KEAMANAN INFORMASI

14. Malware & Computer Forensics

Doni Abdul Fatah
github.com/doniaft
Universitas Trunojoyo Madura

Pokok Bahasan

01. Pengantar Keamanan Informasi

02. Pemodelan Serangan (Attack Tree)

03. Sistem Keamanan Informasi dan Internet

04. Autentikasi

05. Kontrol Akses

06. Firewall dan Intrusion Detection System

07. Network Attack

08. Kriptografi

09. Kriptografi Asimetrik

10. Biometric Authentication

11. Public Key Infrastructure

12. Protokol Keamanan

13. Malware & Computer Forensics

14. UAS

01. Keamanan Informasi

1) Malware & Computer Forensics
2) Contact
3) Referensi

13. Malware & Computer Forensics

Computer Forensics

Computer Forensics

Computer Forensics

- Forensik merupakan sebuah proses ilmiah dalam mengumpulkan, menganalisis, dan menghadirkan berbagai bukti pada sidang pengadilan karena adanya kasus hukum. Lalu, apa yang dimaksud dengan Komputer Forensik?

Computer Forensics

- Perkembangan Teknologi
  - Positif ; Memajuan dan kesejahteraan
  - Negatif ; Kemunduran dan kerugian
- Teknologi informasi dan komputer
  - Dalam perkembangannya telah membuka dimensi lain dari teknologi, yaitu kejahatan komputer
  - Istilah “ Cybercrime “
- Cybercrime : memunculkan masalah baru

Cybercrime

- Cybercrime : Kejahatan komputer
- Masalah baru
  - Mikro ; Perseorangan
  - Makro ; Komunal, publik dan efek domino
- Cybercrime perlu ditangani sebab ;
  - Sifat alami dari TI ; Memungkinkan pelaku kejahatan untuk menyembunyikan jejaknya
  - Cybercrime tidak memiliki batas goegrafis
  - Dapat dilakukan secara jarak dekan atau jauh dan hasilnya sama

Computer Forensics

- Forensik :
  - Suatu proses ilmiah dalam mengumpulkan, menganalisa, dan menghadirkan berbagai buksti dalam sidang pengadilan terkait adanya suatu kasus hukum.
- Forensik Komputer:
  - Suatu proses **mengidentifikasi**, **memelihara, menganalisa** dan **menggunakan bukti digital** menurut hukum yang berlaku (Moroni Parra, 2002). Istilah ini kemudian meluas menjadi ***Forensik Teknologi Informasi***

Komputer Forensik ; Terminologi

- Komputer forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan – penyaringan dan dokumentasi bukti komputer dalam kejahatan komputer
- Melakukan penyelidikan dan analisis komputer untuk menentukan potensi bukti legal

Komputer Forensik

- Mengumpulkan dan analisa data dari sumber daya komputer :
  - Sistem komputer
  - Jaringan komputer
  - Jalur komunikasi
  - Media penyimpanan
  - Aplikasi komputer
- Forensik komputer : mengabungkan keilmuan hukum dan komputer
- Forensik komputer = digital forensik

Data Elektronik : Bukti Digital

- Data elektronik ;
  - Dokumen, informasi keuangan, e-mail, job schedule, log, transkripsi voice-mail
- Bukti digital
  - Informasi yang didapat dalam bentuk / format digital (Scientific Working Group on Digital Evidence, 1999), baik berupa bukti yang riil maupun abstrak (perlu diolah terlebih dahulu sebelum menjadi bukti yang riil),

Kebutuhan Komputer Forensik

- Keperluan investigasi tindak kriminal dan pelanggaran perkara pelanggaran
- Rekontruksi duduk perkara insiden keamanan komputer
- Upaya pemulihan akan keruksakan sistem
- Troubleshooting yang melibatkan hardware dan software
- Keperluan memahami sistem atau berbagai perangkat digital dengan lebih baik

Spesifikasi Komputer Forensik

- Forensik Disk
- Forensik System
- Forensik Jaringan Komputer
- Forensik Internet

Penerapan Komputer Forensik

- Prinsip
  - Harus ada prinsip yang menetapkan bahwa keahlian dan pengalaman lebih penting dari pada tools
- Kebijakan
  - Pertimbangkan kebijakan dalam melakukan investigasi komputer forensik
- Prosedur dan metode
  - Buat prosedur dan metode terhadap peralatan dan mendapatkan – mengumpulkan electronic evidence

Bidang Keilmuan Forensik

- Forensik pathologi
- Forensik dentistry
- Forensik anthropology
- Forensik entomology
- Psikologi forensik
- Forensik kejiwaan
- Fingerprint analysis
- Forensik accounting
- Bloodstain pattern analysis
- Ballistics
- Forensik toxicology
- Forensik footwear evidence
- Questioned document examination
- Explosion analysis
- Forensik teknologi informasi
- Komputer forensik

Empat elemen kunci forensik dalam TI

1. **Identifikasi dari bukti digital.**

   Merupakan tahapan paling awal forensik dalam teknologi informasi. Pada tahapan ini dilakukan identifikasi dimana bukti itu berada, dimana bukti itu disimpan dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya.

