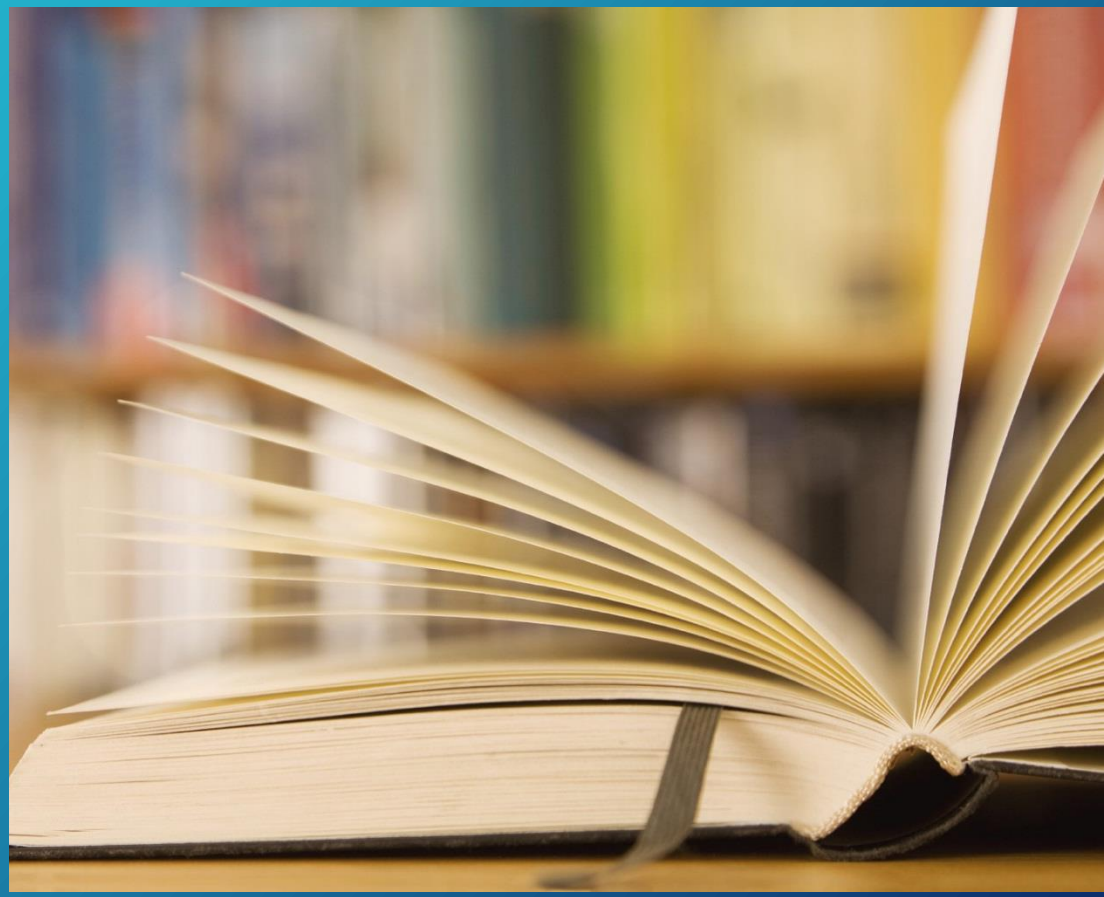
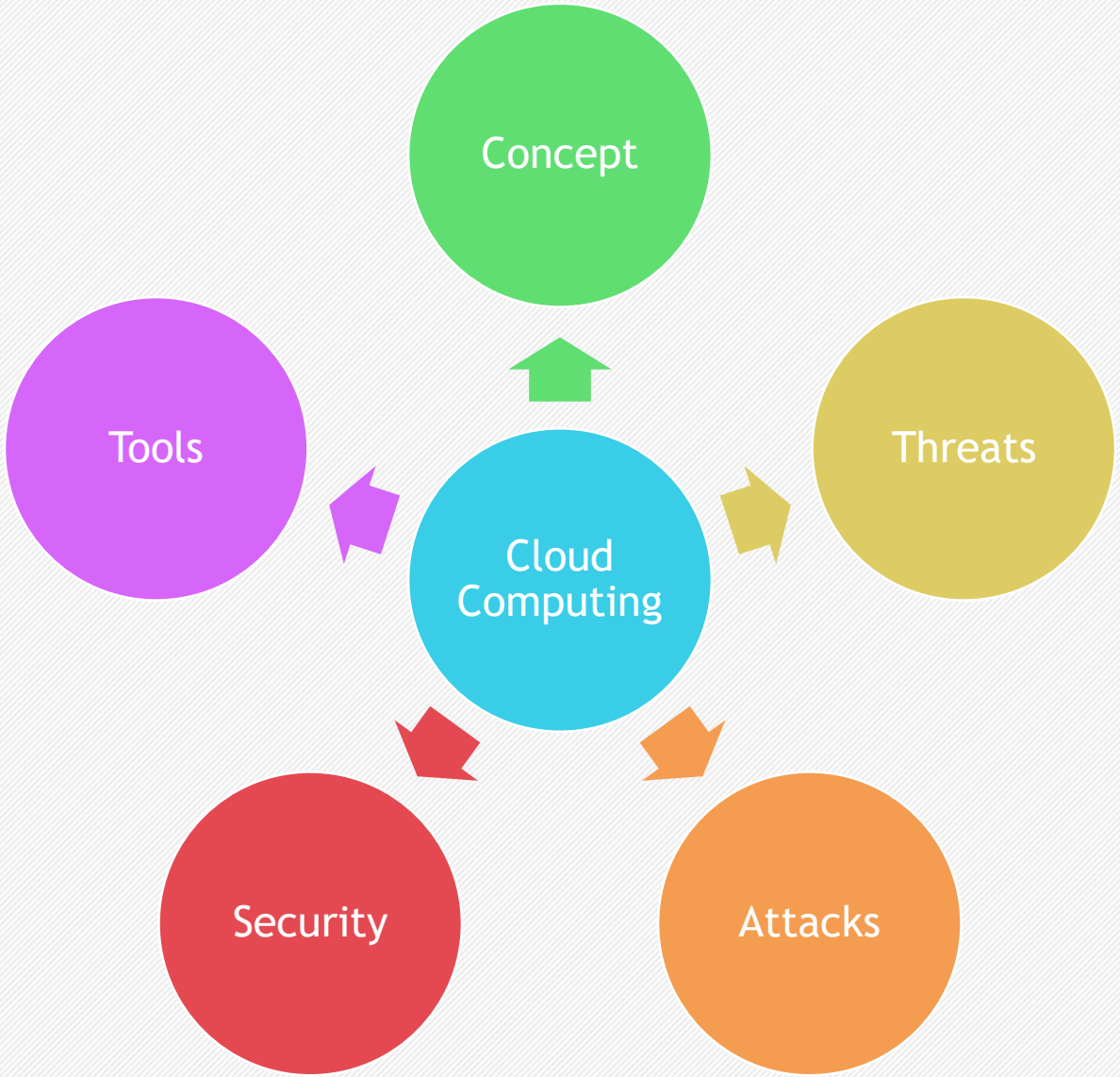
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

