

Prinsip Keamanan -Security Principles-

Klasifikasi Keamanan Sisinfo

[menurut David Icove]

Fisik (physical security)

Manusia (people /
personel security)

Data, media, teknik
komunikasi

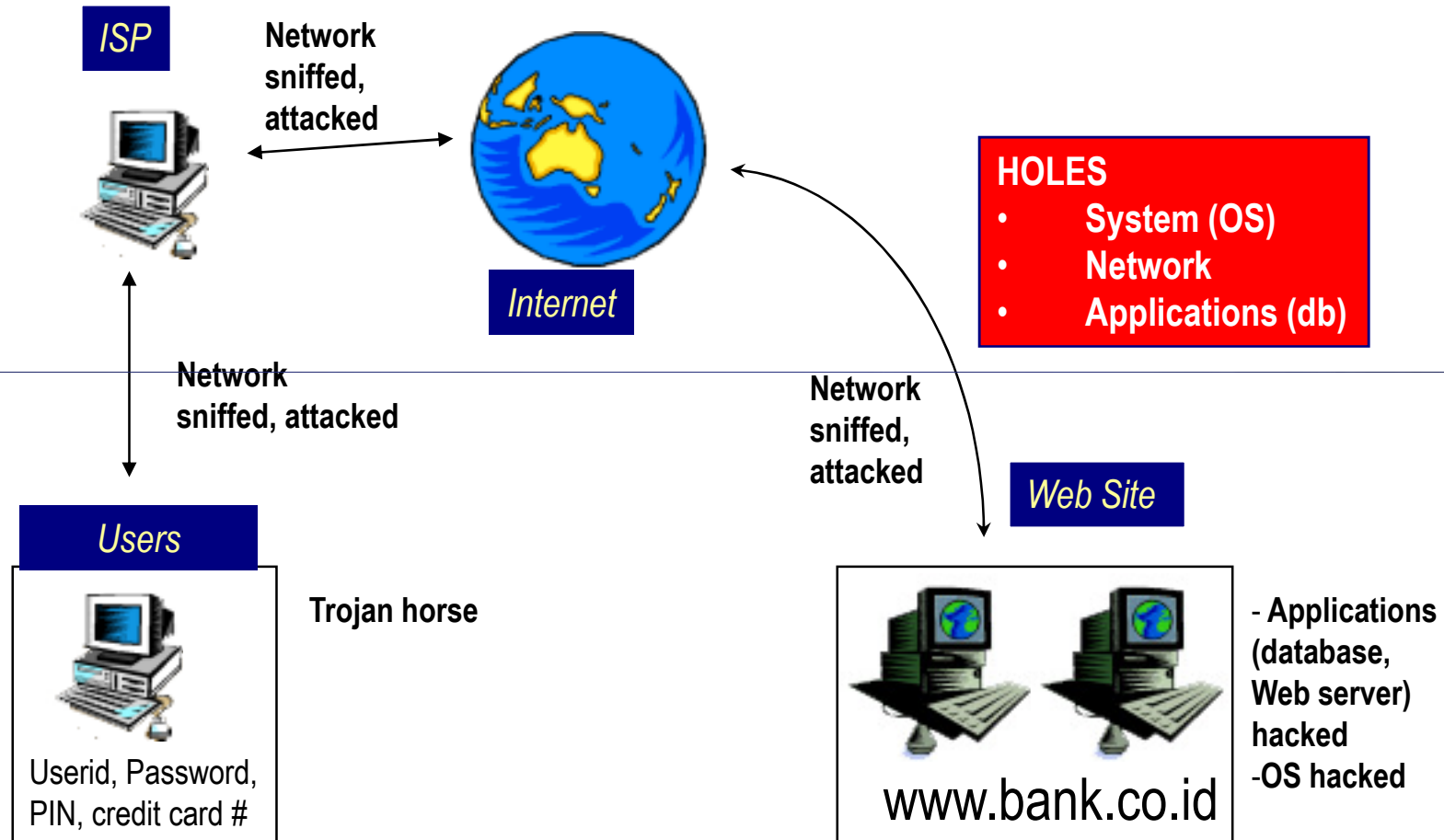
Kebijakan dan prosedur
(policy and procedures)

Biasanya orang terfokus kepada masalah data, media, teknik komunikasi. Padahal kebijakan (policy) sangat penting!

