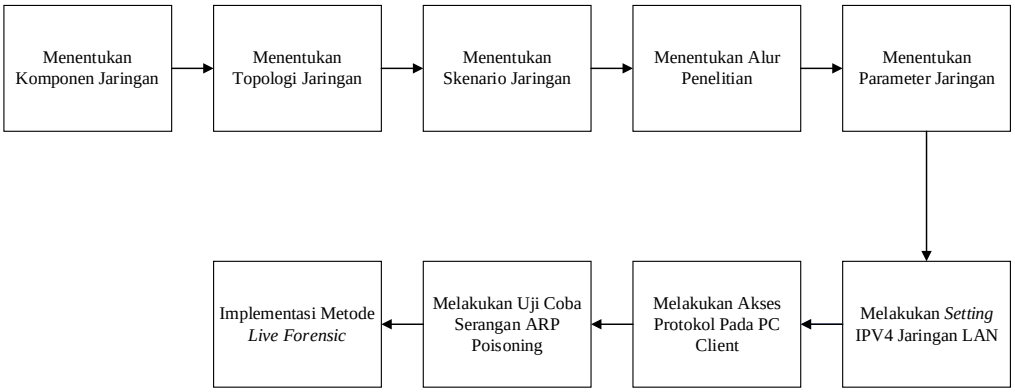
BAB 3
METODE PENELITIAN

3.1 TAHAPAN PENELITIAN

Pada bagian ini akan dijelaskan mengenai alat apa saja yang akan digunakan dalam pembuatan sistem ini serta fungsi masing-masing alat tersebut.



Gambar 3. 1 Diagram Blok Penelitian

3.1.1 KOMPONEN JARINGAN

Dalam penelitian ini, dibutuhkan perangkat keras (*hardware*) dan perangkat lunak (*software*) untuk mengimplementasikan sistem keamanan menggunakan *Live Forensic*. Adapun perangkat yang dibutuhkan adalah :

a. Perangkat Keras (*Hardware*)

Terdapat beberapa perangkat keras (*Hardware*) yang digunakan pada penelitian ini diantaranya adalah :

1. Satu *unit* PC sebagai server untuk penyedia layanan SSL (*Secure Socket Layer*) dan FTP (*File Transfer Protocol*) dengan spesifikasi Intel® Core™ i7-7700 CPU @3.60GHz × 8, RAM 8.00 GB.
2. Satu *unit* PC sebagai *investigator* untuk penarikan data dan analisis dengan spesifikasi Intel® Core™ i7-7700 CPU @3.60GHz × 8, RAM 8.00 GB.
3. Satu *unit* PC sebagai *attacker* (Penyerang) dengan spesifikasi Intel® Core™ i7-7700 CPU @3.60GHz × 8, RAM 8.00 GB.
4. Satu *unit* PC sebagai *Client* dengan spesifikasi Intel® Core™ i7-7700 CPU @3.60GHz × 8, RAM 8.00 GB.
5. Satu buah *switch*

6. Dua buah kabel *straighover*

b. Perangkat lunak (*software*)

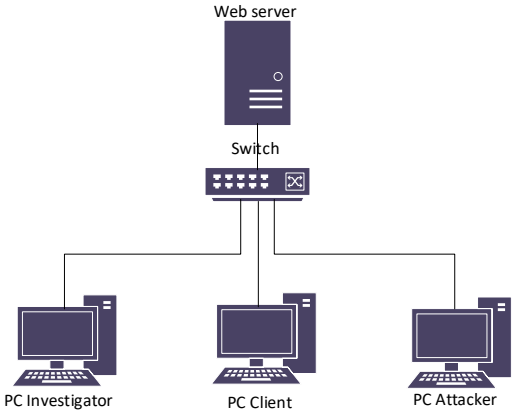
Adapun untuk perangkat lunak (*software*) yang digunakan pada penelitian ini diantaranya adalah :

Tabel 3.1 Prangkat Lunak (*Software*)

No.	Nama	Deskripsi
1.	Linux Ubuntu 18.04	Sistem operasi yang digunakan untuk PC *client*, server dan *attacker.*
2.	Windows 10	Sistem operasi yang digunakan pada PC penyelidik (*investigator*).
3.	Google Chrome	Digunakan sebagai web browser agar *client* dapat mengakses protokol SSL (*Secure Socket Layer*)
4.	XARP	*Tools* yang digunakan untuk mendeteksi serangan berbasis ARP (*Address Resolution Protocol*) dengan memberikan notifikasi dan menampilkan identitas penyerang maupun identitas korban (*victim*).
5.	Wireshark	*Tools* yang digunakan untuk melakukan *monitoring* lalu lintas pada jaringan LAN.
6.	Ettercap	*Tools* yang digunakan untuk melakukan serangan ARP *Poisoning* ke seluruh PC yang terhubung dalam jaringan.
7.	PHP *My Admin*	*Tools* yang digunakan untuk membangun web server dan web browser berbasiskan protokol SSL (*Secure Socket Protocol*).
8.	Filezilla	*Tools* yang digunakan untuk mengirim *file* (berkas) pada server melalui PC *client* dengan berbasis protokol FTP (*File Transfer Protocol*)

3.1.2 TOPOLOGI JARINGAN

Sebelum melakukan simulasi serangan ARP *Poisoning* dalam penelitian ini telah dirancang topologi jaringan. Topologi ini dirancang sesuai dengan yang akan diterapkan dalam simulasi. Berikut adalah topologi yang digunakan pada penelitian ini.



