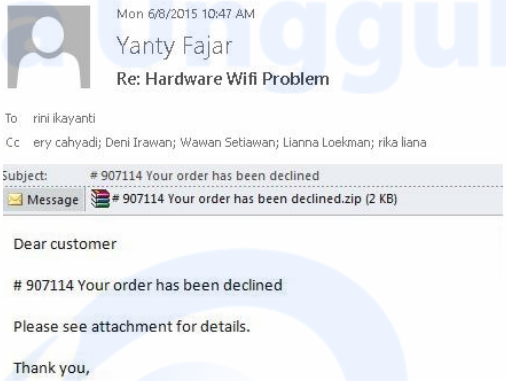
BAB I
PENDAHULUAN

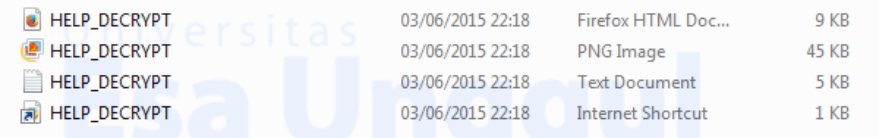
1.1. Latar Belakang

Pada tanggal 8 Jun 2015 jam 17:28 wib, *IT* menemukan *file* yang terinfeksi *wannacry ransomware* di *file server* PT. Royal Lestari Utama (RLU). *Wannacry ransomware* menginfeksi *file server* melalui pesan *email* dan lampiran palsu.



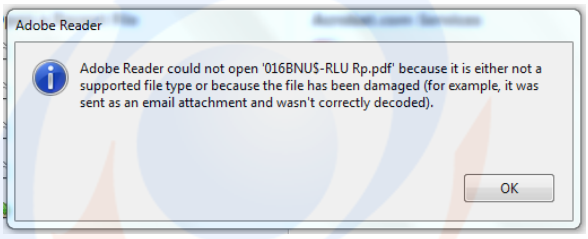
Gambar 1.1 *Screenshot* pesan *email* dan lampiran palsu

Ketika lampiran palsu di ekstrak dan di klik akan berisi *wannacry ransomware* seperti Gambar 1.2, *ransomware* akan mengenkripsi *file* (* .doc, * .docx, * .xls, * .ppt, * .psd, * .pdf, * .eps, * .ai, * .cdr , * .jpg, dll.) yang disimpan di *file server*.

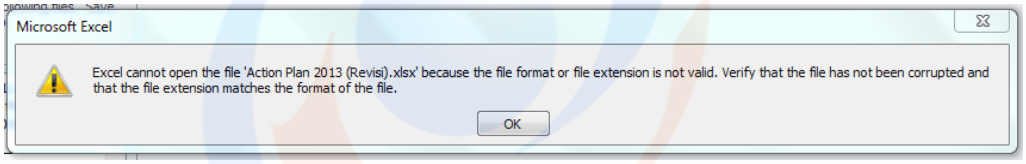


Gambar 1.2 Bentuk *wannacry ransomware*

Gambar 1.3 dan Gambar 1.4 adalah contoh *format file .pdf dan .xlsx* yang terinfeksi *wannacry ransomware.*

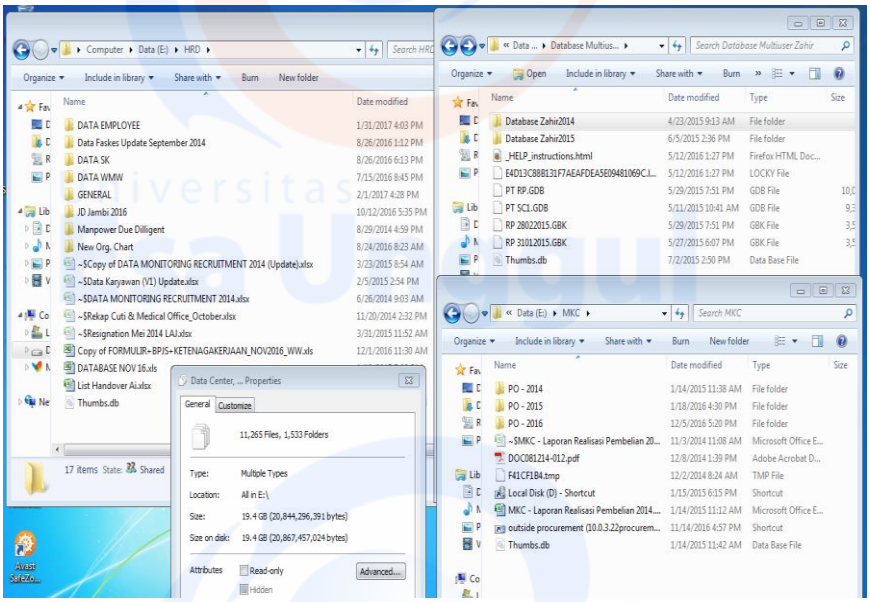


Gambar 1.3 file .pdf yang telah terinfeksi *wannacry ransomware*



Gambar 1.4 *file excel* yang telah terinfeksi *wannacry ransomware*

Wannacry ransomware mengunci data sehingga tidak dapat diakses oleh pengguna. Cara kerja layaknya *virus* komputer pada umumnya, *ransomware* sering tiba di komputer dalam bentuk *spam email* atau pembaruan perangkat lunak palsu. Saat penerima *email* mengklik tautan atau membuka lampirannya. *Wannacry ransomware* kemudian mulai bekerja dan mengenkripsi data pengguna. Ketika data telah benar – benar terkunci, *wannacry ransomware* meminta bayaran. Seringkali dalam bentuk *bitcoin* karena lebih sulit dilacak untuk pengembalian data. Uang tebusan biasanya satu atau dua *bitcoin*, setara dengan $500. Setelah melewati batas waktu pembayaran, jumlah uang tebusan akan bertambah (Ransomware, 2015). Akibat permasalahan ini perusahaan mengalami kehilangan 11.265 data. Dan jika dikonversikan ke uang, perusahaan mengalami kerugian sebesar 11.265 files x $500 = $5.632.500.