Klasifikasi Berdasarkan Elemen Sistem

- Network security
 - fokus kepada saluran (media) pembawa informasi
- Application security
 - fokus kepada aplikasinya sendiri, termasuk di dalamnya adalah database
- Computer security
 - fokus kepada keamanan dari komputer (end system), termasuk operating system (OS)

Letak potensi lubang keamanan



Aspek / Servis Keamanan

(Security Control)

- Confidentiality / Privacy
- Integrity
- Availability
- Authentication
- Non-repudiation
- Access control

Privacy / confidentiality

- Proteksi data [hak pribadi] yang sensitif
 - Nama, tempat tanggal lahir, agama, hobby, penyakit yang pernah diderita, status perkawinan, nama anggota keluarga, nama orang tua
 - Data pelanggan. Customer Protection harus diperhatikan
 - Sangat sensitif dalam e-commerce, *healthcare*
- Serangan: sniffer (penyadap), keylogger (penyadap kunci), social engineering, kebijakan yang tidak jelas
- Proteksi: firewall, kriptografi / enkripsi, policy
- Electronic Privacy Information Center <http://www.epic.org>
Electronic Frontier Foundation <http://www.eff.org>

Integrity

- Informasi tidak berubah tanpa ijin
 - (*tampered, altered, modified*)
- Serangan:
 - Penerobosan pembatas akses, spoof (pemalsuan), virus (mengubah berkas), trojan horse, *man-in-the-middle attack*
- Proteksi:
 - message authentication code (MAC), (digital) signature, (digital) certificate, hash function

Availability

- Informasi harus dapat tersedia ketika dibutuhkan
 - Serangan terhadap server: dibuat hang, down, crash, lambat
 - Biaya jika server web (*transaction*) down di Indonesia
 - Menghidupkan kembali: Rp 25 juta
 - Kerugian (*tangible*) yang ditimbulkan: Rp 300 juta
- Serangan: Denial of Service (DoS) attack
- Proteksi: backup, redundancy, DRC, BCP, IDS, filtering router, firewall untuk proteksi serangan

Authentication

- Meyakinkan keaslian data, sumber data, orang yang mengakses data, server yang digunakan
 - Bagaimana mengenali nasabah bank pada servis Internet Banking? *Lack of physical contact*

Menggunakan:

what you have (identity card)

what you know (password, PIN)

what you are (biometric identity)

Claimant is at a particular place (and time)

Authentication is established by a trusted third party

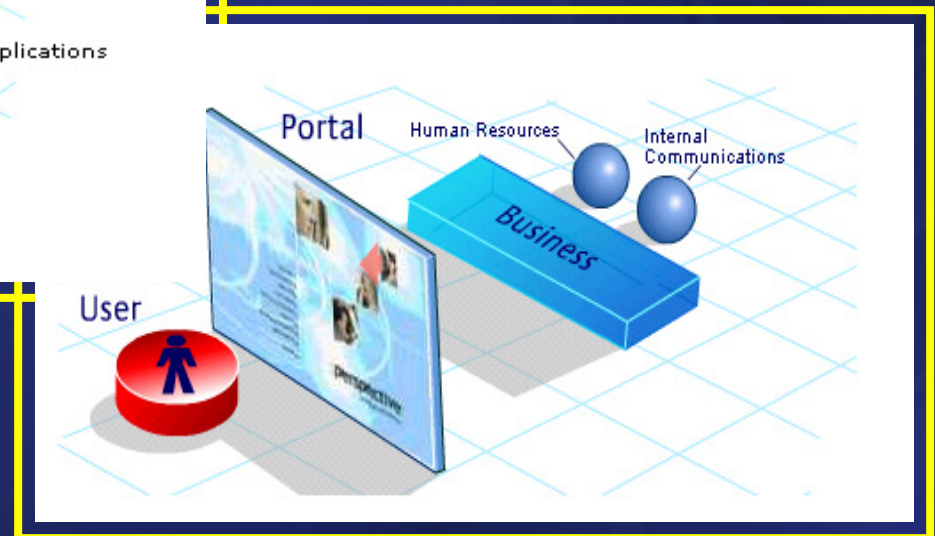
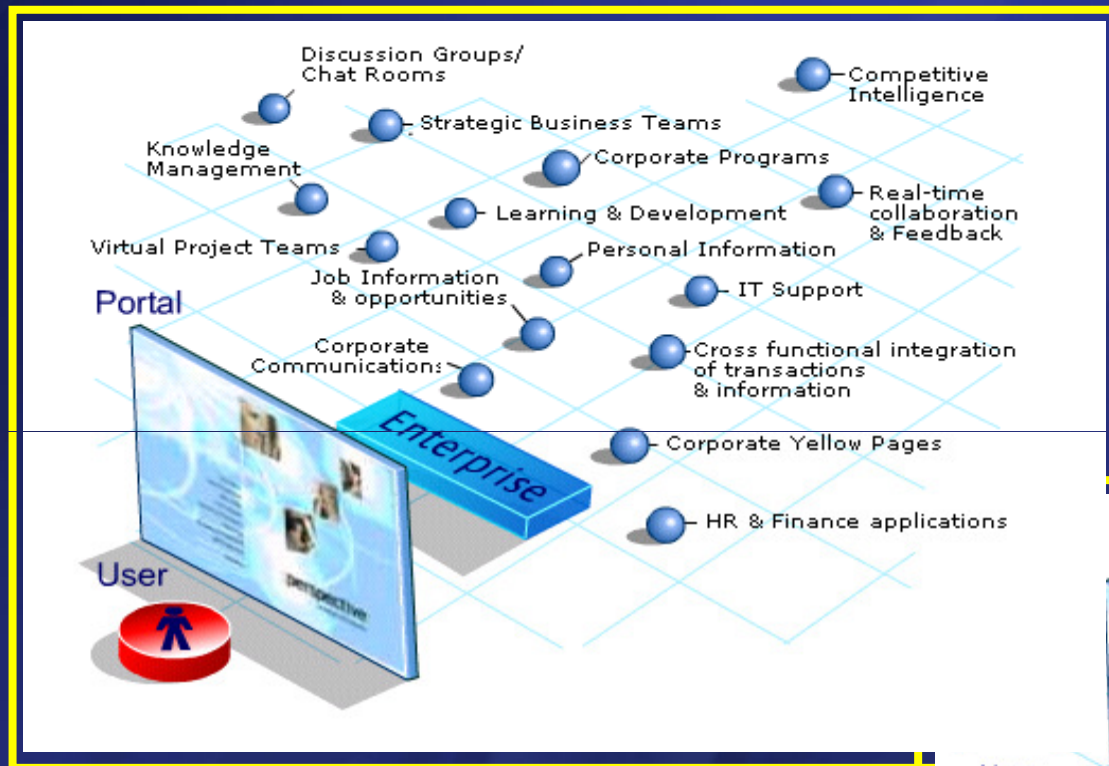
- Serangan: identitas palsu, password palsu, terminal palsu, situs web gadungan
- Proteksi: digital certificates

