UAS Keamanan Informasi Kelas TI-PAGI

Nama : Muhammad Indra Permadi
Nim : 1310651151
Kelas : TI-E
Chapter : 3

Soal!!

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.

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.

Jawab :

1. Chapter 3 : **Informasi Tata Kelola Keamanan dan Manajemen Risiko :**

Tugas kita sebagai profesional keamanan informasi adalah untuk mengevaluasi risiko terhadap kritis kami

aset dan menyebarkan perlindungan untuk mengurangi risiko tersebut. Kami bekerja dalam berbagai peran: firewall

insinyur, penguji penetrasi, auditor, manajemen, dll.

Staf keamanan informasi berpengetahuan dan berpengalaman dengan mendukung dan kepemimpinan pribadi adalah kunci keberhasilan.

Semua profesional keamanan informasi menilai risiko: kita melakukannya begitu sering sehingga menjadi sifat kedua. Analisis Risiko akurat adalah keterampilan penting untuk keamanan informasi profesional.

Kami keputusan risiko akan menentukan yang pengamanan kita menyebarkan untuk melindungi aset dan jumlah uang dan sumber daya yang kami habiskan melakukannya. Keputusan yang buruk akan menghasilkandi buang uang atau, bahkan lebih buruk, data dikompromikan. Aset adalah sumber daya berharga Anda mencoba untuk melindungi. Aset dapat data, sistem, orang, bangunan, properti, dan sebagainya.

Ancaman adalah segala sesuatu yang berpotensi dapat menyebabkan kerusakan pada aset. Ancaman termasuk gempa bumi, listrik padam, atau cacing berbasis jaringan. Dampak adalah keparahan kerusakan, kadang-kadang dinyatakan dalam dolar. Biaya kadang-kadang digunakan untuk alasan itu.

Menghitung Annualized Loss Expectancy

perhitungan memungkinkan Anda untuk menentukan biaya tahunan kerugian akibat risiko. Setelah dihitung, ALE memungkinkan Anda untuk membuat

keputusan untuk mengurangi risiko. Bagian ini akan menggunakan contoh resiko karena laptop tidak terenkripsi hilang atau dicuri. Solusinya adalah mahal, sehingga Anda perlu meyakinkan manajemen yang solusinya adalah berharga.

Menggunakan contoh enkripsi laptop kami, biaya dimuka perangkat lunak enkripsi laptop adalah $ 100 / laptop, atau $ 100.000 untuk 1000 laptop. Vendor biaya 10% per tahun Biaya dukungan atau $ 10,000 / tahun. Anda memperkirakan bahwa ia akan mengambil 4 jam staf per laptop untuk menginstal perangkat lunak atau 4000 jam staf. Staf yang akan melakukan pekerjaan ini membuat $ 50 / jam plus keuntungan. Termasuk manfaat, biaya staf per jam adalah $ 70 kali 4000 jam, yaitu $ 280.000. Perusahaan Anda menggunakan 3-tahun teknologi refresh siklus, sehingga Anda menghitung total Biaya Kepemilikan lebih dari 3 tahun:

Biaya perangkat lunak: $ 100,000

Tiga tahun Vendor dukungan: $ 10.000 3¼ $ 30.000?

Biaya staf per jam: $ 280,000

Biaya Total Kepemilikan lebih dari 3 tahun: $ 410,000

Biaya Total Kepemilikan per tahun: $ 410.000 / 3 ¼ $ 136.667

Atau tahun tahunan Biaya Total Kepemilikan untuk proyek enkripsi laptop adalah $ 136.667 per tahun.

Tunggal Rugi Harapan rugi harapan tunggal (SLE) adalah biaya kerugian tunggal. SLE adalah Nilai Aktiva (AV) kali Factor Exposure (EF). Dalam kasus kami, SLE adalah $ 25.000 (Nilai Aktiva) kali 100% (Exposure Factor) atau $ 25.000. Tingkat tahunan Terjadinya tingkat Tahunan Kejadian (ARO) adalah jumlah kerugian Anda menderita per tahun. Melihat melalui peristiwa masa lalu, Anda menemukan bahwa Anda telah menderita 11 hilang atau dicuri laptop per tahun rata-rata. ARO Anda adalah 11. Annualized Loss Expectancy Rugi Harapan Annualized (ALE) adalah biaya tahunan Anda karena risiko. Hal ini dihitung dengan mengalikan Harapan Loss Tunggal (SLE) kali Rate Tahunan Kejadian (ARO).

