UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

Anti Forensik

Pengantar Komputer Forensik Teknologi Informasi

Pendahuluan

- Computer forensics adalah suatu metode untuk mengidentifikasi, mengekstrak dan menemukan informasi dari media digital seperti komputer dan “hard drives”.
- Computer forensics dalam artian sempit, hanya diaplikasikan kepada proses evaluasi komputer, “data storage’ dan “processing devices”
- Computer forensic biasanya dimanfaatkan terkait dengan hukum dan persidangan

Computer Anti Forensics

- suatu metode untuk membuat para "computer forensics investigator" kesulitan dalam melaksanakan tugasnya.overwrite data sensitif sehingga tidak jatuh ke tangan yang salah, seperti alat lain yang dapat disalahgunakan

TRADITIONAL ANTI-FORENSIC

- SECURE DATA DELETION
- ENKRIPSI
- STEGANOGRAFI
- UNRECOVERABLE DELETE
- PENYEMBUNYIAN FILE
- HASH COLLISION
- ANONYMOUS INTERNET USER

SECURE DATA DELETION

- salah satu teknik tertua/tradisional dari anti-forensics, suatu metode yang sangat mudah, efisien dan "simple" untuk dilakukan, dibanding dengan berbagai teknik lain seperti enkripsi, "steganography", modifikasi data, penyembunyian data, dsb
- Beberapa aplikasi yang bisa dimanfaatkan adalah: srm, wipe, shred, dsb.

ENKRIPSI

- Data-data yang dapat di-enkripsi dapat berupa file image, video, dokumen, dll. Ada beberapa program yang dapat kita gunakan, contohnya TrueCrypt, PGP yang dapat mengenkripsi E-mail, bahkan Wireshark yang dapat menghindarkan data di intip oleh sniffer pada saat mengakses jaringan

STEGANOGRAFI

- Sebuah data atau pesan dapat disembunyikan di dalam suatu file agar orang lain tidak dapat mengenalinya

UNRECOVERABLE DELETE

- Beberapa file atau data yang telah dihapus dari Drive, Memory Card atau Flash Disk dapat dikembalikan menggunakan tool recovery data, misalnya: GetDataBack, Recuva, dsb. Maka ada kemungkinan beberapa data rahasia yang telah terhapus dapat dibaca oleh orang lain.
- Untuk mengantisipasinya dapat menggunakan tool file deleter, atau file shreder, dengan begitu data yang telah dihapus tidak akan dapat di recovery lagi. Aplikasi seperti itu dapat dicari melalui internet

PENYEMBUNYIAN FILE

- Menyembunyikan data rahasia, mungkin salah satu solusi yang dapat dilakukan. Ada beberapa program yang dapat digunakan untuk melakukannya, seperti Folder Lock, Hide My Folder, dsb

HASH COLLISION

- Hash adalah suatu identitas file yang "berbentuk" algoritma. Nah, dengan hash ini ahli forensik menggunakannya sebagai integritas suatu file, dengan begitu ahli forensik dapat membandingkan suatu file adalah asli atau telah di-edit. Ada beberapa program untuk memodifikasi hash, seperti hex editor, Reshacker, eXpress Timestamp Toucher, dsb

ANONYMOUS INTERNET USER

- Ada banyak cara untuk menyembunyikan jejak di internet, mulai dari yang paling sederhana seperti penghapusan history, penggunaan TOR sebagai bounce, menggunakan IP anonymous antar negara (baik dengan aplikasi atau menggunakan jasa situs online), hingga menggunakan Virtual Machine Ware pada saat mengeksekusi browser

Target operasi forensik

- **MEMORY USAGE**
- **REGISTRY**
- **LOG EVENTS**

MEMORY USAGE

- Jumlah pemakaian memory juga akan diolah oleh ahli forensik untuk menganalisa proses apa saja yang sedang berjalan, penggunaan aplikasi seperti Task Manager, Process Explorer, dll dapat digunakan untuk menganalisanya

REGISTRY

- Di lokasi ini juga akan jadi target operasi ahli forensik untuk mengungkap proses startups, services, dan konfigurasi lain

LOG EVENTS

- Pada event viewer tersimpan sejarah penggunaan aplikasi atau aktivitas system, penghapusan log event dapat sedikit menghilangkan jejak. Di dalam event pada antivirus juga tersimpan beberapa aktivitas. Logs USB juga dapat dijadikan sasaran penyelidikan ahli forensik, lokasi dari logs itu tersimpan di dua tempat: Pertama, berada pada file setupapi.log atau setuapi.dev.log

Daftar Pustaka

- http://www.forensicswiki.org/wiki/Anti-forensic_techniques
- http://www.anti-forensics.com/

Terima kasih