On the Internet nobody knows you're a dog



Authentication Terpadu

Terlalu banyak authentication:
mbingungkan



Non-repudiation

- Tidak dapat menyangkal (telah melakukan transaksi)
 - menggunakan digital signature / certificates
 - perlu pengaturan masalah hukum (bahwa digital signature sama seperti tanda tangan konvensional)

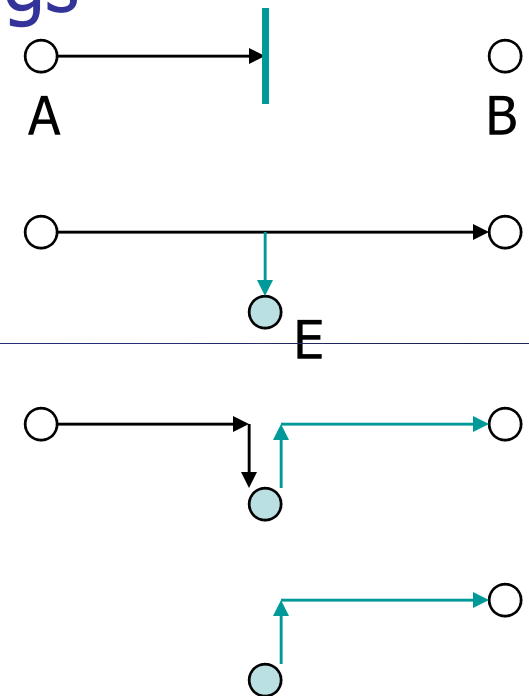
Access Control

- Mekanisme untuk mengatur siapa boleh melakukan apa
 - biasanya menggunakan password, token
 - adanya kelas / klasifikasi pengguna dan data, misalnya:
 - Publik
 - Private
 - Confidential
 - Top Secret

Jenis Serangan (attack)

Menurut W. Stallings

- **Interruption**
DoS attack, network flooding
- **Interception**
Password sniffing
- **Modification**
Virus, trojan horse
- **Fabrication**
spoofed packets



Interruption Attack

- Denial of Service (DoS) attack
 - Menghabiskan bandwidth, network flooding
 - Memungkinkan untuk spoofed originating address
 - Tools: ping broadcast, smurf, synk4, macof, various flood utilities
- Proteksi:
 - Sukar jika kita sudah diserang
 - Filter at router for outgoing packet, filter attack originating from our site

Interception Attack

- Sniffer to capture password and other sensitive information
- Tools: tcpdump, ngrep, linux sniffer, dsniff, trojan (BO, Netbus, Subseven)
- Protection: segmentation, switched hub, promiscuous detection (anti sniff)

Modification Attack

- Modify, change information/programs
- Examples: Virus, Trojan, attached with email or web sites
- Protection: anti virus, filter at mail server, integrity checker (eg. tripwire)

Fabrication Attack

- Spoofing address is easy
- Examples:
 - Fake mails: virus sends emails from fake users (often combined with DoS attack)
 - spoofed packets
- Tools: various packet construction kit
- Protection: filter outgoing packets at router

More on Interruption Attack (cont.)

