DAFTAR ISI

PENDAHULUAN

Dunia Internet seakan tidak akan pernah sesak meski jumlah penggunanya bertambah dengan sangat tajam dari tahun ke tahun. Jenis pengguna Internet pun sangat beragam. Mulai dari mereka yang baru belajar menggunakan mouse hingga mereka yang bahkan mahir mengutak-atik komputer dan membuat aplikasi program dan berselancar ke mana saja di dunia Internet.

Bukan hanya dari sisi ini jenis dan ragam pengguna Internet, motivasi dan kecenderungan serta pola laku penggunanya pun semakin bervariasi. Mereka para netizen ternyata begitu beragam, mulai dari yang "baik-baik" hingga yang berniat berbuat "jahat".

Ya, Internet ... sama seperti seperti alat atau tool lainnya, tergantung siapa yang menggunakannya. "The man behind the gun" kata orang Inggris.

Internet dapat digunakan untuk kebaikan bagi mereka yang ingin berbuat *maslahat*, dan sebaliknya dia dapat menjadi alat yang lebih berbahaya dari pedang maut jika ditangan mereka yang punya kecenderungan berbuat *mudharat*.

Buku ini menyajikan panduan dasar untuk pengguna Internet dalam mengelola informasi pribadi dengan baik dan membangun kesadaran akan urgensi keamanan informasi digital serta mengetahui mekanisme forensik komputer dasar ketika menghadapi masalah keamanan internet.

KONSEP DASAR KEAMANAN INTERNET

Dalam bidang keamanan informasi, ada konsep fundamental keamanan komputer yang umum diterapkan secara teori maupun praktek. Dikenal dengan istilah CIA Triad.

Ketiga aspek dalam Keamanan Informasi (CIA Triad) CIA triad adalah model standar dalam keamanan informasi yang dirancang untuk mengatur dan mengevaluasi bagaimana sebuah organisasi atau perusahaan ketika data disimpan, dikirim, atau diproses.

Adapun CIA adalah singkatan dari Confidentiality, Integrity dan Availability.

CONFIDENTIALITY

Confidentiality berarti kerahasiaan data dan informasi. Jaminan kerahasiaan data adalah aspek terpenting dalam dunia keamanan komputer. Ketika kita membahas mengenai aspek confidentiality atau kerahasiaan informasi, maka kita sedang berbicara mengenai serangkaian upaya perlindungan agar informasi tidak terakses oleh pihak yang tidak berwenang. Informasi rahasia memang dianggap sebagai data yang bernilai oleh para cyber hacker. Informasi yang diincar biasanya berupa informasi pelanggan, data karyawan, kekayaan intelektual, atau informasi mengenai rahasia dagang. Oleh karena itulah para cyber hacker terus mencari kerentanan yang ada pada dalam sistem agar mereka bisa mengakses info-info penting tersebut. Pada umumnya, informasi rahasia dapat jatuh ke tangan yang

salah karena data breach atau ancaman orang dalam. Beberapa jenis serangan yang umum digunakan untuk mengakses informasi rahasia tersebut seperti : Serangan Man in The Middle Pembobolan enkripsi Serangan eavesdropping Untuk melindunginya, terdapat sejumlah langkah yang dapat dipergunakan seperti dengan menerapkan autentikasi dua faktor, penggunaan password yang kuat, enkripsi, dan lain-lain. Meskipun demikian, Anda juga perlu memahami bahwa informasi rahasia juga dapat terakses oleh pihak yang tidak sah karena kecerobohan atau kesalahan pengguna, serta kontrol keamanan yang tidak memadai. Contohnya seperti penggunaan password yang lemah, berbagi akun, atau karena social engineering karena security awareness yang kurang.

INTEGRITY

Integrity berarti kesahihan data dan informasi. Dalam dunia keamanan informasi, integrity adalah jaminan agar data atau informasi tidak mengalami perubahan, penggantian sedikitpun dan terjaga apa adanya. Langkah-langkah ini memberikan jaminan atas keakuratan dan kelengkapan informasi. Seperti halnya dengan perlindungan informasi rahasia, perlindungan integritas juga perlu untuk dilakukan. Ancaman terhadap integritas data, dapat berasal dari akses illegal oleh pihak yang tidak berhak atas sebuah informasi yang kemudian mengubah informasi tersebut. Selain itu, integrity dapat diserang melalui penyusupan virus atau malware. Virus dan malware mampu melakukan

