BAB III
METODE PENELITIAN

3.1 Desain Penelitian

Desain penelitian merupakan tahapan awal yang dilakukan untuk melakukan penelitian sebagai bahan struktur pemecahan masalah dalam penulisan yang nantinya akan dibuat. Untuk penelitian ini, peneliti menggunakan metode eksperimen. Metode eksperimen pada umumnya digunakan penelitian yang bersifat laboratoris. Namun, bukan berarti metode ini tidak bisa digunakan dalam penelitian sosial, penelitian pendidikan. Penelitian eksperimen mendasar pada paradigma *positivistik* pada awalnya memeng banyak di terapkan pada penelitian ilmu biologi dan fisika, yang kemudian diadopsi untuk diterapkan di bidang – bidang lainya, termasuk sosial dan pendidikan. Desain penelitian dibuat sebagai berikut : Tujuan penelitian kualitatif adalah pemahaman subjek terhadap sekitar. Desain penelitian dibuat sebagai berikut :

1. Melakukan studi literatur dengan membaca buku, jurnal, internet, kerangka ilmiah, dan praktik guna untuk memahami teknik teknik penyerangan dan cara bertahan dari serangan tersebut.
2. Melakukan observasi dan wawancara, yang berguna untuk mengetahui lokasi penelitian dan kondisi jaringan yang digunakan.
3. Menganalisa kondisi jaringan yang sudah ada.
4. Installasi dan configurasi tools yang nantinya digunakan untuk penelitian.
5. Melakukan Penyerangan.

3.2 Pengumpulan Data

Pengumpulan data yang dilakukan pada penelitian ini adalah sebagai berikut:

1. **Observasi**

Pengumpulan data yang diperoleh secara langsung dari lapangan dengan mengati skema jaringan yang sudah ada.

2. **Wawancara**

Pengumpulan data dengan cara tanya jawab dengan staff IT pada lokasi penelitian untuk mendapat informasi kondisi jaringan yang sudah ada, spesifikasi jaringan, pengguna dalam jaringan serta jumlah komputer yang ada pada lokasi penelitian.

3. **Studi Literatur**

Mempelajari dari jurnal - jurnal yang ada tentang keamanan jaringan wifi dari serangan paket data *sniffing* sebagai tujuan utama dari penelitian ini.

4. **Analisa**

Pada tahapan ini peneliti menganalisa kondisi jaringan yang sudah ada dan sudah berjalan, dari hasil analisa maka peneliti dapat menyiapkan tools yang nantinya akan digunakan.

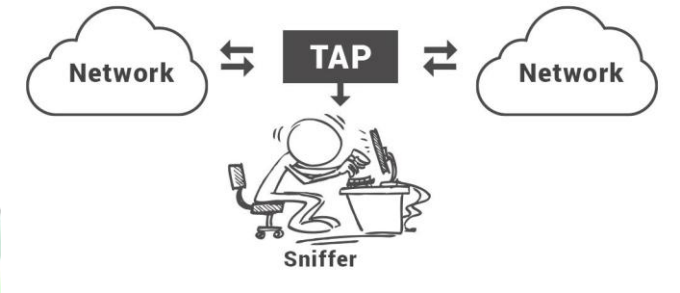
3.3 Pengolahan Awal Data

Tujuan dari pengolahan data awal adalah untuk mengetahui skema jaringan yang sudah ada MA Masalikil Huda, data yang sudah didapat dari MA Masalikil Huda kemudian di analisa untuk mengetahui tingkat keamanan jaringan yang berada di MA Masalikil Huda.

3.4 Metode yang Diusulkan

Metode yang digunakan peneliti untuk melakukan penelitian adalah *sniffing, sniffing m*erupakan suatu teknik atau cara seseorang untuk menyadap lalu lintas sebuah jaringan. Contohnya, jika ada seorangan pengguna yang sedang mengirimkan email kepada temannya yang berada diluar kota, maka email tersebut dikirim dari komputer pengguna kemudian melewati jaringan terhubung

dari komputer pengguna baru kemudian sampai pada temanya. Pada saat email tersebut melewati jaringan yang terhubung oleh komputer pengguna maka disinilah aksi *sniffing* dapat dilakukan, dengan adanya aktifitas *sniffing* maka isi email pengguna tersebut bisa dilihat oleh seorang pelaku penyadapan.[3]



