lalu lintas jaringan. *Packet sniffer* tidak sama dengan jaringan host standar yang hanya menerima dan mengirim lalulintas khusus. Ancaman keamanan yang disajikan oleh penyadapan adalah kemampuan mereka untuk menangkap semua lalu lintas masuk dan keluar, termasuk *password* dan *username*

atau bahan sensitif lainnya. Untuk dapat membaca dan menganalisa setiap protocol yang melintasi jaringan, diperlukan program yang bisa membelokkan paket ke komputer attacker. Biasa disebut serangan spoofing, attacker akan bertindak sebagai Man-In-the-Middle (Asrodia & Patel, 2012:1)

2.3.2 ARP spoofing / ARP poisoning

Menurut Achmad Rizal Fauzi (2018), *ARP (Address Resolution Protocol) poisoning* ini adalah suatu teknik menyerang pada jaringan komputer lokal baik dengan media kabel atau *wireless*, yang memungkinkan penyerang bisa mengendus frame data pada jaringan lokal dan atau melakukan modifikasi *traffic* atau bahkan menghentikan *traffic*. *ARP spoofing* merupakan konsep dari serangan penyadapan diantara terhadap dua mesin yang sedang berkomunikasi atau yang disebut dengan *MITM (Man in The Middle Attack).*

Prinsip serangan *ARP poisoning* ini memanfaatkan kelemahan pada teknologi jaringan komputer itu sendiri yang menggunakan *arp broadcast. ARP* berada pada layer 2, dimana alamat pada layer dua adalah *MAC address*. Misalnya sebuah *host* (contoh: PC) yang terhubung pada sebuah *LAN* ingin menghubungi *host* lain pada *LAN* tersebut, maka dia membutuhkan infomasi *MAC address* dari *host* tujuan (Oktavianto, 2012).

2.3.3 *Probe*

Menurut Rian Eka Fitriani (2019) Sebuah probe dapat dikenali dari adanya usaha-usaha yang tidak lazim untuk memperoleh akses ke dalam suatu sistem atau untuk menemukan informasi tentang sistem tersebut. Salah satu contohnya adalah

usaha untuk login ke dalam sebuah account yang tidak digunakan. Probing ini dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan yang dengan mencoba-coba apakah pintunya terkunci apa tidak.

2.3.4 Scan

Menurut Rian Eka Fitriani (2019) Scan adalah kegiatan probe dalam jumlah yang besar dengan menggunakan tool secara otomatis. Tool tersebut secara otomatis dapat mengetahui port-port yang terbuka pada host lokal maupun host remote, IP address yang aktif, bahkan bisa untuk mengetahui sistem operasi yang digunakan pada host yang dituju.

2.3.5 Account compromise

Menurut Rian Eka Fitriani (2019) Account compromise adalah penggunaan account sebuah komputer secara ilegal oleh seseorang yang bukan pemilik acoount tersebut. Account compromise dapat mengakibatkan korban mengalami kehilangan atau kerusakan data. Sebuah insiden account compromise dapat berakibat lebih lanjut, yaitu terjadinya insiden root compromise, yang dapat menyebabkan kerusakan lebih besar.

2.3.6 Root compromise

Menurut Rian Eka Fitriani (2019) Root compromise mirip dengan account compromise, dengan perbedaan account yang digunakan secara ilegal adalah account yang mempunyai privilege sebagai administrator sistem. Istilah root diturunkan dari sebuah account pada sistem berbasis UNIX yang mempunyai

privelege tidak terbatas. Penyusup yang berhasil melakukan root compromise dapat melakukan apa saja pada sistem yang menjadi korban, termasuk menjalankan program, mengubah kinerja sistem, dan menyembunyikan jejak penyusupan.

2.3.7 Denial of service (Dos)

Menurut (Ridwan Nur Wibowo, Parman Sukarno, Erwid Musthofa Jadied 2018). Denial of Service (DoS) adalah salah satu jenis serangan dimana penyerang menghabiskan sumber daya ja-ringan komputer. Dampak dari serangan DoS menyebabkan komputer tidak dapat berfungsi dengan normal.

Sumber daya jaringan yang berharga antara lain komputer dan database, serta pelayanan-pelayanan (service) yang disediakan oleh organisasi pemilik jaringan. Kebanyakan user jaringan memanfaatkan pelayanan-pelayanan tersebut agar pekerjaan mereka menjadi efisien. Bila pelayanan ini tidak dapat dipergunakan karena sebab-sebab tertentu, maka tentu saja akann menyebabkan kehilangan produktivitas. Sulit untuk memperkirakan penyebab denial of service. Berikut ini adalah contoh penyebab terjadinya denial of service:

a. Kemungkinan jaringan menjadi tidak berfungsi karena kebanjiran traffic.
b. Kemungkinan ada virus yang menyebar dan menyebabkan sistem komputer menjadi lamban atau bahkan lumpuh.
c. Kemungkinan device yang melindungi jaringan dirusak.

2.4 Cara Kerja Secure Socket Layer (SSL)

Secure Socket layer adalah suatu protocol yang diciptakan oleh *Netscape* untuk memastikan keamanan dalam bertransaksi di internet antara webserver dan web browser dari client. Protokol ini menggunakan sebuah badan yang biasa disebut CA *(Certificate Authority)* untuk mengidentifikasi memverifikasi pihak-pihak yang bertransaksi (Adzan Abdul Zabar, Fahmi Novianto, 2015). Skema diagram proses SSL Handshake dapat dilihat pada gambar 2.1 berikut:

Gambar 2.1 Proses Handshake Pada SSL

1. Pada Proses Pertama client mengirimkan pesan 'Hello' kepada website yang sudah diamankan dengan *Secure Socket Layer* (SSL). Maka client ingin meminta kepada web server untuk melakukan proses identifikasi kepadanya.
2. Pada Proses Kedua kemudian web server akan merespon pesan 'Hello' dengan mengirimkan salinan sertifikat *Secure Socket Layer* (SSL), termasuk didalamnya adalah Public key server.
3. Klien melakukan verifikasi sertifikat *Secure Socket Layer* (SSL) server kepada *Certificate Authority* (CA) dan memastikan *Secure Socket Layer* (SSL) tersebut valid, jika proses ini berhasil

maka akan dilakukan enkripsi dan dikirimkan kembali dengan symmetric session key menggunakan public key server.

4. Server kemudian melakukan dekripsi syimmetric session key dengan public key dan mengirimkan kembali kepada klien dengan session key untuk memulai encryption session.

2.5 Transport Layer Security (TLS)

Protokol *TLS/SSL* memiliki dua bagian yang pertama adalah *handshaking protocol,* yang kedua adalah *record protocol*. *Handshaking protocol* menegoisasi *suite cipher,*mengotentikasi *server* dan secara opsional mengotentikasi klien dan menetapkan *session keys*. Sedangkan *record protocol* mengamankan data aplikasi dengan *session keys* yang dibuat pada *record protocol* dan memverifikasi keaslian dan integritas aplikasi (Turner, 2014).

2.6 Hipotesis

Hipotesis merupakan jawaban sementara terhadap rumusan masalah penelitian, dimana rumusan msalah penelitian telah dinyatakan dalam bentuk pernyataan. Hipotesis dirumuskan atas dasar kerangka pikir yang merupakan jawaban sementara atas masalah yang dirumuskan. Berdasarkan kajian teori dan kerangka berfikir diatas maka dapat dirumuskan hipotesis yaitu dengan adanya sebuah bentuk penyerangan terhadap protocol yang di*secure* dengan yang tidak di*secure* ini maka orang-orang awam dapat memahami secara terperinci dalam menguji tingkat keamanan sebuah jaringan local wlan serta mengetahui bagaimana

bentuk atau kondisi sebuah sniffer melakukan serangan sniffing terhadap website yang memiliki kemanan lebih seperti protocol https dan website yang tidak memiliki keamanan seperti protocol http.

BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode deskriptif. Metode penelitian deskriptif adalah salah satu metode penelitan yang banyak digunakan pada penelitian yang bertujuan untuk menjelaskan suatu kejadian. Seperti yang dikemukakan oleh Moh. Nazir (2003) bahwa "Penelitian deskriptif adalah suatu metode dalam meneliti status sekelompok manusia, suatu objek, suatu set kondisi, suatu sistem pemikiran ataupun suatu kelas peristiwa pada masa sekarang".

Pada metode ini juga menjelaskan bagaimana pengujian sebuah protocol HTTP dan HTTPS, pengujian ini dilakukan beberapa kali untuk memastikan serangan dengan teknik *Man in the middle attack* ini berhasil mengetahui dan melihat username dan password korban. Pada saat simulasi penyerangan ini berjalan nantinya penulis akan menganalisa setiap paket data dan juga mengamati setiap perubahan yang terjadi pada protocol http dan https yang lewat pada jaringan lokal *wi-fi*. Paket data yang penulis amati terdapat beberapa komponen, berikut 5 komponen dari paket data:

1. Time

   Menjelaskan format waktu packet yang tertangkap.

2. Source

   Merupakan IP sumber dari suatu packet data.

3. Destination

   Merupakan IP tujuan kemana suatu packet data akan diteruskan.

4. Protocol

   Merupakan jenis protocol apa yang digunakan.

5. Packet Length

   Merupakan Panjang dari suatu packet data yang digunakan.

6. Info

   Merupakan Info lebih lanjut mengenai suatu packet.

3.2 Alat Analisis

Menurut Rahadi (2010), Tujuan pokok suatu penelitian adalah untuk menjawab pertanyaan dan hipotesis. Untuk itu peneliti merumuskan hipotesis, mengumpulkan data, memproses data, membuat analisis dan interpretasi. Analisis data ini belum dapat menjawab pertanyaan penelitian. Setelah data dianalis dan diperoleh informasi yang lebih sederhana, hasil analisis tersebut harus diinterpretasi untuk mencari makna dan implikasi dari hasil analisis tersebut.

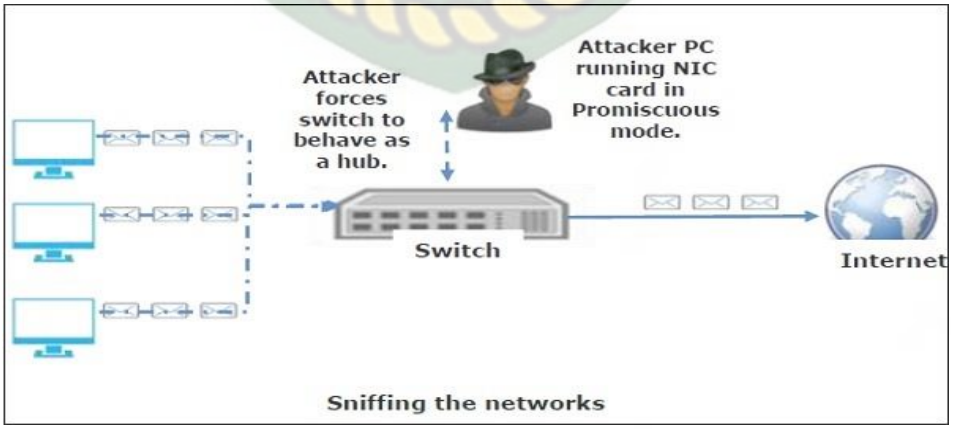
Analisa data adalah mengelompokkan, membuat suatu urutan, memanipuilasi serta meningkatkan data sehingga mudah untuk dibaca. Setelah itu langkah pertama yaitu mencari kesimpulan dari dua protocol HTTP dan HTTPS bagaimana tingkat keamanan dari kerentanan website oleh eksploitasi informasi yang dilakukan penyerang seperti username dan password korban. Alat analisis yang penulis gunakan untuk mengeksploitasi informasi dan mencari kerentanan dari sebuah website yang menggunakan protocol HTTP dan HTTPS sebagai berikut:

1. *Burpsuite*

Merupakan aplikasi yang digunakan untuk mencari kerentanan dari aplikasi web. Tujuan dari Burpsuite ini adalah untuk mencari celah terhadap website HTTPS yaitu facebook. Karena pada burpsuite memiliki sertifikat yang sudah ditandatangani sendiri yaitu sertifikat CA yang dikeluarkan oleh pengembang aplikasi burpsuite ini. Dan memungkinkan tools ini dapat melihat dan membaca jalur lalu lintas protocol HTTPS yang memiliki keamanan lebih.

