BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam menggunakan media elektronik digital sekarang ini, memungkinkan banyak orang mengakses dan mengunduh berbagai macam sistem *file* yang ada pada internet [1]. Sebagian orang mengunduh suatu program disembarang website memungkinkan bersamaan dengan jenis *malware*. Setelah beberapa tahun, Trojan telah menjadi salah satu ancaman paling serius di dunia, mencuri informasi sensitif dan menghancurkan sistem manajemen informasi dari organisasi dan bisnis. Trojan sebagai jenis *malware* dengan latensi tinggi, tersembunyi tinggi, dan dalam situasi beresiko tinggi yang dapat merusak *psikologis* secara signifikan, selain kerugian finansial [10]. *Malware* menyebar dengan tujuan mendapatkan suatu informasi hanya dengan beberapa klik [2]. Ketika jumlah pengguna internet bertambah, kejahatan dunia maya menjadi lebih *kompleks* dan tersebar luas di kalangan penjahat. Setiap kejahatan yang dilakukan mengarah pada *system* komputer yang disebut sebagai *computer-related crime*, kejahatan yang dilakukan tidak menggunakan kejahatan fisik, melainkan hukum pidana yang bertindak dalam kejahatan dunia maya atau yang dikenal dengan istilah *cybercrime law*, pelaku tersebut dikenal dengan istilah *cybercriminal* [26].

Malware atau *Malicious software* umunya adalah program jahat yang dirancang untuk melakukan tugas tertentu seperti, mencuri informasi sensitive, mendapatkan akses tidak sah ke komputer, dan menyebabkan kegagalan sistem dalam berbagai situasi [3]. *Malware* digambarkan sebagai perangkat lunak berbahaya atau program komputer berbahaya dikategorikan sebagai, Virus, Trojan, Spyware, dan Worm. Salah satu jenis serangan malware trojan yang berbahaya adalah jenis *remote access trojan* RAT [9]. RAT adalah Trojan *malware* yang biasa digunakan oleh *Advanced Persistent Threat* (APT), untuk memberikan akses interaktif ke komputer yang disusupi data sensitive. Dalam

suatu sistem operasi ada beberapa peran penting dalam menyelesaikan tugas yang dikerjakan oleh pengguna melalui *software* pada sistem komputer. Namun, ada juga beberapa *software* yang tidak dapat membantu dalam menyelesaikan pekerjaan, melainkan malah merusak seperti jenis *software* yang dibuat untuk menyamar sebagai program yang sah, jenis *software* tersebut dikategorikan sebagai *Malicious software* jenis trojan [1].

Salah satu yang dapat dilakukan untuk memastikan *efektivitas* keamanan data atau komputer dengan memperbarui sistem operasi secara teratur [5]. Untuk itu perlu dilakukan analisis untuk tujuan menentukan *file* atau *software* pada komputer tersebut teridentifikasi dengan benar. Dalam dua dekade terakhir, deteksi malware telah menjadi salah satu masalah paling mendesak di bidang penelitian keamanan cyber [4]. Penelitian dilakukan dengan analisis statis (analisis kode), dan analisis dinamis (analisis sampel malware) dilakukan dengan memerlukan pengeksekusian pada contoh malware kemudian akan dipelajari perilaku yang muncul sehingga dapat memperoleh informasi terhadap cara sebuah malware tersebut berkembang dan pada sistem apa saja malware tersebut akan berkomunikasi, meskipun antara kedua tipe analisis tersebut mempunyai arah yang sama yaitu menjelaskan bagaimana malware bekerja namun, kemampuan, waktu dan peralatan yang dibutuhkan dalam menganalisa sangatlah berbeda [6].

Maka berdasarkan latar belakang diatas, maka perlu diketahui bagaimana mendeteksi *malware* menggunakan wireshark dalam proses *network analysis* pada komputer yang telah terinfeksi malware RAT. File dari malware yang telah menginfeksi komputer sebelumnya akan dilakukan analisis statis dan dinamis untuk melihat apakah malware telah berhasil di deteksi, untuk uji deteksi dilakukan dengan menggunakan VirusTotal dan Cuckoo. Maka dengan mengetahui deteksi *malware* dapat mempermudah kita dalam menganalisa malware njRAT.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka dapat dirumuskan permasalahan yang akan dibahas yaitu tentang, Bagaimana menganalisis malware Trojan dari njRAT menggunakan, analisis statis, analisis dinamis dan *network analysis* menggunakan *tools* VirusTotal, Cuckoo Sandbox dan Wireshark.