Hilangnya nyawa manusia memiliki dampak dekat-tak terbatas pada ujian.

Matrix Analisis Risiko menggunakan kuadran untuk memetakan kemungkinan risiko terjadi terhadap konsekuensi (atau dampak) risiko yang akan memiliki. ditunjukkan pada Matrix Analisis Risiko memungkinkan Anda untuk melakukan Kualitatif Analisis Risiko (lihat

Bagian "Kualitatif dan Analisis Risiko Kuantitatif") berdasarkan kemungkinan (dari "Langka" untuk "hampir pasti") dan konsekuensi (atau dampak), dari "tidak signifikan" untuk "Bencana." Skor yang dihasilkan rendah (L), sedang (M), tinggi (H), dan ekstrim risiko (E). Risiko rendah ditangani melalui proses normal, risiko moderat memerlukan manajemen pemberitahuan, risiko tinggi memerlukan pemberitahuan manajemen senior.

ISO 17799 adalah nomornya untuk ISO 27002 pada tahun 2005 untuk membuatnya konsisten dengan 27000 seri standar keamanan ISO. ISO 27001 adalah standar terkait, secara resmi disebut "ISO / IEC 27001: 2005 techniques- Informasi teknologi Security Keamanan Sistem Informasi- Persyaratan Manajemen. "ISO 27001 didasarkan pada BS 7799 .

Perhatikan bahwa judul ISO 27002 termasuk kata "teknik"; ISO 27001 mencakup kata "persyaratan." Sederhananya, ISO 27002 menjelaskan keamanan informasi terbaik praktek (Teknik), dan ISO 27001 menjelaskan proses untuk audit (Persyaratan).

COBIT (Kontrol Tujuan Informasi dan Teknologi yang terkait) adalah kontrol

kerangka kerja untuk mempekerjakan pemerintahan keamanan informasi praktik terbaik dalam sebuah organisasi. COBIT dikembangkan oleh ISACA (Audit Sistem Informasi dan Control Association, lihat http://www.isaca.org).

ITIL (Information Technology Infrastructure Library) adalah suatu kerangka kerja untuk menyediakan pelayanan terbaik di IT Service Management (ITSM).

Sertifikasi adalah pemeriksaan rinci yang memverifikasi apakah sistem memenuhi didokumentasikan persyaratan keamanan. Akreditasi penerimaan pemilik data tentang risiko yang diwakili oleh sistem itu. Proses ini disebut Sertifikasi dan Akreditasi atau C & A. NIST Special Publication 800-37 "Panduan untuk Sertifikasi Keamanan dan Akreditasi Sistem Informasi Federal "(lihat http://csrc.nist.gov/publications / nistpubs / 800-37-Rev 1 / sp800-37-Rev 1-final.pdf) menjelaskan US Sertifikasi federal dan Akreditasi.

Sertifikasi dapat dilakukan oleh pihak ketiga yang terpercaya seperti auditor. Sertifikasi menyelidiki sistem, memeriksa dokumentasi, dan mungkin mengamati operasi.

Mereka mengaudit sistem untuk memastikan kepatuhan. Sertifikasi ini hanya rekomendasi sertifikasi tidak memiliki kemampuan untuk menyetujui sistem atau lingkungan. Hanya pemilik data (accreditor) dapat melakukannya.

