IT FORENSIK

Di Susunoleh :

ARIF NURROHIM / 41113328

JOSAFATINO MORGANI / 44113683

MUHAMMAD NURSAIFUL A / 46113056

TEKNIK KOMPUTER (D3)

UNIVERSITAS GUNADARMA

2015

DAFTAR ISI

KATA PENGANTAR

Puji syukur saya panjatkan kehadirat Tuhan Yang Maha Esa yang telah memberikan Rahmat serta karunia-Nya kepada saya. Sehingga saya dapat menyelesaikan penulisan makalah ini yang dengan tepat pada waktunya. Yang dimana penulisan ini bernama "IT FORENSIK".

Penulisan makalah ini berisikan tentang bagaimana cara IT Forensik bekerja dan mengetahui cara IT Audit bekerja serta mengetahui tools yang digunakan dalam bidang tersebut.

Diharapkan penulisan makalah ini dapat memberikan informasi kepada kita semua tentang cara IT Forensik dan IT Audit bekerja. Saya menyadari bahwa penulisan makalah ini masih jauh dari sempurna, oleh karena itu kritik dan saran dari semua pihak yang bersifat membangun selalu saya harapkan demi kesempurnaan penulisan makalah ini.

Akhir kata, saya sampaikan terima kasih kepada semua pihak yang telah berperan serta dalam penyusunan makalah ini dari awal sampai akhir. Semoga Tuhan senantiasa melindungi kita semua dari segala usaha kita. Amin.

Bekasi, 10 November 2015

IT FORENSIK

IT AUDIT TRAIL

Audit Trail merupakan salah satu fitur dalam suatu program yang mencacat semua kegiatan yang dilakukan tiap user dalam suatu tabel log. Secara rinci, Audit Trail secara default akan mencacat waktu, user, data yang diakses dan berbagai jenis kegiatan. Jenis kegiatan bisa berupa menambah, merubah, dan menghapus. Audit Trail apabila diurutkan berdasarkan waktu bisa membentuk suatu kronologis manipulasi data. Dasar ide membuat fitur Audit Trail adalah menyimpan histori tentang suatu data (Dibuat, Diubah, atau Dihapus) dan oleh siapa serta bisa menampilkannya secara kronologis. Dengan adanya trail ini, semua kegiatan dalam program yang bersangkutan diharapkan bisa dicatat dengan baik. Cara Kerja Audit Trail Audit Trail yang disimpan dalam suatu tabel 1. Dengan menyisipkan perintah penambahan record ditiap query Insert, Update dan Delete 2. Dengan memanfaatkan fitur trigger pada DBMS. Trigger adalah kumpulan SQL statement, yang secara otomatis menyimpan log pada event INSERT, UPDATE, ataupun DELETE pada sebuah tabel. Hasil Audit Trail Record Audit Trail disimpan dalam bentuk, yaitu : Binary File - Ukuran tidak besar dan tidak bisa dibaca begitu saja Text File - Ukuran besar dan bisa dibaca langsung Tabel.

Real Time Audit

Real Timer Audit atau RTA adalah suatu sistem untuk mengawasi kegiatan teknis dan keuangan sehingga dapat memberikan penilaian yang transparan status saat ini dari semua kegiatan, dimana pun mereka berada. Ini mengkombinasikan prosedur sederhana dan logis untuk merencanakan dan melakukan dana untuk kegiatan dan "Siklus Proyek" pendekatan untuk memantau kegiatan yang sedang berlangsung dan penilaian termasuk cara mencegah pengeluaran yang tidak sesuai. Real Time Audit menyediakan teknik ideal untuk memungkinkan mereka yang bertanggung jawab untuk dana, seperti bantuan donor, investor dan sponsor kegiatan untuk dapat "Terlihat Di Atas Bahu" dari manajer kegiatan di danai

sehingga untuk memantau kemajuan. Sejauh kegiatan manajer prihatin Real Time Audit meningkatkan kinerja karena sistem ini tidak mengganggu dan donor atau investor dapat memperoleh informasi yang mereka butuhkan tanpa menuntut waktu manajer. Pada bagian ini dari pemodal Real Time Audit adalah metode biaya yang sangat nyaman dan rendah untuk memantau kemajuan dan menerima laporan rinci reguler tanpa menimbulkan beban administrasi yang berlebihan baik untuk staf. Mereka sendiri atau manajemen atau bagian dari aktivitas manajer. Penghematan biaya overhead administrasi yang timbul dari penggunaan Real Time Audit yang signifikan dan meningkat seiring kemajuan teknologi dan teknik dan kualitas pelaporan dan kontrol manajemen meningkatkan menyediakan kedua manajer dan pemilik modal dengan cara untuk mencari kegiatan yang dibiayai dari sudut pandang beberapa manfaat dengan minimum atau tidak ada konsumsi waktu di bagian aktivitas manajer.