2. *Wireshark*

Merupakan sebuah *network packet analyzer* yang digunakan untuk membaca dan menganalisa paket-paket data serta dapat menampilkan isi paket dengan sedetail mungkin dari memfilter packet, menampilkan packet list yang sudah terurut secara numerik dan menganalisa jumlah byte dari setiap packet. Tools ini merupakan tools yang sangat populer pada saat ini karena dapat menangkap packet data secara real time.



Gambar 3.1 Model Penyerangan Man In The Middle Attack

Pada Gambar 3.1 dijelaskan bahwa klien akan melakukan transaksi terhadap server https. Antara klien dan server nantinya akan bertukar data jaringan, sedangkan penyerang bertindak sebagai *gateway* dalam aliran lalu lintas. Penyerang tersebut ialah disebut MITM (*man in the middle attack*) yang bertujuan untuk memotong lalu lintas antara client dan server.sehingga dapat mengubah pesan dan menyisipkan pesan baru sebelum lalu lintas dari sumber diteruskan ke tujuannya. Sehingga tindakan tersebut tidak disadari sama sekali.

3.2.1 Bahan dan Alat Penelitian

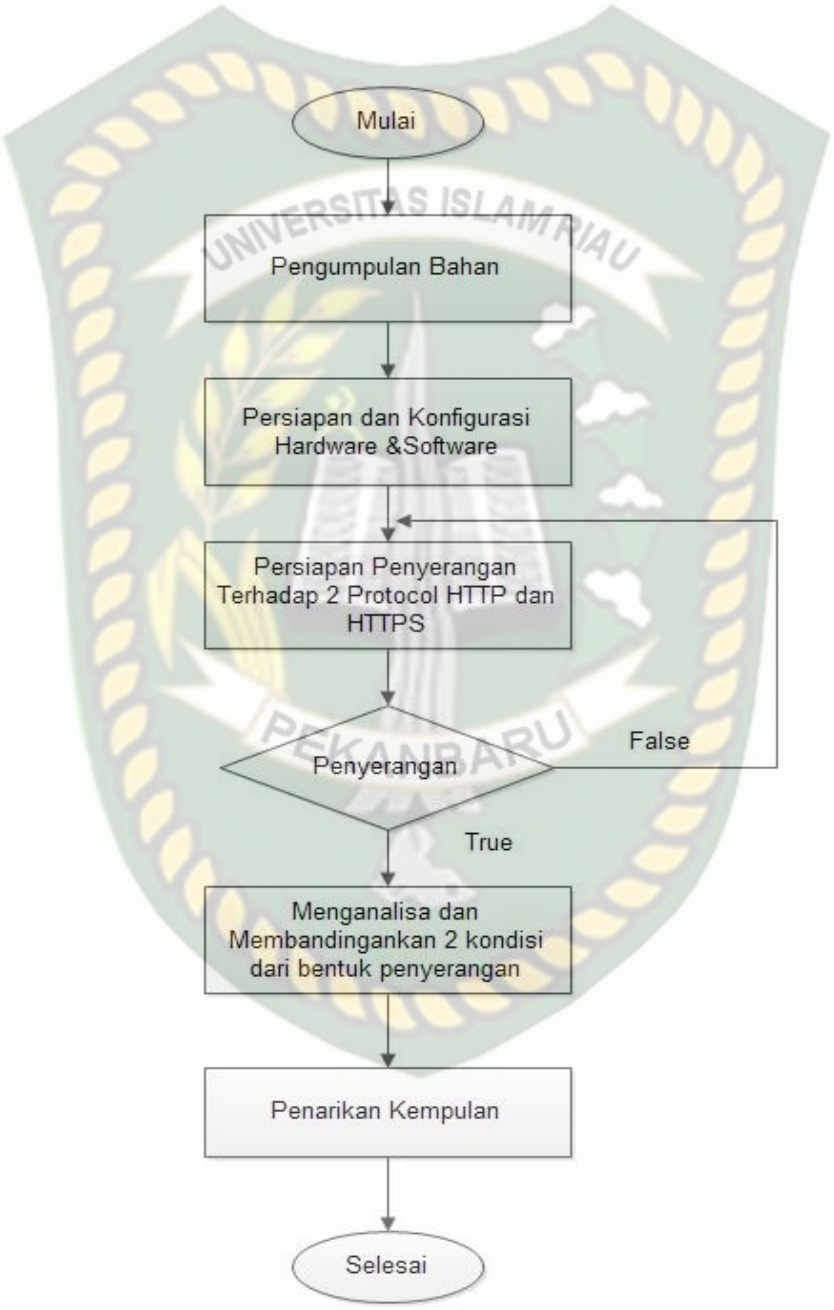
Adapun bahan dan alat penellitian ini ialah penulis menggunakan beberapa software dan hardware sebagai literatur penelitian. Untuk spesifikasi kebutuhan *software* dan *hardware* sebagai berikut:

1. Spesifikasi kebutuhan *hardware* dan sistem operasi.
    a. Laptop ASUSTek Computer Inc, *Processor intel celeron* 1.10Ghz, memori (RAM) 4 GB.
    b. Sistem Operasi *Kali Linux*

2. Spesifikasi kebutuhan *software*
    a. Software *Wireshark* (untuk serangan *Packet sniffing*)
    b. Software *Burpsuite* (untuk mengambat lalu lintas https menggunakan proxy yang disetting pada firefox)

3.3 Flowchart Alur Penelitian

Untuk dapat dipahami maka penulis menjabarkan alur penelitian menggunakan metode yang digunakan dalam flowchart.alur penelitian



Gambar 3.2 Flowchart Alur Penelitian

Pada gambar 3.2 dijelaskan bahwa penelitian ini terbagi menjadi beberapa tahapan alur penelitian. Tahapan alur penelitian sebagai berikut:

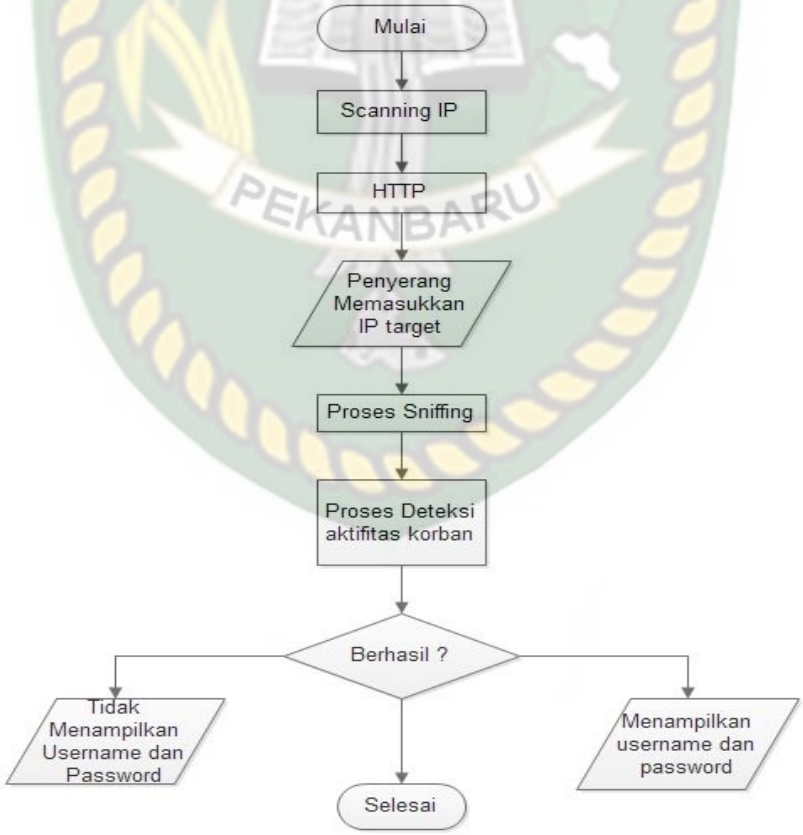
a. Sebelum penulis melakukan tahap awal penelitian, penulis menyiapkan semua ketersedian referensi sebagai literatur seperti jurnal, buku, artikel dengan tujuan sebagai penunjang pelaksanaan penelitian
b. Penulis menyiapkan kebutuhan *software* dan *hardware* yang dibutuhkan dalam pelaksanaan penelitian.
c. Penulis mengaktifkan jaringan *wi-fi* pada laptop dan siap untuk melakukan penyerangan guna untuk mendapatkan informasi penting tentang keamanan suatu *website* yang di*secure* dengan *protocol* https dan *website* yang tidak di*secure* dengan *protocol* http.
d. Setelah melakukan penyerangan ,penulis menganalis membandingkan dua kondisi dari masing-masing website yang di*secure* dan tidak di*secure*
e. Penulis dapat menarik kesimpulan dari perbedaan terhadap bentuk penyerangan dan nantinya dapat memberikan saran dalam mengamankan jaringan kabel LAN dan *wi-fi.*

3.3 Tahapan Tahapan Penyerangan

3.3.1 Tahapan Penyerangan Protocol HTTP

Pada Gambar 3.3 merupakan tahapan dalam melakukan penyerangan menggunakan tools wireshark. Adapun tahapannya sebagai berikut:

1. Penyerang melakukan scannin ip yang tertangkap untuk mengetahui ip target
2. Langkah selanjutnya memasukkan ip terget untuk melakukan metode sniffing
3. Proses selanjutnya yaitu proses untuk mengetahui aktifitas korban dengan menganalisa apakah korban melakukan proses login pada web browser
4. Jika benar maka tools wireshark akan mencapture username dan password. Untuk lebih jelasnya dapat dilihat pada Gambar 3.3.

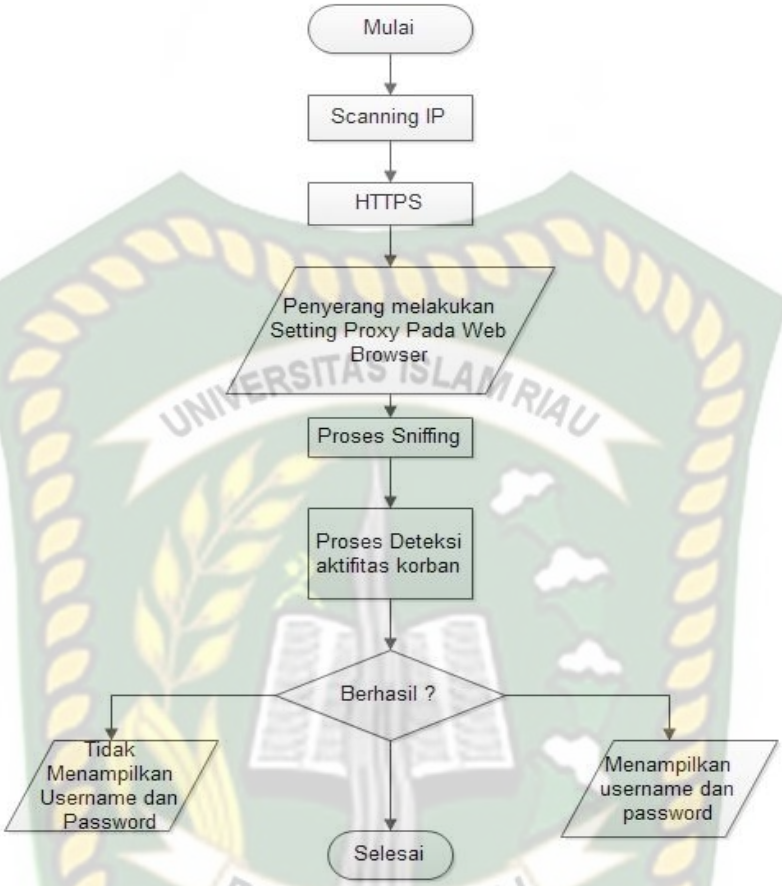


Gambar 3.3 Tahapan Penyerangan Protocol HTTP

3.3.2 Tahapan Penyerangan Protocol HTTPS

Berikut merupakan tahapan dalam metode penyerangan terhadap protocol https yang memiliki keamanan data yang sangat aman. Adapun tahapannya sebagai berikut:

1. Penulis melakukan scanning ip guna untuk mengatahui ip target yang akan disniffing
2. Selanjutnya memasukkan ip target tadi kedalam tools yang penulis pakai, untuk melakukan sniffing
3. Proses selanjutnya yaitu proses untuk mengetahui aktifitas korban dengan menganalisa apakah korban melakukan proses login pada web browser.
4. Jika tidak berhasil penulis akan mencoba melakukan beberapa kali pengujian.
5. Penulis mengatur settingan pada web browser yaitu firefox dengan membuat proxy menjadi localhost.
6. Selanjutnya penulis akan mencoba menggunakan aplikasi *Burpsuite* yang mana dengan aplikasi ini dapat membaca celah dari kerentanan dari sebuah website karena burpsuite memiliku sertifikat yang sudah ditandatangani sendiri yaitu sertifikat CA. dengan adanya sertifikat itu dapat melihat serta membaca lalu lintas jaringan yang menggunakan protocol HTTPS. Untuk lebih jelasnya dapat dilihat pada Gambar 3.4.