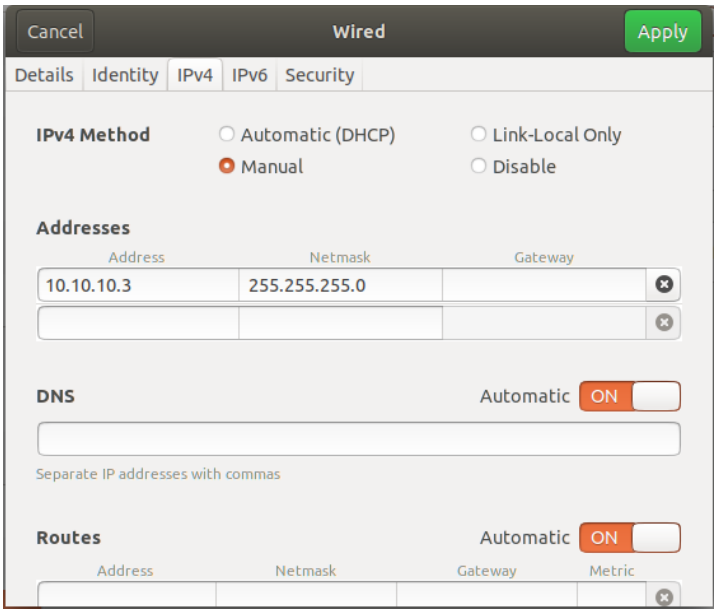
Gambar 3.2 Topologi Jaringan

Pada topologi penelitian ini, terdapat 4 buah PC yang memiliki peranannya masing-masing, PC *client* digunakan untuk skenario akses terhadap protokol FTP (*File Transfer Protocol*), protokol apache dan protokol SSL (*Secure Socket Layer*) yang tersedia pada PC server dengan memasukkan verifikasi *login*. Pada PC server telah diatur akses *client* agar dapat mengakses file pada PC server yaitu dengan memasang *tools* diantaranya PHP My Admin dan Filezilla. Ketika PC *client* berhasil mengakses webserver dan melakukan komunikasi maka PC *attacker* akan melancarkan *sniffing* ke PC server dengan melakukan *scaning host* dan menjalankan serangan ARP Poisoning sehingga data *client* dapat disadap melalui *tools* Ettercap. Pada PC investigator telah ter *install tools* XARP, *tools* ini mampu mengidentifikasi setiap *port* yang terhubung pada jaringan LAN sehingga *tools* ini bertugas untuk memberi tahu kepada *investigator* mengenai aktifitas *sniffing* yang dilakukan oleh penyerang dengan memberikan notifikasi *alert* secara *realtime* sehingga *investigator* dapat secara langsung mengambil tindakan forensik jaringan. IP *address private* yang telah dikonfigurasi pada masing-masing PC berdasarkan rancangan topologi penelitian ini dapat dilihat seperti pada tabel 3.2 berikut ini.

Tabel 3.2 Konfigurasi Jaringan LAN (*Local Area Network*)

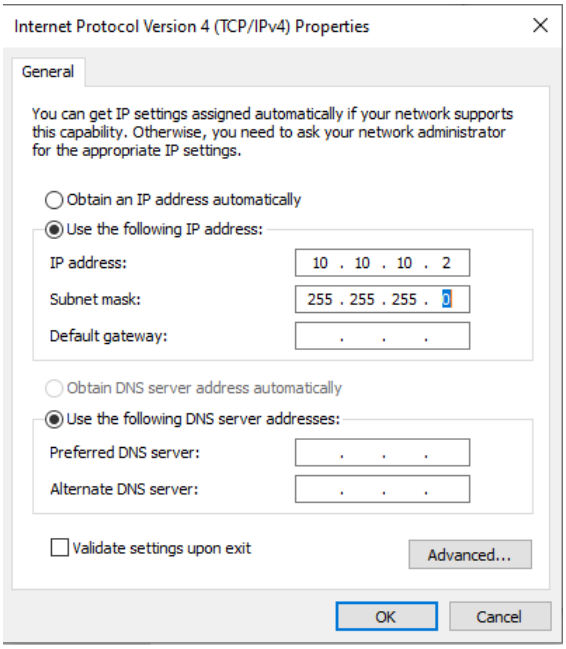
No	Perangkat	Alamat IP
1	Client (PC 1)	10.10.10.3/24
2	Investigator (PC 2)	10.10.10.2/24
3	Web Server (PC 3)	10.10.10.1/24
4	Attacker (Ettercap) (PC 4)	10.10.10.4/24

Konfigurasi jaringan LAN (*Local Area Network*) mencakup beberapa PC yang digunakan, berdasarkan tabel 3.2 terdapat 4 buah PC yang dikonfigurasi menggunakan IPv4 (*private*) diantara lain adalah PC *client*, PC *investigator*, PC server dan PC *attacker*. Seluruh PC tersebut telah terhubung dengan perangkat *switch* untuk memudahkan proses transmisi data antar *host* yang dituju sehingga dapat menentukan lalu lintas yang terbaik dalam proses pengiriman paket ke tujuan dengan optimal. Proses konfigurasi masing-masing PC pada penelitian ini dapat dilihat sebagai berikut.



