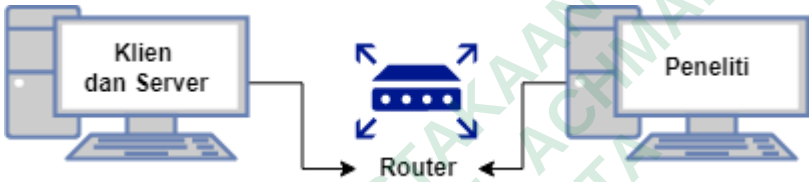
BAB 3
METODE PENELITIAN

3.1 DESAIN PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental untuk mengidentifikasi dan menganalisis kerentanan yang ada pada konfigurasi *server* HTTPS menggunakan OpenSSL dan Node.js. Lingkungan penelitian melibatkan simulasi serangan SSL *Hijacking* dengan menggunakan alat *sniffing* yaitu *mitmproxy*.



Gambar 3. 1 Topologi jaringan

Berikut adalah penjelasan mengenai Topologi dalam gambar 3.1:

1. Klien dan *Server*
    a. Klien: Merupakan komputer atau perangkat yang mengakses layanan yang disediakan oleh *server*. Klien ini mengirimkan permintaan (*request*) ke server melalui jaringan.
    b. *Server:* Merupakan komputer atau perangkat yang menyediakan layanan atau data yang diminta oleh klien. *Server* ini merespons permintaan dari klien dan mengirimkan data yang diminta.
2. *Router*

    Router ini berfungsi sebagai penghubung antara klien, server, dan peneliti. *Router* meneruskan paket data dari klien ke *server* dan sebaliknya. *Router* juga menghubungkan perangkat peneliti dengan jaringan yang digunakan oleh klien dan *server*.

3. Peneliti

Komputer atau perangkat yang digunakan oleh peneliti untuk mengamati dan menganalisis lalu lintas jaringan antara klien dan *server*. Peneliti ini menggunakan perangkat lunak *sniffing* (*mitmproxy*) untuk mencegat dan menganalisis data yang dikirimkan melalui jaringan.

3.2 PENGUMPULAN DATA

Data dikumpulkan melalui serangkaian pengujian yang dilakukan pada *server* yang telah dikonfigurasi menggunakan OpenSSL dan Node.js. Pengujian melibatkan:

1. Instalasi dan Konfigurasi OpenSSL dan Node.js
    a. Instalasi OpenSSL dan Node.js pada sistem operasi *Windows.*
    b. Pembuatan sertifikat SSL/TLS menggunakan OpenSSL.
    c. Konfigurasi *server* Node.js untuk menggunakan sertifikat SSL/TLS tersebut.
2. Pengaturan dan Pengujian Koneksi HTTPS
    a. Pengaturan koneksi HTTPS pada *server.*
    b. Pengujian koneksi HTTPS untuk memastikan bahwa data yang dikirimkan antara klien dan *server* dienkripsi dengan benar.
3. Simulasi Serangan *Sniffing* Menggunakan *mitmproxy*
    a. Instalasi dan konfigurasi *mitmproxy* pada perangkat penyerang.
    b. Pengaturan perangkat target untuk menggunakan *proxy* yang dijalankan oleh mitmproxy.
    c. Simulasi serangan MITM untuk mencegat dan memodifikasi lalu lintas HTTPS antara klien dan *server.*

3.3 ANALISIS DATA

Analisis data dilakukan untuk mengidentifikasi kerentanan yang muncul selama pengujian. Langkah-langkah analisis meliputi:

1. Analisis Sertifikat SSL/TLS
    a. Evaluasi keabsahan dan kepercayaan sertifikat SSL/TLS yang digunakan.
    b. Analisis dampak penggunaan sertifikat *self-signed* versus sertifikat yang diterbitkan oleh *Certificate Authority* (CA) terpercaya.
2. Evaluasi Konfigurasi *Server*
    a. Analisis pengaturan *cipher suite* dan versi protokol SSL/TLS yang digunakan.
    b. Identifikasi konfigurasi yang lemah dan rentan terhadap serangan.
3. Pengamatan Lalu Lintas yang Dicegat
    a. Analisis lalu lintas yang dicegat oleh *mitmproxy* untuk mengidentifikasi data sensitif yang terekspos.
    b. Evaluasi efektivitas serangan MITM dalam mencegat dan memodifikasi data.