Gambar 3.4 Tahapan Penyerangan Protocol HTTPS

BAB IV

HASIL DAN PEMBAHASAN

Analisis ini perlu dilakukan untuk mengetahui bagaimana bentuk dari sebuah penyerangan packet *sniffing* terhadap *protocol-protocol* jaringan yaitu HTTP dan HTTPS. Pada umumnya tingkat keamanan bukan berasal dari *software* maupun *hardware* yang ada melainkan ada peran penting dari pengguna/manusia yang melakukan koneksi terhadap suatu perancangan jaringan tersebut.

Keamanan dari jaringan *wi-fi* yang terkoneksi ke internet pada umumnya rentan terhadap ancaman. Maka dari itu perlu mengevaluasi kembali bagaimana tingkat keamanan *website* terhadap serangan *packet sniffing*.

4.1 Analisis Hasil Penelitian

a. Mengkoneksikan Komputer Pada Jaringan *Wi-fi*

Pada Simulasi ini penulis melakukan koneksi terhadap jaringan lokal *wi-fi*, Penulis melakukan koneksi menggunakan jaringan *wi-fi indihome* ,sehingga komputer terkoneksi dengan *wi-fi*. Hal ini dapat memudahkan penulis dalam melakukan menggunakan komputer sendiri.

b. Analisis Jaringan *Wi-fi*

Percobaan analisis ini dilakukan untuk memastikan aktivitas korban dalam membuka website, Apakah *website* tersebut menggunakan keamanan atau tidak. Hal

ini juga berguna untuk perbandingan bagaimana *respons*e terhadap website yang terkena *packet sniffing* baik dengan Protocol HTTP maupun HTTPS.

c. Packet Sniffing

Penelitian ini dilakukan guna untuk mengetahui suatu informasi penting seperti *account username, password*, akses DNS yang akan dituju dan informasi lainnya. Pada penelitian ini penulis ingin memberikan gambaran bagaimana simulasi dari penyerangan *website* yang menggunakan keamanan maupun tidak. Dan hal ini dilakukan agar penyerang dapat melakukan akses internet secara tidak sah untuk memberikan keuntungan pribadi tetapi dapat merugikan bagi orang lain karena sama-sama terhubung pada jaringan lokal *wi-fi.*

Pada penelitian ini penyerang berhasil mendapatkan *username* dan *password* korban. Percobaan kali ini *wi-fi* itu hanya sebagai gerbangnya saja, penulis akan melakukan penyadapan terhadap komputer yang terkoneksi internet yang kebetulan melakukan *autentifikasi* login pada suatu *website* yang menggunakan *protocol* HTTP dan HTTPS. Dengan demikian penulis mendapatkan suatu pernyataan bagaimana kondisi dari *website* tanpa keamanan yang menerima serangan *packet sniffing* dan kondisi dari *website* dengan keamanan yang menerima serangan *packet sniffing* tersebut.

d. Kali Linux

Pada penelitian ini penulis memilih menggunakan sistem operasi *kali linux* karena untuk melakukan serangan terhadap website dan situs-situs lainnya dan keperluan dalam *penetration test*. sangat dibutuhkan sistem operasi yang dapat

memuat semua aplikasi dalam melakukan teknik hacking. Pada *kali linux* banyak terdapat aplikasi security yang terkenal yaitu *Nmap, Aircrack-ng, Kismet, Wireshark, Metasploit Framework, Burp suite, John the Ripper, Social Engineering Toolkit, Maltego, Ettercap, OWASP ZAP.*

e. *Certificate Authority* (CA)

Pada *Secure Socket Layer* (SSL) tentunya memiliki peranan yang sangat penting salah satunya adalah melakukan *validasi* terhadap identitas *server* dan memastikan *client* melakukan komunikasi pertukaran data dengan *server* yang benar. Agar *server* tidak dipalsukan maka dibutuhkan *Certificate Authority (CA)* yang memberikan client jaminan bahwa gembok (*public-key)* memiliki *certificate* dari pihak ketiga.

4.2 Skenario Penyerangan Sniffing

Skenario penyerang dalam melakukan penyerangan *packet sniffing* yaitu dengan membagikan 2 target. Target pertama yaitu website yang tidak menggunakan *security* dan target kedua website yang menggunakan *security*. Penulis akan melakukan penyerangan terhadap 2 *protocol* yaitu HTTP dan HTTPS lalu membandingkan dua kodisi bagaimana *response* terhadap serangan *packet sniffing* yang penulis lakukan.

4.2.1 Penyerangan Sniffing Website HTTP

a. Berikut langkah-langkah terhadap target 1 yaitu protocol HTTP dari skenario yang dilakukan:

1. Penyerang memastikan target berada didalam satu jaringan yang sama dengan penyerang
2. Penyerang mencari suatu website tanpa keamanan yang menggunakan protocol HTTP yang mana tidak memiliki sistem keamanan yang terenkripsi.
3. Selanjutnya penyerang melakukan proses login pada sistem website tersebut.
4. Proses login yang dicoba yaitu menggunakan *username* dan *password* yang salah karena penyerang ingin mengetahui tingkat keamanan terhadap website tersebut.
5. Penyerang berhasil mengetahui aktivitas dari target dan software *wireshark* dapat merekam beberapa *packet list* yang masuk.

b. Berdasarkan website HTTP yang akan diserang, ada beberapa website tanpa keamanan yang penulis ingin coba. Dapat dilihat pada Tabel 4.1 Sebagai berikut:

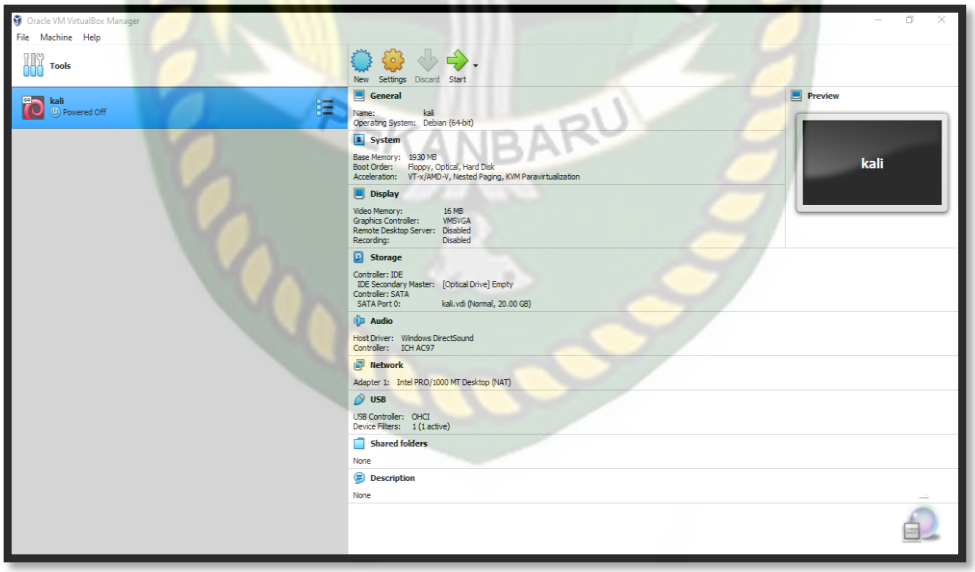
Tabel 4.1 Beberapa website HTTP yang diserang

No	Nama Website	Link Website
1	Open Jurnal System Halu Oleo University(UHO)	http://ojs.uho.ac.id/
2	Portal mahasiswa UMMY	http://portalmhs.ummy.ac.id/

3	EJOURNAL-STMIK TIME	http://www.ejournal.stmik-time.ac.id/
4	E-Administrasi FEB UNRI	http://febunri.id/
5	Jurnal UNPAD	http://jurnal.unpad.ac.id/

c. Hasil Penyerangan skenario dari website HTTP

1. Pada penelitian ini penulis menggunakan *kali linux* dengan virtualbox. Sebelumnya penulis sudah melakukan instalasi *Kali Linux*, Setelah berhasil menginstall barulah *Kali Linux* dapat dioperasikan seperti pada gambar 4.1.

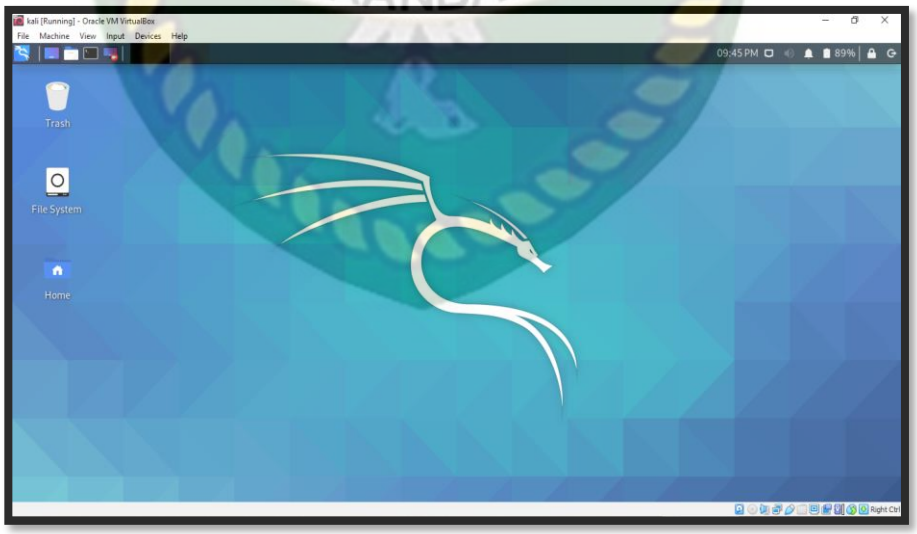


Gambar 4.1 Tampilan VirtualBox

2. Penulis Membuat *Virtual Machine* dengan nama kali lalu mengkonfigurasikan *Operating System (OS) Kali Linux*.
3. Selanjutnya penulis menekan tombol *Log in* untuk menjalankan *Operating System (OS) Kali Linux*. Seperti Gambar 4.2.

Gambar 4.2 Tampilan *Login Kali Linux*

4. Penulis Memasukkan *Username* kali dan *password* kali. Sesuai dengan yang diset pada saat menginstalasi *Operating System Kali Linux* Pada Gambar 4.3.



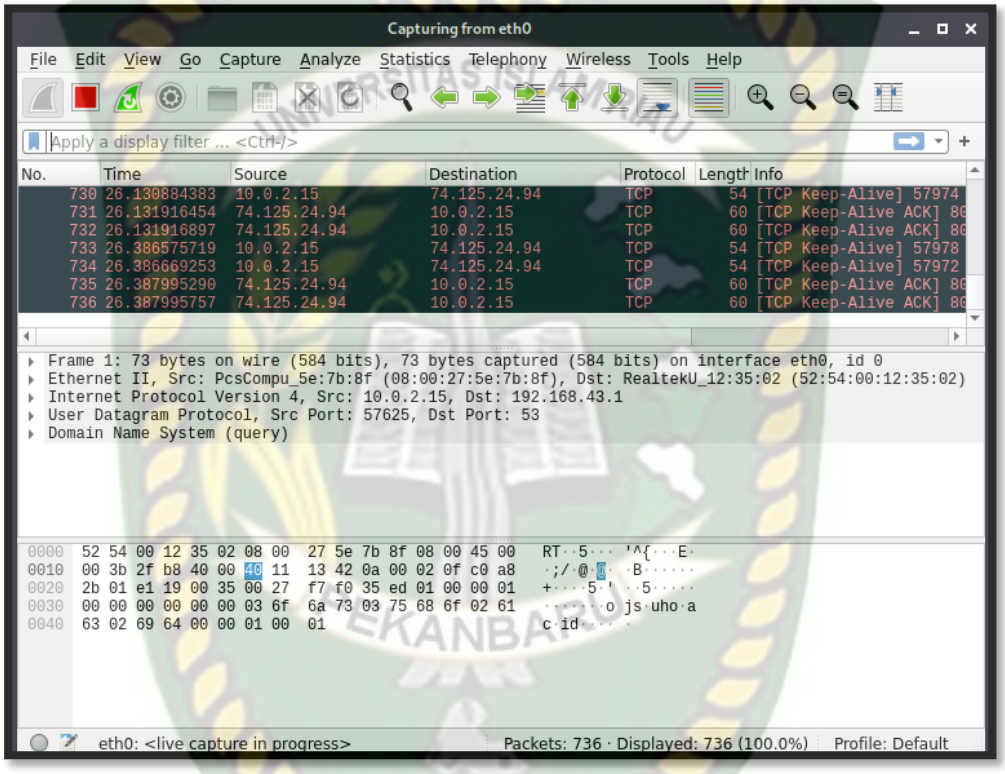
Gambar 4.3 Tampilan Dekstop *Kali Linux*

5. Selanjutnya penulis membuka *software wireshark.* Langkah pertama penyerangan adalah pilih *interface* jaringan yang diinginkan.Terdapat

beberapa *interface* yang bertugas untuk meng*capture packet.* Pada tahap ini penulis memilih *interface eth0.* Seperti gambar 4.4.