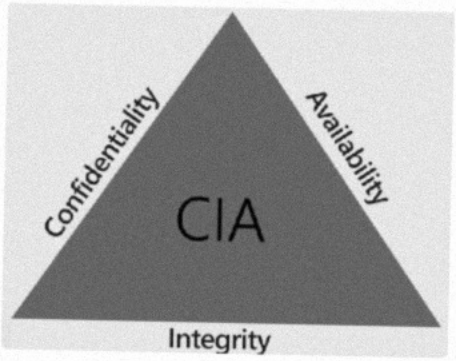
pengubahan terhadap data sehingga keaslian data mengalami perubahan.

AVAILABILITY

Aspek ini berarti ketersediaan. Hal penting dalam keamanan informasi, adalah bahwa data yang dibutuhkan harus selalu tersedia kapanpun diperlukan. Perlindungan availability adalah jaminan bahwa sistem dan data dapat diakses oleh pemiliknya kapanpun informasi tersebut dibutuhkan.

Jika informasi tidak dapat diperoleh ketika dibutuhkan, maka Availability mengalami masalah. Diantara ancamanterhadap aspek availability adalah :

- Bencana alam,
- Kerusakan system computer
- Akses internet yang terhambat
- Serangan DDOS dimana serangan tersebut membanjiri lalu lintas server, jaringan, atau sistem sehingga gagal merespon



Gambar. 1 CIA Triad

Linux

Komponen Arsitektur Keamanan Linux :

1. Account Pemakai (user account)

Keuntungan :

- Kekuasaan dalam satu account yaitu root, sehingga mudah dalam administrasi system.
- Kecerobohan salah satu user tidak berpengaruh kepada system secara keseluruhan.
- Masing-masing user memiliki privacy yang ketat

Macam User :

Root : kontrol system file, user, sumber daya (devices) dan akses jaringan

User : account dengan kekuasaan yang diatur oleh root dalam melakukan aktifitas dalam system.

Group : kumpulan user yang memiliki hak sharing yang sejenis terhadap suatu devices tertentu.

2. Kontrol Akses secara Diskresi (Discretionary Access control)

Discretionary Access control (DAC) adalah metode pembatasan yang ketat, yang meliputi :

- Setiap account memiliki username dan password sendiri.
- Setiap file/device memiliki atribut(read/write/execution) kepemilikan, group, dan user umum.

> Virus tidak akan mencapai file system, jika sebuah user terkena, maka akan berpengaruh pada file-file yang dimiliki oleh user yang mengeksekusi file tersebut.

Jika kita lakukan list secara detail menggunakan $ls –l, kita dapat melihat penerapan DAC pada file system linux :

```
d rw-  - -x  - - -  5  fade  users  1024  Feb   8
12:30 Desktop
- rw-  r - -  r - -  9  Goh  hack   318  Mar  30
09:05 borg.dead.letter
```

-	rw-	r - -	r - -	9	Goh	hack	318	Mar	30	09:05	borg. dead. letter
1	2	3	4	5	6	7	8	9		10	11

Keterangan :

1 = tipe dari file ; tanda dash (-) berarti file biasa, d berarti directory, l berarti file link, dsb

2 = Izin akses untuk owner (pemilik), r=read/baca, w=write/tulis, x=execute/eksekusi

3 = Izin akses untuk group

4 = Izin akses untuk other (user lain yang berada di luar group yang didefinisikan sebelumnya)

5 = Jumlah link file

6 = Nama pemilik

7 = (owner)
Nama Group

8 = Besar file dalam
9 = byte

10 = Bulan dan tanggal update terakhir
Waktu update terakhir

11 = Nama file/device

Perintah-perintah penting pada DAC :

- Mengubah izin akses file :
  1. bu : **chmod < u | g | o > < + | - > < r | w | e > nama file**,
     contoh :
     chmod u+x g+w o-r borg.dead.letter ; tambahkan akses eksekusi(e) untuk user (u), tambahkan juga akses write(w) untuk group (g) dan kurangi izin akses read(r) untuk other(o) user.
  2. chmod metode octal, bu: **chmod - - - namafile** , digit dash (-) pertama untuk izin akses user, digit ke-2 untuk izin akses group dan digit ke-3 untuk izin akses other, berlaku ketentuan : r(read) = 4, w(write) = 2, x (execute) = 1 dan tanpa izin akses = 0.
     Contoh :
     Chmod 740 borg.dead.letter
     Berarti : bagi file *borg.dead.letter* berlaku
     digit ke-1 → 7=4+2+1=izin akses r,w,x penuh untuk user.
     digit ke-2 → 4=4+0+0=izin akses r untuk group
     digit ke-3 → 0=0+0+0=tanpa izin akses untuk other user.