NIST SP 800-37 menjelaskan Sertifikasi empat langkah dan proses Akreditasi: Fase inisiasi Fase sertifikasi keamanan Fase akreditasi keamanan Terus menerus fase pemantauan Sistem keamanan informasi dan rencana mitigasi risiko yang diteliti selama inisiasi fase. Keamanan Systemis dinilai dan didokumentasikan selama keamanan fase sertifikasi. Keputusan untuk menerima risiko yang diwakili oleh sistem yang dibuat dan didokumentasikan selama fase akreditasi keamanan. Akhirnya, setelah terakreditasi, yang

keamanan yang sedang berlangsung dari sistem diverifikasi selama fase pemantauan terus menerus.

TOP LIMA PERTANYAAN terberat

1. Manakah dari berikut ini akan menjadi contoh dari pernyataan kebijakan?

A. Melindungi PII oleh pengerasan server

B. Harden Windows 7 dengan terlebih dahulu memasang gambar OS pre-hardened

C. Anda dapat membuat password yang kuat dengan memilih huruf pertama dari setiap kata dalam kalimat dan pencampuran dalam angka dan simbol

D. Download patokan CISecurity Windows dan menerapkannya

Gunakan skenario berikut untuk menjawab pertanyaan 2-4:

Perusahaan Anda menjual Apple iPod online dan telah mengalami banyak Denial of Service (DoS) serangan. Perusahaan Anda membuat rata-rata $ 20.000 laba per minggu, dan khas Serangan DoS menurunkan penjualan sebesar 40%. Anda menderita tujuh serangan DoS rata-rata per tahun. Sebuah layanan DoS-mitigasi yang tersedia untuk biaya berlangganan sebesar $ 10.000. per bulan. Anda telah diuji layanan ini dan percaya akan mengurangi serangan.

2. Apa Rate Tahunan Kejadian dalam skenario di atas?

A. $ 20.000

B. 40%

C. 7

D. $ 10.000

3. Apa Loss Expectancy Annualized (ALE) dari kehilangan penjualan iPod karena DoS
serangan?

A. $ 20.000

B. $ 8.000

C. $ 84.000

D. $ 56.000

4. Apakah layanan DoS-mitigasi investasi yang baik?

A. Ya, itu akan membayar sendiri

B. Ya, $ 10.000 kurang dari $ 56.000 Rugi Annualized Harapan

C. Tidak, Total Biaya tahunan Kepemilikan lebih tinggi dari Loss Annualized
Harapan

D. Tidak Total Biaya tahunan Kepemilikan lebih rendah dari Loss Annualized Harapan

5. Manakah dari berikut ini menggambarkan tugas dari pemilik data ?

A. patch

B. Laporan aktivitas yang mencurigakan

C. Pastikan file mereka yang didukung

D. Pastikan Data memiliki label keamanan yang tepat

1. Benar jawaban dan penjelasan: A. Jawaban A benar; kebijakan tingkat tinggi dan menghindari spesifik teknologi.

Jawaban yang salah dan penjelasan: B, C, dan D. Jawaban B, C, dan D adalah

salah. B adalah pernyataan prosedural. C adalah pedoman. D adalah garis dasar.

2. Jawaban yang benar dan penjelasan: C. Jawaban C benar; Tingkat Tahunan

Kejadian adalah jumlah serangan dalam setahun.

Jawaban yang salah dan penjelasan: A, B, dan D. Jawaban A, B, dan D adalah

salah. $ 20.000 adalah Nilai Aktiva (AV). Empat puluh persen adalah Faktor Exposure (EF). $ 10.000 adalah biaya bulanan layanan DoS (digunakan untuk menghitung TCO).

3. Jawaban yang benar dan penjelasan: D. Jawaban D adalah benar; Rugi tahunan Harapan (ALE) dihitung dengan terlebih dahulu menghitung Loss Harapan Tunggal (SLE), yang merupakan Nilai Aset (AV, $ 20.000) kali Factor Exposure (EF,40%). The SLE adalah $ 8.000; kalikan dengan Tingkat Tahunan Kejadian (ARO, 7) untuk ALE dari $ 56.000. Jawaban yang salah dan penjelasan: A, B, dan C. Jawaban A, B, dan C adalah salah. $ 20.000 adalah Nilai Aktiva. $ 8.000 adalah Loss Expectancy Tunggal.