2. **Penyimpanan bukti digital.**

   Termasuk tahapan yang paling kritis dalam forensik. Bukti digital dapat saja hilang karena penyimpanannya yang kurang baik.

3. **Analisa bukti digital.**

   Pengambilan, pemrosesan, dan interpretasi dari bukti digital merupakan bagian penting dalam analisa bukti digital.

4. **Presentasi bukti digital.**

   Proses persidangan dimana bukti digital akan diuji dengan kasus yang ada. Presentasi disini berupa penunjukkan bukti digital yang berhubungan dengan kasus yang disidangkan.

Investigasi kasus teknologi informasi.

1. Prosedur forensik yang umum digunakan, antara lain :
   a. Membuat copies dari keseluruhan log data, file, dan lain-lain yang dianggap perlu pada suatu media yang terpisah.
   b. Membuat copies secara matematis.
   c. Dokumentasi yang baik dari segala sesuatu yang dikerjakan.

Investigasi kasus teknologi informasi.

2. Bukti yang digunakan dalam IT Forensics berupa:
   a. Harddisk.
   b. Floopy disk atau media lain yang bersifat removeable.
   c. Network system.

Investigasi kasus teknologi informasi.

3. Beberapa metode yang umum digunakan untuk forensik pada komputer ada dua yaitu :

1. Search dan seizure.

Dimulai dari perumusan suatu rencana.

2. Pencarian informasi (discovery information).

Metode pencarian informasi yang dilakukan oleh investigator merupakn pencarian bukti tambahan dengan mengandalkan saksi baik secara langsung maupun tidak langsung terlibat dengan kasus ini.

Aktivitas Penyelidik Forensik

- Perlindungan sistem komputer selama pengujian forensik dari semua kemungkinan perubahan, kerusakan, korupsi data, atau virus
- Temukan semua file pada sistem. Termasuk file normal, terhapus, *hidden, pasword-protected*, dan terenkripsi.
- *Recovering* file terhapus sebisa mungkin.
- Ambil isi file *hidden* juga file *temporary* atau *swap* yang dipergunakan baik oleh sistem operasi atau program aplikasi
- Lakukan akses (jika dimungkinkan secara legal) isi dari file terproteksi atau terenkripsi

Aktivitas Penyelidik Forensik

- Analisa semua data yang relevan pada area spesial di disk. Misal *unnalocated* (tidak terpakai, tapi mungkin menyimpan data sebelumnya), *slack space* (area di akhir file pada *last cluster* yang mungkin menyimpan data sebelumnya juga)
- Cetak semua analisis keseluruhan dari sistem komputer, seperti halnya semua file yang relevan dan ditemukan. Berikan pendapat mengenai layout sistem, struktur file yang ditemukan, dan informasi pembuat, setiap usaha menyembunyikan, menghapus, melindungi, mengenkripsi informasi, dan lainnya yang ditemukan dan nampak relevan dengan keseluruhan pengujian sistem komputer.
- Berikan konsultasi ahli dan kesaksian yang diperlukan

Kategori software forensik

- Forensic software tools for Windows
- Image and Document Readers
- Data Recovery/Investigation
- Password Cracking
- Network Investigation
- Phone Investigation
- PDA Investigation
- Lab Tools
- Assessments utilities
- Foundstone SASS Tools
- Intrusion Detection Tools
- Scanning Tools
- Stress Testing Tools

Tool Forensik

- Contoh dari aplikasi yang dapat digunakan dalam komputer forensik, yaitu :
  - Encase www.guidancesoftware.com
  - Forensics toolkit www.accessdata.com
  - LoPe www.evidencetalks.com
  - Forager www.inforenz.com/software/forager.html
  - X-Ways Forensics www. x-ways.net/forensic/index-m.html