- Mengubah kepemilikan : chown <owner/pemilik><nama file>
- Mengubah kepemilikan group : chgrp <group owner><nama file>

- Menggunakan account root untuk sementara :
  ~$su ; system akan meminta password
  password : **** ; prompt akan berubah jadi pagar, tanda login sebagai root
  ~#

- Mengaktifkan shadow password, yaitu membuat file **/etc/passwd** menjadi dapat dibaca (readable) tetapi tidak lagi berisi password, karena sudah dipindahkan ke **/etc/shadow**

Contoh tipikal file **/etc/passwd** setelah diaktifkan shadow:

...
root:x:0:0::/root:/bin/bash
fade:x:1000:103: , , , :/home/fade:/bin/bash
...

Lihat user fade, dapat kita baca sebagai berikut :

username : fade
Password : x
User ID (UID) : 1000
Group ID (GUID) : 103
Keterangan tambahan : -
Home directory : /home/fade
Shell default : /bin/bash

Password-nya bisa dibaca (readable), tapi berupa huruf x saja, password sebenarnya disimpan di file **/etc/shadow** dalam keadaan dienkripsi :

```
...
root:pCfouljTBTX7o:10995:0:::::
fade:oiHQw6GBf4tiE:10995:0:99999:7:::
...
```

Perlunya Pro aktif password

Linux menggunakan metode DES (Data Encription Standart) untuk password-nya. User harus di training dalam memilih password yang akan digunakannya agar tidak mudah ditebak dengan program-program crack password dalam ancaman bruto force attack. Dan perlu pula ditambah dengan program Bantu cek keamanan password seperti :

- Passwd+ : meningkatkan loging dan mengingatkan user jika mengisi password yang mudah ditebak, ftp://ftp.dartmouth.edu/pub/security
- Anlpasswd: dapat membuat aturan standar pengisian password seperti batas minimum, gabungan huruf besar dengan huruf kecil, gabungan angka dan huruf dsb, ftp://coast.rs.purdue.edu/pub/tools/unix/

5. Deteksi Penyusupan (Intrusion Detection)

Intrusion Detection System adalah program yang dirancang khusus untuk monitoring jaringan dan dapat pula mendeteksi penyusupan secara cepat dengan menggunakan mekanisme algoritma tertentu

Tipe dasar IDS :

- Ruled based system : mencatat lalu lintas data jika sesuai dengan database dari tanda penyusupan yang telah dikenal, maka langsung dikategorikan penyusupan.
  Pendekatan Ruled based system :
  - Preemptory (pencegahan) ; IDS akan memperhatikan semua lalu lintas jaringan, dan langsung bertindak jika dicurigai ada penyusupan.
  - Reactionary (reaksi) ; IDS hanya mengamati file log saja.
- Adaptive system : penerapan expert system dalam mengamati lalu lintas jaringan.

Program IDS :

- **Chkwtmp** : program pengecekan terhadap entry kosong
- **Tcplogd** : program pendeteksi stealth scan (scanning yang dilakukan tanpa membuat sesi tcp)
- **Host entry** : program pendeteksi login anomaly (perilaku aneh) → bizarre behaviour (perilaku aneh), time anomalies (anomaly waktu), local anomaly.

Mewaspadai Social Engineering (rekayasa sosial) :

1. Mengaku sebagi eksekutif yang tidak berhasil mengakses, menghubungi administrator via telepon/fax.
2. Mengaku sebagai administrator yang perlu mendiagnosa masalah network, menghubungi end user via email/fax/surat.
3. Mengaku sebagai petugas keamanan e-commerce, menghubungi customer yang telah bertransaksi untuk mengulang kembali transaksinya di form yang disediakan olehnya.
4. pencurian surat, password.
5. penyuapan, kekerasan.

D. Membedakan Sumber daya internal dan Eksternal :

Memanfaatkan teknologi firewall yang memisahkan network internal dengan network eksternal dengan rule tertentu.