4. Jawaban yang benar dan penjelasan: C. Jawaban C benar; Total Biaya Kepemilikan (TCO) dari layanan DoS-mitigasi lebih tinggi dari Loss Annualized. Harapan (ALE) dari penjualan yang hilang akibat serangan DoS. Ini berarti itu lebih murah untuk menerima risiko serangan DoS (atau menemukan strategi mitigasi lebih murah).

Jawaban yang salah dan penjelasan: A, B, dan D. Jawaban A, B, dan D adalah

salah. A adalah salah: TCO yang lebih tinggi, tidak lebih rendah. $ 10.000 adalah bulanan TCO; Anda harus menghitung TCO tahunan untuk membandingkan dengan ALE.

D adalah salah:

TCO tahunan lebih tinggi, tidak lebih rendah.

5. Jawaban yang benar dan penjelasan: D. Jawaban D adalah

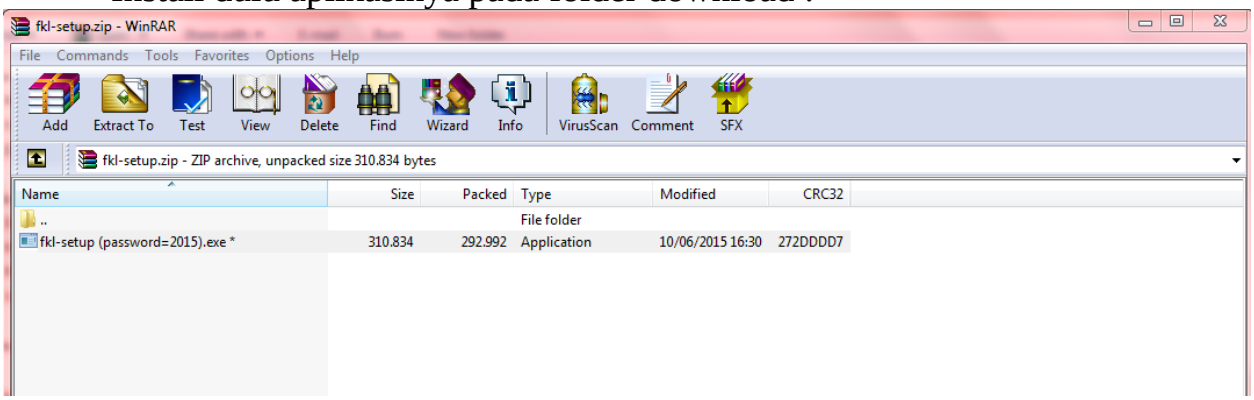
memperbaiki; memastikan pemilik data bahwa Data memiliki label keamanan yang tepat. Jawaban yang salah dan penjelasan: A, B, dan C. Jawaban A, B, dan C adalah salah. Sistem Patch penjaga. Pengguna harus sadar dan melaporkan mencurigakan aktivitas. File memastikan yang didukung adalah jawaban lemah untuk tugas pemilik data, digunakan untuk membingungkan pemilik data dengan "pemilik file" pada diskresioner sistem kontrol akses.

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.

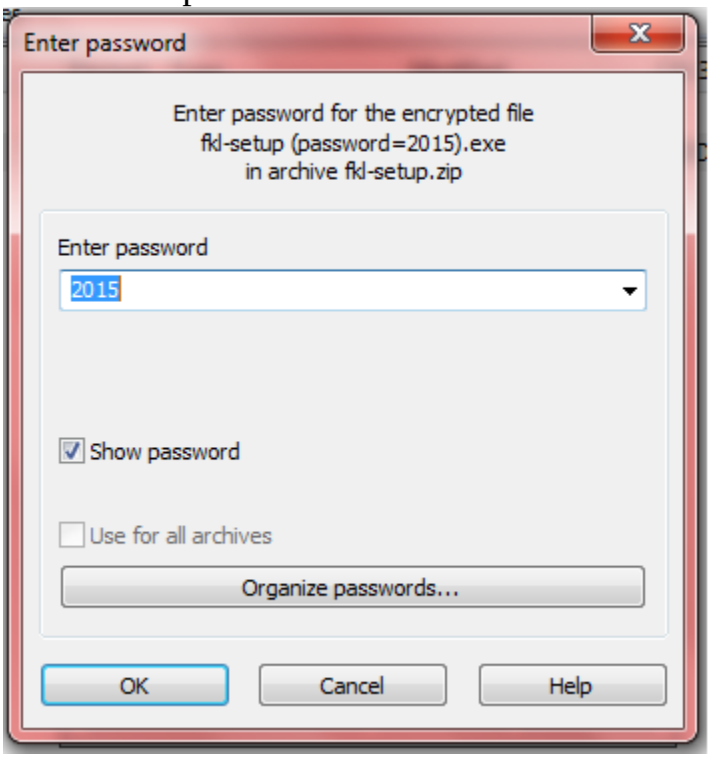
Jawab :