- Distributed Denial of Service (DDoS) attack
 - Flood your network with spoofed packets from many sources
 - Based on SubSeven trojan, “phone home” via IRC once installed on a machine. Attacker knows how many agents ready to attack.
 - Then, ready to exhaust your bandwidth
 - See Steve Gibson’s paper <http://grc.com>

Teknologi Kriptografi

- Penggunaan enkripsi (kriptografi) untuk meningkatkan keamanan
 - **Tidak semua** dapat diamankan dengan enkripsi!
- Konsep: Private key vs public key
 - Contoh: DES, IDEA, RSA, ECC
- Lebih detail, akan dijelaskan pada bagian terpisah

Security Requirement

- Tidak semua aspek keamanan dibutuhkan
 - Berbeda untuk proses bisnis / aktivitas yang berbeda
 - Berbeda untuk industri yang berbeda
 - Ada prioritas
 - Perlu ditegaskan aspek mana yang harus disediakan

Ancaman (*Security Threats*)

- Perlu diidentifikasi ancaman terhadap sistem
 - Darimana saja ancaman tersebut?
 - Dari dalam organisasi (pegawai)?
 - Dari luar organisasi (crackers, kompetitor)?
 - Sumber: oleh manusia (sengaja, tidak sengaja) atau alam (bencana, musibah)?
 - Tingkat kesulitan
 - Probabilitas ancaman menjadi kenyataan

Mempelajari crackers

- Mempelajari:
 - Perilaku perusak
 - Siapakah mereka?
 - Apa motifnya?
 - Bagaimana cara masuk?
 - Apa yang dilakukan setelah masuk?
- Tools:
 - honeypot, honeynet