SECURE CLOUD COMPUTING

Keamanan Sistem Informasi – Aditya Putra, ST., MT.



Agenda



CONCEPTS - Pendahuluan

DEFINISI

- Cloud Computing adalah layanan IT on-demand dimana infrastruktur dan aplikasinya tersedia sebagai layanan berbayar-terukur pada jaringan internet

KARAKTERISTIK

- On-demand self service
- Distributed storage
- Rapid elasticity
- Automated management
- Broad network access
- Resource pooling
- Measured service
- Virtualization technology

TIPE-TIPE LAYANAN CLOUD COMPUTING

Sysadmin – Infrastructure as a Service (IaaS)

- Layanan berupa Virtual Machine, virtual hardware, OS yang dikendalikan melalui API (Cth: Amazon EC2, DigitalOcean, dll)

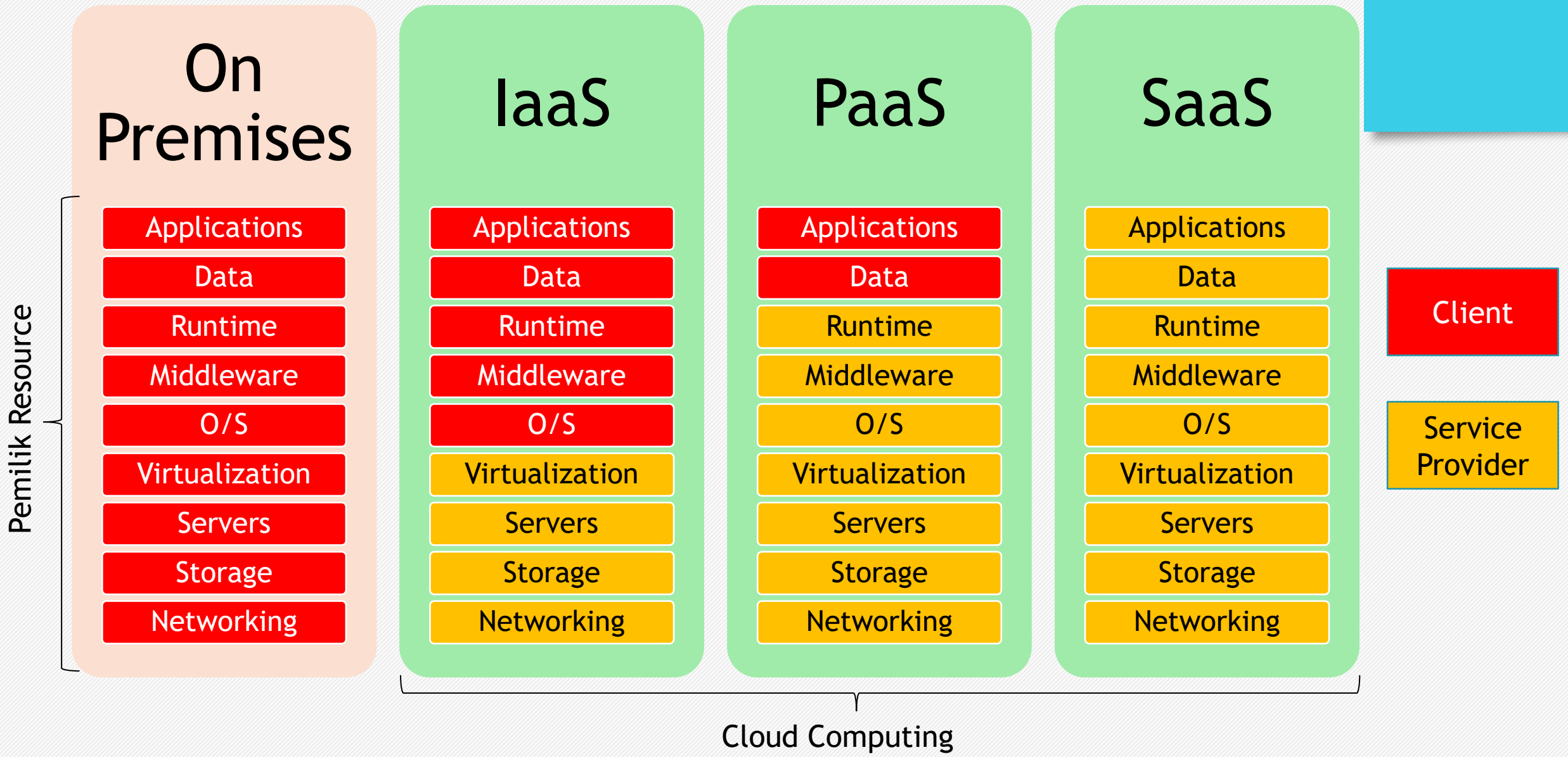
Developers - Platform as a Service (PaaS)

- Layanan berupa development tools, configuration management, dan deployment platform yang diperlukan untuk mengembangkan aplikasi (Cth: Microsoft Azure, dan Provide Hosting lain)

End Customers – Software as a Services (SaaS)

- Layanan berupa Software on-demand di internet (Cth: Google Docs, Drive, Meet, dll)