IT Forensik

Menurut Wikipedia, IT forensic atau forensic computer atau forensic digital adalah cabang forensic, TI forensic berkaitan dengan penyelidikan insiden yang mencurigakan yang melibatkan IT sistem dan penentuan fakta-fakta dan pelaku akuisisi, analisis, dan evaluasi jejak digital dalam sistem computer.

Secara umum IT forensic adalah ilmu yang berhubungan dengan pengumpulan fakta dan bukti pelanggaran keamanan sistem informasi serta validasinya menurut metode yang digunakan (misalnya metode sebab-akibat).

IT forensic bertujuan untuk mendapatkan fakta-fakta obyektif dari sebuah insiden/pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti envidence yang akan digunakan dalam proses hukum.

Pengertian Audit Around The Computer

Audit around the computer adalah pendekatan audit dimana auditor menguji keandalan sebuah informasi yang dihasilkan oleh komputer dengan terlebih dahulu mengkalkulasikan hasil dari sebuah transaksi yang dimasukkan dalam sistem. Kemudian, kalkulasi tersebut dibandingkan dengan output yang dihasilkan oleh sistem. Apabila ternyata valid dan akurat, diasumsikan bahwa pengendalian sistem telah efektif dan sistem telah beroperasi dengan baik.

Jenis audit ini dapat digunakan ketika proses yang terotomasi dalam sistem cukup sederhana. Kelemahan dari audit ini adalah bahwa audit around the computer tidak menguji apakah logika program dalam sebuah sistem benar. Selain itu, jenis pendekatan audit ini tidak menguji bagaimana pengendalian yang terotomasi menangani input yang mengandung error. Dampaknya, dalam lingkungan IT yang komplek, pendekatan ini akan tidak mampu untuk mendeteksi banyak error.

Pengertian Audit Through The Computer

Audit through the computer adalah audit yang dilakukan untuk menguji sebuah sistem informasi dalam hal proses yang terotomasi, logika pemrograman, edit routines, dan pengendalian program. Pendekatan audit ini menganggap bahwa apabila program pemrosesan dalam sebuah sistem informasi telah dibangun dengan baik dan telah ada edit routines dan pengecekan pemrograman yang cukup maka adanya kesalahan tidak akan terjadi tanpa terdeteksi. Jika program berjalan seperti yang direncanakan, maka semestinya output yang dihasilkan juga dapat diandalkan.

Prosedur Audit

Pada dasarnya prosedur audit dapat diuraikan sebagai berikut :

1. Perencanaan Audit (Planning the Audit)

   Terlebih dahulu harus merencanakan sasaran yang akan di audit kemudian harus memahami sasaran tersebut, kemudian mengumpulkan informasi awal yang dibutuhkan dan mengidentifikasikan resiko.
2. Pengujian Pengendalian (Test of Controls)

   Melakukan observasi terhadap pengendalian control dan mengevaluasi system yang telah ada, apakah system sudah berjalan dengan baik atau belum.
3. Pengujian Subtantif

   3.1 Pengujian Transaksi (Test of Transactions)

   Melakukan pengujian terhadap seluruh aktivitas transaksi yang terjadi

   3.2 Pengujian Keseluruhan Hasil (Test of Overall Result)

   Melakukan pengujian terhadap efektifitas dan efisiensi dalam kegiatan komputerisasi
4. Penyelesaian Audit (Completion of the Audit)

Membuat kesimpulan atau rekomendasi untuk dikomunikasikan pada manajemen

Lembar kerja

Lembar kerja audit adalah Sebuah catatan yang dibuat oleh auditor tentang prosedur audit yang dikerjakan, pengujian yang dilakukannya, serta informasi yang diperolehnya dan kesimpulan sehubungan dengan auditnya.

Tipe Lembar Kerja :

1. Program Audit (Audit Program)

   Merupakan daftar prosedur audit untuk seluruh audit unsur tertentu, sekaligus berfungsi sebagai alat yang bermanfaat untuk menetapkan jadwal pelaksanaan dan pengawasan pekerjaan audit.
2. Working Trial Balance

   Suatu daftar yg berisi:
   - saldo-saldo akun buku besar pada akhir tahun yg diaudit dan pada akhir tahun sebelumnya.
   - kolom untuk adjustment & penggolongan kembali yg diusulkan auditor.
   - saldo-saldo setelah koreksi auditor yg akan tampak dlm laporan keuangan auditan.
3. Ringkasan Jurnal adjustment

   Lembar kerja berisi temuan-temua kekeliruan dalam laporan keuangan & catatan akuntansi.
4. Skedul Utama (lead schedule atau top schedule)

   Lembar kerja yg digunakan untuk:
   - meringkas informasi yg dicatat dalam skedul pendukung untuk akun-akun yg berhubungan
   - menggabungkan akun-akun sejenis, yang jumlah saldonya akan dicantumkan di dalam laporan keuangan dalam satu jumlah
5. Skedul Pendukung (Supporting Schedule)

   Lembar kerja yang menguatkan informasi keuangan dan operasional yang dikumpulkan, memuat berbagai simpulan yang dibuat auditor.