Gambar 4.4 Tampilan *Interface* Pada *wireshark*

6. Setelah melakukan start pada *interface* yang sudah dipilih tadi, maka dengan otomatis tools pada *wireshark* berjalan dan menangkap hasil *capture packet* dari *web browser* yang telah dibuka. Seperti pada Gambar 4.5.



Gambar 4.5 Proses *Capture* Pada *interface eth0*

7. Dari beberapa *website* HTTP yang ingin dilakukan simulasi percobaan penyerangan *packet sniffing* pada Tabel 4.1. Maka penulis hanya memilih satu *website* yang akan ditampilkan dalam laporan. *Website* HTTP yang akan dijelaskan dalam pembahasan kali ini yaitu *website* jurnal unpad.

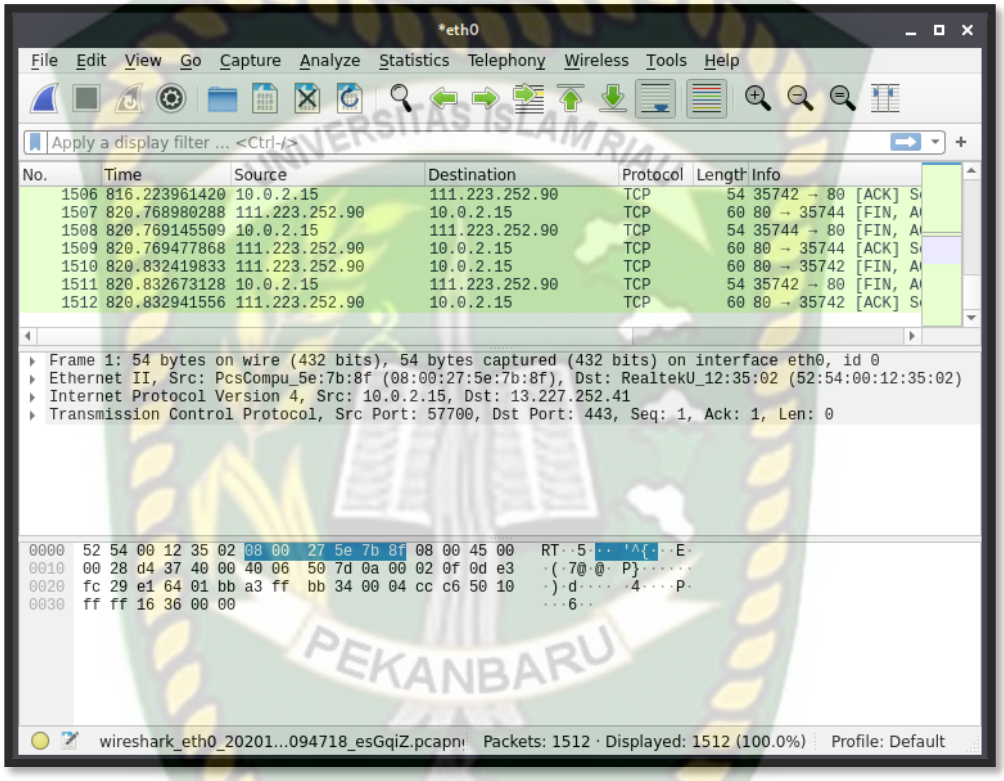
a. Penyerangan *Website* Jurnal UNPAD

Pada tampilan login *website* unpad, penyerang mencoba melakukan serangan *packet sniffing* terhadap *website* jurnal Universitas Padjajaran (UNPAD). Pada tahap ini penyerang melakukan proses login menginput username dan password yang salah dengan tujuan ingin mencoba kerentanan terhadap website tersebut. Seperti pada gambar 4.6.

Gambar 4.6 Tampilan Login Website Universitas Padjajaran (UNPAD)

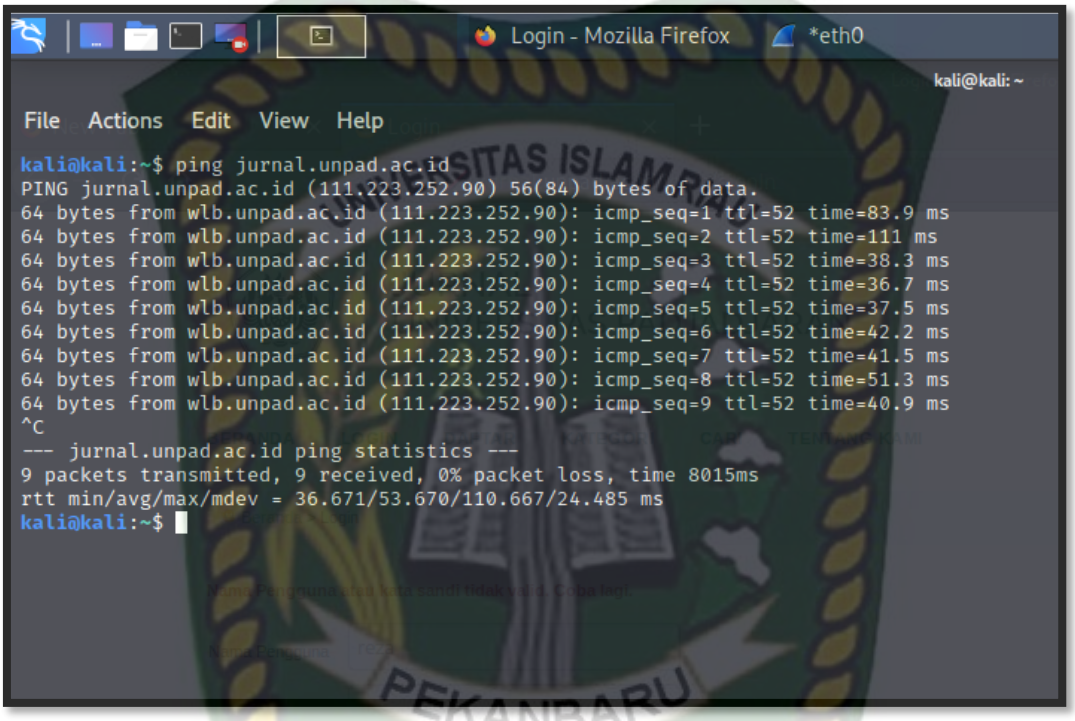
Selanjutnya proses *capture packet* akan terjadi, lalu penyerang menekan stop untuk menghentikan proses *capturing packet*. Pada tampilan *capturing packet* dapat dilihat beberapa informasi seperti *packet list* dan *packet byte.* Pada *packet list* dapat dilihat beberapa informasi *packet* yang terurut secara *numerik* informasi dari *packet*

list yaitu waktu, sumber paket, ip tujuan, protocol yang digunakan,panjang peket dan informasi lebih lanjut tentang paket sedangkan pada *packet byte* hasil paket ditampilkan dalam bilangan *Hexadecimal* dan *ASCII*, Seperti pada gambar 4.7.



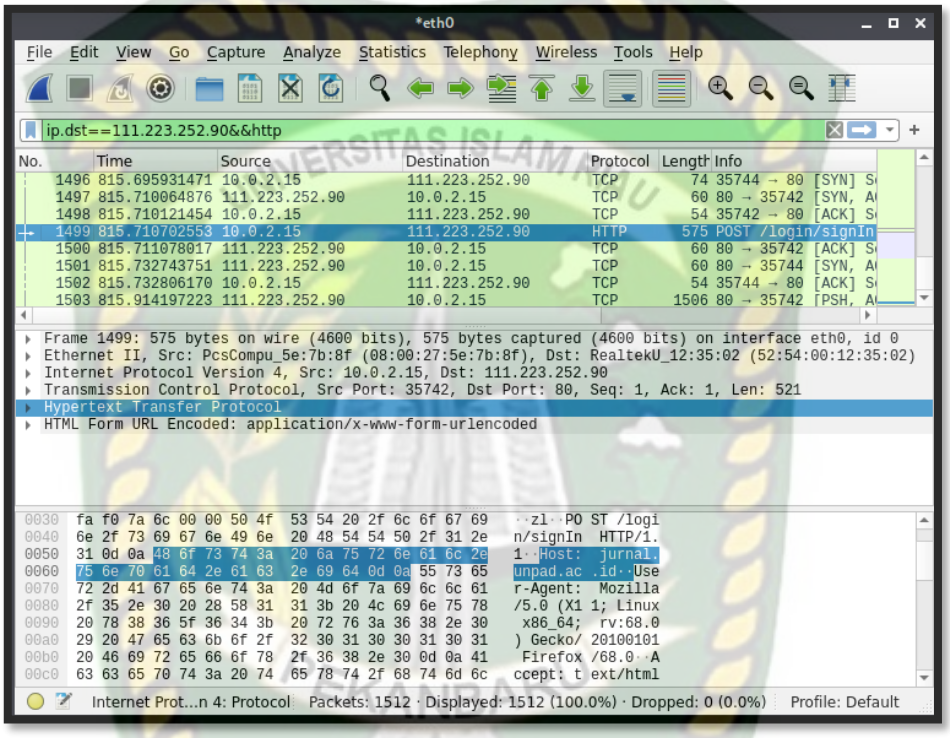
Gambar 4.7 Proses Stop *Capture Packet*

Pada proses ini dilakukan pencarian *ip address* atau alamat website pada terminal jika tidak ditemukan *ip address* pada *capture packet* yang tertangkap. Seperti pada gambar 4.8.



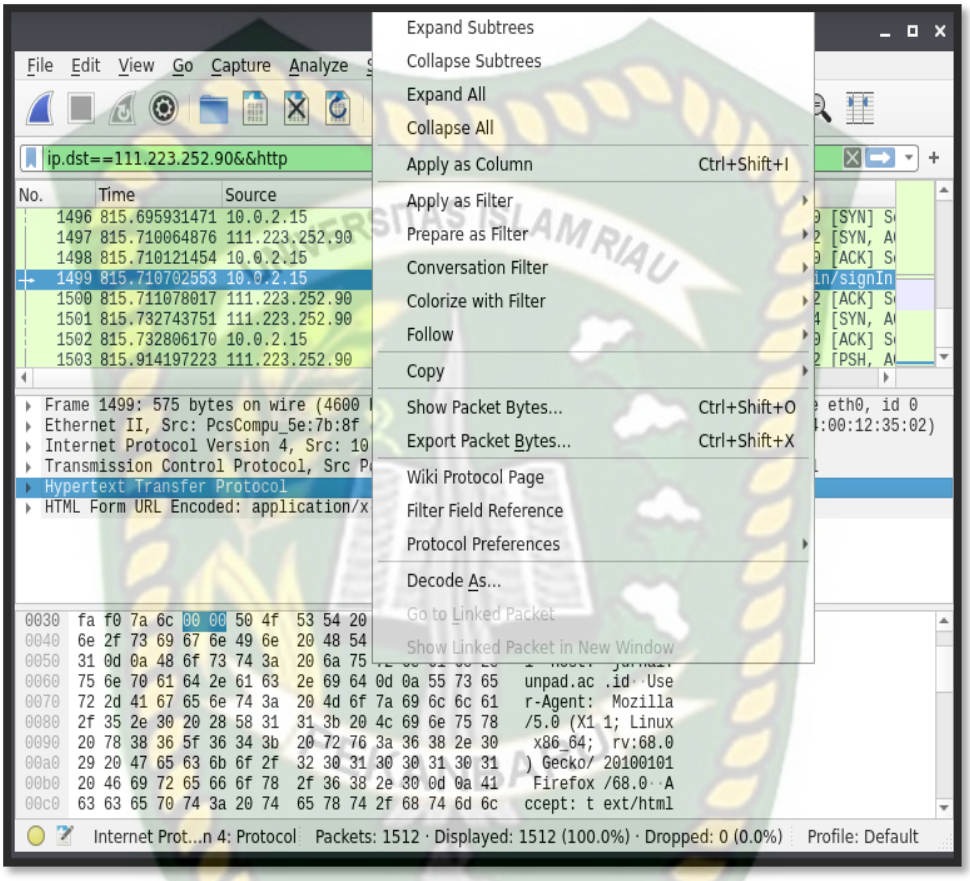
Gambar 4.8 Proses Mengetahui IP Website Pada Terminal

Pada proses pencarian *packet* penyerang memasukkan perintah pada *display filter* untuk menampilkan parameter login pada *packet* yang *tercapture*.Seperi pada gambar 4.9.



