

BAB I PENDAHULUAN

1.1 Latar Belakang

Komputer dan jaringan merupakan bagian terpenting dalam kehidupan sehari-hari. Jaringan komputer adalah protokol yang mendefinisikan sebuah pesan dan aturan untuk sebuah sistem. Sedangkan protokol adalah aturan yang mengatur peraturan pesan dalam jaringan komunikasi atau antara dua atau lebih perangkat lunak.

Analisis jaringan adalah proses menangkap *traffic* jaringan dan menganalisis secara detail untuk menentukan apa yang terjadi pada jaringan. Analisis paket melakukan *dissector* paket data yang ditangkap mengikuti protokol yang dikenal oleh analis, dan menghasilkan *traffic* dalam format yang mudah dibaca oleh manusia (de Vivo *et al.*, 1998).

Paket analisis adalah sebuah program perangkat lunak yang dapat mencegat dan mencatat *traffic* yang melewati jaringan digital (Connolly, 2003). Pada umumnya, paket analisis aktif digunakan oleh peretas kriminal untuk mengambil informasi sensitif dengan cara *sniffing*, meretas sistem komputer, merancang untuk menguji, memantau jaringan, perangkat yang terkoneksi, dan implementasi perangkat lunak yang berjalan di dalam sebuah jaringan (Orebaugh & Ramirez, 2004). Saat ini, paket analisis terkenal di dunia, beberapa industri dan institusi akademik adalah Wireshark. Oleh karena itu, Wireshark dipilih sebagai subjek peralatan utama dan target analisis yang akan dihasilkan.

Jaringan yang tidak terproteksi seperti jaringan nirkabel di tempat umum, membawa risiko serta ancaman bagi pengguna yang mengakses jaringan tersebut. Pada umumnya, koneksi nirkabel dilindungi dengan protokol WPA2-PSK atau disebut sebagai kata sandi. Tetapi, jaringan nirkabel pada tempat umum jarang dilengkapi dengan kata sandi untuk memudahkan pengguna terkoneksi dengan jaringan tersebut. Tentu saja hal ini membawa risiko bagi para penggunanya, dimana seseorang yang tidak bertanggung jawab yang juga terkoneksi pada jaringan tersebut dapat melakukan *sniffing* terhadap pengguna lainnya.

Wireshark merupakan alat *networking administrator* yang bekerja sebagai analisis lalu-lintas jaringan termasuk protokol yang ada di dalam jaringan tersebut, baik secara TCP, UDP maupun HTTP. Wireshark mampu menangkap paket-paket informasi dalam berbagai format protokol secara lengkap dan mudah untuk dianalisis. Wireshark sangat mirip dengan *tcpdump*, tetapi Wireshark memiliki antarmuka grafis serta mampu melakukan pencarian sortir serta

filtering tergantung pengguna. Terlepas dari kekurangan yang ada, Wireshark tetaplah sebuah aplikasi yang telah membantu banyak pengguna.

Tujuan dari tugas akhir ini yaitu untuk mempelajari penggunaan *add on* dengan perspektif yang berbeda dari standar alat Wireshark, dan dampak dari menggunakan jaringan terbuka, terutama dari sudut pandang keamanan informasi, dan implementasi alat antarmuka pengguna grafis untuk membuat *dissector* protokol khusus untuk Wireshark. Penulisan manual dapat memakan waktu yang lama dan membosankan. Namun, sangat baik untuk memiliki *add on* dengan cara membuat dua protokol buatan yang lebih cepat dan mudah dicari tanpa menghitung secara manual. Pengguna hanya perlu memahami dan mengetahui, dengan kata lain bagaimana paket protokol dibangun.

Pengembangan *scripting* Lua di dalam aplikasi Wireshark dapat dilakukan agar pengguna dapat membuat *scripting* yang dapat menghasilkan protokol baru dengan cara penyaringan, menjelaskan kegunaanya, dan untuk membuktikan fungsinya dengan beberapa pengujian kasus serta memanfaatkan *dissector* yang dihasilkan di Wireshark.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka dirumuskanlah masalah dalam penelitian ini, yaitu:

- a. Apa manfaat dari analisis paket menggunakan *scripting* Lua?
- b. Bagaimana cara kerja *scripting* Lua dalam analisis paket pada Wireshark?
- c. Bagaimana cara melindungi diri dari *sniffing* untuk mencegah pencurian data?