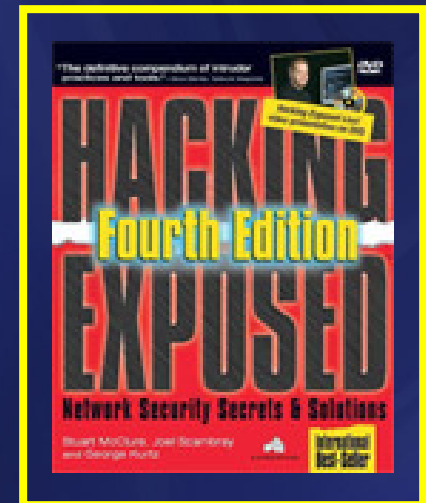
Know Your Enemy



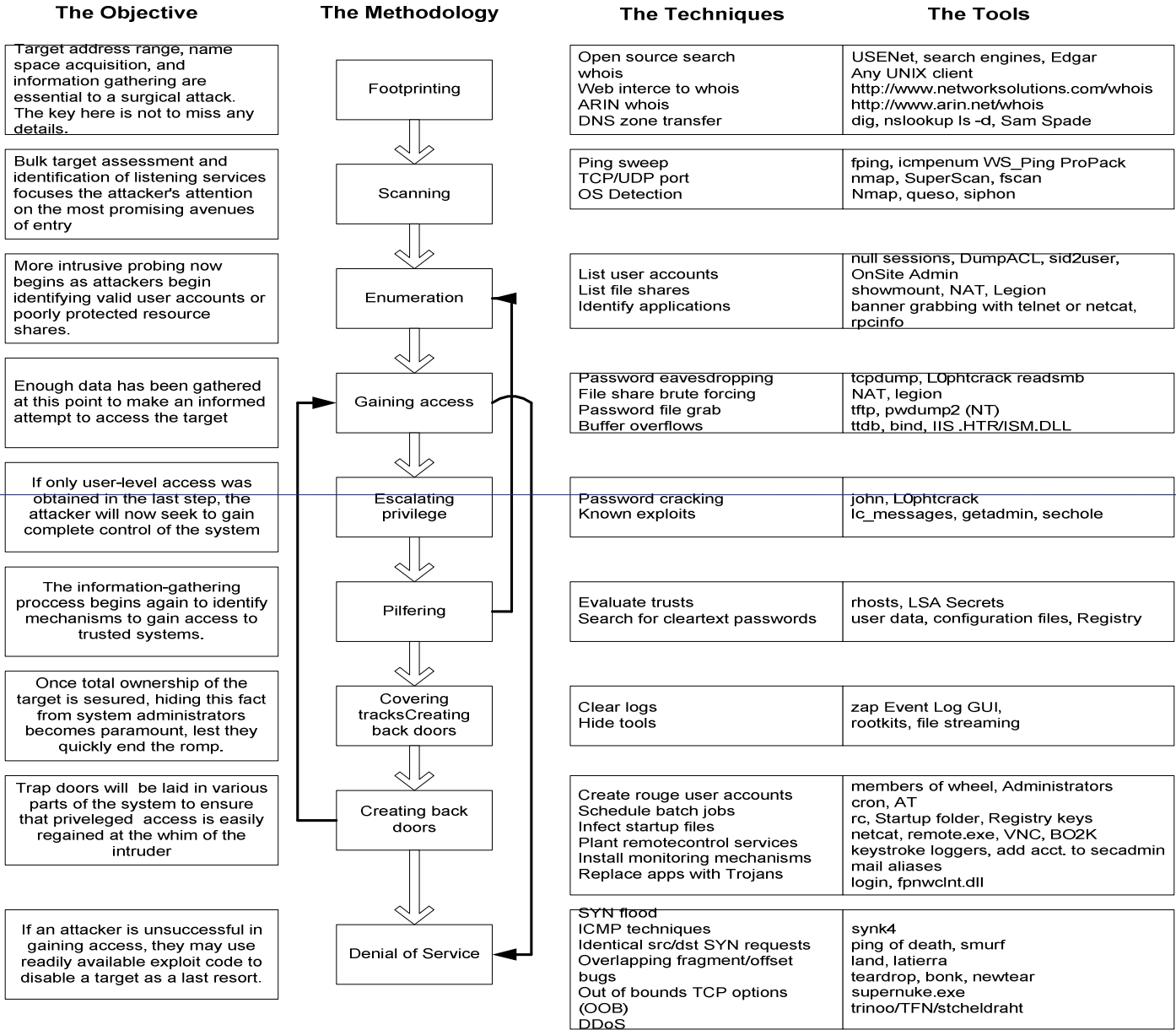
Crackers SOP / Methodology

Dari "Hacking Exposed":

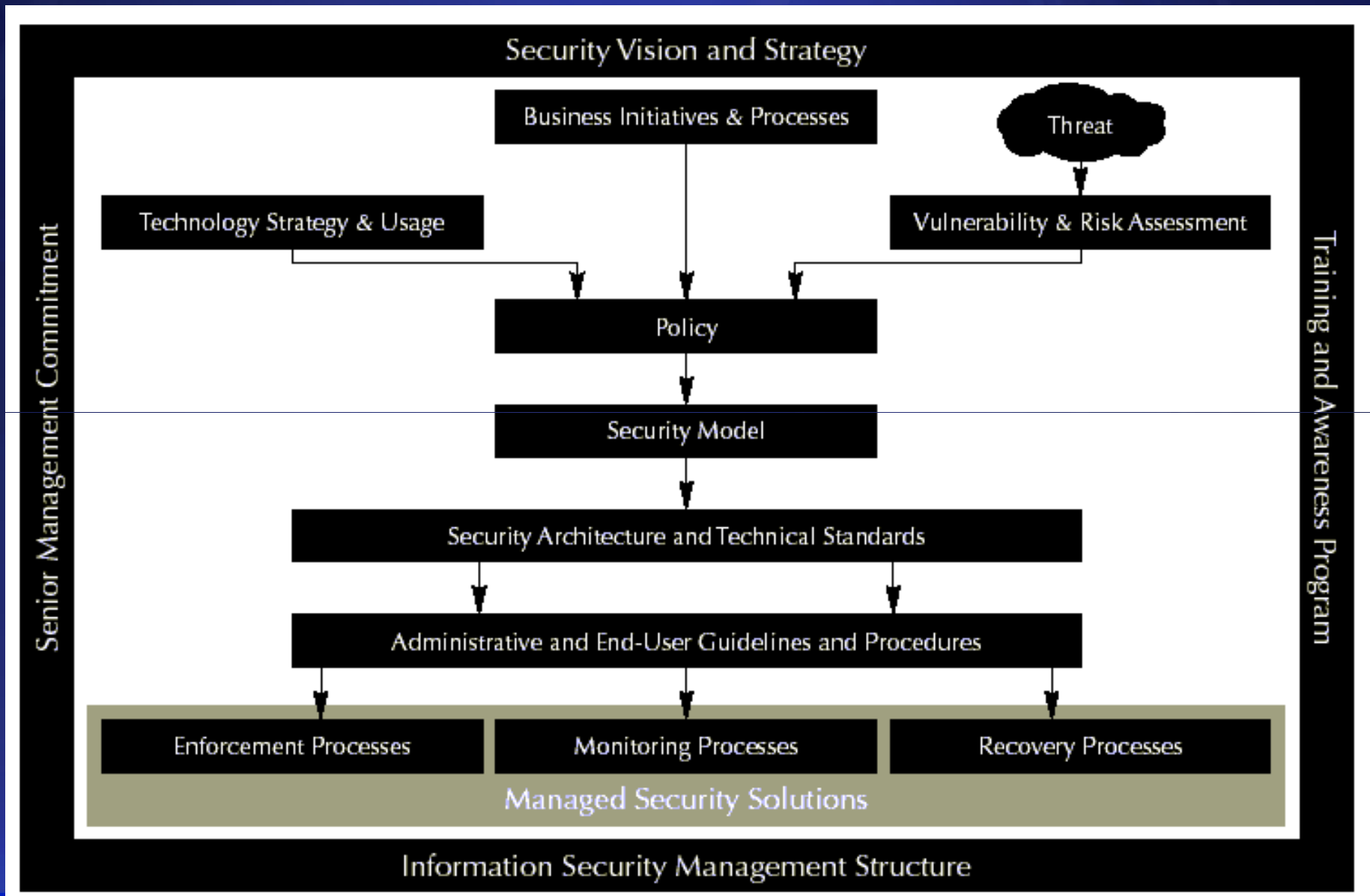
- Target acquisition and information gathering
- Initial access
- Privilege escalation
- Covering tracks
- Install backdoor
- Jika semua gagal, lakukan DoS attack



