# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang

Ancaman serangan siber menjadi masalah yang semakin mengkhawatirkan seiring dengan perkembangan teknologi informasi yang pesat. Di tahun 2024, serangan siber semakin meningkat dan merambah berbagai sektor, mulai dari pemerintahan, kesehatan, hingga dunia bisnis. Salah satu jenis serangan yang terjadi pada 2024 di Indonesia adalah *ransomware*, yang mengunci *data* penting dan menuntut tebusan untuk membuka aksesnya (BSI NEWS, 2024). Selain itu, serangan yang menggunakan *malware* perangkat lunak berbahaya dirancang untuk tujuan merusak sistem juga terus berkembang. Para peretas semakin canggih dalam memanfaatkan kelemahan perangkat lunak dan sistem operasi untuk melancarkan aksinya.

Serangan siber umumnya dibagi dalam beberapa kategori, seperti *phishing*, yang bertujuan untuk memperoleh *data* pribadi korban dengan cara menipu, serta serangan *denial-of-service* (*DoS*) dan *distributed denial-of-service* (*DDoS*) yang menyebabkan sistem atau layanan menjadi tidak dapat diakses (Al-Khater et al., 2020). Namun, salah satu ancaman yang paling berbahaya adalah serangan yang melibatkan *malware*. *Malware* sendiri merujuk pada perangkat lunak yang dirancang untuk merusak, mengakses, atau mengendalikan perangkat korban tanpa izin. Jenis *malware* yang paling umum meliputi *virus*, *trojan*, *worm*, dan *spyware*. *Malware* ini bisa menyebar melalui *email*, unduhan perangkat lunak yang terinfeksi, atau bahkan perangkat *USB* yang tidak aman (Fleury et al., 2021).

Salah satu bahaya terbesar yang dibawa oleh *malware* adalah kemampuannya untuk memberikan akses jarak jauh (*remote access*) ke sistem korban. Dengan akses semacam ini, penyerang dapat mengontrol perangkat secara penuh tanpa diketahui oleh pemiliknya. Akibatnya, serangan tersebut bisa menyebabkan pencurian *data* sensitif, kerusakan sistem, atau pemanfaatan perangkat untuk tujuan yang lebih merusak. Hal yang paling buruk adalah jika penyerang berhasil mengendalikan seluruh sistem tanpa terdeteksi, yang dapat menimbulkan kerugian besar baik dari segi keuangan maupun reputasi.

Untuk mengatasi ancaman ini, berbagai solusi deteksi *malware* telah dikembangkan. Pendekatan *manual*, seperti memeriksa proses mencurigakan melalui *Task Manager*, masih sering digunakan (Hama Saeed, 2020). Dalam metode ini, nama *file malware* harus diketahui dengan menggunakan *program Task Manager*. Namun, deteksi *manual* memiliki keterbatasan, terutama dalam menghadapi *malware* yang baru dan canggih. Dalam beberapa tahun terakhir, teknologi kecerdasan buatan (*AI*) dan *machine learning* telah digunakan untuk meningkatkan efektivitas deteksi serangan seperti *malware polymorphic* yang lebih adaptif dibandingkan dengan generasi *virus* sebelumnya. Algoritma seperti *Random Forest*, *Support Vector Machines* (*SVM*), *K-Nearest Neighbors* (*KNN*), *Convolutional Neural Network* (*CNN*), *Naïve Byes*, dan *Decision Tree* (*DT*) telah terbukti dapat mendeteksi dengan keakuratan yang berbeda berdasarkan pola tertentu. Penelitian sebelumnya menunjukkan penggunaan algoritma *Decision Tree* pada deteksi *malware polymorphic* dapat menghasilkan akurasi yang tinggi dan baik yaitu 99.01% akurasi pada tahun 2022 (Akhtar & Feng, 2022). Oleh karena itu, akan dilakukan pengkajian ulang untuk menentukan apakah relevan atau tidaknya dalam melakukan deteksi pada *malware* khususnya dari *Framework Metasploit* pada 2024.

Dalam penelitian ini, akan diusulkan penggunaan *Decision Tree* sebagai algoritma untuk deteksi *file malware*. *Decision Tree* dipilih karena kemampuannya yang cepat dalam melakukan pelatihan dan deteksi, serta kesederhanaannya yang memungkinkan pemahaman yang lebih mudah terhadap proses pengambilan keputusan dalam deteksi *malware*. Selain itu, algoritma ini tidak membutuhkan sumber daya komputasi yang besar, yang menjadikannya pilihan yang baik untuk diterapkan pada sistem yang memerlukan respon cepat terhadap serangan.

Dengan menggunakan *Decision Tree*, diharapkan deteksi *malware* tidak memerlukan sumber daya yang besar. Penelitian ini bertujuan untuk memberikan solusi yang *optimal* dalam menghadapi ancaman *malware* yang terus berkembang, sehingga dapat memberikan perlindungan yang lebih baik bagi pengguna dan organisasi dari serangan siber yang merugikan.

## 1.2. Rumusan Masalah

Adapun rumusan masalah yang didapatkan dari latar belakang diatas adalah sebagai berikut:

1. Bagaimana cara pembuatan *malware* dan simulasi serangan *malware* dilakukan?
2. Bagaimana cara mengimplementasikan sistem deteksi *file malware* dengan menggunakan algoritma *decision tree*?
3. Bagaimana hasil evaluasi terhadap sistem deteksi *file malware* yang menggunakan algoritma *decision tree*?