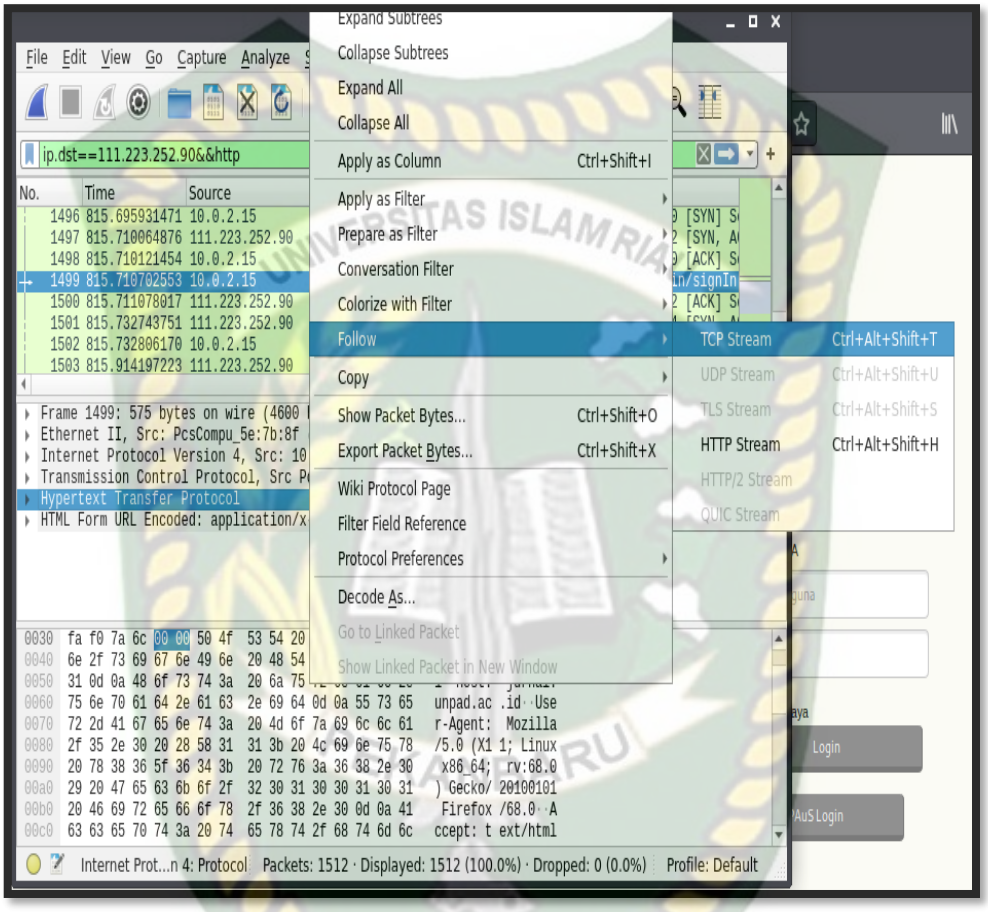
Gambar 4.9 Proses Pencarian *Packet* Pada Display Filter

Selanjutnya pada proses ini penyerang melakukan klik kanan pada *Hypertext Transfer Protocol (HTTP).* Seperti pada gambar 4.10.



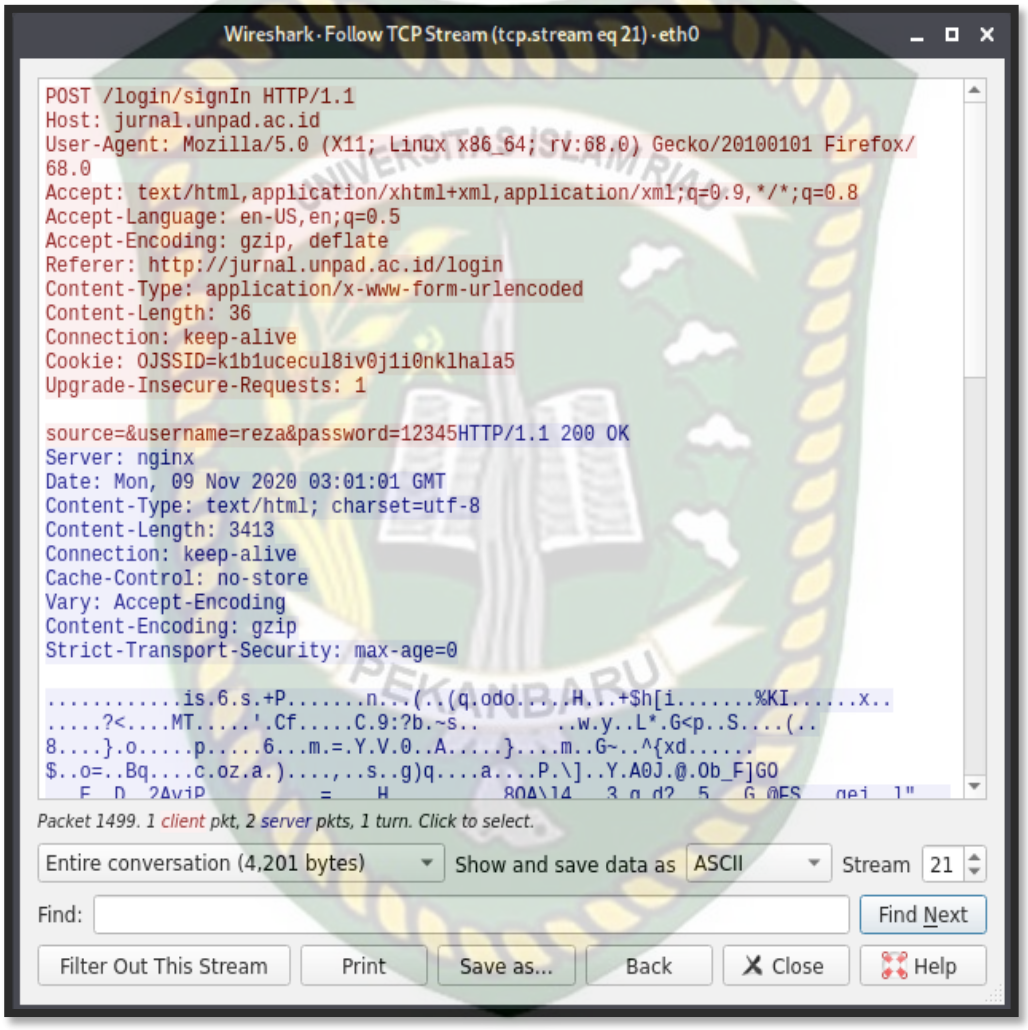
Gambar 4.10 Proses Follow Pada HTTP

Pada proses ini setelah melakukan klik kanan pada *Hypertext Transfer Protocol (HTTP)* selanjutnya pilih *Follow –TCP Stream*. Sepeti pada gambar 4.11.



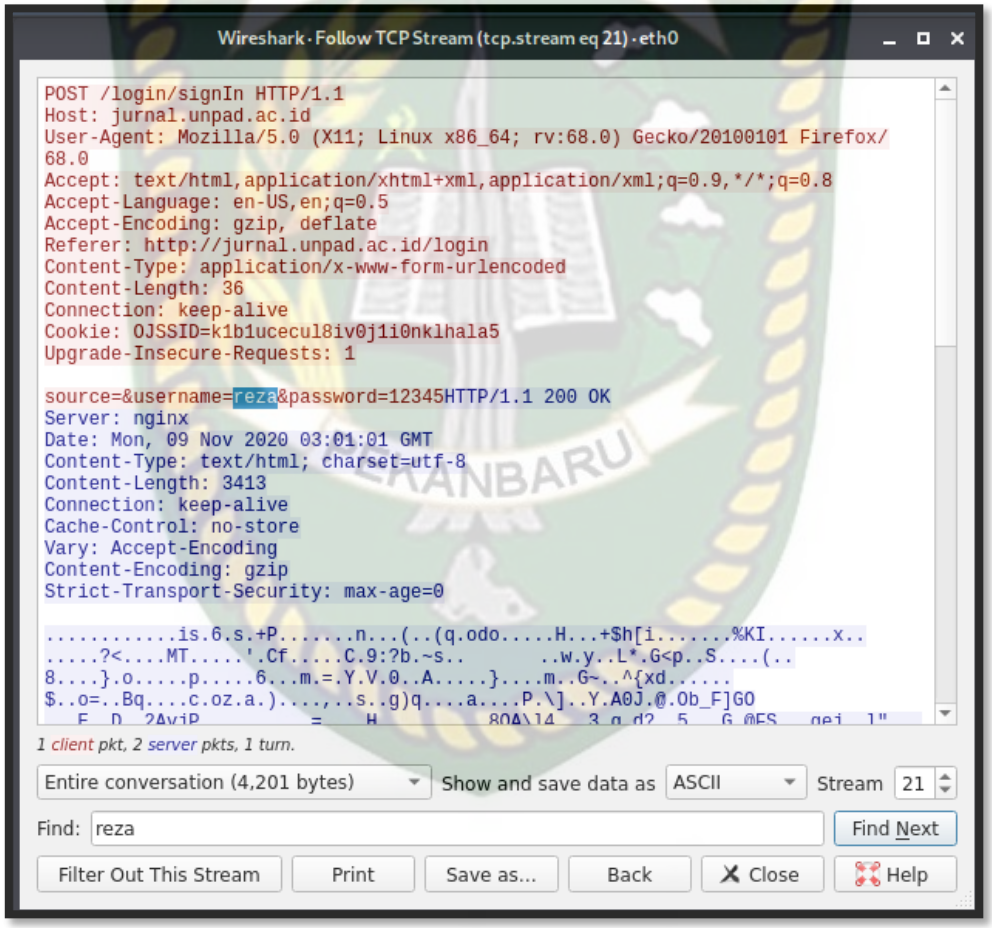
Gambar 4.11 Proses Follow TCP Stream

Berikut adalah hasil tampilan setelah melakukan proses *follow TCP stream*, maka dapat dilihat arsitektur web pada informasi *packet* data. Seperti pada gambar 4.12.



Gambar 4.12 Hasil Tampilan *TCP Stream*

Pada proses ini setelah melihat tampilan informasi packet data maka, tahap selanjutnya adalah melakukan *find* next untuk mencari kata dari username yang di tuju. Dan dapat disimpulkan bahwa penyerangan website tanpa keamanan HTTP dapat dengan mudah terbaca oleh t*ools wireshark.* Hasil penyerangan berhasil, *tools wireshark* mampu menampilkan username reza dan password 12345. Seperti Pada Gambar 4.13.



Gambar 4.13 Hasil Find Next Pada TCP Stream

Pada hasil *capture packet tools wireshark* dapat membaca data API dari website yang terdiri dari hostnya adalah jurnal.unpad.ac.id, length atau panjang.

paket adalah 36. Dan juga *administrator* dapat mengetahui bahwa paket yang tertangkap merupakan hasil dari serangan packet sniffing dari sebuah kode dari packet list yaitu *Reassembled* TCP Data.

4.2.2 Skenario Penyerangan Website HTTPS

a. Berikut langkah-langkah terhadap target 2 yaitu protocol HTTPS dari skenario yang dilakukan:

1. Penyerang menyiapkan beberapa website dengan protocol HTTPS guna untuk menguji bagaimana respons website terhadap penyerangan *sniffing* dan *spoofing*, guna untuk menguji keamanan dari sebuah *website.*
2. Selanjutnya penyerang membuka aplikasi *burpsuite,* pada tahap ini penyerang mengatur *proxy* pada settingan di *browser* guna untuk membuat burpsuite bertindak sebagai *proxy*.
3. Pada tools burpsuite penyerang mematikan *intercept is on* menjadi *off* sehingga *website* dapat dibuka pada browser .penyerang akan melakukan serangan untuk mencari kerentanan dari suatu website.
4. Penyerang melakukan proses login terhadap *website*.
5. Aplikasi burpsuite memonitor setiap *request* maupun *respon*se dari *web browser* dengan *server.*
6. Penyerang berhasil menemukan *username* dan *password* target.