CONCEPTS - Perbedaan Responsibility pada CC



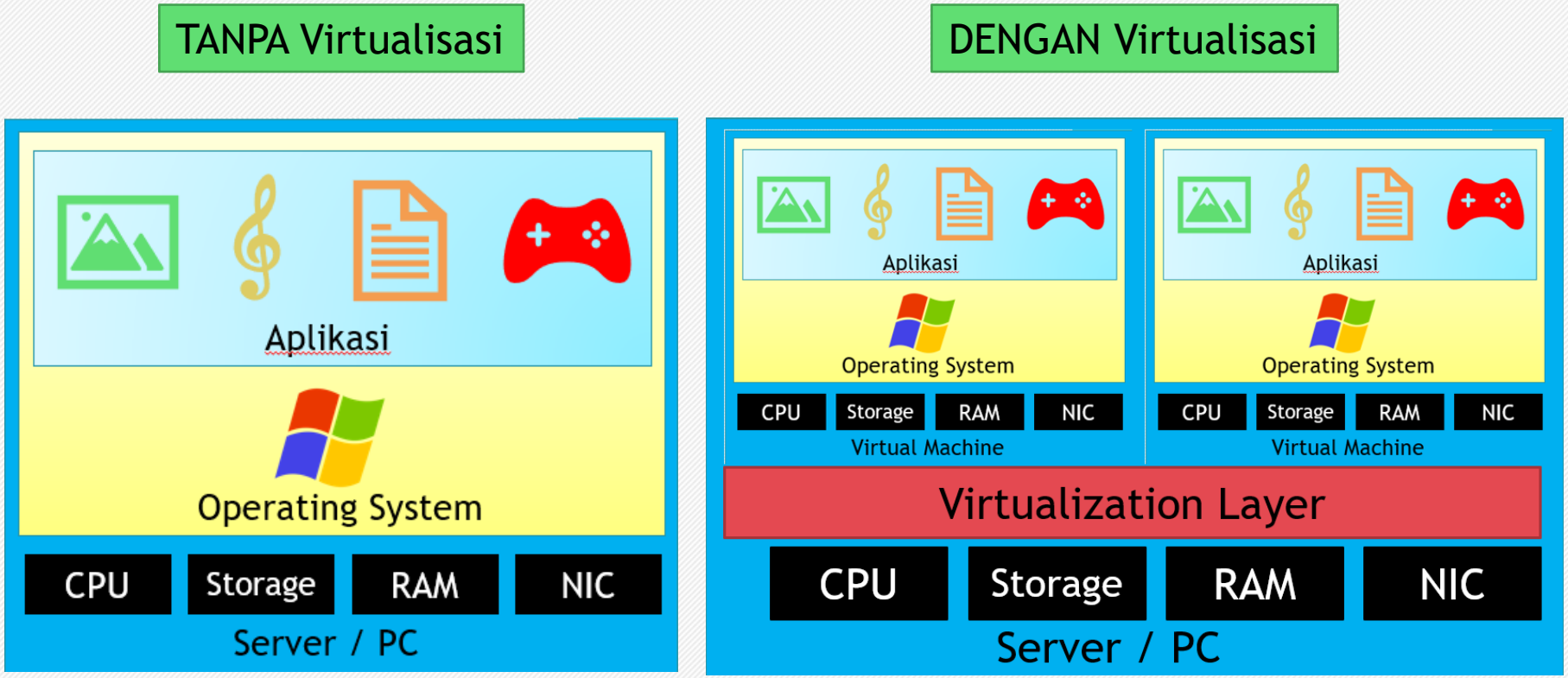
CONCEPT - Virtualization

DEFINISI

- Virtualisasi adalah kemampuan untuk menjalankan multiple OS pada satu sistem fisik hardware dan berbagi resource seperti storage, RAM, CPU, atau NIC

CONTOH TOOLS VIRTUALISASI

- VMware
- VirtualBox
- QEMU
- Parallels Desktop



THREATS

- Data Breach/Loss

  Data erased, modified or lost. Encryption are lost, misplaced or stolen. Misuse of data by CSP

- Abuse Use of Cloud Services

  Attackers create anonymous access to cloud services and perpetrate various attacks such as: Password and Key Cracking, Building rainbow table, DDoS, dll

- Insecure Interfaces

  Is not credential leak proof, unknown API dependencies, Reusable passwords/token

- Insufficient Due Diligence

  Ignorance from CSP in operational responsibilities such as security, encryption, IR, dll

- Unknown Risk Profile

  Clients don't get the big picture of the rented resource since they are not involved in hardware and software ownership

