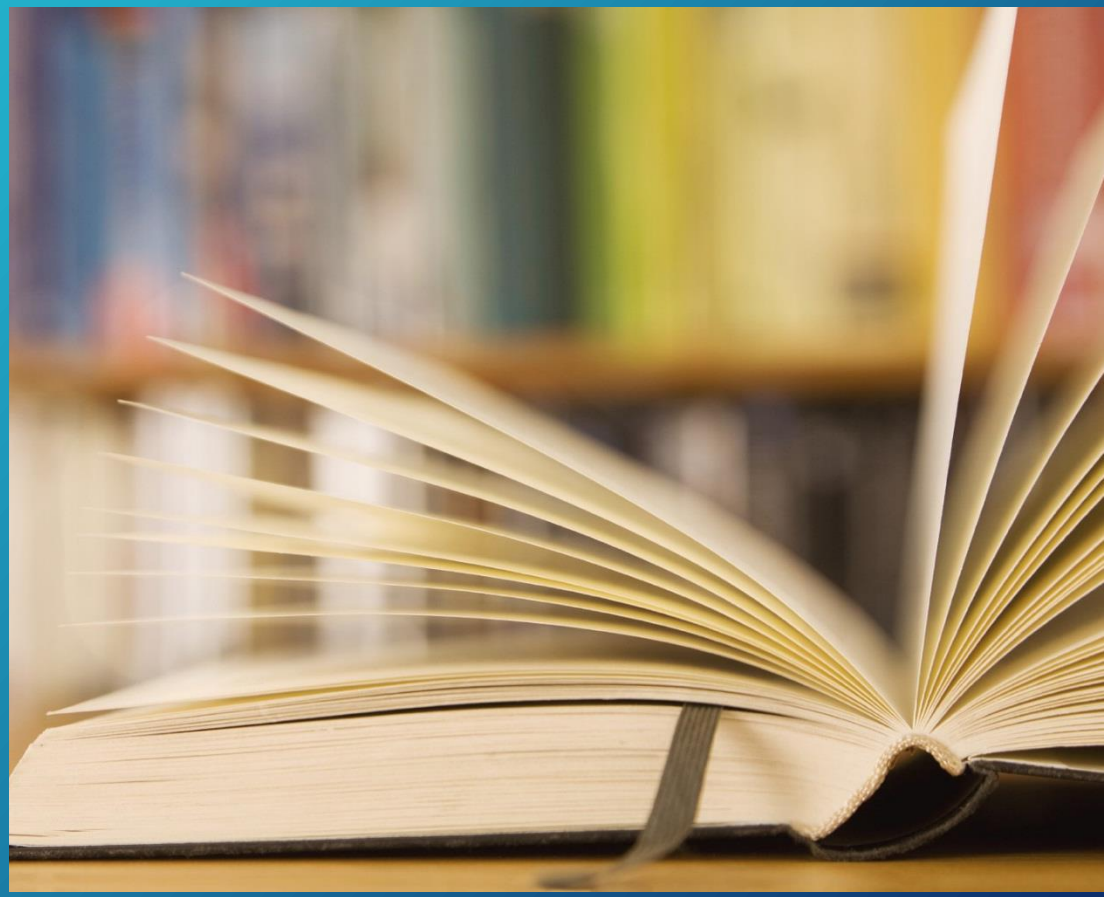
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

SERANGAN DAN KERENTANAN



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

Agenda

- Hacker vs Cracker
- Beberapa Hacker Dunia
- PC vs Workstation vs Server
- Penggunaan Nilai dan Data pada PC
  - Ancaman Keamanan PC
- Penggunaan Nilai dan Data pada Workstation
  - Ancaman terhadap Workstation
- Penggunaan Nilai dan Data pada Server
  - Ancaman terhadap Server
- Serangan
- Kerentanan