Tool Forensik

- Beberapa tool untuk komputer forensik :
  - The Coroner Toolkit - Dan Farmer & Wietse Venema , www.fish.com
  - Byte Back - oleh TechAssist, http://www.toolsthatwork.com/
  - DriveSpy - http://www.digitalintel.com/
  - EnCase - oleh Guidance Software, http://www.encase.com/
  - Forensic ToolKit - http://www.accessdata.com/
  - Maresware Suite - http://www.dmares.com/
  - Drive Image Pro – PowerQuest
  - Linux "dd" - Red Hat
  - Norton Ghost 2000 – Symantec
  - SafeBack - New Technologies
  - SnapBack DatArrest oleh Columbia Data Products

SERTIFIKASI AHLI FORENSIK TI

- EnCase Certified Examiner Program (EnCE)
  http://www.iacis.com
- Computer Forensics External Certification (CCE)
  http//:www.giac.org/certifications/security/gcfa.php
- GCFA – GIAC Certified Forensics Analyst
  http//:www.giac.org/certifications/security/gcfa.php
- Q/FE Qualified Forensics Expert
  http://www.securityuniversity.net/certification.htm
- TruSecure ICSA Certified Security Associate
  http://www.icsalabs.com
- CCE – Certified Computer Examiner
  http://www.certified-computer-examiner.com
- Computer Forensic Training Online
  http://www.kennesaw.edu/coned/sci/for_online.htm

3) Kontrak Perkuliahan

a) Tata Tertib
b) Contact
c) Referensi

Tata Tertib Perkuliahan SI4B

- Masuk sesuai jadwal 15.25 WIB, Toleransi keterlambatan adalah 20 menit.
- Pakaian bebas rapi berkerah, bersepatu.
- Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Tata Tertib Perkuliahan SI4C

- Masuk sesuai jadwal 09.15 WIB, Toleransi keterlambatan adalah 15 menit.
- Pakaian bebas rapi berkerah, bersepatu.
- Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Tata Tertib Perkuliahan SI4D

- Masuk sesuai jadwal 12.45 WIB, Toleransi keterlambatan adalah 15 menit.
- Pakaian bebas rapi berkerah, bersepatu.
- Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Proyek : Kelompok
dibuat 2 s.d 4 Mahasiswa

- Membuat aplikasi sederhana dengan fokus **Keamanan Informasi dalam Penggunaan** Aplikasi/berInternet
- **Tahapannya :**
  - Penentuan Studi Kasus
  - Membuat aplikasi Login Spoofing Attack
  - Dalam aplikasi Login Spoofing Attack untuk pemberian passwordnya di lakukan dengan menggunakan teknik Kriptografi (enkripsi) dengan menggunakan enkripsi asimetris
  - Untuk memecahkan enkripsi tersebut maka dilakukan deskripsi dari enkripsi tersebut.
  - Untuk Aplikasi boleh Web atau Desktop, sesuai yang dikuasai.
  - Pembuatan Laporan atau Dokumentasi.
- **Poin penilaian:** Aplikasi, Dokumentasi, Presentasi.

5) Contact

Contact

- Bahan Kuliah : github.com/doniaft
- Email : doniaft@gmail.com
- WA/Telegram :
- Komting Keamanan Informasi
  - SI4C : Yusril : 0856 5509 5641
  - SI4D : Ikrom : 0852 3027 9767
  - SI4B :
    - Rahma : : 0852 5707 1554
    - Adi : 0899 3616 728

6) Referensi

Referensi (1)

- Anderson, Ross, “Security Engineering”, First Edition, Wiley, 2001, tersedia dalam e-Book : URL: http://www.cl.cam.ac.uk/~rja14/book.html
- Menezes et.al, “Handbook of Applied Cryptography”, Fifth Edition, CRC Printing, 2001, tersedia dalam e-Book URL: http://cacr.uwaterloo.ca/hac
- Bishop, Matt, “Computer Security: Art and Science”, Addison Wesley, 2002
- Stinson, Douglas R, “Cryptography: Theory and Practice”, CRC Press, 1995
- Electronic Frontier Foundation, “Cracking DES”, O'Reilly, 1998
- Stamp, Mark, “Computer Security: Principles and Practices”, Willey, 2011
- Eric Cole, Ronald Krutz, and James W. Conley, “Network Security Bible”,
- Wiley Publishing, Inc., 2005.
- Matthew Strebe, “Network Security Foundations”, Sybex, 2004.
- Chris McNab, “Network Security Assessment”, O’reilly, 2008.
- James D. McCabe, dkk, “Network Security Know It All”,Morgan
- Kaufmann, 2008.
- Ibisa, “Keamanan Sistem Informasi”, Penerbit Andi, Yogyakara, 2011