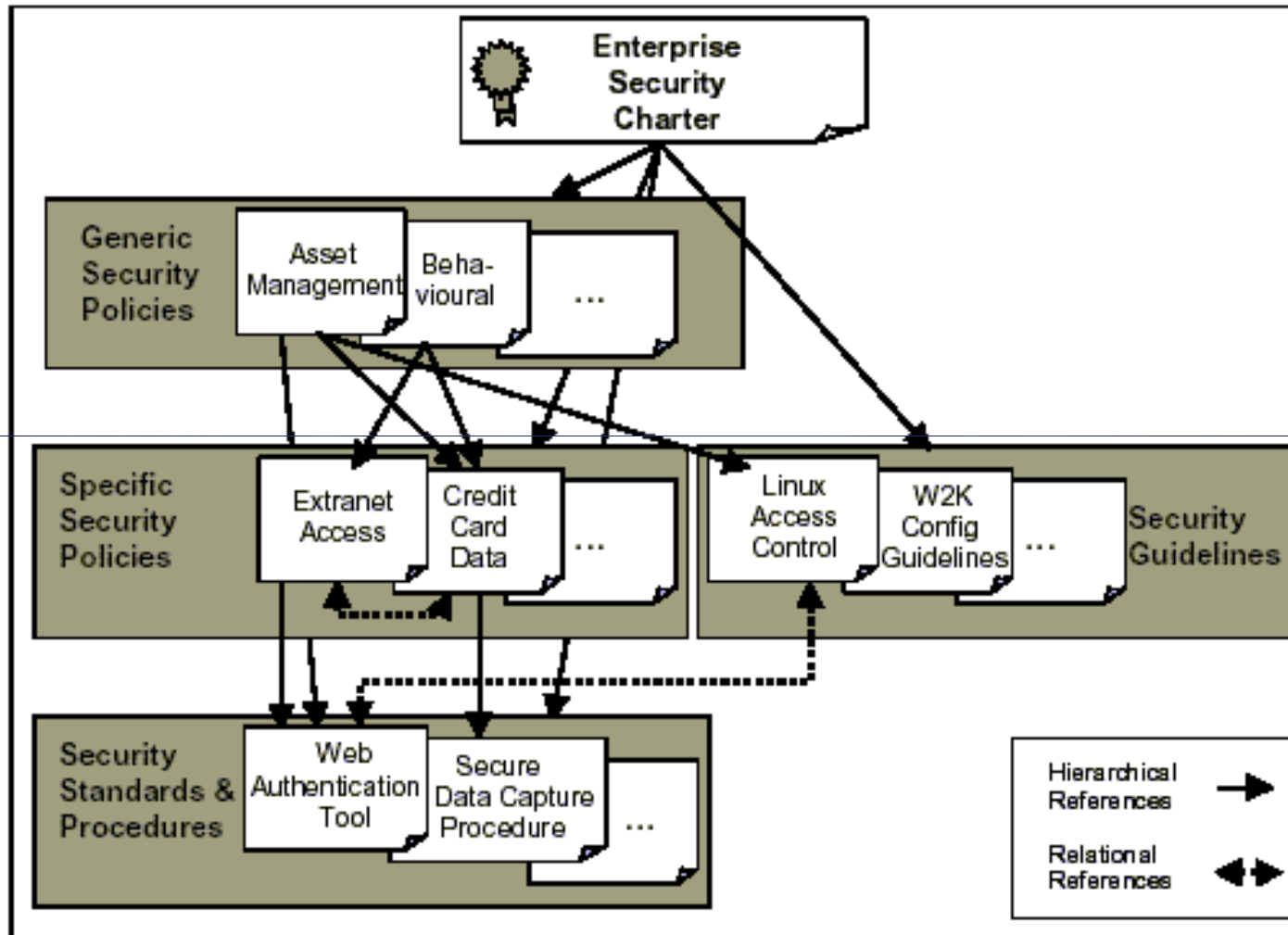
ANATOMY OF A HACK



IT SECURITY FRAMEWORK



Security Policy Framework



Source: META Group

Pengamanan Menyeluruh

- Harus menyeluruh - holistic approach

PEOPLE

- awareness, skill
- ...