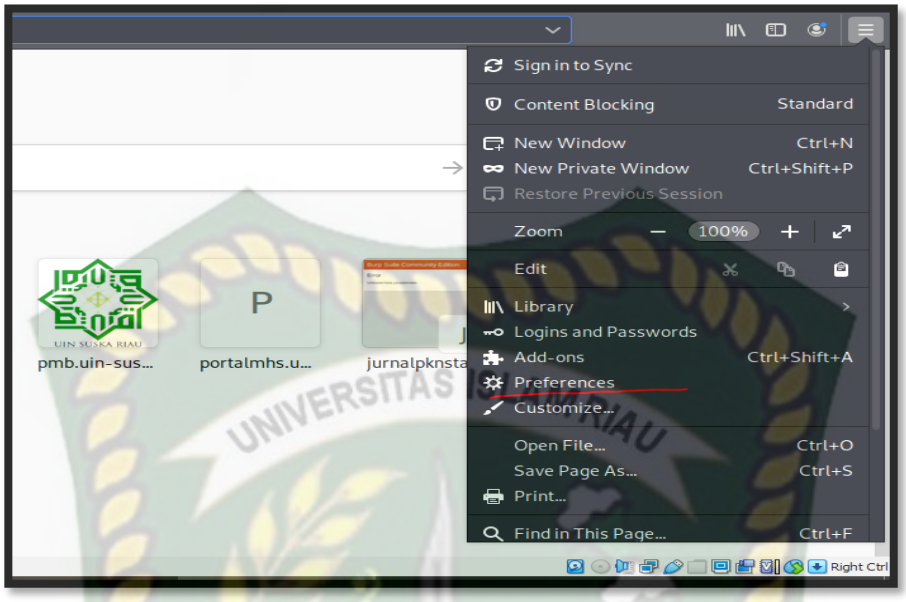
b. Berikut beberapa website HTTPS yang penyerang ingin mencari kerentanan dari tingkat keamanan *website*:

Tabel 4.2 Beberapa Website HTTPS yang akan diserang

No	Nama Website	Link Website
1	Foto Alumni UIR	https://foto.alumni.uir.ac.id/
2	Instagram	https://www.instagram.com/
3	Portal Akademik UNRI	https://portal.unri.ac.id/
4	Facebook	https://facebook.com/
5	Sistem Informasi Akademik(SIKAD)	https://sikad.uir.ac.id/

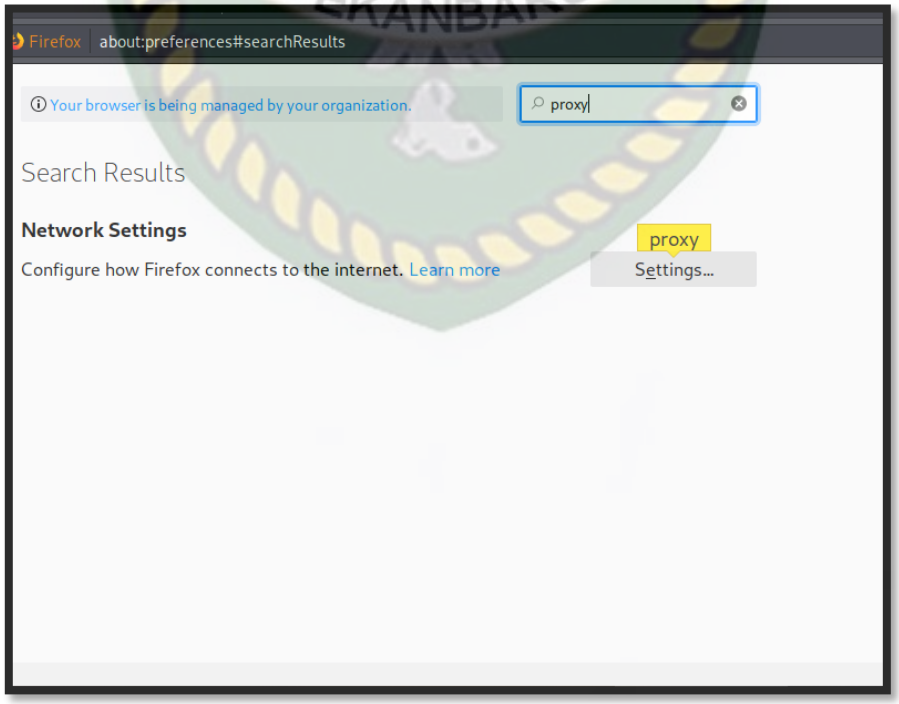
c. Hasil Skenario Penyerangan Website HTTPS

1. Pertama sebelum penyerang membuka aplikasi *burpsuite*, penyerang mengatur proxy yang tersedia pada browser guna untuk membuat burpsuite bertindak sebagai *proxy*. Pada Tahap ini pilih settingan pada browser pilih *preferences*. Seperti gambar 4.14.



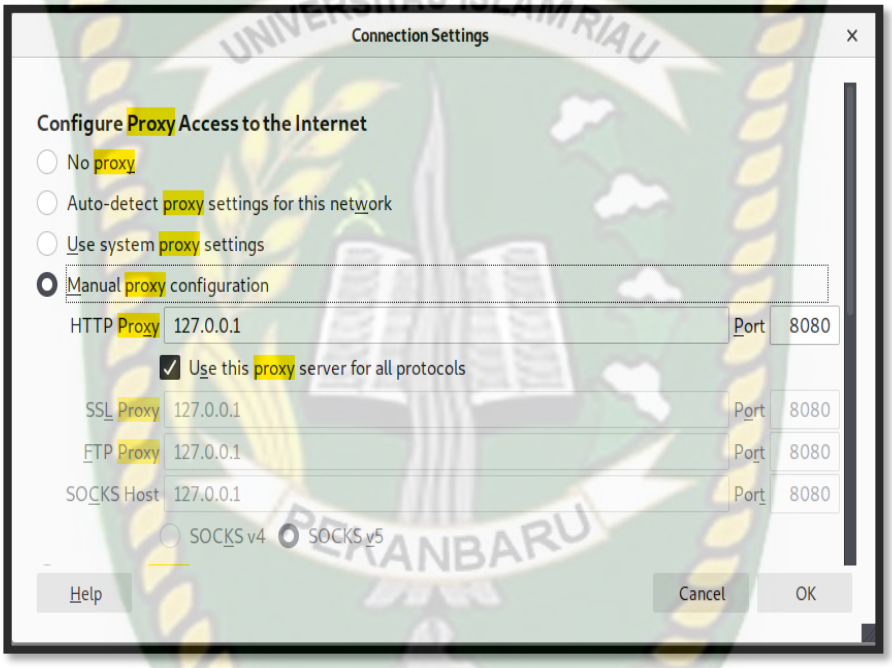
Gambar 4.14 Tahap Pertama Mengatur Proxy

2. Selanjutnya memilih *Proxy* dengan mengetik *proxy* pada kolom pencarian. Seperti pada gambar 4.15.



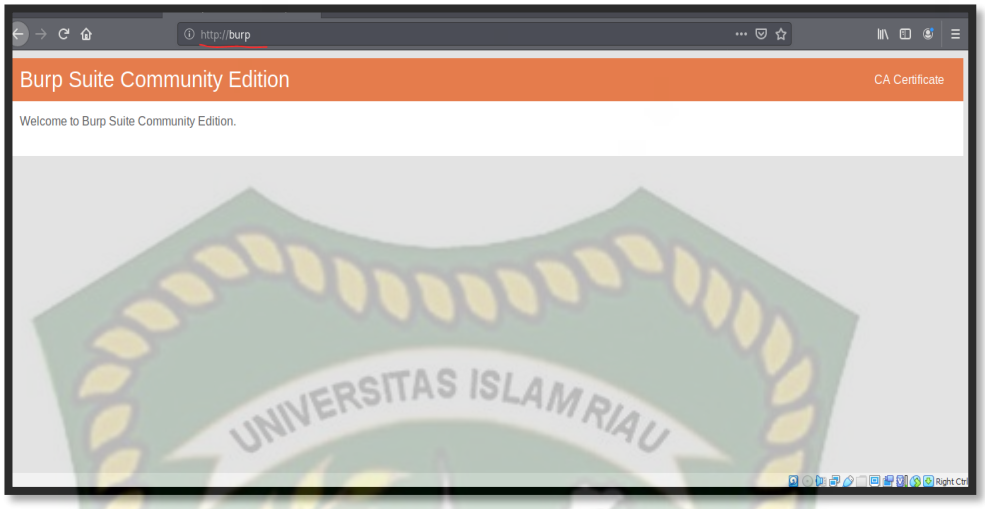
Gambar 4.15 Tahap Kedua Mengatur Proxy

3. Pada tahap ketiga penyerang memilih konfigurasi proxy secara manual dengan meenginputkan HTTP Proxy 127.0.0.1 dengan port 8080 dan juga bisa mengatur HTTP Proxy menjadi localhost tetapi penyerang memilih HTTP Proxy 127.0.0.1 supaya proxy berjalan dengan lancar. Seperti pada gambar 4.16.



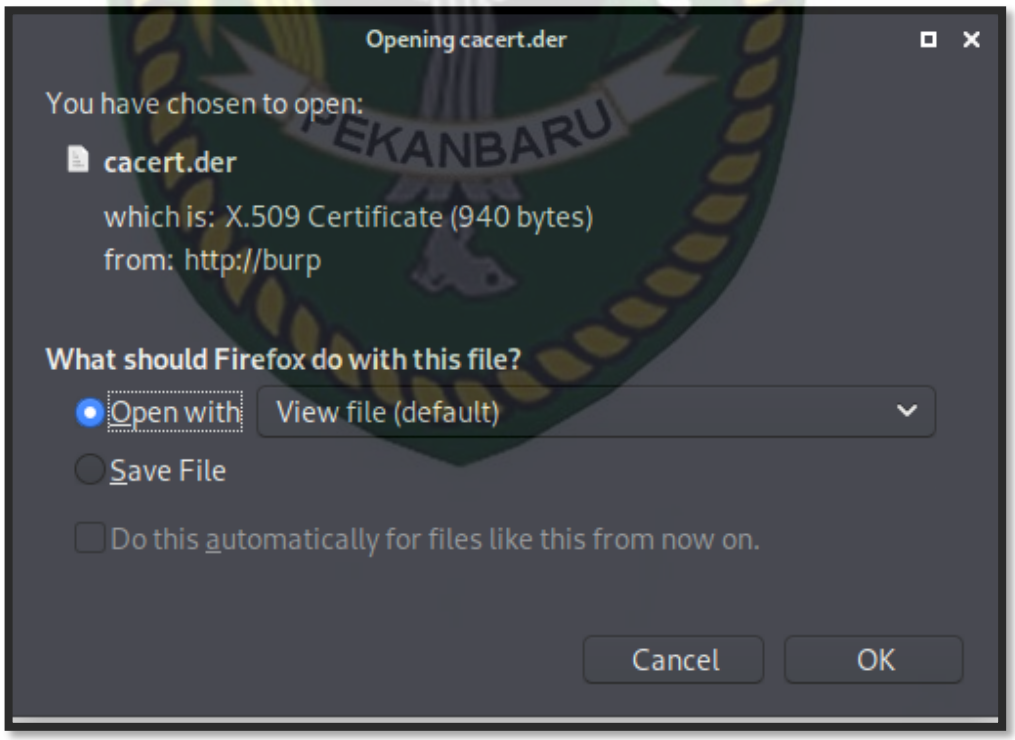
Gambar 4.16 Tahap Ketiga Mengatur Proxy

4. Dan apabila proxy tidak dapat berjalan maka langkah selanjutnya dengan mendownload kembali sertifikat CA yang telah disediakan oleh *tools burpsuite* ini. Ketikkan link http://burp pada url browser. Seperti pada gambar 4.17.