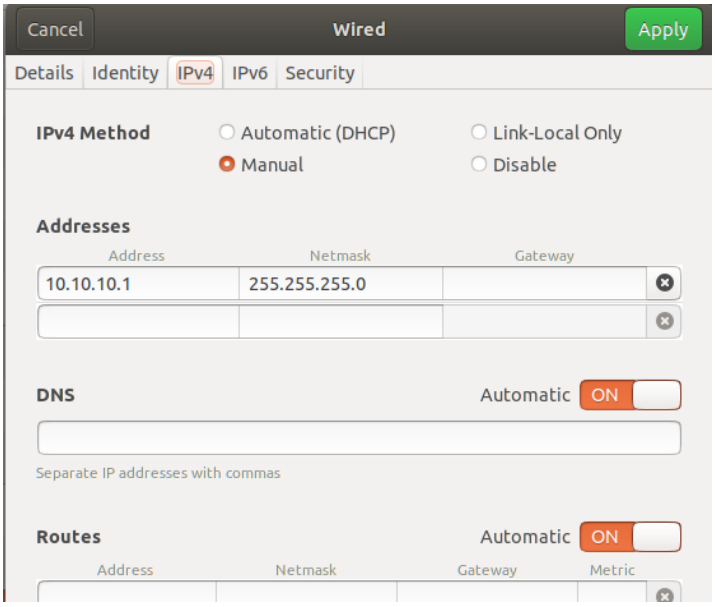
Gambar 3.3 Konfigurasi IPv4 Pada PC (*Client*)

Pada gambar 3.3 dilakukan konfigurasi terhadap PC *client* dengan alamat IP *private* 10.10.10.1 dengan netmask 255.255.255.0.



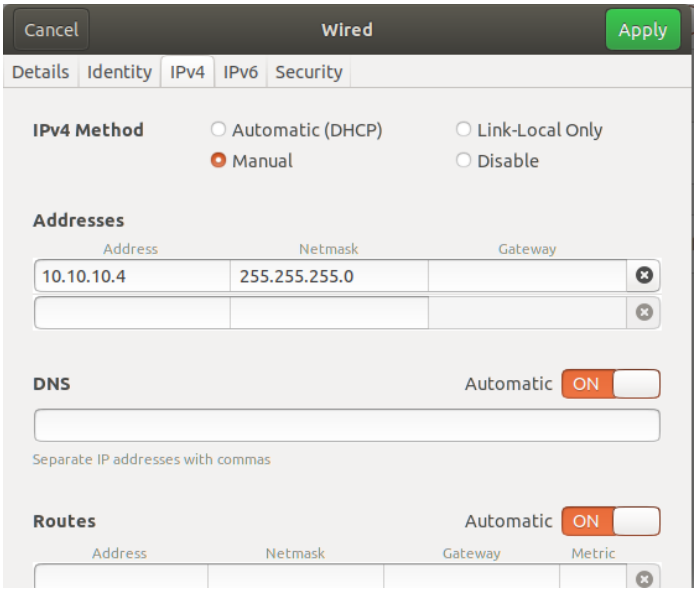
Gambar 3.4 Konfigurasi IPv4 Pada PC *Investigator*

Pada gambar 3.4 dilakukan konfigurasi terhadap PC *investigator* dengan alamat IP *private* 10.10.10.2 dan netmask 255.255.255.0.



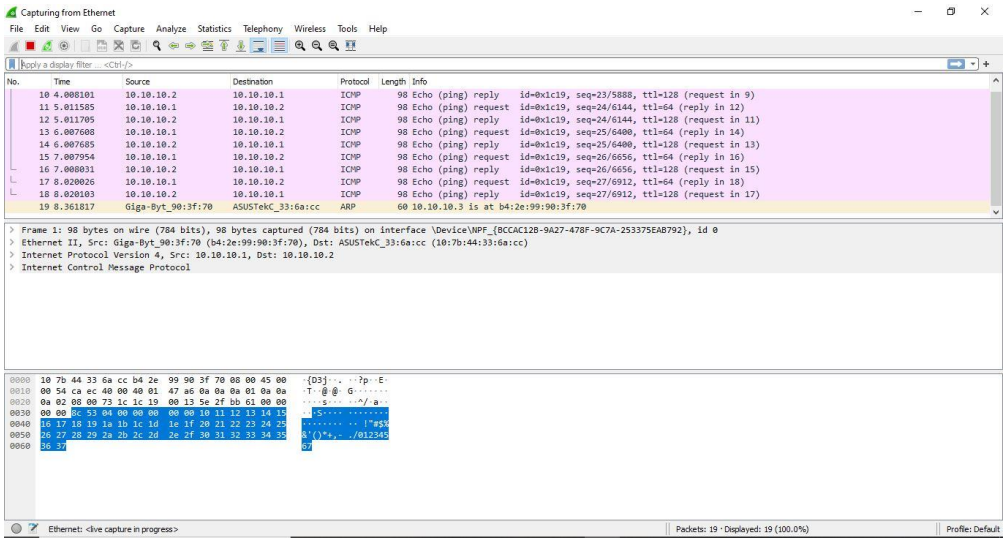
Gambar 3.5 Konfiguarasi IPv4 Pada PC Server

Pada gambar 3.5 dilakukan konfigurasi terhadap PC server dengan alamat IP *private* 10.10.10.1 dan netmask 255.255.255.0.