Disini saya menggunakan aplikasi family keylogger dimana aplikasi ini dapat mengetahui password atau kata sandi yang tersembunyi dengan cara seperti dibawah ini :

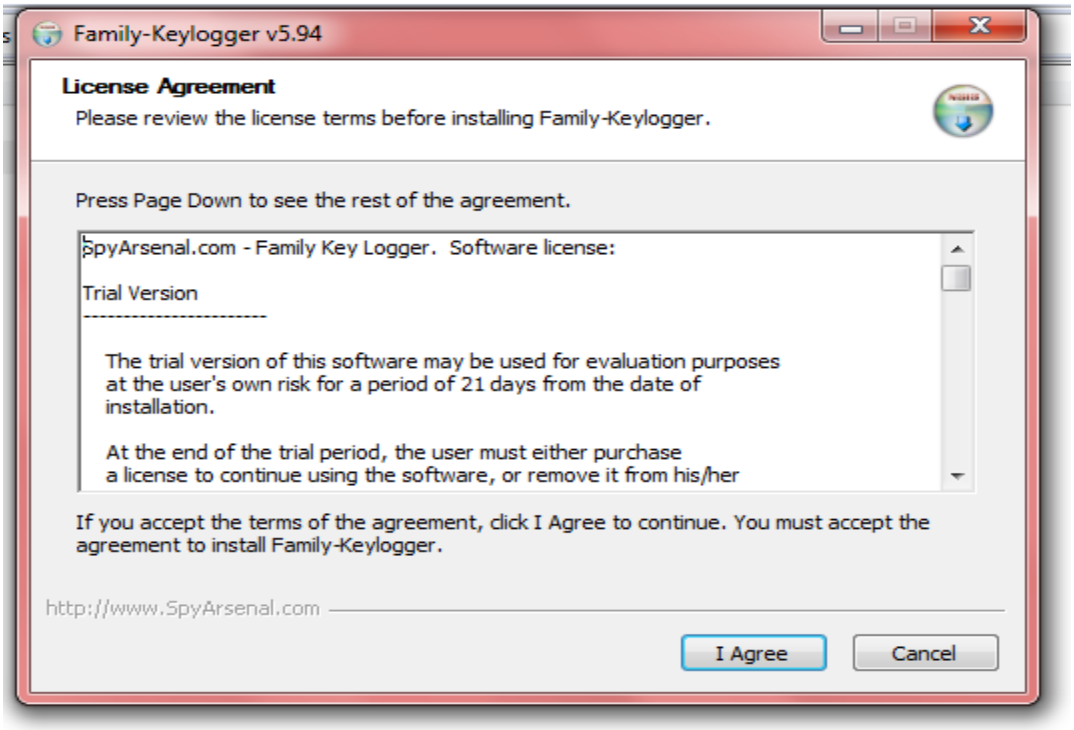
Langkah awal :
Install dulu aplikasinya pada folder download :