IT Audit Tools (Software)

Tool-tool yang dapat digunakan untuk membantu pelaksanaan Audit Teknologi Informasi. Tidak dapat dipungkiri, penggunaan tool-tool tersebut memang sangat membantu Auditor Teknologi Informasi dalam menjalankan profesinya, baik dari sisi kecepatan maupun akurasinya.

Berikut beberapa software yang dapat dijadikan alat bantu dalam pelaksanaan audit teknologi informasi

A. ACL

ACL (Audit Command Language) merupakan sebuah software CAAT (Computer Assisted Audit Techniques) yang sudah sangat populer untuk melakukan analisa terhadap data dari berbagai macam sumber.

ACL for Windows (sering disebut ACL) adalah sebuah software TABK (TEKNIK AUDIT BERBASIS KOMPUTER) untuk membantu auditor dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektronik.

B. Picalo

Picalo merupakan sebuah software CAAT (Computer Assisted Audit Techniques) seperti halnya ACL yang dapat dipergunakan untuk menganalisa data dari berbagai macam sumber.Picalo bekerja dengan menggunakan GUI Front end, dan memiliki banyak fitur untuk ETL sebagai proses utama dalam mengekstrak dan membuka data, kelebihan utamanya adalah fleksibilitas dan front end yang baik hingga Librari Python numerik.

Berikut ini beberapa kegunaannya :

· Menganalisis data keungan, data karyawan

· Mengimport file Excel, CSV dan TSV ke dalam databse

· Analisa event jaringan yang interaktif, log server situs, dan record sistem login

· Mengimport email kedalam relasional dan berbasis teks database

· Menanamkan kontrol dan test rutin penipuan ke dalam sistem produksi.

C. Powertech Compliance Assessment

Powertech Compliance Assessment merupakan automated audit tool yang dapat dipergunakan untuk mengaudit dan mem-benchmark user access to data, public authority to libraries, user security, system security, system auditing dan administrator rights (special authority) sebuah serverAS/400.

D. Nipper

Nipper merupakan audit automation software yang dapat dipergunakan untuk mengaudit dan mem-benchmark konfigurasi sebuah router.

Nipper (Jaringan Infrastruktur Parser) adalah alat berbasis open source untuk membantu profesional TI dalam mengaudit, konfigurasi dan mengelola jaringan komputer dan perangkat jaringan infrastruktur.

E. Nessus

Nessus merupakan sebuah vulnerability assessment software, yaitu sebuah software yang digunakan untuk mengecek tingkat vulnerabilitas suatu sistem dalam ruang lingkup keamanan yang digunakan dalam sebuah perusahaan

F. Metasploit

Metasploit Framework merupakan sebuah penetration testing tool, yaitu sebuah software yang digunakan untuk mencari celah keamanan.

G. NMAP

NMAP merupakan open source utility untuk melakukan security auditing. NMAP atau Network Mapper, adalah software untuk mengeksplorasi jaringan, banyak administrator sistem dan jaringan yang menggunakan aplikasi ini menemukan banyak fungsi dalam inventori jaringan, mengatur jadwal peningkatan service, dan memonitor host atau waktu pelayanan. Secara klasik Nmap klasik menggunakan tampilan command-line, dan NMAP suite sudah termasuk tampilan GUI yang terbaik dan tampilan hasil (Zenmap), fleksibel data transfer, pengarahan ulang dan tools untuk

debugging (NCAT) , sebuah peralatan untuk membandingan hasil scan (NDIFF) dan sebuah paket peralatan analisis untuk menggenerasikan dan merespon (NPING)

H. Wireshark

Wireshark merupakan aplikasi analisa netwrok protokol paling digunakan di dunia, Wireshark bisa mengcapture data dan secara interaktif menelusuri lalu lintas yang berjalan pada jaringan komputer, berstandartkan de facto dibanyak industri dan lembaga pendidikan.

DAFTAR PUSTAKA

- https://ba9uez.wordpress.com/it-forensik/
- http://juliocaesarz.blogspot.co.id/2011/03/it-audit-trail.html\
- http://nillafauzy.blogspot.co.id/2013/03/pengertian-it-audit-trail-real-time.html
- http://id.wikipedia.org/wiki/Audit
- http://kitakuliahlagi.blogspot.com/2012/07/perbedaan-audit-through-computer- audit.html
- http://henindya.blogspot.co.id/2011/10/it-audit-tools.html