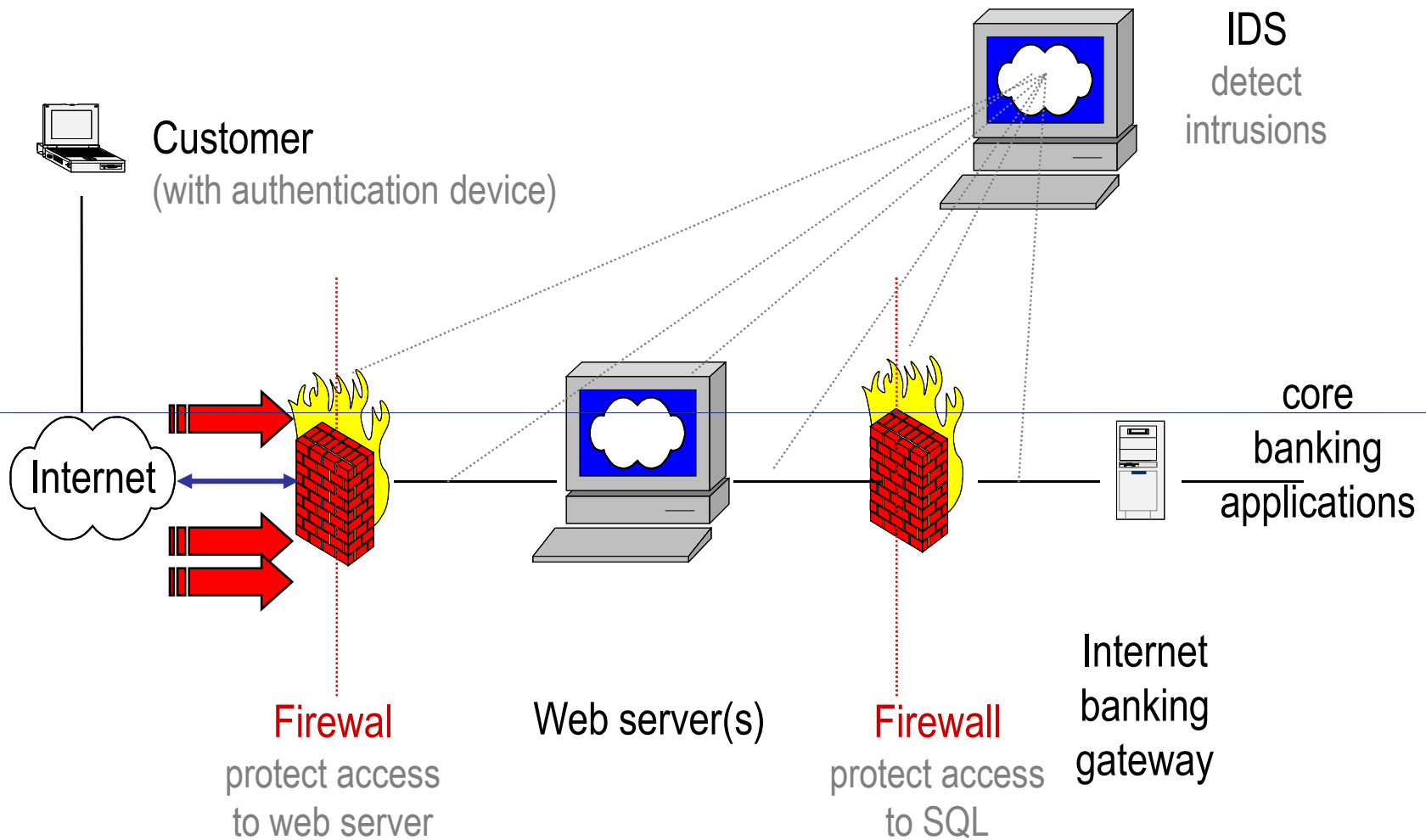
PROCESS

- security as part of business process
- ...