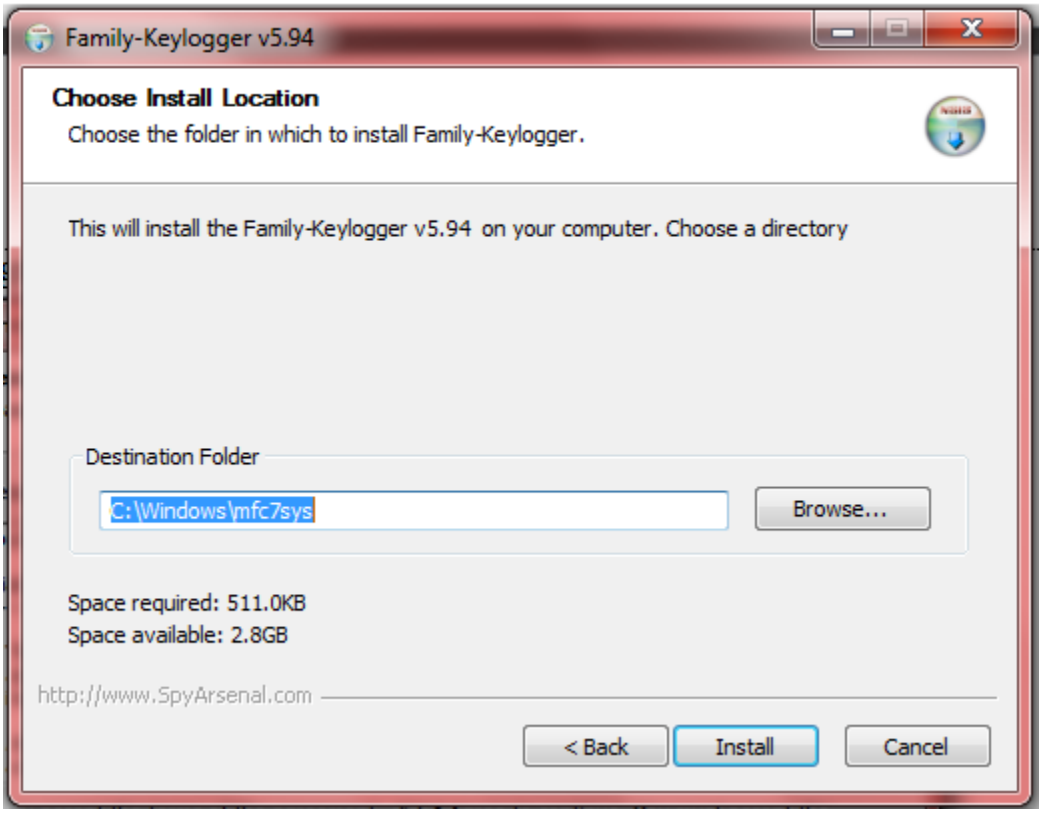
Pada langkah ini isikan password aplikasi yang sudah ada pada gambar dibawah ini : contoh password = 2015 lalu klik OK untuk mulai menginstallnya :



