BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer menelusuri awal tahun 1960an. Sudah disepakati secara luas bahwa Internet global saat ini dimulai dari Advanced Research Projects Agency Network (ARPANet) Departemen Pertahanan A.S. pada tahun 1969, berdasarkan konsep yang diterbitkan pada tahun 1967. (Zeng, Gu, & Guo, 2015).

Indonesia merupakan salah satu negara dengan rata-rata *traffic* internet paling tinggi di dunia dalam beberapa tahun terakhir, berdasarkan informasi dari *detik.com* sekitar 38% dari seluruh lalu lintas di dunia berasal dari indonesia. Ini menunjukkan tingkat konektivitas dan penggunaan yang sangat tinggi. Teknologi sangat mempengaruhi proses aktivitas atau kinerja untuk organisasi besar seperti PT. LFC Teknologi Indonesia.

Menurut *Techrepublic.com* pada tahun 2007, sebuah pemadaman komputer di Bandara Internasional Los Angeles menyebabkan 17.000 penumpang berdiri pada penerbangan internasional selama 10 jam. Masalahnya terjadi karena otoritas Bea Cukai AS tidak bisa menyaring penumpang tanpa perangkat lunak. Menurut berita dari Techrepublic.com, cacat jaringan memungkinkan peretas mencuri hampir 46 juta nomor kartu kredit pada tahun 2007 dari TJX, perusahaan induk T.J. Maxx, Marshalls, HomeGoods, A.J. Wright, dan lainnya. Dipercaya bahwa keamanan yang lemah di sekitar LAN nirkabel perusahaan adalah masalahnya.

Menurut csoonline.com awalnya dilaporkan pada awal Oktober oleh blogger keamanan Brian Krebs, butuh beberapa minggu untuk mengetahui skala pelanggaran dan apa yang disertakan. Perusahaan tersebut awalnya melaporkan bahwa peretas telah mencuri hampir 3 juta catatan kartu kredit pelanggan terenkripsi, ditambah data masuk untuk sejumlah akun pengguna yang belum ditentukan.

Kemudian di bulan tersebut, Adobe mengatakan bahwa penyerang telah mengakses ID dan kata sandi terenkripsi untuk 38 juta pengguna aktif. Namun Krebs melaporkan bahwa sebuah file yang diposkan beberapa hari sebelumnya, "tampaknya menyertakan lebih dari 150 juta *username* dan *password hash* yang diambil dari Adobe "Setelah berminggu-minggu penelitian, akhirnya ternyata, begitu juga kode sumber beberapa produk Adobe, hack juga telah membuka nama pelanggan, *ID*, *password* dan informasi debit dan kartu kredit.

Berdasarkan berita dari *csoonline.com* pada bulan September 2016, raksasa internet yang dulu dominan, saat melakukan negosiasi untuk menjual dirinya ke Verizon, mengumumkan bahwa mereka telah menjadi korban pelanggaran data terbesar dalam sejarah, kemungkinan oleh "aktor yang disponsori negara," pada tahun 2014. Serangan tersebut membahayakan nama asli, alamat email, tanggal lahir dan nomor telepon dari 500 juta pengguna. Perusahaan mengatakan "mayoritas besar" kata kunci yang terlibat telah digabung menggunakan algoritma *bcrypt* yang kuat.

Beberapa bulan kemudian, pada bulan Desember, ia mengubur catatan sebelumnya dengan pengungkapan bahwa sebuah pelanggaran pada tahun 2013,

oleh sekelompok *hacker* yang berbeda telah membahayakan 1 miliar akun. Selain nama, tanggal lahir, alamat email dan kata kunci yang tidak terlindungi dengan baik seperti pada tahun 2014, pertanyaan dan jawaban keamanan juga dikompromikan. Pada bulan Oktober 2017, Yahoo merevisi perkiraan tersebut, dengan mengatakan bahwa, pada kenyataannya, semua 3 miliar akun pengguna telah disusupi.

Berdasarkan artikel dari *csoonline.com* Sony's Playstation Network dipandang sebagai pelanggaran data game terburuk yang pernah terjadi sepanjang masa. Dari lebih dari 77 juta akun terpengaruh, 12 juta memiliki nomor kartu kredit yang tidak dienkripsi. Hacker mendapatkan akses ke nama lengkap, kata sandi, *e-mail*, alamat rumah, riwayat pembelian, nomor kartu kredit dan login dan kata kunci *PSN / Qriocity*. "Cukup untuk membuat setiap orang keamanan yang baik bertanya-tanya, 'Jika seperti apa rasanya di Sony, seperti apa di perusahaan multi nasional lainnya yang duduk di jutaan catatan data pengguna?'" Kata John Linkous dari John. Dia mengatakan bahwa pihaknya harus mengingatkan mereka pada keamanan TI untuk mengidentifikasi dan menerapkan kontrol keamanan secara konsisten di seluruh organisasi mereka. Bagi pelanggan, "Hati-hati dengan siapa Anda memberikan data Anda. Mungkin tidak sepadan dengan harga untuk mendapatkan akses ke game online atau aset virtual lainnya."