Hacker vs Cracker

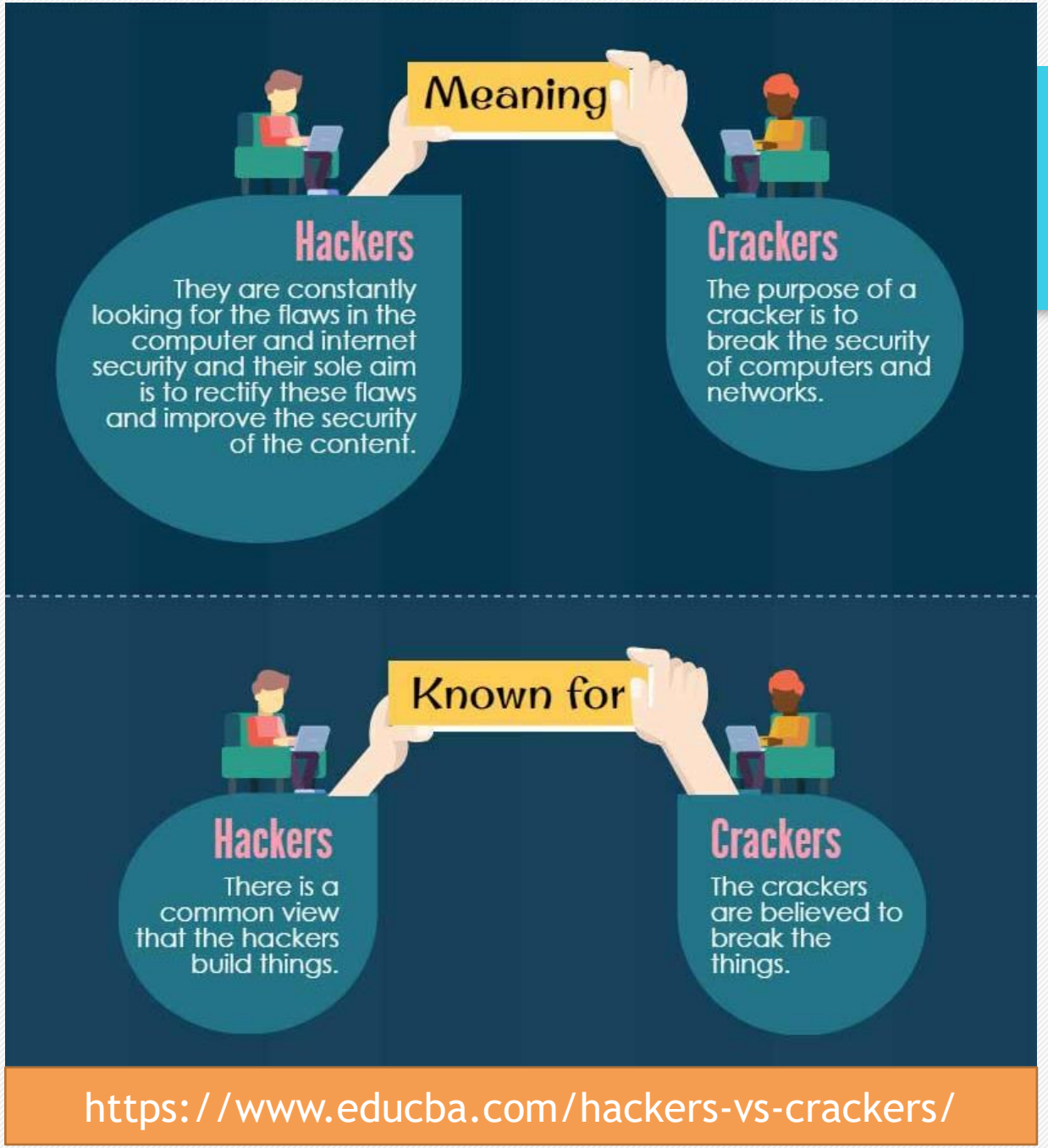
Hacker vs Cracker

Makna

- Hacker pada awalnya adalah istilah untuk para programmer yang ingin melakukan serangkaian uji keamanan terhadap computer dan interner dengan tujuan memperbaiki kekurangan keamanan yang ada
- Sedangkan Cracker adalah orang yang sedari awal bertujuan untuk melewati bahkan merusak keamanan computer dan jaringan

