BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam beberapa tahun terakhir ini telah terjadi serangan malware yang cukup mengganggu komunitas dunia TIK. Trend keamanan sekarang ini telah berubah dari serangan oleh perseorangan (hacker) menjadi espionage dari sebuah negara (cyberwar). Ditemukan bukti dari catatan serangan malware terhadap sistem komputer didunia,bahwa malware dapat memberikan dampak yang lebih besar dari segi kerugian materiil dan non materiil. Setiap orang mengalami kemungkinan besar untuk terserang *malware* dalam sistem komputer yang dimiliki karena *malware* dapat menyerang melalui media disk (offline) maupun internet, sms, chat (online).

Malcious software (malware) merupakan program komputer yang diciptakan dengan tujuan mencari kelemahan atau bahkan merusak software atau sistem operasi komputer. *Malware* dalam *bentuk virus, worm, dan trojan horses* merupakan ancaman utama bagi keamanan sistem jaringan komputer. *Malware* telah dirancang secanggih mungkin untuk membuat celah didalam sistem. Berbagai upaya untuk memproteksi seperti memasang IDS, IFS, Firewall tidak menjamin sebuah sistem aman dari serangan *malware*. Setiap *malware* diberikan teknologi pertahanan untuk melindungi dirinya sendiri dari segala ancaman. Dengan alasan tersebut dibutuhkan sebuah solusi dari serangan *malware*. Salah

satu solusi dari serangan *malware* adalah mengetahui gerak malware ketika berada pada sebuah sistem.

Wireshark merupakan salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya terrmasuk protokol didalamnya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis. Wireshark mampu menangkap paket-paket data atau informasi yang melakukan aktivitas dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karena itu tak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting seperti password email atau account lain) dengan menangkap traffic di dalam jaringan dan menganalisanya.

Mininet adalah emulator untuk membuat topologi dengan skala yang besar dan bisa menguji performanya dengan mudah. Mininet memungkinkan pemakai untuk membuat topologi jaringan.

Dari latar belakang dituliskan diatas dapat diambil penelitian yang dengan judul "Analisis Serangan Malware Menggunakan Wireshark Pada Simulasi Jaringan di Mininet". Penelitian serangan malware ini dari host penyerang ke host target , dan mencoba mengetahui informasi malware dari wireshark kemudian memberikan solusi untuk memproleh keamanan dalam jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan, maka dapat diambil rumusan masalah bagaimana "Analisis Serangan Malware Menggunakan Wireshark Pada Simulasi Jaringan di Mininet".

1.3 Batasan Masalah

Beberapa batasan masalah yang akan digunakan dalam penelitian ini adalah sebagai berikut.

1. Alamat IP yang digunakan adalah statis bukan dinamis.
2. Identifikasi serangan terbatas pada alamat IP sumber serangan dan jenis serangan dilakukan secara manual oleh manusia atau otomatis oleh *malware*.
3. Penggunaan wireshark pada mininet untuk mengetahui traffic serangan *malware* dan mengetahui informasi yang dibawa oleh *malware* tersebut.
4. Sistem operasi menggunakan LINUX Ubuntu 15.04.
5. Malware akan dinyatakan sebagai *malware* yang baru jika tidak berhasil diidentifikasi oleh antivirus.

1.4 Maksud dan Tujuan Penelitian

Berdasarkan permasalahan yang dibahas didalam penelitian ini, adapun tujuannya adalah sebagai berikut.

1. Mengidentifikasi alamat IP penyerang dan mengidentifikasi jenis serangan dilakukan oleh manusia atau oleh *malware*.
2. Menghasilkan analisis terhadap serangan *malware* yang dilihat dari traffic pada wireshark.

3. Syarat kelulusan bagi setiap mahasiswa STMIK AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memproleh gelar Sarjana Komputer.

1.5 Metode Penelitian

Penulis dalam melakukan penelitian dengan analisis serangan *malware* pada jaringan dimininet untuk mendapatkan informasi dari serangan *malware* dalam jaringan. Analisis dilakukan dengan cara mengetahui data dari host penyerang dan host target untuk mengidentifikasi malware lebih spesifik. Penggunaan software seperti wireshark pada mininet berguna untuk melihat traffic yang ada didalam jaringan dan menemukan masalah atau kendala yang dihadapi. Adapun metode yang digunakan :

1.5.1 Metode Pengumpulan Data

Teknik pengumpulan data yang digunakan oleh peneliti adalah studi pustaka. Teknik ini dipakai untuk mendapatkan informasi dari pustaka berupa buku referensi, journal, atau penelitian sebelumnya yang berkaitan.

1.5.2 Metode Analisis

Metode analisis adalah teknik pemecahan masalah yang menguraikan bagian-bagian komponen dengan mempelajari seberapa sistem bekerja. Setelah data terkumpul akan dilakukan analisa terhadap keseluruhan data yang sudah diperoleh.

1.5.3 Metode Pengembangan

Tahap ini merupakan tahap pengembangan dan pemeliharaan terhadap sebuah sistem setelah uji coba. Pengembangan sistem yang baru yang tidak ada sebelumnya menjadikan sistem mengalami perubahan semakin lebih baik.

1.5.4 Metode Testing

Pada tahap ini dilakukan pengujian terhadap sistem secara keseluruhan yang telah dibuat. Tujuan dari pengujian ini untuk menemukan kesalahan-kesalahan dalam sebuah sistem tersebut kemudian akan dilakukan perbaikan.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan akan memuat uraian secara garis besar isi laporan Skripsi per bab, adalah sebagai berikut:

BAB I : PENDAHULUAN

Bab ini merupakan pengantar dari pokok permasalahan yang dibahas dalam skripsi ini, yaitu tentang Latar Belakang Masalah, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Metode Penelitian dan Sistematika Penulisan.

BAB II : LANDASAN TEORI

Bab ini membahas teori-teori yang menjadi landasan dan pendukung dalam pelaksanaan penulisan penelitian.

BAB III : ANALISIS DAN PERANCANGAN

Bab ini menjelaskan tentang metode yang akan digunakan dalam penelitian serta menjelaskan secara singkat objek kemudian menganalisis masalah dan perancangan topologi kemudian melakukan penelitian secara langsung untuk mengetahui informasi yang dibawa oleh *malware* melalui wireshark pada jaringan SDN Openflow di mininet.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini menjelaskan tentang implementasi dari proses penelitian keamanan yang telah dibangun meliputi implementasi, analisa dan skenario uji coba serangan malware dari host penyerang ke host target.

BAB V : PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilaksanakan dan saran-saran dari masalah yang terkait untuk pengembangan sistem yang lebih baik lagi.

DAFTAR PUSTAKA

Pada bagian ini akan dipaparkan tentang sumber-sumber dan literatur yang digunakan dalam pembuatan laporan tugas akhir.

LAMPIRAN

Berisi tentang keseluruhan yang digunakan dan listing program dalam desain dan perancangan sistem.