Nama: Frizario Yuda Hanggara
NIM : 1210651115
Kelas : TI – D

1. Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning. Resume bukan hasil translate, melainkan inti-intinya saja dari materi yang sudah Anda pahami pada ebook tersebut. Hasil resume **tidak boleh** sama dengan teman-temannya, akan tetapi tema yang dibahas boleh sama.

Saya memilih untuk meresume **Cryptography**.
Cryptography (Kriptografi) adalah suatu cara bagaimana caranya agar pengiriman suatu pesan dapat dilakukan dengan aman. Crypto berarti secret (rahasia), sedangkan graphy berarti writing (tulisan). Cara yang dilakukan dalam menggunakan media elektronik adalah dengan menyandikan informasi dengan suatu kode tertentu (encryption) sehingga tidak bisa terbaca (ciphertext) dan mengembalikan hasil sandi tersebut (decryption) sehingga dapat dibaca oleh penerima pesan (plaintext).

Tugas utama Cryptogrphy adalah untuk menjaga agar baik plaintext maupun kunci ataupun keduanya tetap terjaga kerahasiaannya dari penyadap (disebut juga dengan lawan, penyerang, pencegat, penyelundup pesan, musuh, attacker dan sebagainya). Selain untuk keamanan, manfaat dari Cryptography ini adalah untuk :

- Authentication : Penerima pesan dapat memastikan keaslian pengirimnya. Penyerang tidak dapat berpura-pura sebagai orang lain.
- Integrity : Penerima harus dapat memeriksa apakah pesan telah dimodifikasi ditengah jalan atau tidak. Seorang penyusup seharusnya tidak dapat memasukkan tambahan ke dalam pesan, mengurangi atau merubah pesan selama data berada diperjalanan.
- Nonrepudiation : Pengirim seharusnya tidak dapat mengelak bahwa dialah pengirim pesan sesungguhnya. Tanpa Cryptography, seseorang dapat mengelak bahwa dialah pengirim pesan yang sesungguhnya.
- Authority : Informasi yang berada pada sistem jaringan seharusnya hanya dapat dimodifikasi oleh pihak yang berwenang. Modifikasi yang tidak diinginkan, dapat berupa penulisan tambahan pesan, pengubahan isi, pengubahan status, penghapusan, pembuatan pesan baru (pemalsuan), atau menyalin pesan untuk digunakan oleh penyerang.

Untuk membuka (decrypt) data tersebut dapat digunakan dua buah cara :
1. Menggunakan kunci yang sama dengan kunci yang digunakan untuk mengenkripsi (digunakan pada kasus private key cryptography).
2. Menggunakan kunci yang berbeda (digunakan pada kasus public key cryptography).

2. Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan temen-temennya.

Keylogger adalah sebuah modul perangkat lunak yang berjalan diam – diam di komputer, ponsel, atau tablet. Perangkap penekanan tombol dimasukkan pada keyboard atau keypad mereka. Informasi yang ditangkap kemudian dikirim ke orang yang melakukan monitoring. Tetapi keyloggers melakukan lebih karena anda akan melihat. Mereka dipaketkan dengan fitur lain yang memungkinkan Anda melihat hampir semua kegiatan yang dilakukan pada perangkat dimonitor.