Gambar 3.6 Konfigurasi IPv4 Pada PC *Attacker*

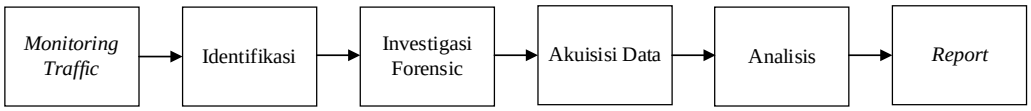
Pada gambar 3.6 telah dilakukan konfigurasi terhadap PC *attacker* dengan alamat IP *private* yaitu 10.10.10.3 dan netmask 255.255.255.0. Setelah konfigurasi jaringan LAN (*Local Area Network*) telah selesai dilakukan, untuk memastikan masing-masing perangkat komputer saling terhubung dengan benar maka dilakukan proses *ping* pada setiap komputer untuk mengetahui konektifitas jaringan yang telah dibangun. Hal ini dapat dilihat pada gambar 3.7 dimana IP 10.10.10.2 sedang melakukan *ping* secara terus-menerus ke target yaitu IP 10.10.10.1.



Gambar 3.7 Keadaan Lalu Lintas Jaringan

3.1.3 SKENARIO JARINGAN

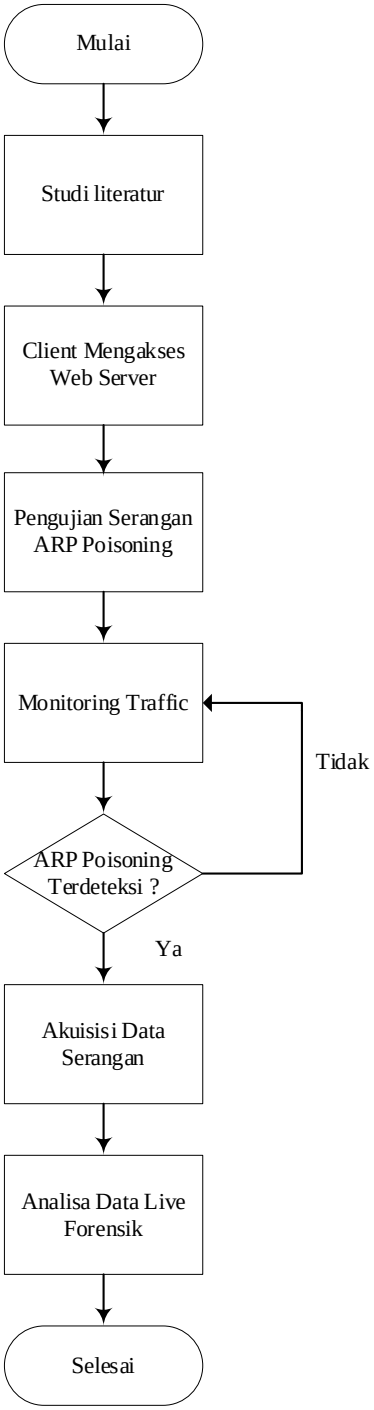
Pada skenario jaringan penelitian ini, penulis akan melakukan perancangan investigasi forensik yang dilakukan pada aplikasi XARP dan wireshark menggunakan metode *Live Forensic*. *Live Forensics* merupakan sebuah metode yang digunakan untuk mengumpulkan data informasi dan barang bukti data elektronik pada suatu jaringan komputer dalam kondisi menyala, metode ini bertujuan untuk penanganan yang lebih cepat [5]. Fokus utama dalam melakukan investigasi forensik pada penelitian ini adalah melakukan analisis terhadap bukti-bukti yang didapat dari proses identifikasi yang didapat dari aktifitas yang mencurigakan pada *Log Activity* dan IP *Address List* selama *monitoring* berlangsung, hal ini dapat membantu *investigator* dalam menacari identitas pelaku serangan terutama pada kasus serangan ARP *Poisoning* dimana serangan ini berusaha memanipulasi identitas MAC *Address* dan IP Adress sehingga pelaku sulit ditemukan, maka dari itu dibutuhkan aplikasi XARP dan wireshark untuk mendukung proses investigasi *Live Forensic*. Apabila semua data yang diperlukan dalam proses *Live Forensic* telah didapatkan, *investigator* dapat memberikan kesimpulan secara lengkap terkait dengan informasi yang didapatkan dengan membuat laporan berisi data-data yang diperlukan untuk kebutuhan forensik jaringan, terdapat beberapa data-data yang akan disajikan dalam sebuah laporan diantara lain adalah tanggal serangan, waktu terjadi serangan, MAC address penyerang, IP *address* penyerang, MAC *Address victim* dan IP Address *victim*. Data-data yang diperlukan tersebut dapat diidetifikasi melalui PC *investigator*. Pada tahap analisis *live forensic*, terdapat beberapa tahapan yang harus dipenuhi, diantara lain seperti pada gambar 3.8 berikut :



Gambar 3.8 Tahapan *Live Forensic*

3.1.4 ALUR PENELITIAN

Adapun untuk tahap penelitian ini, penulis mendeskripsikan terkait dengan langkah-langkah selama proses penelitian berlangsung. Bagan alir atau *flowchart* dalam penelitian ini adalah :



Gambar 3.9 *Flowchart* Penelitian

Penjelasan tentang alur penelitian sebagai berikut :

1. Studi Literatur

   Pada tahap studi pustaka, penulis mengumpulkan berbagai informasi dan teori-teori yang berkaitan dengan penelitian yang akan dilakukan. Pengumpulan teori ini dilakukan guna memperkuat referensi dari hasil penelitian sebelumnya. Sumber teori yang didapatkan oleh penulis yaitu dari berbagai jurnal nasional, buku, dan situs web resmi. Dari berbagai sumber tersebut, penulis telah mendapatkan referensi-referensi yang berkaitan dengan penelitian yang akan dilakukan sehingga penulis dapat melakukan perancangan untuk menjalankan tahap-tahap dalam penelitian ini.