Gambar 3. 1 Metode *Sniffing*

Aktifitas *sniffing* merupakan serangan yang sangat bahaya dan ditakuti berikut ini potensi bahaya dari serangan ini :

1. Hilangnya Privasi

   Seperti dalam kasus diatas jika suatu email berhasil ditangkap oleh pelaku *sniffing*, maka isi email bisa dilihat atau dibaca oleh pelaku *sniffing*.[10]

2. Tercurinya Informasi Penting yang Bersifat Pribadi

   Password dan username merupakan informasi yang sangat penting dan pelaku *sniffing* dapat dengan mudah dapat mencurinya apabila seorang pengguna melakukan aktifitas login pada sebuah website.[10]

3.5 Evalusai dan Hasil

Proses evaluasi dari hasil penelitian tentang metode *sniffing* digunakan untuk menganalisa keamanan jaringan wifi di MA Masalikil Huda. peneliti akan melakukan beberapa kali percobaan untuk menganlisa keamanan jaringan wifi diantaranya :

3.5.1 Percobaan Pertama

Dalam Percobaan pertama peneliti menggunkan metode *sniffing* untuk menganalisa keamanan jaringan wifi di MA Masalikil Huda. *Sniffing* merupakan aktivitas penyadapan paket data melalui lalu lintas sebuah jaringan, aksi *sniffing* dibedakan menjadi dua yaitu sniffing aktif dan pasif, *sniffing* pasif melakukan penyadapan tanpa mengubah data atau paket apapun dalam jaringan sedangkan sniffing aktif melakukan penyadapan dengan mengubah atau merusak paket data dalam jaringan. Pada dasarnya cara kerja *sniffing* dibedakan ke beberabagain yaitu *collecting, conversion, analysis* dan pencurian data. Cara kerja *sniffing* collection dengan mengubah *interface* yang digunakan menjadi *promicius* mode dan mulai mengumpulkan data yang lewat dalam bentuk binary, *sniffing conversion* dengan mengubah data data yang berbentuk binary ke dalam bahasa yang mudah dipahami, *sniffing analysis* mengklasifikasikan data yang sudah di conversion ke dalam blok protokol yang berdasarkan sumber transmisi, sedangkan yang terakhir adalah tahapan pencurian data setelah melewati tahapan - tahapan collecting, conversion, analysis maka hacker dengan mudah mencuri informasi penting dalam jaringan.[4]

3.5.2 Percobaan Dua

Pada percobaan ke dua peneliti menggunakan teknik penyerangan *ARP Poison, ARP Poison* merupakan teknik penyerangan jaringan lokal komputer baik menggunakan media kabel maupun tanpa kabel,yang memungkinkan penyerang bisa melakukan pengendusan pada frame data jaringan lokal, memodifikasi traffic dan menghentikan traffic. ARP Poison merupakan konsep dari serangan *Man in The Middle Attack* (MITM) inti dari serangan ini adalah dengan memanfaatkan kelemahan jaringan itu sendiri yang menggunakan ARP broadcast.[2]

3.5.3 Percobaan Tiga

Pada percobaan ketiga peneliti akan menggunakan teknik serangan *DNS Spoofing* merupakan salah satu metode hacking MITM, konsep dari serangan ini hampir sama dengan *ARP Poison* namun yang membedakan adalah penyerang membedakan alamat IP dengan sebuah domain. DNS merupakan Server yang digunakan untuk mengetahui IP *address* suatu *host lewat host namenya*. Di dalam dunia internet komputer berkomunikasi satu sama lain dengan menggunakan IP *address*, tetapi bagi manusia tidak mungkin menghafal IP *address* tersebut, manusia sering menggunakan kata kata seperti *www.google.com*, *www.gmail.com*, *www.facebook.com*. DNS bertujuan untuk mengkonversikan nama yang bisa manusia ke dalam IP *address host* yang bersangkutan untuk melakukan sebuah komunikasi. Pada dasarnya korban tidak akan mengenali dampak dari serangan tersebut, umumnya di dalam dunia maya siapa saja bisa terserangan seperti serangan diatas oleh karena itu admin sebuah jaringan dan Pengguna harus tau sifat dalam serangan tersebut agar dapat menemukan solusi bertahan yang tujuan untuk mempertahankan diri serangan pencurian data ataupun perusakan jaringan.[3]