1.3 Batasan Masalah

Untuk lebih fokus dan terarahnya penelitian yang dilakukan berdasarkan Rumusan masalah yang diuraikan, Maka batasan dalam penelitian ini yaitu:

1. Penelitian ini hanya fokus pada analisis sampel malware *remote access Trojan (RAT)* dari hasil configurasi njRAT.
2. Sistem yang digunakan untuk menganalisis malware yaitu *Virtual Machine* (VM) dengan sistem operasi *windows 7*.
3. Penelitian ini hanya menggunakan sampel file dengan ekstensi *.exe* sebagai contoh analisis dan deteksi.
4. Anlisis statis dan dinamis pada malware dilakaukan secara otomatis dengan *tools* Cuckoo Sandbox.
5. *Network analysis* hanya menggunakan *tools* wireshark.

1.4 Tujuan Penelitian

Dari latar belakang sebelumnya adapun tujuan yang ingin dicapai dalam penelitian ini yaitu:

1. Untuk mengetahui proses analisis statis, analisis dinamis dan *network analysis.*
2. Untuk mengetahui hasil *scanning* yang dilakukan oleh *tools* Virus Total, Cuckoo Sandbox dari *file* yang berekstensi *server.exe.*
3. Untuk mengetahui hasil temuan pada malware njRAT yang dijalankan pada sistem operasi windows 7.

1.5 Metodologi Penelitian

Untuk memenuhi syarat dalam penulisan skripsi ini, dilakukan penelitian menggunakan metodologi dalam melewati tahapan-tahapan sebagai berikut:

1. Studi Pustaka (Literatur)

   Pada tahapan ini merupakan tahapan mencari referensi atau bukti-bukti yang berkaitan dengan tema yang diangkat dari judul untuk menunjang penelitian yang dilakukan.
2. Membangun *environment* untuk dilakukan instalasi modul serta *library* yang dibutuhkan oleh *tools* supaya bisa dijalankan dalam melakukan analisis sampel malware njRAT pada penelitian ini.
3. Implementasi

   Pada tahap ini penelitian akan mengimplementasikan 3 teknik yang akan digunakan saat proses analisis diantaranya yaitu analisis statis, analisis dinamis, dan network analisis. Analisis statis dan dinamis dilakukan secara otomatis menggunakan tools Cuckoo dan untuk *network analysis* akan di lakukan secara *realtime* saat malware sudah menginfeksi sistem.
4. Analisis Data

   Kegiatan analisis dilakukan terhadap malware njRAT, sampel malware yang berekstensi *.EXE* menggunakan metode analisis statis dan dinamis.
5. Penulisan Laporan

   Pada tahap ini, segala temuan yang terdapat selama proses analisis statis dan dinamis akan ditulis pada laporan akhir.

1.6 Manfaat Penelitian

Berdasarkan Latar belakang, Rumusan masalah, Batasan masalah, dan Tujuan penelitian yang diuraikan pada bagian sebelumnya. Dapat disimpulkan manfaat pada penelitian ini yaitu mampu memberikan gambaran tentang karakteristik dan prilaku dari malware njRAT khususnya pada pengguna windows.

1.7 Sistematika Penulis

Sistematika penulis terdiri dari beberapa tingkat yaitu sebagai berikut:

Bab I Pendahuluan

Pendahuluan, merupakan pengantar pada permasalahan yang akan dibahas. Menjelaskan tentang gambaran suatu penelitian yang terdiri dari, Latar belakang, Rumusan masalah, Batasan masalah, Tujuan penelitian, Metode penelitian, Manfaat penelitian dan Sistematika penulis.

Bab II Landasan Teori

Pada bagian ini menjelaskan tentang penelitian terkait berdasarkan teori-teori, referensi, jurnal dan laporan skripsi yang ada.

Bab III Metode Penelitian

Bab ini membahas tentang kerangka konsep penelitian yang digunakan dalam memperoleh pengetahuan lebih banyak tentang objek penelitian, hasil observasi atau pengumpulan data, dan gambaran umum pada objek penelitian, hingga rencana alur penelitian yang dilakukan.

Bab IV Pembahasan

Bab ini membahas tentang, rancangan proyek, Implementasi *coding* dan desain hingga evaluasi rancangan.

Bab V Penutup

Tahap ini adalah tahapan akhir yang dilakukan dalam penelitian, memuat tentang kesimpulan dari penilaian proyek yang dikerjakan serta memberikan saran terkait dengan kekurangan yang dihasilkan dalam penelitian untuk pengembangan ilmu di kemudian hari.

DAFTAR PUSTAKA

Pada bagian daftar pustaka akan diterapkan tentang penulisan sumber-sumber literatur atau referensi yang digunakan dalam penulisan ini.