1.3 Batasan Masalah

Berdasarkan latar belakang di atas, penelitian ini untuk lebih fokus pada masalah yang akan diselesaikan, batasan masalah dalam penelitian yang akan dibahas adalah sebagai berikut:

- a. Penelitian ini hanya terlingkup pada perangkat di tempat umum.
- b. Mengambil seluruh paket yang ada di lingkungan.
- c. Mengembangkan *scripting* Lua yang akan digunakan.
- d. Menunjukkan kelebihan dan kekurangan yang ada pada *scripting* atau cara tersebut.

1.4 Tujuan Penelitian

Setiap penelitian yang dilakukan tentunya memiliki maksud dan tujuan yang jelas. Tujuan penelitian ini adalah untuk analisis paket menggunakan aplikasi Wireshark, dengan menggunakan informasi yang didapatkan dari hasil data *capture* sebagai uji coba, serta

membantu dan mempermudah pengguna dalam mengambil informasi dengan cara filter yang lebih cepat dari biasanya.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut:

- a. Secara akademis, penelitian ini diharapkan memberi kontribusi ilmiah pada kajian tentang *scripting* Lua di dalam aplikasi Wireshark.
- b. Secara praktis, penelitian ini diharapkan memberi manfaat melalui analisis yang dipaparkan pada pihak-pihak yang berkepentingan dalam analisis jaringan.
- c. Memberikan pandangan bagi pembaca maupun pada pihak – pihak yang ingin mencoba dan mengetahui manfaat *scripting* Lua untuk *Debugging* maupun untuk dilakukan penelitian lain.
- d. Bagi peneliti, peneliti mampu menerapkan media yang sesuai dalam materi pembelajaran tertentu. Serta peneliti mempunyai pengetahuan dan wawasan mengenai materi dan media pembelajaran yang sesuai.

1.6 Metode Penelitian

Metodologi penelitian berfungsi sebagai gambaran metode yang dilakukan dalam penelitian, penelitian ini terbagi menjadi empat tahap, yaitu:

- a. Studi Literatur: Penulis ini dilandaskan pada studi pustaka dengan mengumpulkan beberapa teori yang akan diambil secara relevan untuk menunjang tujuan ini melalui beberapa buku, jurnal, artikel, paper, makalah dan e-book yang berkaitan dengan jaringan komputer dan Bahasa Lua.
- b. Pengumpulan Hasil Data: Pada tahap pengambilan data *traffic*, penulis menggunakan aplikasi Wireshark yang akan terhubung ke *Router*.
- c. Analisis: Tahapan: analisis ini dilakukan untuk membandingkan menggunakan *scripting* Lua dan tanpa menggunakan *scripting* Lua.
- d. Kesimpulan dan Saran: tahapan ini adalah tahapan akhir untuk menyampaikan kesimpulan hasil yang diperoleh dari penelitian ini, dan saran dari kelebihan dan kekurangan pada hasil yang telah uji coba.

1.7 Sistematika Penulisan

Sistematika penulisan laporan bertujuan untuk memudahkan dalam memahami laporan Tugas Akhir. Berikut sistematika penulisan laporan Tugas Akhir ini, yaitu:

BAB I PENDAHULUAN

Bab ini berisikan tentang pengantar terhadap masalah – masalah yang akan dibahas seperti latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menguraikan hal-hal yang berhubungan dan mendukung dalam hal Jaringan, aplikasi, serta pemaparan teori.

BAB III METODE PENELITIAN

Bab ini membahas tentang pengumpulan kebutuhan, analisis dan alat *scripting* yang akan digunakan sebagai objek penelitian.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini akan diuraikan secara lengkap tentang masing-masing *scripting*, kelebihan dan kekurangan, serta baiknya digunakan sebagai uji coba dalam *filtering* atau *decoder*.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dari beberapa *scripting* yang telah dilakukan, serta saran – saran selama pengujian *scripting* diselesaikan.

DAFTAR PUSTAKA

Berisi referensi yang terkait dengan penelitian.

LAMPIRAN

Lampiran berisi hasil gambar–gambar dan *sourcecode* terkait penelitian (jika ada).