E. Sistem Otentikasi User :

Def : adalah proses penentuan identitas dari seseorang yang sebenarnya, hal ini diperlukan untuk menjaga keutuhan (integrity) dan keamanan (security) data, pada proses ini seseorang harus dibuktikan siapa dirinya sebelum menggunakan layanan akses.

Upaya untuk lebih mengamankan proteksi password, antara lain :

1. Salting.

   Menambahkan string pendek ke string password yang diberikan pemakai

   sehingga mencapai panjang password tertentu.

2. One time password.
   - Pemakai harus mengganti password secara teratur. Upaya ini membatasi peluang password telah diketahui atau dicoba-coba pemakai lain.
   - Bentuk ekstrim pendekatan ini adalah one time password, yaitu pemakai mendapat satu buku berisi daftar password. Setiap kali pemakai login, pemakai menggunakan password berikutnya yang terdapat di daftar password.
   - Dengan one time password, pemakai direpotkan keharusan menjaga agar buku passwordnya jangan sampai dicuri.
3. Satu daftar panjang pertanyaan dan jawaban.
   - Variasi terhadap password adalah mengharuskan pemakai memberi satu daftar pertanyaan panjang dan jawabannya. Pertanyaan-pertanyaan dan jawabannya dipilih pemakai sehingga pemakai mudah mengingatnya dan tak perlu menuliskan di kertas.
   - Pertanyaan berikut dapat dipakai, misalnya :
     - Siapa mertua abang ipar Badru ?

- Apa yang diajarkan Pak Harun waktu SD ?
- Di jalan apa pertama kali ditemukan simanis ?

- Pada saat login, komputer memilih salah satu dari pertanyaan-pertanyaan secara acak, menanyakan ke pemakai dan memeriksa jawaban yang diberikan.

4. Tantangan tanggapan (chalenge response).
   - Pemakai diberi kebebasan memilih suatu algoritma, misalnya x3.
   - Ketika pemakai login, komputer menuliskan di layar angka 3. Dalam kasus ini pemakai mengetik angka 27. Algoritma dapat berbeda di pagi, sore, dan hari berbeda, dari terminal berbeda, dan seterusnya.

Contoh Produk Otentikasi User, antara lain :

1. Secureid ACE (Access Control Encryption)
   System token hardware seperti kartu kredit berdisplay, pemakai akan menginput nomor pin yang diketahui bersama, lalu memasukkan pascode bahwa dia pemilik token.

2. S/key (Bellcore)
   System software yang membentuk one time password (OTP) berdasarkan informasi loginterkhir dengan aturan random tertentu.

- Adanya program yang secara tidak sengaja diset menjadi "setuid root" sehingga ketika dijalankan pemakai memiliki akses seperti super user (root) yang dapat melakukan apa saja.

4. Salah menggunakan program atau sistem

Contoh :

- Kesalahan menggunakan program yang dijalankan dengan menggunakan account root (super user) dapat berakibat fatal.

PENGUJI KEAMANAN SISTEM

Untuk memudahkan administrator dari sistem informasi membutuhkan "automated tools", perangkat pembantu otomatis, yang dapat membantu menguji atau meng-evaluasi
keamanan sistem yang dikelola.

Contoh Tools Terintegrasi:

Perangkat lunak bantu	Sistem Operasi
Cops	UNIX
Tripwire	UNIX
Satan/Saint	UNIX
SBScan:	UNIX
Ballista	Windows NT

Contoh Tools Pengujian yang dibuat para hacker :

Tools	Kegunaan
Crack	program untuk menduga atau memecahkan password dengan menggunakan sebuah atau beberapa kamus (dictionary). Program crack ini melakukan brute force cracking dengan mencoba mengenkripsikan sebuah kata yang diambil dari kamus, dan kemudian membandingkan hasil enkripsi dengan password yang ingin dipecahkan.
land dan latierra	sistem Windows 95/NT menjadi macet (hang, lock up). Program ini mengirimkan sebuah paket yang sudah di"spoofed" sehingga seolah-olah paket tersebut berasal dari mesin yang sama dengan menggunakan port yang terbuka
ping-o-death	sebuah program (ping) yang dapat meng-crash-kan Windows 95/NT dan beberapa versi Unix.
Winuke	program untuk memacetkan sistem berbasis Windows

PROBING SERVICES

- Defenisi Probing : "probe" (meraba) servis apa saja yang tersedia. Program ini juga dapat digunakan oleh kriminal untuk melihat servis apa saja yang tersedia

di sistem yang akan diserang dan berdasarkan data-data yang diperoleh dapat melancarkan serangan.