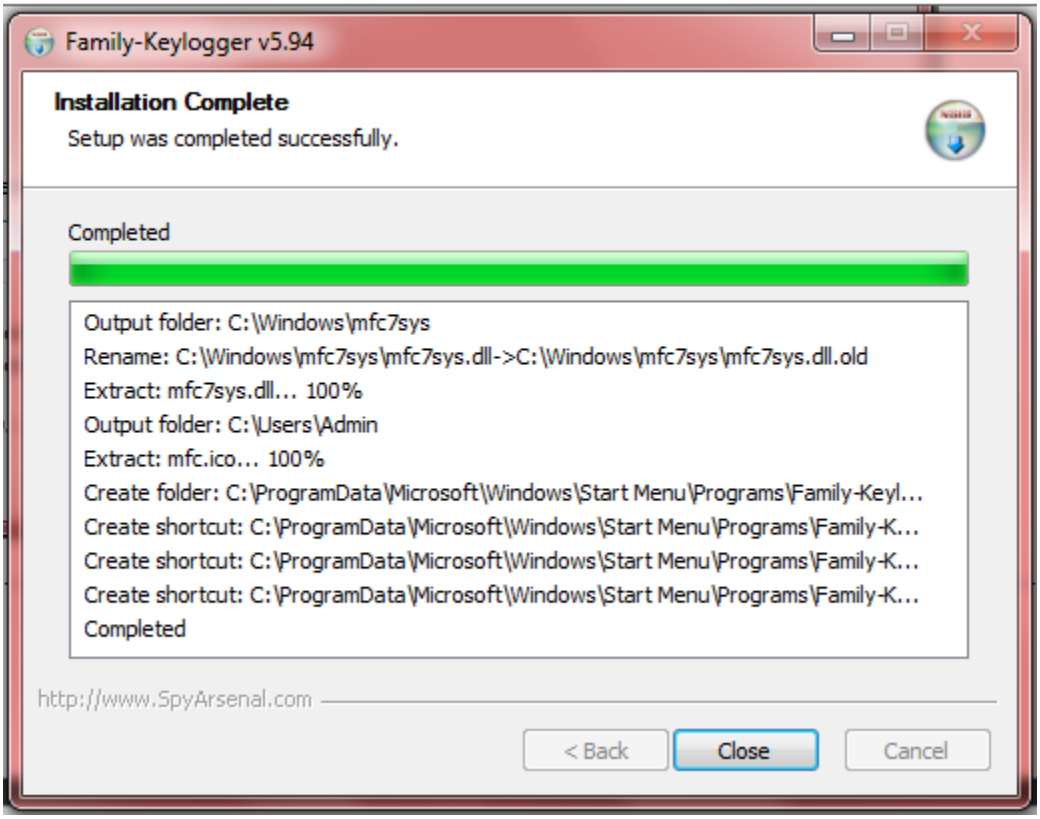
Klik agree untuk melanjutkan langkah selanjutnya :



Setelah tinggal klik install maka aplikasinya otomatis akan terinstall :

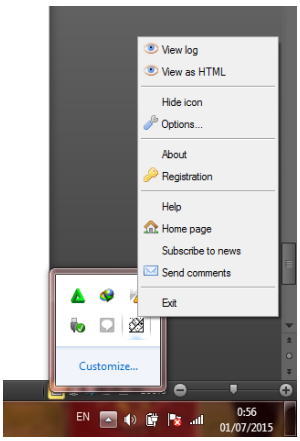


Tampilan saat proses installasi berjalan :

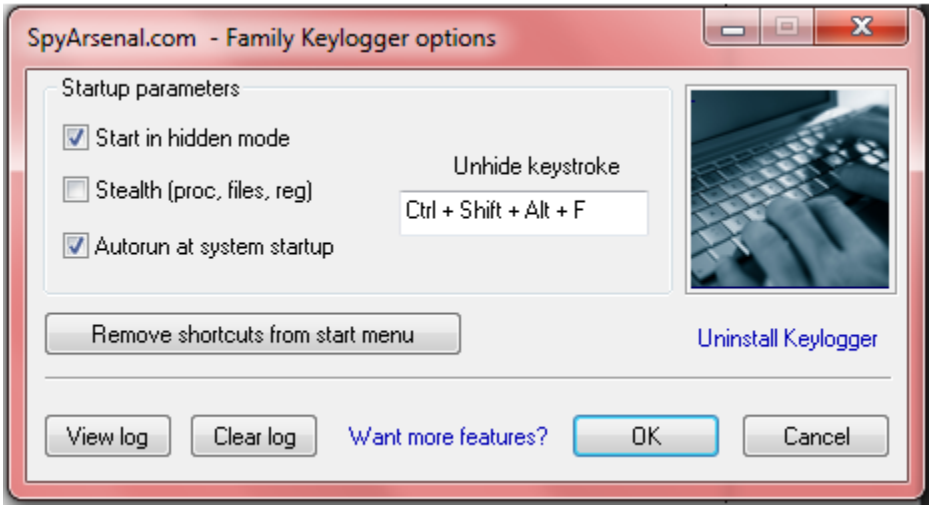


Dan mengetahui bagaimana proses menggunakan aplikasi ini maka ikuti langkah berikut ini :