2. *Client* Mengakses Web Server

   Pada tahap client mengases web server, terdapat beberapa aplikasi yang digunakan untuk menjalankan beberapa protokol pada server diantaranya adalah *tools* PHP My Admin dan Filezilla. *Tools* PHP *My Admin* digunakan untuk mendukung berbagai operasi MySQL diantaranya mengelola basis data, tabel-tabel, bidang (*field*), relasi (*relation*), indeks, pengguna (*users*), perizinan (*permission*), dan lain-lain. Dalam penelitian ini PHP *My Admin* dijalankan pada PC server agar *client* dapat mengakses layanan pada web server, untuk akses alamatnya adalah https://192.168.10.247, setelah *client* melakukan akses tersebut *client* akan masuk ke dalam halaman *login* pada web server dan masuk ke tampilan web PHP MySQL, sedangkan untuk *tools* Filezilla dijalankan pada PC server dan PC *client* yang mana *tools* ini beroperasi pada port 21 FTP (*File Transfer Protocol*) dalam penilitian ini *tools* Filezilla digunakan untuk melakukan pengiriman data dan melakukan akses terhadap *file* yang berada pada PC server, sehingga ketika *client* mengakses server melalui *tools* Filezilla ini *clinet* dapat melakukan *tranfer file* (berkas) yang tersimpan pada penyimpanan PC server.

3. Pengujian Serangan ARP *Poisoning*

   Pada tahap pengujian serangan, penulis melakukan pengujian terhadap PC target dari PC *attacker*. Pengujian ini dilakukan dengan melakukan serangan ARP *Poisoning* dari PC *attacker* ke PC target menggunakan *tool* Ettercap. Langkah awal untuk melakukan serangan, yaitu melakukan *scanning host*

untuk menampilkan IP *address* dan MAC *address* dari PC target, ketika telah muncul IP dan MAC *address* dari PC target maka selanjutnya *host* tersebut dipilih sebagai target untuk dilakukan pengujian serangan. Pada teknik serangan ARP *Poisoning*, memanfaatkan protokol ARP dengan memanipulasi alamat MAC tujuan menjadi alamat MAC *attacker*. Sehingga ketika target akan mengirimkan paket data ke *host* tujuan, maka paket data tersebut akan terkirim ke PC *attacker* terlebih dahulu kemudian paket tersebut diteruskan ke MAC *address* tujuan yang membuat paket data *clinet* disadap oleh pihak *attacker.*

4. *Monitoring Traffic* Jaringan

   Pada tahap *monitoring* trafik jaringan, *tool* Wireshark akan digunakan sebagai alat untuk melakukan perekaman lalu lintas trafik data pada saat serangan ARP *Poisoning* sedang berjalan. Setelah *tools* Wireshark mampu menangkap aktivitas yang mencurigakan dalam trafik jaringan, maka hasil tersebut kemudian akan di analisa dengan menggunakan metode *live forensic.* Bukti-bukti yang dapat dihasilkan oleh Wireshark adalah IP *address list* dari *attacker* yang mencoba untuk melakukan serangan dan *log activity* dari trafik jaringan sehingga bukti-bukti tersebut dapat diidentifikasi untuk kemudian dijadikan barang bukti atas tindakan serangan yang dilakukan oleh pihak *attacker*. Namun, untuk memastikan bahwa serangan tersebut merupakan serangan dari uji coba serangan yaitu ARP *poisoning* maka sebelum melakukan *monitoring* menggunakan *tools* Wireshark, dibutuhkan pendeteksian serangan terlebih dahulu menggunakan *tools* yang telah dipersiapkan sebelumnya yaitu *tools* XARP. Dengan menggunakan *tools* XARP, maka akan didapat berupa *alert* atau peringatan bahwa telah terjadi usaha *sniffing* atau penyadapan melalui *port* ARP. Setelah dapat dipastikan serangan ARP *poisoning* telah benar-benar masuk, maka langkah selanjutnya yaitu melakukan identifikasi menggunakan wireshark untuk mengambil bukti-bukti serangan ARP *poisoning.*

5. Akuisisi Data Serangan

   Dalam melakukan tahap akuisisi data serangan, kondisi utama yang harus dipenuhi untuk melakukan proses investigasi menggunakan metode *live*

forensic adalah keadaan dimana suatu sistem sedang berjalan atau running dikarenakan informasi akan berubah atau hilang jika sistem tersebut dimatikan ataupun dilakukan *restart*, sehingga PC *investigator* harus terhubung dahulu sebagai *client* dalam jaringan yang sama untuk mendapatkan akses melakukan akuisisi data. Tahapan akuisisi data adalah proses menganalisa data atau bukti-bukti yang sebelumnya telah didapatkan oleh investigasi menggunakan *tools* Wireshark, dimana tahapan sebelumnya disebut dengan *collection*. Proses akuisisi data dilakukan dengan menganalisa hasil dari *capture* trafik jaringan sebelumnya yang didapat dari *tool* Wireshark. Dalam *capture* trafik jaringan, akan didapat berupa filterisasi paket-paket dari *tool* Wireshark sehingga *investigator* dapat mengetahui *port* mana saja yang telah dilakukan serangan dan *file-file* yang mencurigakan juga dapat diketahui.