(Prihantono dan dkk, 2013) *Raspberry* Pi adalah komputer berukuran kartu kredit yang dihubungkan ke TV dan *keyboard* Anda. Ini adalah komputer kecil yang mumpuni yang bisa digunakan dalam proyek elektronik, dan untuk banyak hal yang dilakukan PC *desktop* Anda, seperti *spreadsheet*, pengolah kata, *browsing* internet, dan permainan. Ini juga memainkan video berdefinisi tinggi. Kami ingin

melihatnya digunakan oleh orang dewasa dan anak-anak di seluruh dunia untuk belajar pemrograman dan pembuatan *digital*. Berdasarkan informasi dari *alphr.com* pada Februari 2016, generasi ketiga dari Model B *Raspberry* Pi telah dirilis. Di luar revisi ini, yang *mengupgrade* prosesor utama di papan tulis ke versi 64-bit, tidak ada rencana segera untuk merilis model baru lagi.

PT. LFC Teknologi Indonesia adalah sebuah perusahaan penanaman modal asing yang bergerak pada bidang distribusi, pemeliharaan dan penyedia solusi di bidang metrologi, pemotongan, *laser* dan mesin industri berat. Banyak perusahaan pokok dari berbagai negara seperti Belanda, China, Italia, Jepang, Jepang, beserta Taiwan dan lain-lain bekerja sama dengan PT.LFC Teknologi Indonesia. Dengan bekerja sama dengan perusahaan yang berada di luar negara tentunya dibutuhkan alat bantu komunikasi jarak jauh seperti *e-mail*, *Cisco WebEx*, *Skype* maupun di *remote* secara langung menggunakan aplikasi *teamviewer*. Dengan alat komunikasi yang ada memerlukan koneksi internet yang stabil dan cepat sehingga proses komunikasi antar perusahaan bisa berjalan lancar. Akan tetapi sering ditemukannya masalah pada saat berkomunisi dengan pelanggan karena koneksi internet yang tidak stabil yang biasanya kita sebut sebagai *packet loss*.

Pada tahun 2000-2007 banyak terjadinya kejahatan komputer yang merugikan aktivitas manusia dan dari situlah banyak yang melihat sisi negatif dari perkembangan teknologi, maka dari itu kita membutuhkan Keamanan Jaringan. Keamanan Jaringan sangatlah penting dalam kehidupan keseharian kita. Setiap individu memiliki privasi dan privasi itu akan berbahaya jika diketahui oleh orang lain, misalnya pin kartu kredit maupun KTP. Asal mula kejahatan komputer itu

sendiri berawal dari “iseng”, karena pertama kali kesalahan sesuatu ditemukan karena kesengajaan. Seiring perkembangan waktu rasa ingin tahu akan muncul dan mereka mulai mencoba meretas keamanan sekolah, kantor dan bank.

PT. LFC Teknologi Indonesia juga memiliki masalah yang sama seperti beberapa perusahaan yang ada diatas. Pada saat PT. LFC Teknologi Indonesia baru berjalan mengalami masalah dalam kinerja mereka seperti *data crash,* internet tidak jalan, tidak bisa *sharing file* satu antar lain beserta pernah di retas oleh pihak luar. Maka dari itu mereka membangun TI yang berfungsi dalam mengatasi masalah yang ada pada aktivitas jaringan dalam perusahaan. Untuk dapat memastikan perbaikan yang telah dilakukan oleh bagian TI perusahaan tersebut perusahaan memberikan penelit akses untuk melaksanakan penelitian ini untuk mengukur sejauh mana keamanan jaringan dan *network monitoring* yang telah ada berjalan.

Dalam jaringan data hari ini, analisis lalu lintas - menentukan tautan mana yang semakin padat dan mengapa - biasanya dilakukan oleh komputer di tepi jaringan, yang mencoba menyimpulkan keadaan jaringan dari waktu paket data yang berbeda mencapai tujuan mereka. Layanan pemantauan media telah banyak disebut dari waktu ke waktu, karena pemeran baru memasuki pasar, bentuk baru media diciptakan, dan karena penggunaan baru dari konten yang tersedia dikembangkan. Kelompok yang ada dapat menyediakan layanan pemantauan semacam itu, yang berkaitan dengan tujuan utama mereka, sementara lembaga pemantau umumnya menyediakan seperti bisnis utama mereka. *Packet loss* yang ada pada PT.LFC Indonesia dapat disebabkan juga banyaknya aktivitas yang sedang berjalan dalam jaringan perusahaan pada waktu yang bersamaan. Untuk

memastikan apakah aktivitas yang sedang dalam jaringan perusahan yang menyebabkan terjadinya *packet loss* maka peneliti menggunakan aplikasi *Wireshark* untuk memonitoring aktivitas jaringan yang ada pada PT. LFC Teknologi Indonesia.