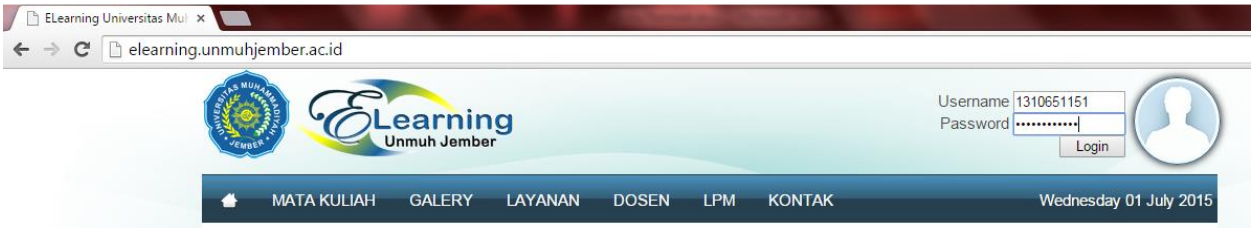
Klik kanan pada tampilan aplikasi keylogger seperti dibawah ini, lalu pilih option.



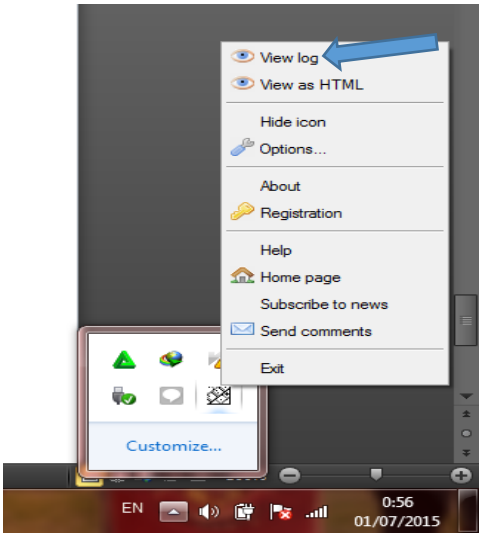
Lalu centang start in hidden mode, atau pun yang lainnya, tergantung pemakaian penggunanya sendiri. Ketika langkah ini sudah selesai.
Maka saya akan mengaplikasikan software ini untuk mengetahui password, salah satu dielearning.unmuhjember.ac.id



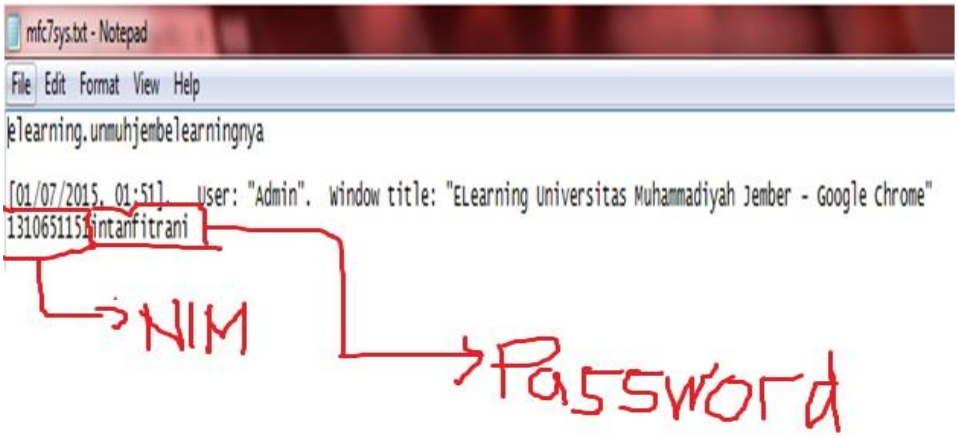
Buka elearningnya yang akan anda cari passwordnya missal :



Maka cara mengetahui passwordnya dan akunnya tinggal kita buka aplikasi femillykeyloggernya dengan klik kanan pilih view log, seperti gambar dibawah ini:



Dan Akan tampil lognya seperti berikut ini :



NB : Bagi yang mengetahui tolong jangan dibajak karena ini privas, terima kasih semoga bermanfaat.

Ini Buka elearning yang didapat kita Hack :