- Unsynchronized System Clocks

  Failed configuring automated tasks. Inaccurate analysing log files, malicious activity due to mismatched time stamp

- Conflicts between Client Hardening Procedures and Cloud Environment

  Certain client hardening procedures may conflict with a cloud provider's environment, making their implementation by the client impossible

- Privilege Escalation

  Mistake in access allocation which may lead to gain higher level of actions

- Loss of Encryption Keys

  The loss of encryption keys required for secure communication

- Lock in

  Inability of the client to migrate from 1 CSP to another due to lack of procedures, tools, for data, services portability

ATTACKS

1. Service Hijacking using Social Engineering
   - Social Engineering adalah intrusi yang mengenksploitasi dari sisi manusia dengan mengelabuhi manusia untuk melakukan aktivitas yang melanggar security policy
   - Attacker bisa menyerang CSP untuk melakukan reset password atau hal lain untuk mengetahui credential
   - Cara lain untuk mengetahui password adalah dengan menggunakan keylogging malware, phishing mail, dll
2. Service Hijacking using Network Sniffing
   - Network Sniffing adalah upaya intersep dan monitoring trafik jaringan yang dikirimkan antara 2 node cloud
   - Attacker melakukan sniffing pajet untuk menangkat data-data penting seperti password, session cookies dan konfigurasi keamanan lain yang ada pada layanan web
3. DNS Attacks
   - Contoh Serangan DNS adalah DNS Poisoning yang dilakukan dengan memberikan respon palsu yang berisi informasil DNS reply palsu terhadap sebuah query DNS. Dengan begitu user akan diarahkan ke website palsu. Jika user tidak menyadari, maka user akan memasukkan credential yang dapat dilihat oleh attacker

ATTACKS

4. Cryptanalysis Attacks

   - Enkripsi yang tidak aman dan ketinggalan jaman membuat CSP sangat rentan terhadap Cryptanalysis
   - Data yang disimpan di cloud memang dienkripsi. Namun, algoritma kriptografi yang memiliki critical flaw dapat membuatnya mudah untuk dipecahkan.

5. DoS / DDoS

   - Serangan DoS maupun DDoS dapat membuat layanan terhenti
   - Serangan DoS dapat dilakukan dengan Flooding Server dengan jumlah request yang gigantik, memberikan input yang menyebabkan crash pada sistem, dan memasukkan password salah berulang sehingga user di-lock
   - DoS yang melibatkan botnet disebut dengan Distributed DoS karena lokasi dan IP asal serangan yang beragam

SECURITY - Control Layers

Application	• SDLC, Scanners, WAF
Information	• DLP, CMF, Encryption
Management	• VA/VM, Patch Management, Configuration Management
Network	• NIDS/NIPS, Filtering, DPI, Anti DDoS, QoS, DNSSEC
Trusted Computing	• Software and Hardware RoT
Computer and Storage	• HIDS/HIPS, Host-based Firewall, Integrity Monitoring, Encryption
Physical	• Pyhsical Plant Security, CCTV, Guards

SECURITY - Security Considerations

- CSP harus mengimplementasikan Disaster Recovery Plan yang memungkinkan pengembalian layanan seperti semula jika terjadi disaster
- Monitoring yang kontinyu untuk QoS diperlukan untuk menjaga SLA antara konsumen dan service provider
- Data yang disimpan pada layanan cloud harus dibarengi dengan keamanan yang memadai untk menjaga integritas data
- Cloud Computing harus fast, reliable, dan mampu menyediakan fast response untuk permintaan layanan baru
- Algoritma kriptografi baik simetrik maupun asimetrik perlu diterapkan untuk menjaga keamanan data secara optimal
- Proses Operasi Cloud ini haruslah dijalankan dengan aman secara keseluruhan berdasarkan manajemen keamanan organisasi
- Load balancing perlu diimplementasikan untuk mengantisipasi okupansi layanan yang tinggi dan meningkatkan respon time sehingga tercapai throughput ang maksimal

TOOLS

Qualys Cloud Platform

CloudPassage Halo

Core CloudInspect

Nessus Enterprise for AWA

Symantec Cloud Workload Protection

Alert Logic

Deep Security

SecludIT