## 1.3. Tujuan Penelitian

Adapun tujuan melakukan penelitian ini, antara lain:

1. Mengimplementasikan Langkah-langkah proses pembuatan *malware* dan melakukan simulasi serangan untuk menguji efektivitas dan dampak dari *malware* pada lingkungan uji
2. Mengembangkan dan mengimplementasikan sistem deteksi *file malware* dengan menggunakan algoritma *decision tree* untuk mengidentifikasi pola dalam lalu lintas jaringan.
3. Melakukan evaluasi terhadap sistem deteksi *file malware* berbasis algoritma *decision tree* untuk mengukur akurasi, kecepatan, dan efektivitas deteksi dalam menghadapi serangan *malware*.

## 1.4. Batasan Masalah

Adapun batasan masalah dalam penelititan ini, yaitu:

1. Jenis Serangan dan Tipe *file Malware*

   Penelitian ini hanya menganalisis jenis serangan *malware* yang menggunakan akses jarak jauh (*remote access*) dan terbatas pada tipe *file* seperti '*.exe'*, '*.pdf*', dan '*.doc', 'docx'*. Serangan *malware* dari sumber atau jenis lain tidak akan dibahas dalam penelitian ini.

2. Ruang Lingkup Analisis

Penelitian ini berfokus pada analisis pola *data* jaringan yang berkaitan dengan deteksi unduhan *file malware* dan tidak mencakup pencegahan atau aspek lainnya.

3. Sistem Operasi dan Konfigurasi

Penelitian ini dilakukan pada sistem operasi '*Windows 10 Pro Ghost Spectre*' versi *21h2* sebagai *Host* korban, yang tidak menggunakan *Windows Defender*. Untuk kemudahan analisis pada jaringan dan sistem operasi '*MacOS Sonoma 14.7.3'* untuk *Host* penyerang.

4. Proses Penyebaran *File*

Dalam penelitian ini, *XAMPP localhost* dari penyerang akan digunakan untuk mendistribusikan *file malware* dalam simulasi serangan jaringan.

5. Proses Unduhan *File*

Dalam penelitian ini, *WGET* dari korban akan digunakan untuk mengunduh *file* dalam simulasi.

6. Lingkup Jaringan

Dalam penelitian ini antara penyerang dan korban akan terjadi pada lingkup Jaringan Lokal (*LAN*) yang sama, dan tidak akan mencakup diluar jaringan lokal

## 1.5. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini antara lain sebagai berikut:

1. Bagi Peneliti dan Pengembang Keamanan Siber

Penelitian ini memberikan wawasan yang lebih dalam mengenai penggunaan *framework metasploit* untuk mengeksploitasi kerentanannya melalui pembuatan *malware* yang memberikan akses jarak jauh. Hasil dari penelitian ini dapat menjadi referensi bagi peneliti dan pengembang yang ingin mempelajari atau mengembangkan teknik-teknik penetrasi dalam konteks pengujian dan evaluasi keamanan jaringan. Selain itu, penerapan algoritma *Decision Tree* dalam deteksi *malware* juga dapat memberikan kontribusi pada pengembangan metode deteksi berbasis *machine learning*.

2. Bagi Organisasi atau Perusahaan

Penelitian ini memberikan manfaat langsung dalam meningkatkan sistem keamanan jaringan organisasi atau perusahaan. Dengan mengimplementasikan deteksi serangan *malware* berbasis algoritma *Decision Tree*, perusahaan dapat meningkatkan kemampuannya dalam mengidentifikasi ancaman secara lebih cepat dan akurat, sehingga dapat mengurangi risiko terhadap *data* dan sistem yang berharga. Selain itu, pemahaman tentang teknik-teknik serangan dari penggunaan *Framework Metasploit* dapat membantu organisasi dalam memperkuat kebijakan dan infrastruktur keamanan.

3. Bagi Pengguna dan Masyarakat Umum

Masyarakat umum, khususnya pengguna sistem informasi dan jaringan, dapat memperoleh manfaat dari penelitian ini dengan lebih memahami bagaimana *malware* dapat diidentifikasi dan diatasi. Penelitian ini dapat membantu pengguna, baik individu maupun perusahaan, untuk lebih waspada terhadap potensi ancaman serangan *malware* dan bagaimana melindungi perangkat dan pencegahannya.

## 1.6. Sistematika Penulisan

Penulisan proposal skripsi ini disusun dengan mengikuti sistematika yang memiliki kerangka sebagai berikut:

- **BAB I** **Pendahuluan**

  Bab ini berisi mengenai latar belakang, rumusan masalah, tujuan, manfaat, serta batasan masalah terkait simulasi dan deteksi serangan *malware* dengan menggunakan algoritma *Decision Tree*.

- **BAB II** **Tinjauan Pustaka**

  Bab ini memuat tinjauan pustaka dari penelitian sebelumnya serta pembahasan tentang teori, konsep, model, dan metode yang relevan dengan simulasi dan deteksi serangan *malware* menggunakan algoritma *Decision Tree*.

- **BAB III** **Metode Penelitian**

  Bab ini mengulas mengenai alur penelitian, rancangan sistem, metode pengumpulan data dan tahapan yang diterapkan dalam pengembangan sistem deteksi.

- **BAB IV** **Pengumpulan dan Pengolahan Data**

  Bab ini berisi proses pengumpulan data, tahap pengolahan data, dan hasil akhir yang telah diperoleh.

- **BAB V** **Analisis dan Pembahasan**

  Bab ini memuat kesimpulan dari analisis dan pembahasan mengenai rancangan yang telah dibuat, serta jawaban atas rumusan masalah dan tujuan penelitian.