Peneliti memakai *Raspberry Pi* karena mengikuti persetujuan dengan PT. LFC, dimana alat peneliti perlu ditinggalkan didalam perusahaan sebagai jaminan untuk memastikan bahwa peneliti tidak melakukan manipulasi data. Beserta *Raspberry Pi* yang peneliti gunakan adalah baru tidak ada cantum tangan dari pihak luar sehingga dapat dipastikan alat yang peneliti pakai bersih dari *virus* ataupun *malware*. Peneliti juga memberikan perusahaan akses untuk memakai atau menggunakan fitur dari alat yang peneliti siapkan sehingga pihak TI perusahaan dapat memperbaiki masalah yang ditemukan.

Sistem pengamanan yang dapat menangani ancaman dari pihak luar melalui jaringan internet menjadi suatu hal yang mutlak dimiliki sebuah perusahaan atau organisasi. Dibalik itu, pengawasan atas pengguna koneksi internet dalam organisasi tersebut juga harus diperhatikan. Akses berlebih yang diberikan kepada pengguna akan mengakibatkan penyimpangan di luar kepentingan organisasi. Dalam hal ini, diperlukan pembatasan hak akses pengguna ke situs berisiko dan yang tidak diperkenankan oleh pihak organisasi. Maka dari kutipan diatas penulis mengangkat judul "**IMPLEMENTASI *RASPBERRY PORTABLE* SEBAGAI PENGUKURAN KEAMANAN JARINGAN DAN *NETWORK MONITORING***".

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan diatas, masalah dapat di identifikasikan sebagai berikut:

1. Adanya ancaman berupa usaha untuk mengakes data pada *server* perusahaan yang dilakukan pengamanan berupa *password security*
2. PT. LFC Teknologi Indonesia pernah terjadi *data crash,* internet tidak jalan, tidak dapat *sharing file*.
3. Terdapat banyaknya instasi yang tidak kebal terhadap serangan *cybercrime*
4. Seringnya terjadi paket *loss*, *ping* dan *jitter yang tinggi*

1.3 Pembatasan Masalah

Mengingat banyaknya perkembangan yang bisa ditemukan dalam permasalahan ini, maka penulis membatasi lingkup penelitian sebagai berikut:

1. Hanya berfokus dalam pengukuran keamanan jaringan *LAN/WLAN* tentang *Authentication*, *Privacy* dan *Availability*.
2. Hanya menggunakan aplikasi *Wireshark* dan *Nagios* sebagai alat bantu menganalisis keamanan jaringan dan *network monitoring*.
3. Penelitian ini akan dilakukan PT.LFC Teknologi Indonesia.
4. Aplikasi *Nagios* yang dipakai adalah *Nagios Core* (*Open Source*).
5. *Nagios* hanya menganalisis servis *basic* tiap *host*.

6. Aplikasi *website speedtest.net*

1.4 Rumusan Masalah

Berdasarkan identifikasi masalah yang diatas, maka penulis dapat merumuskan masalah penelitian sebagai berikut:

1. Bagaimana mendeteksi sejauh mana kualitas keamanan jaringan topologi lama pada PT.LFC Teknologi Indonesia secara lokal?
2. Bagaimana kondisi komputer setiap user setelah sejak diterapkan TI untuk perusahaan?
3. Bagaimana kita dapat mendeteksi adanya celah *cybercrime*?
4. Bagaimana kita dapat mengetahui adanya paket *loss*, *ping* dan *jitter yang tinggi?*

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang ada diatas, maka tujuan penelitian ini adalah:

1. Untuk mengetahui sejauh mana kualitas keamanan jaringan dengan memakai topologi yang sudah ada pada PT.LFC Teknologi Indonesia dalam lokal.
2. Untuk mengetahui apakah masalah komputer yang ada pada *user* yang terjadi sebelumnya akan terjadi lagi
3. Untuk mengetahui cara mendeteksi adanya celah *cybercrime*.

4. Untuk mengetahui cara mendeteksi paket *loss*, *ping* dan *jitter yang tinggi*

1.6 Manfaat/kegunaan

Penelitian yang penulis lakukan ini diharapkan memberikan manfaat secara teoretis maupun praktis.:

1. Manfaat teoritis

   Penelitian memuat ilmu pengetahuan tentang kegunaan fungsi dari menganalisis keamanan jaringan menggunakan *Wireshark* dan *Nagios*

2. Manfaat Praktis

   a) Bagi Lembaga Pendidikan

      Penelitian ini dapat digunakan sebagai masukan untuk pengembangan keamanan jaringan dan network monitoring yang akan datang.

   b) Bagi Kantor/Perusahaan

      Penelitian ini bermanfaat untuk mengetahui betapa bahayanya kejahatan komputer dan kantor/perusahaan akan lebih teliti dalam mengatur keamanan jaringan dan melakukan *network monitoring*.