TUGAS KEAMANAN JARINGAN KOMPUTER

Computer Forensic Analysis

NAMA: EDI SUKRISNO
NIM: 09011181320043

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER
2017

I. PENDAHULUAN

scan kerentanan situs publik yang dilakukan pada 2013 oleh Symantec kerentanan Situs Web Jasa Penilaian menemukan bahwa 77 persen dari situs yang terdapat kerentanan, dan 16 persen dari mereka diklasifikasikan sebagai kerentanan kritis yang dapat memungkinkan penyerang untuk mengakses data sensitif, mengubah konten website, atau kompromi pengunjung komputer (Internet Security Threat Report 2014,). OWASP (Open Web Application Security Project) Top Ten 2013 menawarkan daftar kerentanan aplikasi Web yang paling penting, termasuk berbagai jenis injeksi, otentikasi rusak dan manajemen sesi, cross-site scripting, kesalahan konfigurasi aman, dll Banyak organisasi kehilangan reputasi atau pendapatan mereka, karena serangan berbagai hacker. Hari ini, cybercrime adalah masalah global, dan komputer forensik adalah salah satu cara untuk memerangi itu. Komputer forensik mempersiapkan bukti-bukti hukum dan memberikan jawaban atas banyak pertanyaan dari sistem hukum yang berhubungan dengan komputer. Dianalisis gambar forensik adalah bukti utama.

II. Computer Forensics

Komputer forensik, juga dikenal sebagai sebagai digital forensic menyinggung ke imaging, ekstrasi dan analisa data sebagai penyediaan penyimpanan digital pada komputer untuk tujuan memperoleh bukti yang legal. Dibawah merupakan 3 langkah utama untuk proses komputer forensik yaitu :

1. Imaging
   Menentukan bagian pada hard drive. Sebuah lisensi dan akreditasi penguji pada komputer forensic akan memanfaatkan tools khusus untuk melengkapi byte per byte gambar dari komputer (server, PC, Mac, laptop dan smartphone). Bahwa penguji komputer forensik akan dapat memiliki akses ke perangkat personal untuk menvisualisasikan perangkat keras jika menduga mengkin ada bukti kesalahan pada hubungan komputer tertentu. Gambaran data lalu di analisa untuk menentukan apa yang harus di ekstraksi.

2. Extraction
   Menentukan data yang akan di ekstraksi. Jumlah data yang sangat besar akan di visualisasikan. Sehingga penentuan harus dibuat mengenai data apa yang dibutuhkan untuk analisis. Secara khas, file program dan file lain dikontribusikan untuk fungsionalitas normal dari komputer yang cukup besar dan tidak terekstraksi. Data yang membutuhkan ekstraksi akan menjadi file email, dokumen word, excel spreadsheets, presentasi, PDF, gambar autocad, dll.

3. Analisis
   Sekali setelah data sudah diekstraksi dari hard drive visual, maka harus segera di upload ke analisis tools. Hal ini bertujuan agar data bisa terbaca dan dicari dengan tagging dan mengindex-kan fungsionalitasnya agar menjadi key untuk analisis efektif. Penyimpanan cloud dari data memastikan bahwa data bisa diakses dari koneksi internet manapun, kapanpun, dengan tool analitik. Ini ditawarkan dengan software sebagai service.

Sumber referensi : https://www.youtube.com/watch?v=rTyZJwSk-HY .