Gambar 1.5 Jumlah data yang telah terinfeksi *wannacry ransomware*

Sistem keamanan jaringan dalam *core business* PT. RLU saat ini menggunakan *traditional firewall* yang tidak dapat mendeteksi paket data berdasarkan *behavior* dan *content* sehingga keamanan jaringan komunikasi di

jaringan internal dan eksternal PT. RLU sangatlah riskan. Dimana saat ini serangan yang dilakukan semakin bervariatif seperti *Distributed Denial Of Service* (DDOS) dan *Wannacry ransomware.*

Next Generation Firewall (NGFW) dapat melakukan inspeksi paket data berdasarkan *behaviour* dan *content* sehingga paket data yang mencurigakan dapat dideteksi melalui fitur *Intrusion Prevention System* (*IPS*)*, Anti-Bot, Antivirus,* dan *Anti-Spam & Email Security*. Pendekatan *waterfall* adalah model yang digunakan untuk memastikan keberhasilan memperbaiki permasalahan keamanan jaringan di PT. RLU. Menanggapi perihal temuan tersebut, *corporate management* PT. RLU memutuskan untuk mengambil langkah-langkah *preventif* agar permasalahan tersebut bisa diminimalisir.

1.2. Identifikasi Masalah

Identifikasi masalah membahas masalah yang dijadikan sebagai topik tugas akhir. Identifikasi masalah digali sedemikian rupa sehingga dapat dibuat hubungan fungsional antar *variable* yang diteliti. Dalam konteks diatas, tugas akhir ini mencoba untuk menemukan dan menggali informasi terkait dengan identifikasi masalah sebagai berikut:

1. Apa *NGFW* yang paling direkomendasikan?,
2. Bagaimana cara menguji keamanan jaringan *NGFW* menggunakan metode serangan *DDOS* dan *Wannacry ransomware*,
3. Bagaimana konfigurasi dan fitur keamanan yang harus digunakan untuk mengatasi serangan tersebut?.

1.3. Tujuan Tugas Akhir

Tujuan yang ingin dicapai dalam tugas akhir ini adalah:

1. Memperbaiki permasalahan keamanan jaringan di PT. RLU.
2. Mencegah risiko kehilangan data, kerugian material, dan melumpuhnya pelayanan publik.
3. Agar efisien dan efektif dalam melakukan *scanning* dari variasi serangan tanpa mempengaruhi performa dari jaringan.

1.4. Manfaat Tugas Akhir

Manfaat dari tugas akhir ini dikelompokkan menjadi 3 (tiga) yaitu:

1. Bagi Akademis

   Dengan adanya tugas akhir ini diharapkan agar memberikan manfaat untuk meningkatkan dan mengembangkan ilmu pengetahuan di bidang keamanan jaringan serta penerapannya dilapangan.

2. Bagi Perusahaan

   Teknologi *NGFW* ini dapat mencegah, mendeteksi, dan meredakan serangan dari varian *DDOS* dan *wannacry ransomware*.

3. Bagi Penulis

   Mengembangkan dan menambahkan wawasan berpikir sehingga tercapai keselarasan antara teori yang didapat dari perkuliahan dan praktek yang terjadi di dunia kerja.

1.5. Lingkup Tugas Akhir

Lingkup dari tugas akhir ini:

1. *Life cycle* yang digunakan adalah *waterfall* model.
2. Uji coba serangan *DDOS* menggunakan *Tool Low Orbit Ion Canon (LOIC) GUI* dengan jenis serangan *UDP Flood Attack* dan *wannacry ransomware* yang diujikan terhadap kedua *firewall* di PT. RLU.
3. Melakukan perancangan dan pembangunan *NGFW* berbasis *DDOS* dan *wannacry ransomware* di PT. RLU.

1.6. Sistematika Penulisan

Sistematika penulisan tugas akhir ini dibuat berdasarkan urutan dibawah ini:

BAB I PENDAHULUAN

Berisi tentang latar belakang pemilihan judul, identifikasi masalah, tujuan tugas akhir, manfaat tugas akhir, lingkup tugas akhir, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini membahas tentang teori-teori yang menjadi acuan dalam pembahasan analisa dan pemecahan dari permasalahan yang dibahas, sehingga memudahkan penulis dalam menyelesaikan masalah.

BAB III ANALISIS SISTEM BERJALAN

Bab ini membahas mengenai proses bisnis dan analisa masalah, solusi pemecahan masalah, dan memberikan sejarah singkat perusahaan sebagai objek riset.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan tahapan-tahapan yang dilalui dalam penyelesaian penelitian ini, mulai dari gambaran umum PT.RLU, pengolahan atau analisis data, pemaparan data kuantitatif, pembahasan data penelitian.

BAB V KESIMPULAN DAN SARAN

Membahas kajian dan penelitian terhadap hasil analisis temuan penelitian. Ada dua alternatif cara penulisan kesimpulan dan saran, yakni dengan cara butir demi butir atau dengan uraian padat.