3.4 BAHAN DAN ALAT PENELITIAN

Penelitian ini melibatkan berbagai bahan dan alat yang digunakan untuk konfigurasi *server*, simulasi serangan, dan analisis kerentanan. Berikut adalah rincian bahan dan alat yang digunakan:

3.4.1 Perangkat Keras

1. Komputer peneliti
    a. Spesifikasi minimum: *Prosesor Intel Core i5* atau setara, RAM 8 GB, penyimpanan 256 GB.
    b. Sistem operasi: *Windows* 10 atau yang lebih baru.
    c. Fungsi: Digunakan untuk mengatur dan menjalankan seluruh proses penelitian.
2. Perangkat jaringan
    a. *Router* untuk menghubungkan perangkat dalam satu jaringan lokal.

b. Kabel *ethernet*

c. Fungsi: Menghubungkan komputer peneliti dan komputer klien dalam jaringan yang sama untuk keperluan pengujian dan simulasi serangan.

3. Komputer klien

a. Spesifikasi minimum: *Prosesor Intel Core i3* atau setara, RAM 4 GB, penyimpanan 128 GB.

b. Sistem operasi: *Windows* 10 atau yang lebih baru.

c. Fungsi: Berperan sebagai *server* yang akan diuji keamanannya.

3.4.2 Perangkat Lunak

1. OpenSSL

a. Versi: 3.3.1 atau yang lebih baru.

b. Fungsi: Membuat dan mengelola sertifikat SSL/TLS untuk mengamankan koneksi HTTPS.

2. Node.js

a. Versi: 14.x atau yang lebih baru.

b. Fungsi: Menjalankan server yang akan dikonfigurasi untuk menggunakan HTTPS.

3. Mitmproxy

a. Versi: 7.0 atau yang lebih baru.

b. Fungsi: Alat untuk melakukan serangan *Man-in-the-Middle* (MITM) dan *sniffing* lalu lintas jaringan.

4. Browser

a. *Firefox* dan *Chrome.*

b. Fungsi: Menguji koneksi HTTPS dan memverifikasi sertifikat SSL/TLS.

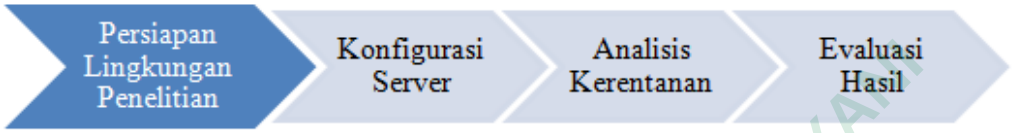
5. Text Editor

a. Visual Studio Code

b. Fungsi: Mengedit skrip Node.js dan file konfigurasi.

3.5 JALAN PENELITIAN

Penelitian ini dilakukan melalui beberapa tahapan yang sistematis untuk menganalisis kerentanan penggunaan OpenSSL dan Node.js terhadap ancaman serangan SSL *hijacking* dengan metode *sniffing*. Berikut adalah langkah-langkah yang ditempuh dalam penelitian ini:



Gambar 3. 2 Jalan penelitian

3.5.1 Persiapan Lingkungan Penelitian

1. Instalasi Perangkat Lunak
    a. Instalasi OpenSSL dan Node.js pada komputer peneliti dengan sistem operasi Windows.
    b. Instalasi *mitmproxy* untuk kebutuhan analisis jaringan dan simulasi serangan.
2. Konfigurasi Perangkat Keras
    a. Pengaturan jaringan lokal yang menghubungkan komputer peneliti dan komputer target.
    b. Verifikasi koneksi jaringan antara perangkat untuk memastikan lingkungan penelitian siap digunakan.

3.5.2 Konfigurasi Server

1. Pembuatan Sertifikat SSL/TLS
    a. Menggunakan OpenSSL untuk membuat sertifikat *self-signed.*
    b. Menyimpan sertifikat dan kunci pribadi pada direktori yang sesuai.
2. Konfigurasi *Server* Node.js

a. Mengedit skrip Node.js untuk menggunakan sertifikat SSL/TLS yang telah dibuat.
b. Menjalankan *server* Node.js dengan konfigurasi HTTPS dan memverifikasi koneksi melalui *browser*.

3.5.3 Analisis Kerentanan

1. Pengujian Koneksi HTTPS
    a. Mengakses server Node.js melalui browser untuk memastikan koneksi HTTPS berfungsi dengan benar.
    b. Mengidentifikasi potensi masalah, seperti peringatan sertifikat tidak valid.
2. Simulasi Serangan Sniffing Menggunakan *mitmproxy*
    a. Menjalankan *mitmproxy* pada komputer peneliti untuk mencegat lalu lintas jaringan.
    b. Mengatur perangkat target untuk menggunakan proxy mitmproxy dan mengamati lalu lintas yang dicegat.

3.5.4 Evaluasi Hasil

1. Hasil Pengamatan : Menganalisis hasil simulasi serangan.
2. Rekomendasi Keamanan : Memberikan rekomendasi keamanan yang tepat.
3. Langkah Mitigasi : Memberikan solusi mitigasi supaya terhindar dari serangan.