- Servis di Internet umumnya dilakukan dengan menggunakan protokol TCP atau UDP. Setiap servis dijalankan dengan menggunakan port yang berbeda, misalnya:
    - SMTP, untuk mengirim dan menerima e-mail, TCP, port 25
    - POP3, untuk mengambil e-mail, TCP, port 110

  Contoh di atas hanya sebagian dari servis yang tersedia. Di system UNIX, lihat berkas /etc/services dan /etc/inetd.conf untuk melihat servis apa saja yang dijalankan oleh server atau komputer yang bersangkutan.

- Pemilihan servis apa saja tergantung kepada kebutuhan dan tingkat keamanan yang diinginkan. Sayangnya seringkali sistem yang dibeli atau dirakit menjalankan beberapa servis utama sebagai "default". Kadang-kadang beberapa servis harus dimatikan karena ada kemungkinan dapat dieksploitasi oleh cracker. Untuk itu ada beberapa program yang dapat digunakan untuk melakukan

- Untuk beberapa servis yang berbasis TCP/IP, proses probe dapat dilakukan dengan menggunakan program telnet. Misalnya untuk melihat apakah ada servis e-mail dengan menggunakan SMTP digunakan telnet ke port 25 dan port 110.

```
unix% telnet target.host.com 25
unix% telnet localhost 110
```

Program penguji probing (penguji semua port otomatis) :

Paket probe untuk sistem UNIX

- nmap
- strobe
- tcpprobe

Probe untuk sistem Window 95/98/NT

- NetLab
- Cyberkit
- Ogre

Program yang memonitor adanya probing ke system

Probing biasanya meninggalkan jejak di berkas log di system anda. Dengan mengamati entry di dalam berkas log dapat diketahui adanya probing. Selain itu, ada juga program untuk memonitor probe seperti paket program courtney, portsentry dan tcplogd.

Digital Evidence in Court

Upaya untuk memperoleh bukti digital adalah target utama dari setiap investigasi yang berhubungan dengan kejahatan komputer. Vacca (2002) menyatakan bahwa bukti digital didefinisikan sebagai informasi yang memiliki nilai pembuktian yang disimpan atau ditransmisikan dalam bentuk digital. Definisi lain dari bukti elektronik adalah informasi dan data nilai investigasi yang disimpan atau dikirimkan oleh perangkat elektronik.

Bukti tersebut diperoleh saat data atau barang fisik dikumpulkan dan disimpan untuk tujuan pemeriksaan (Technical Working Group for Electronic Crime Scene Investigation, 2001).

Dijelaskan pula bahwa alat bukti elektronik memiliki beberapa karakteristik. Pertama, seringkali laten dalam arti yang sama seperti sidik jari atau bukti DNA, kedua dapat melampaui batas dengan mudah dan cepat, kemudian rapuh dan dapat dengan mudah diubah, rusak, atau dihancurkan dan terakhir terkadang sensitif terhadap waktu (Technical Working Group for Electronic Crime Scene Investigation, 2001). Karena bukti digital dapat dengan mudah diubah, dirusak, atau bahkan dihapus, bukti digital sangat rentan.

PENUTUP

Buku ini menyajikan konsep dasar keamanan komputer secara mendasar, metode dasar untuk meningkatkan keamanan computer, serta gambaran dasar mengenai peran komputer forensic.

Diharapkan materi yang disajikan dalam buku ini mampu berkontribusi dalam membangun kesadaran pembaca akan urgensi keamanan informasi yang semakin hari semakin meningkat ancamannnya.

Semoga penjelasan dalam bentuk konsep-konsep pokok fundamental dalam buku ini mampu menjadi salah satu referensi dalam dunia keamanan komputer di tanah air.

REFERENSI

Bishop, M. A. (2002). The art and science of computer security.

Bosworth, S., & Kabay, M. E. (Eds.). (2002). Computer security handbook. John Wiley & Sons.

Casey, E. (Ed.). (2001). Handbook of computer crime investigation: forensic tools and technology. Elsevier.

Rahardjo, B. (2002). Keamanan Sistem Berbasis Internet. Bandung: PT. Insan Komunikasi Indonesia.