6. Analisa *Live Forensics*

   Pada tahap *preparation* dilakukan studi literatur terlebih dahulu kemudian juga melakukan identifikasi kebutuhkan untuk menyiapkan alat dan perangkat yang dibutuhkan. Pada tahap perancangan simulasi, dilakukan simulasi untuk uji coba serangan ARP *poisoning*. Kemudian tahap selanjutnya adalah investigasi forensik, dalam proses investigasi forensik dilakukan tahap pendeteksian, pengumpulan data-data untuk dijadikan sebagai bukti, dan proses akuisisi data dari bukti-bukti yang telah didapat. Tahap selanjutnya yaitu analisis, proses analisis ini melakukan analisa data ketika *monitoring* trafik jaringan dilakukan dan analisa dari bukti *capture* trafik jaringan yang didapat dari *tools* Wireshark.

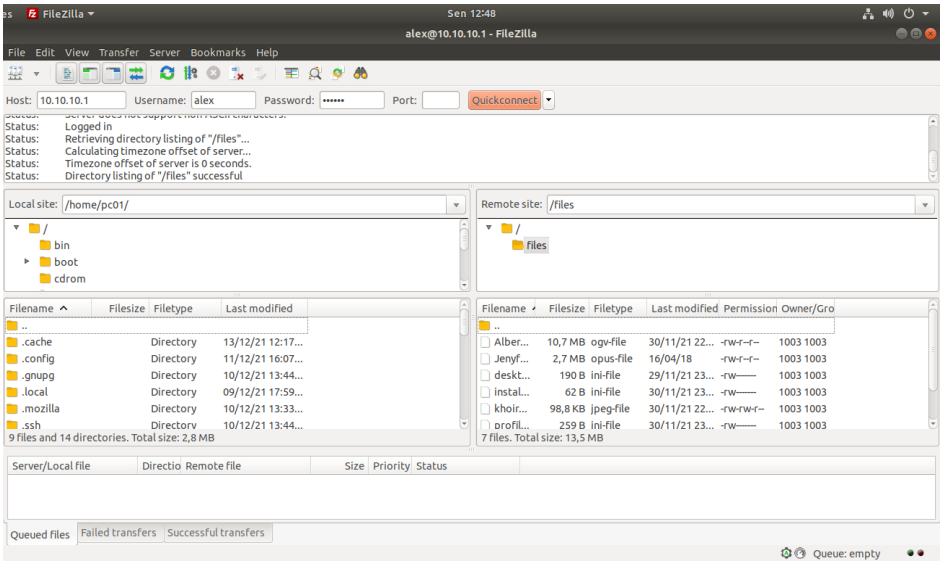
3.1.5 PARAMTER SERANGAN

Investigasi serangan dengan metode *Live Forensic* digunakan pada saat jaringan komputer sudah mengalami serangan oleh pihak yang tidak berwenang, oleh karena itu dibutuhkan tindakan pemerikasaan secara *real time* agar dilakukan penanganan yang cepat. Parameter yang mempengaruhi target dari serangan yang diberikan adalah *confidentiality* dan *integrity* sesuai dengan aspek-aspek keamanan jaringan. *ARP Poisoning* dapat berpeluang mempengaruhi

confidentiality pada suatu sistem jaringan komputer. *Confidentiality* merupakan kerahasiaan informasi yang dimiliki suatu sistem sehingga aspek ini mempengaruhi kerahasiaan data yang dimiliki oleh seseorang secara (personal). Hal ini dapat merugikan pengguna karena kerahasiaan data penting guna kenyamanan seseorang dalam mengakses suatu layananan pada jaringan komputer, namun pada penelitian ini mengacu pada proses pemerikasaan dan investigasi yang dilakukan oleh *tools Wireshark* sebagai pemeriksaan aktifitas lalu lintas jaringan dan *tools* XARP sebagai pemberi peringatan (*alert*) sekaligus untuk memerikasa identitas penyerang, identitas *victim* dan waktu serangan dilakukan.