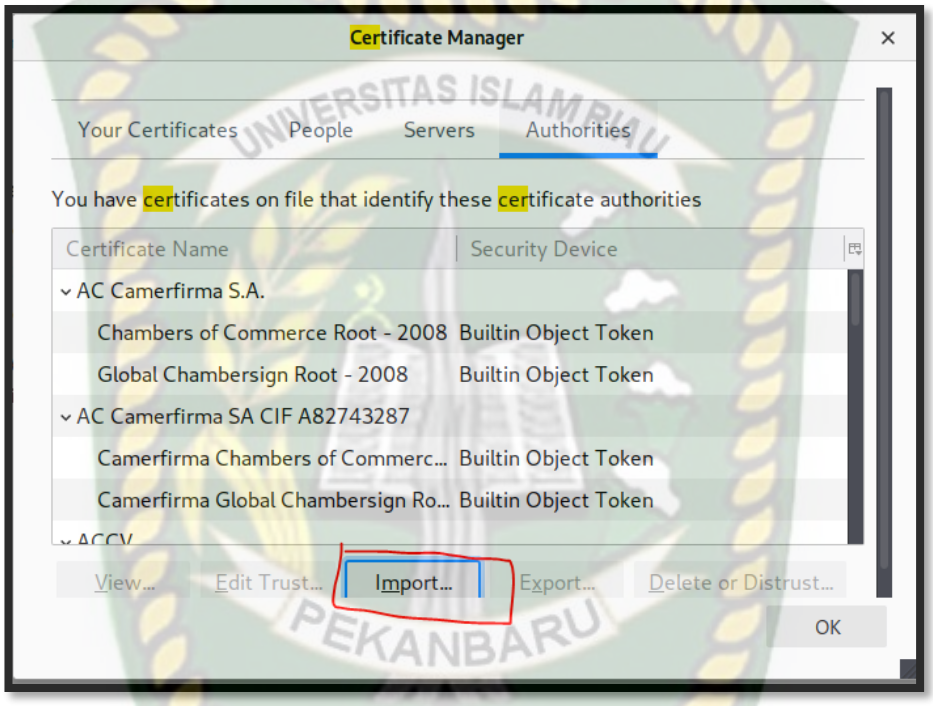
Gambar 4.17 Tahap Pertama Mengatur CA Certificate

5. Selanjutnya pilih CA Certificate di pojok kanan maka akan muncul tampilan download cacert.der lalu pilih save file. Seperti pada gambar 4.18.



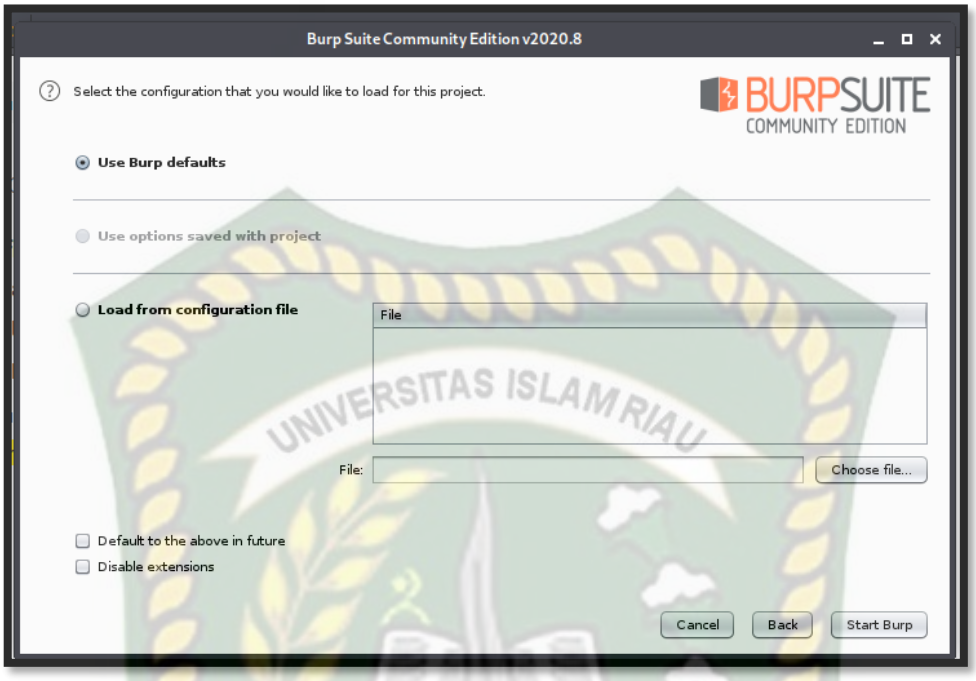
Gambar 4.18 Tahap Kedua Mengatur CA Certificate

6. Selanjutnya setelah download selesai , tahap selanjutnya ialah melakukan import certificate yang telah didownload dengan cara pilih preferences-certificate pada pengaturan browser.lalu pilih import.Seperti pada gambar 4.19.



Gambar 4.19 Tahap Ketiga Mengatur CA Certificate

7. Jika sudah melakukan import CA Certificate maka langsung saja menjalankan *burpsuite* dengan cara klik start *burpuite*.



Gambar 4.20 Menjalankan Burpsuite

8. Dari berbagai website HTTPS yang akan penyerang lakukan , Penyerang hanya memilih satu website yang akan ditampilkan pada laporan yaitu website SIKAD UIR.

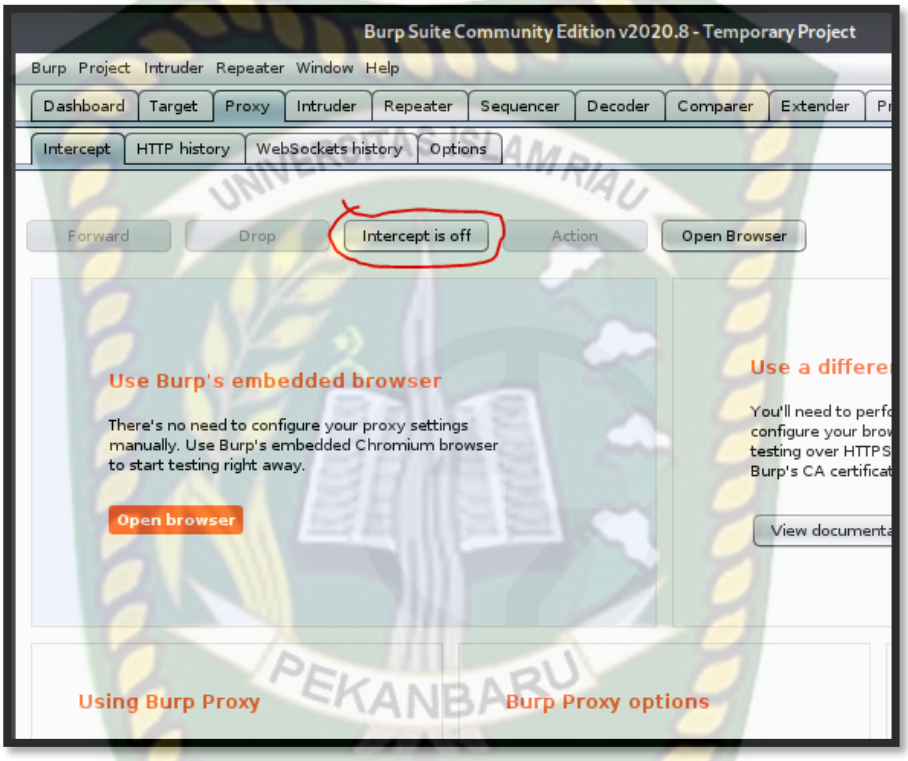
a. Penyerangan Website Sistem Informasi Akademik (SIKAD) Universitas Islam Riau.

Pada target pertama dalam penyerangan website HTTPS, penyerang melakukan penyerangan terhadap website yang sudah terenkripsi dan mencoba apakah dapat menembus keamanan yang dimiliki website tersebut dan apakah terdapat kerentanan sehingga pesan *request* dan *respons* dari browser dan server dapat diketahui oleh aplikasi *burpsuite* ini. Pada tahap ini penyerang melakukan proses login dengan memasukkan *account* palsu untuk melakukan *testing* apakah *burpsuite* dapat mendapatkan celah dari website terenkripsi tersebut.

Dikerenakan pada aplikasi *burpsuite* ini sudah mendukung sertifikat yang sudah ditandatangani sendiri bisa disebut *private key*, ada kemungkinan *burpsuite* dapat melihat isi paket dari pesan yang disampaikan browser ke server.

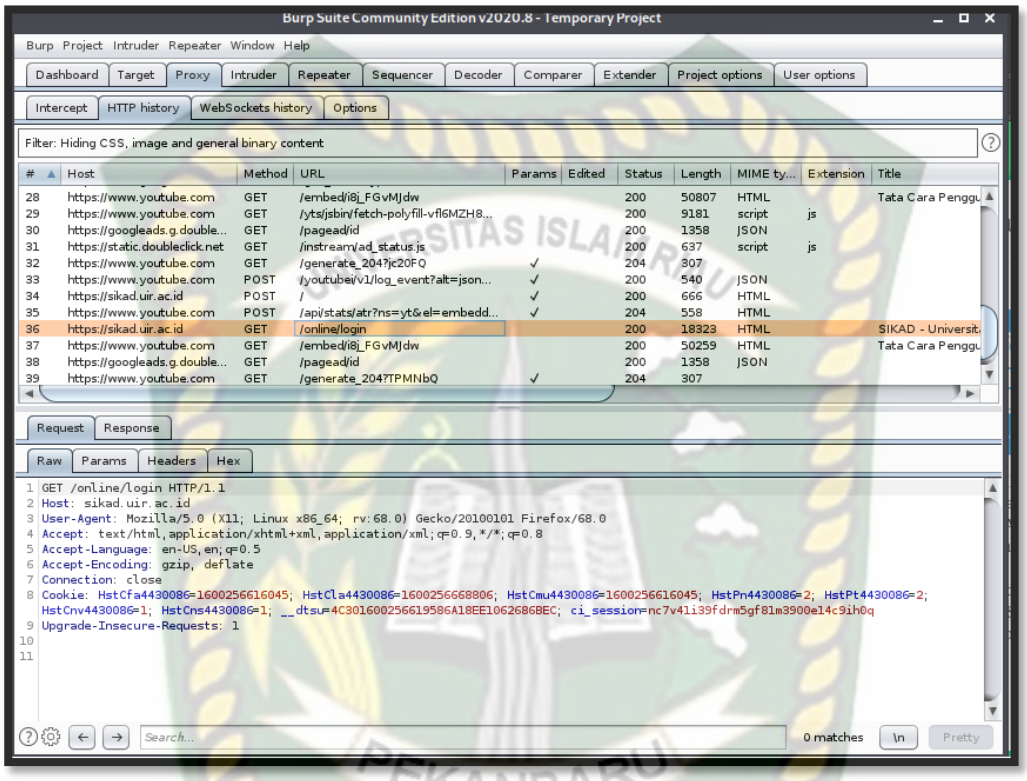
Gambar 4.21 Proses Login Website SIKAD

Selanjutnya apabila *intercept* pada menu *proxy* ini dalam status *on* maka browser tidak dapat berjalan, penyerang perlu menonaktifkan *intercept* menjadi *off* sehingga browser dapat berjalan. Seperti Gambar 4.22.