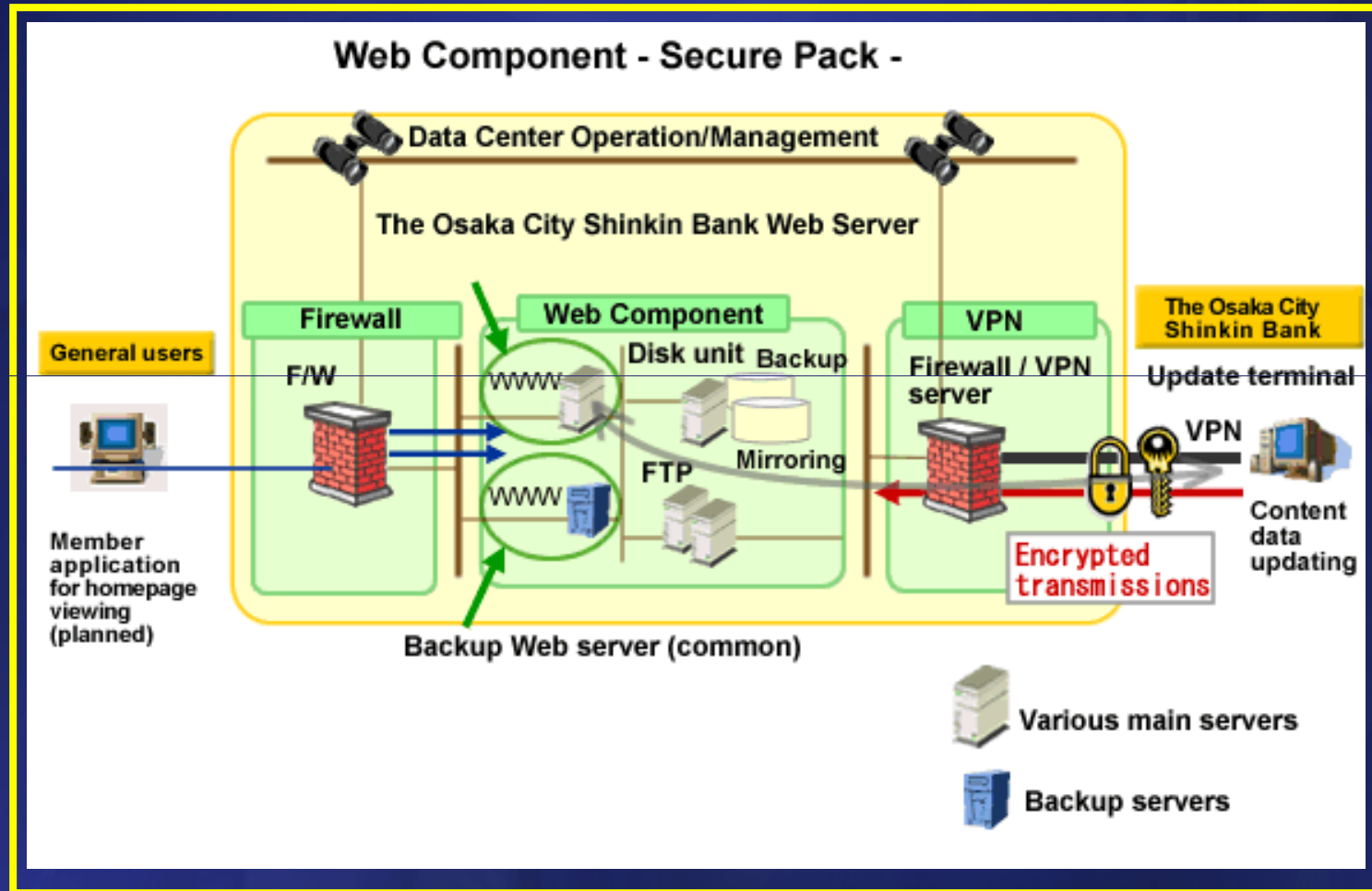
TECHNOLOGY

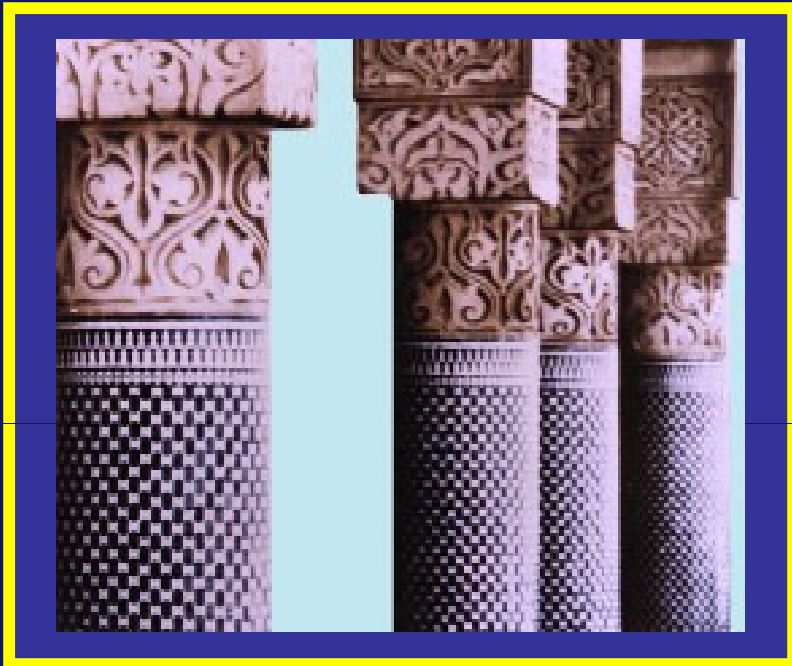
- implementation
- ...

Pengamanan Berlapis



Contoh Implementasi: Osaka Bank





Terima Kasih