3.1.6 AKSES *CLIENT* TERHADAP PROTOKOL FTP

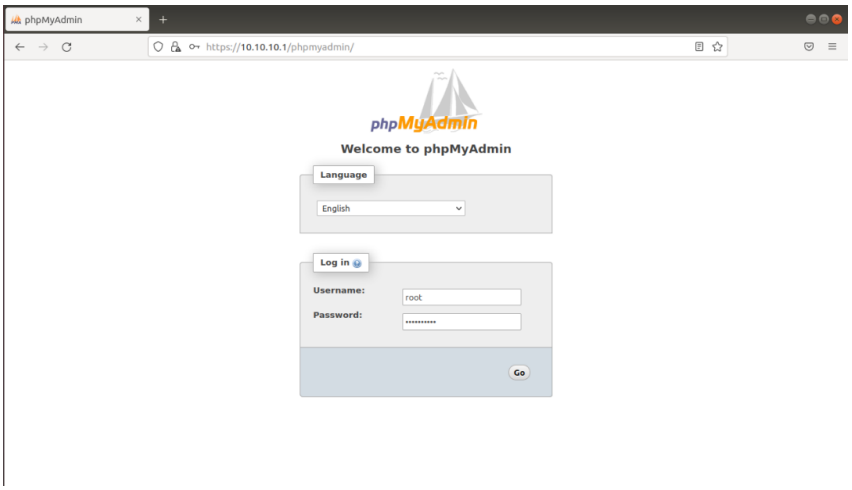
Berdasarkan topologi jaringan pada gambar 3.2, untuk skenario awal penelitian ini adalah *client* mengakses server dengan menggunakan protokol FTP (*File Transfer Protocol*) protokol ini berada pada lapisan aplikasi yang dapat melakukan proses transfer berkas (*file*) antar komputer yang terhubung. Aplikasi Filezilla merupakan aplikasi berbasikan protokol FTP (*File Transfer Protocol*) yang berada pada *port* 21 maka dari itu *client* mengaksesnya melalui *port* 21 dengan alamat IP *host* tujuan yaitu 10.10.10.1 kemudian *client* memasukkan id dan *password* yang telah diatur pada server. Setelah *client* berhasil *login*, *client* dapat mengakses *file* apapun yang ada pada penyimpanan PC server seperti yang terlihat pada gambar 3.10 berikut ini.



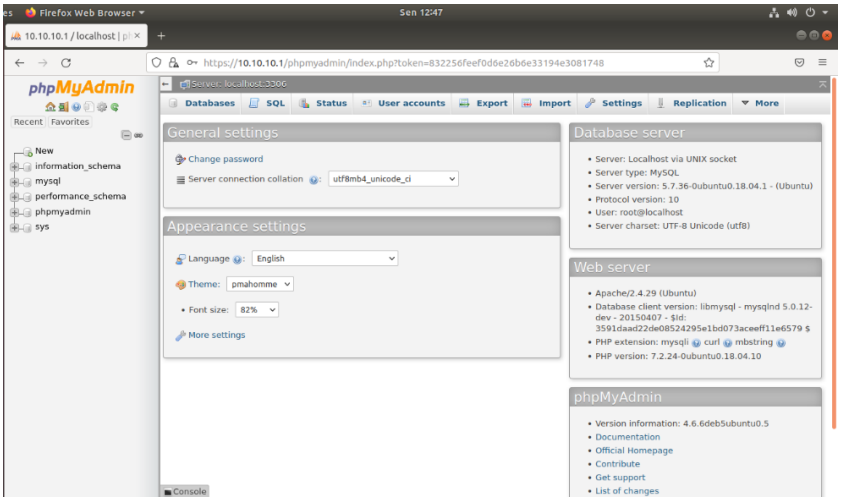
Gambar 3.10 *Transfer* Berkas Pada Filezilla

3.1.7 AKSES *CLIENT* TERHADAP PROTOKOL SSL

Pada skenario ini menggunakan protokol SSL, dalam hal ini menggunakan aplikasi PHP MyAdmin untuk mengakses web browser dari sisi *client* dan melakukan pengaturan database MySQL dari sisi server. PHP My Admin berada pada protokol SSL yang mana protokol ini digunakan untuk membangun sebuah website yang aman (terenkripsi) antara server dengan *client* sehingga protokol ini tidak mudah di akses oleh pihak yang tidak berkepentingan. Pada gambar 3.11 memperlihatkan *client* melakukan akses terhadap server dengan cara *login* melalui host tujuan yaitu https://10.10.10.1/phpmyadmin kemudian *client* akan masuk kedalam *database* MySQL seperti yang terlihat pada gambar 3.12 berikut.



Gmabar 3.11 Akses MySQL pada PC *Client*

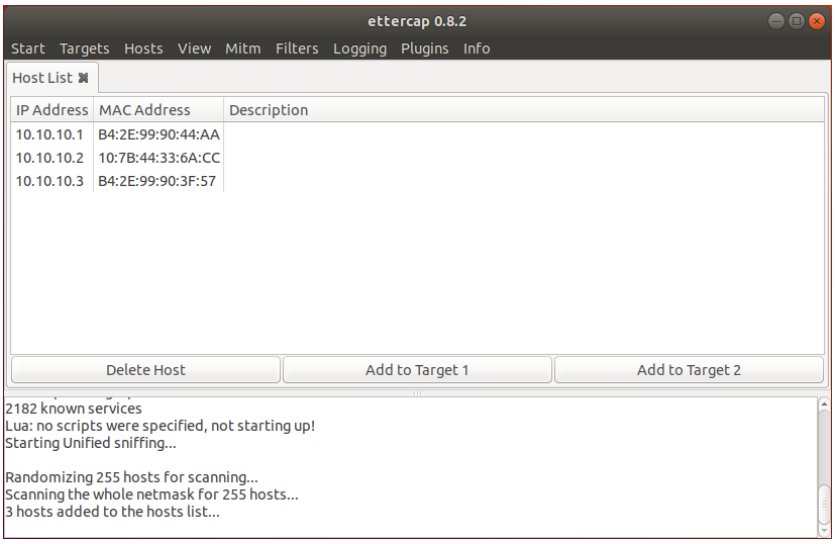


Gambar 3.12 *Client* Mengakses *Database* MySQL

3.1.8 IMPLEMENTASI SERANGAN ARP *POISONING*

Tahap selanjutnya setelah *client* berhasil mengakses layanan FTP (*File Transfer Protocol*) dan SSL (*Secure Socket Layer*) pada server adalah melakukan uji coba serangan ARP *Poisoning* yang ditujukan pada server menggunakan *tools* ettercap. Seperti yang peneliti sudah jelaskan sebelumnya bahwa serangan ini dibagi menjadi 2 sesi sebagai berikut ini :