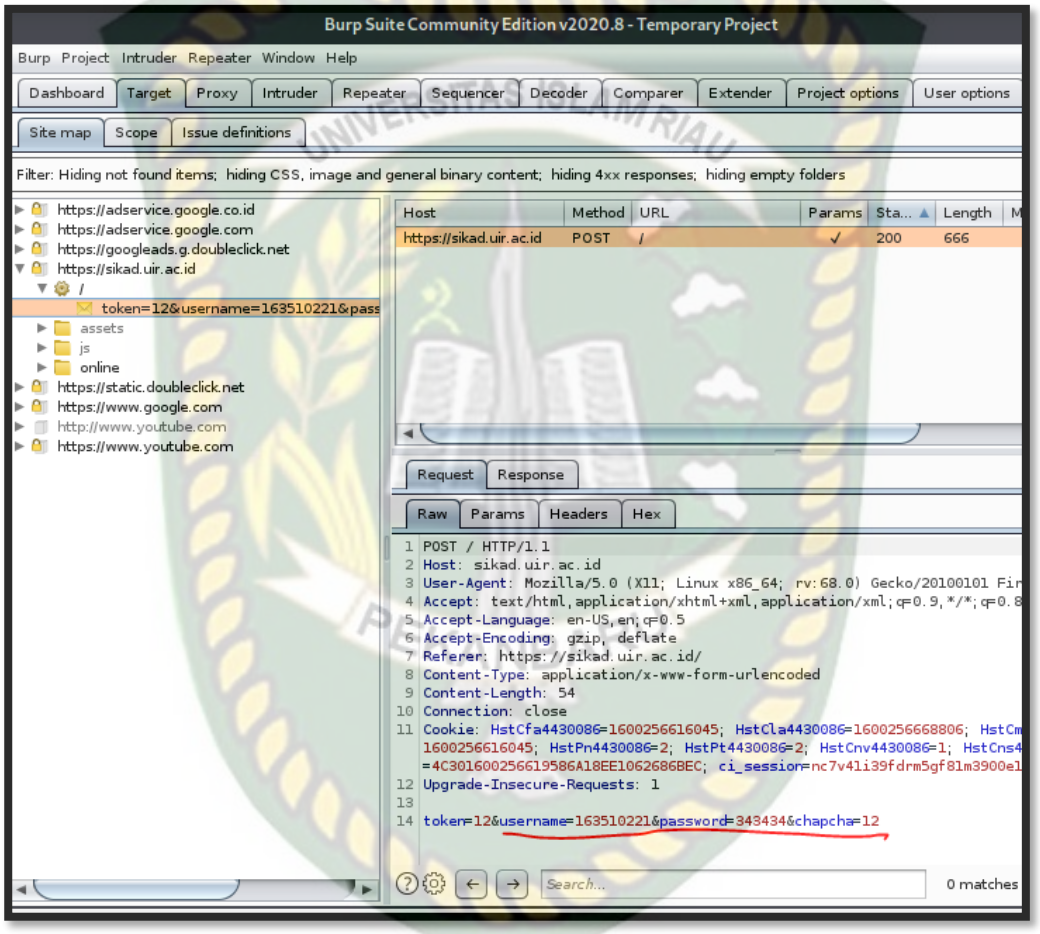
Gambar 4.22 Tahap Mengatur Intercept

Pada tampilan *capture packet* pada http history dapat dilihat *detail packet* yang tertangkap dan beberapa situs *website*. Seperti gambar 4.23.



Gambar 4.23 Proses Capture Packet pada HTTP History

Pada tahap ini tampilan site map juga dapat menampilkan beberapa website yang tertangkap juga dapat menampilkan arsitruktur dari data API-nya sehingga didapatkan hasil token berupa username 163510221 dan password 343434 dan nilai chapcha 12. Seperti gambar 4.24.



Gambar 4.24 Tampilan Site Map

Pada hasil site map tools burpsuite mampu menampilkan pesan request dari web browser. Tampilan site map dapat membaca data APInya yang terdiri dari hostnya adalah sikad.uir.ac.id dan juga content-length 54.

Tabel 4.3 Hasil Capture Packet Menggunakan *Burpsuite*

Host	Method	Url	Status	Length	IP	Cookies	Time
https://sikad.uir.ac.id	GET	/online/login	200	18323	103.140.54.59	Ci_session=nc7	14 : 37 : 33
https://youtube.com	GET	/embed/i8j_FGvMjdw	200	50259	172.217.194.91	-	14 : 37 : 34

Tabel 4.4 Hasil Capture Packet Menggunakan *Wireshark*

No	Time	Source	Destination	Protocol	Lenghth	Info
1499	815. 710702553	**10.0.2.15**	**111.223.252.90**	**HTTP**	**575**	**POST /login/signIn**
1500	**815. 711078017**	**111.223.252.90**	**10.0.2.15**	**TCP**	**60**	**80 – 35742 [ACK]**

Tabel 4.5 Perbedaan Penyerangan antara *Burpsuite* dan *Wireshark*

Burpsuite	**Wireshark**
• Menyiapkan proxy yang memungkinkan penyerang dapat menguji arsitektur web	• Memilih Interface pada menu capture interface yang mana akan mencapture paket yang lewat
• Melakukan *monitoring* pada menu *proxy* dan *intercept* ,apabila *intercept* dalam keadaan on maka setiap request dan response daripada data API-nya akan terlihat jelas ,serta penyerang dapat memanipulasi dan mengubah data request pada arsitektur web nya.	• Setelah memilih interface dan memulai wireshark maka pada tampilan *wireshark* akan menampilkan tangkapan paket yang lewat pada tampilan *wireshark* saat menangkap paket terbagi menjadi 3 bagian yaitu: bagian 1, Terdapat Detail Informasi dari waktu mulai ,*IP Source, IP Destination, Protocol* yang digunakan, panjang paket, dan informasi tentang paket secara umum. bagian 2, pada bagian tengah menampilkan detail informasi yang terbagi menjadi

	5 lapisan yaitu lapisan fisik, data link,network, transport dan aplikasi. Bagian 3, *wireshrak* menampilkan paket dalam format hexadecimal dan ASCII.

4.3 Perbedaan Analisis Hasil Capture Antara Protocol HTTP dan HTTPS

Pada dasarnya tingkat keamanan dalam mengamankan proses *transimisi packet* data masih lebih aman HTTPS dikarenakan adanya proses enkripsi pesan yang diterima oleh tools *wireshark* dan kenapa pada *burpsuite* dapat membaca pesan request maupun reponse karena aplikasi burpsuite telah didukung dengan adanya *CA Certificate* yang bertindak sebagai pihak ketiga yang terpercaya yang memungkinkan dapat menandatangani sertifikat yang digunakan protocol HTTPS.

4.4 Solusi dan Tahap Selanjutnya Saat Menghadapi Serangan Packet Sniffing

Setelah melakukan beberapa penyerangan dari skenario, langkah selanjutnya adalah meningkatkan keamanan *website* saat pengguna internet melakukan akses secara ilegal. Ada beberapa solusi untuk mencegah dari serangan packet *sniffing* ,Untuk dapat mengaanalisis suatu keamanan jaringan *wi-fi* sebagai berikut:

1. Dengan Mengganti Protocol HTTP menjadi HTTPS

   Hal yang dilakukan dari tindakan *snifing* adalah dengan mengganti *protocol* HTTP menjadi HTTPS, karena pada dasarnya HTTP

(Hypertext Transfer protocol) dapat mengirimkan paket data tanpa adanya enkripsi sehingga dapat dengan mudah terkena tindakan *sniffing* maka dengan HTTPS (*Hypertext Transfer protocol security)* banyak memiliki kelebihan seperti keamanan dalam transmisi data serta keamanan data karena telah terenkripsi dan pada saat ini *protocol* HTTPS masih dipercaya.

2. Binding IP dan Mac Address

   Hal yang dilakukan untuk mengatasi *ARP Spoofing* dalam jaringan ialah dengan *Binding IP* dan *Mac Address.* Dengan mengikuti langkah ini dapat bekerja dengan cara mendaftarkan setiap pengguna yang terkoneksi dengan jaringan *gateway.* Karena setiap pengguna diikat dengan *ip address* dan *mac addressnya* sehingga gateway tidak salah dalam mengirimkan pesan atau *packet* kepada pengguna.

3. Gunakan keamanan WPA2-PSK (*Wi-fi protected Acces- Pre Shared Key*)

   Dengan metode ini dapat mengamankan jaringan *wi-fi* karena ini merupakan *security* terbaru yang disediakan untuk jaringan *wireless*.jika ada yang ingin melakukan *cracking* akan memakan waktu yang cukup lama.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pembahasan yang sudah penulis lakukan dengan penelitian yang berjudul "Analisis Keamanan Fasilitas Jaringan *Wi-fi* Terhadap Serangan Packet Sniffing pada Protocol HTTP dan HTTPS, dengan manganalisis kedua protocol tersebut masih perlu adanya evaluasi dalam meningkatkan keamanan, Maka hasil penelitian ini dapat disimpulkan sebagai berikut :

1. Penyerangan packet sniffing menggunakan metode MITM (*Man in The Middle Attack*) antara *web browser* dengan *web server* dapat memonitoring hasil aktivitas pertukaran data yang lewat dan dapat menampilkan *username* dan *password* saat melakukan autentifikasi login pada target. Dengan menggunakan *tools* dalam mencari kerentanan bagaimana pesan *request* dan *response* dapat terbaca oleh tools *wireshark* dan *burpsuite.*
2. Kondisi dari *website* dengan *protocol* HTTPS dan HTTP saat terkena serangan *packet sniffing* ,yaitu *tools burpsuite* dapat merekam jejak dari aktivitas target saat mengakses *website* yang sudah terenkripsi dikarenakan tools ini memiliki hak istimewa karena memiliki sertifikat CA yang memungkinkan *tools* ini dapat melihat dan membaca pesan *request* dan *response* antara *web browser* dan *web server* yang terjadi dalam internet. Pada

penyerangan website HTTP tools wireshark juga mampu merekam serta menampilkan *username* dan *password* dikarenakan tidak adanya enkripsi saat *wab brow*ser dan *web server* melakukan komunikasi.

3. Perbedaan Serangan antara *website* HTTPS dan *website* HTTP ialah terletak pada tingkat keamanan *website* tersebut. Jika memiliki keamanan yang lebih maka seperti *website facebook* dan instagram penyerang tidak dapat menampilkan *username* dan *password* dikarenakan adanya *enkripsi* data menggunakan SSL(*Secure Socket Layer*) dan TLS(*Transport Layer Security*) yang memungkinkan website tersebut tidak dapat dibobol dengan mudah dan membutuhkan waktu yang cukup lama karena saat ini keamanan HTTPS masih aman sampai sekarang.

5.2 Saran

Simulasi yang penyerang lakukan jauh dari kata sempurna, masih banyak terdapat kekurangan-kekurangan. Maka dari itu dibutuhkan perkembangan lebih lanjut agar simulasi ini terlihat sempurna. Adapaun saran-saran dari simulasi ini sebagai berikut:

1. Simulasi ini lebih baik menggunakan 2 PC untuk melakukan serangan *packet sniffing*. Pada simulasi ini penulis hanya menggunakan 1 pc dalam melakukan pencurian data dan menggambarkan bagaimana serangan seperti *packet sniffing* terjadi.

2. Agar dapat melakukan serangan *packet sniffing* menggunakan *wireshark.* Penulis harus terhubung pada jaringan *wi-fi* yang sama. Maka dari itu diperlukan keamanan terhadap jaringan *wi-fi* dengan menggunakan keamanan WPA2-PSK. Dengan ini dapat meminimalisir serangan *Packet sniffing*. Sedangan serangan menggunakan *burpsuite* penyerang hanya terhubung kedalam jaringan yang dapat mengakses internet dan menjalankan *burpsuite* untuk bertindak sebagai *proxy*.

DAFTAR PUSTAKA

Adzan Abdul Zabar, Fahmi Novianto. 2015. Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux. Universitas Komputer Indonesia

Achmad Rizal Fauzi. 2018. Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids. Surabaya: Universitas Negeri Surabaya

Didi Susianto, Anisa Rachmawati. 2018. Implementasi dan Analisis Jaringan Menggunakan Wireshark, Cain and Abels, Network Minner. Bandar Lampung: Amik Dian Cipta Cendikia.

Dian Kurnia. 2019. Pemanfaatan Bettercap Sebagai Teknik Sniffing Pada Trafik Jaringan Wi-fi. Medan: Universitas Pembangunan Panca Budi.

Edwin Mandala Putra, Baibul Tujni, Edi Surya Negara. Analisis Keamanan Jaringan Internet (wi-fi) dari Serangan Packet Data Sniffing Di Universitas Muhamadiyah Palembang. Palembang: Universitas Bina Darma.

Heru Pranata, Leon Andretti Abdillah, Usman Ependi. 2015. Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan. Palembang : Universitasa Bina Darma.

Henni Endah Wahanani, Firza Prima Aditiawan, Retno Mumpuni. 2020. Uji Coba Serangan Man in The Middle Pada Keamanan SSL Protokol Http. Jawa Timur :UPN Veteran.

I Gede Putu Krisna Juliharta. Bussiness Impact Analysis Aplikasi Jaringan Komputer Dengan Teknik Packet Sniffing. Bali: STMIK STIKOM.

Kurniawan, A. (2012). *Network Forensik.* Yogyakarta: Andi Offset.

Muh Nasir, Roby Kasamudin. 2012. Dampak Sniffing Pada Keamanan Data Di Jaringan Lan. Universitas Cokroaminoto Palopo.

M.Ferdy Adriant, Is Mardiyanto.2015. Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan. Universitas Trisakti.

Putri Tsania Mahmud, Muhamad Tsani Arafi, Lina Lulus Destianti, Intan Cahyani. 2019. Sniffing Jaringan Menggunakan Wireshark. Jakarta: Universitas Bina Sarana Informatika

Setiawan, Thomas. 2004. Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal. Bandung : Tugas Akhir Institut Teknologi Bandung,