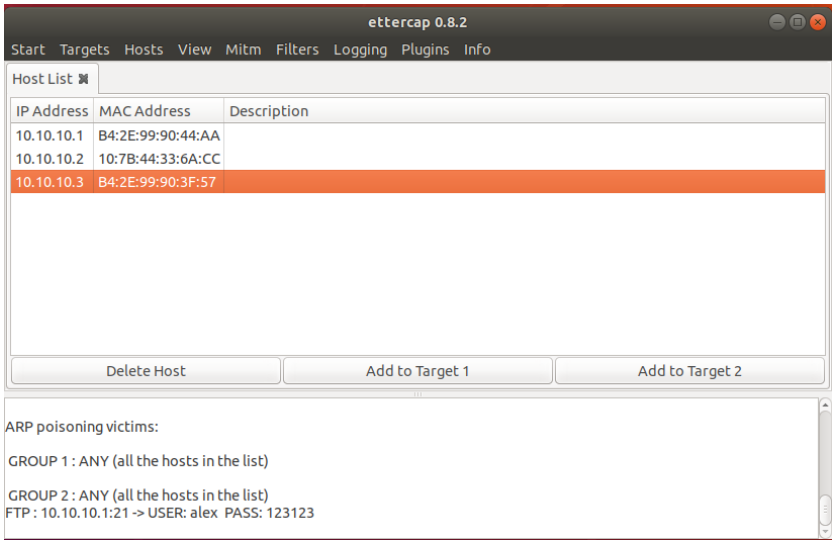
1. Sesi yang pertama menggunakan aplikasi Ettercap untuk melakukan serangan ARP *Poisoning*. Langkah pertama untuk melakukan serangan ARP *Poisoning* yaitu melakukan *start sniffing*, kemudian *scanning host* yang bertujuan untuk mengetahui identitas korban (*victim*) yang terhubung *switch* sehingga penyerang dapat memperoleh akses untuk melakukan penyadapan terhadap PC yang sedang melakukan aktifitas pertukaran data maupun *transfer* data dalam jaringan LAN. Identitas yang berhasil ditangkap oleh penyerang yaitu IP *address victim* dan MAC *address* korban (*victim*) seperti yang terlihat pada gambar 3.13 dimana penyerang berhasil mememperoleh *scanning host* dengan memperoleh 3 identitas korban (*victim*) berupa alamat IP dan alamat MAC, hal tersebut dapat dilihat sebagai berikut.



Gambar 3.13 *Attacker* Melakukan *Scanning Host*

2. Sesi kedua saat melakukan serangan ARP *Poisoning*, langkah yang dilakukan yaitu dengan memilih menu pada MITM, berdasarkan serangan yang digunakan penilitian ini serangan ARP *Poisoning* dipilih untuk melakukan proses penyadapan terhadap informasi data *client*, maka dari itu *attacker*

memilih serangan ARP *Poisoning* yang dijalankan pada aplikasi ettercap, ketika serangan ini berhasil dilakukan terlihat pada *command victim* Ettercap menampilkan beberapa data *client* yang diantaranya adalah protokol yang digunakan, IP host tujuan, *username* dan *password* yang dimiliki oleh *client.* Hal tersebut dapat dilihat pada gambar 3.1 sebagai berikut.



Gambar 3.14 *Attacker* Menyadap Informasi Data *Client*

Seperti yang terlihat pada gambar 3.14 dapat diketahui bahwa *attacker* hanya mampu memperoleh data *client* dari sisi layanan protokol FTP (*port* 21) yang digunakan untuk proses *transfer* berkas (*file*) dari server menuju *client* sedangkan *attacker* tidak berhasil melakukan penyadapan terhadap protokol SSL (*Secure Socket Layer*) yang diakses oleh *client* seperti yang terlihat pada gambar 3.8 seperti yang peneliti sudah jelaskan sebelumnya bahwa protokol SSL tidak dapat diakses oleh pihak yang tidak berkepentingan salah satunya dengan menggunakan serangan ARP *Poisoning* yang digunakan pada penelitian ini disebabkan protokol SSL yang sudah sangat terenskripsi dengan tingkat kemanan tinggi sehingga komunikasi antara *client* dengan menggunakan web browser dan server yang beroperasi menggunakan webserver tidak bisa ditembus oleh pihak penyerang, maka dari itu penyerang pada kasus ini hanya dapat melakukan penyadapan data *client* dari sisi layanan FTP saja yang mana digunakan *client* untuk melakukan transfer *file* (berkas) dengan menggunakan *tools* Filezilla.