Dikenal juga

- Hacker melakukan development suatu aplikasi/sistem
- Sedangkan Cracker adalah yang melakukan sebaliknya



https://www.educba.com/hackers-vs-crackers/

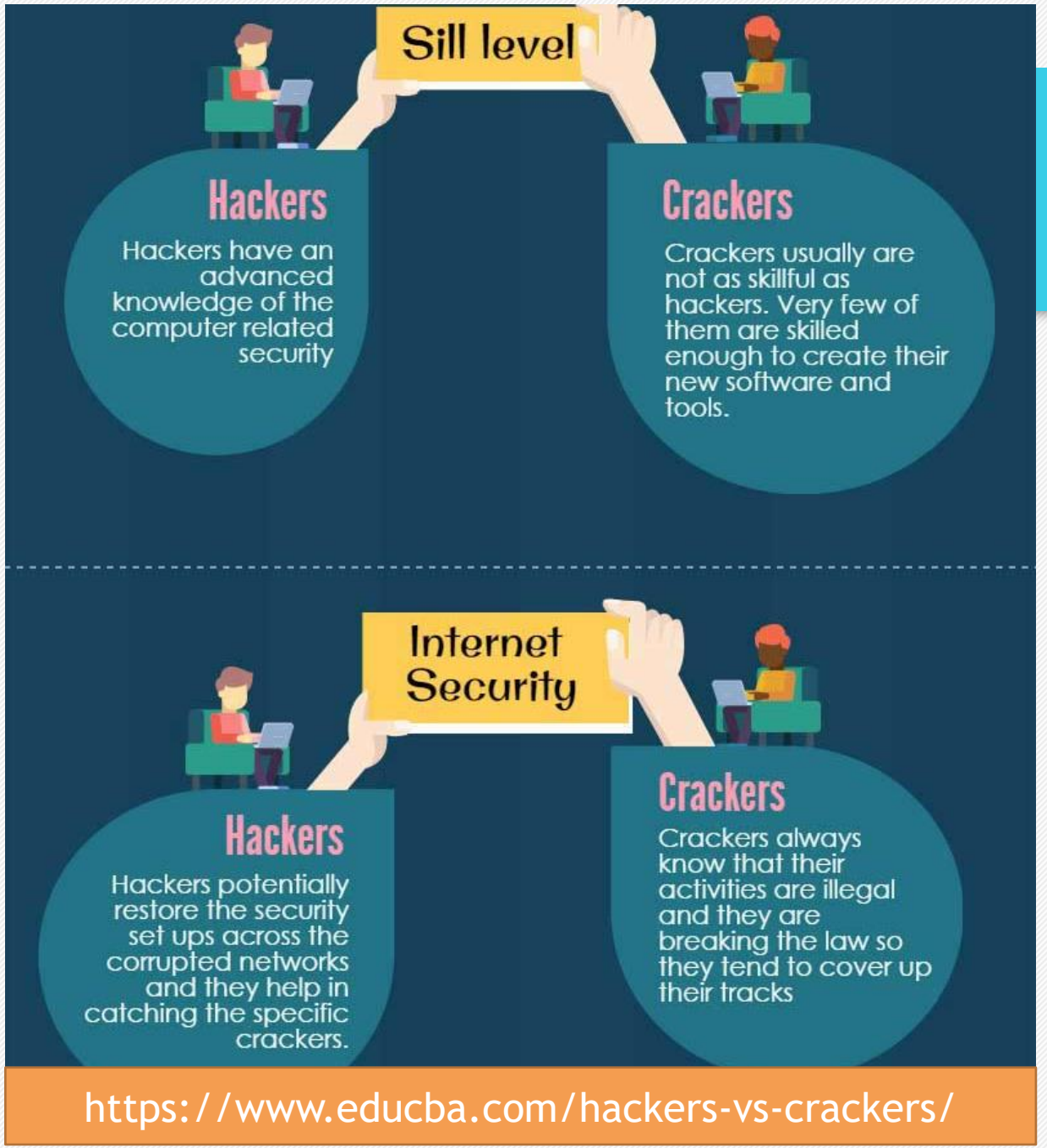
Hacker vs Cracker

Skill Level

- Hacker memiliki pengetahuan yang mumpuni dibidang keamanan komputer
- Cracker bukanlah orang yang memiliki skill seperti hacker. Namun, hal ini tidak boleh membuat cracker dipandang sebelah mata

Internet Security

- Hacker melakukan serangkaian perbaikan keamanan dan ada juga yang membantu menangkap cracker yang berkeliaran
- Cracker tahu bahwa aktivitasnya illegal namun tetap melakukan Tindakan yang menimbulkan kerugian/kerusakan sistem



https://www.educba.com/hackers-vs-crackers/

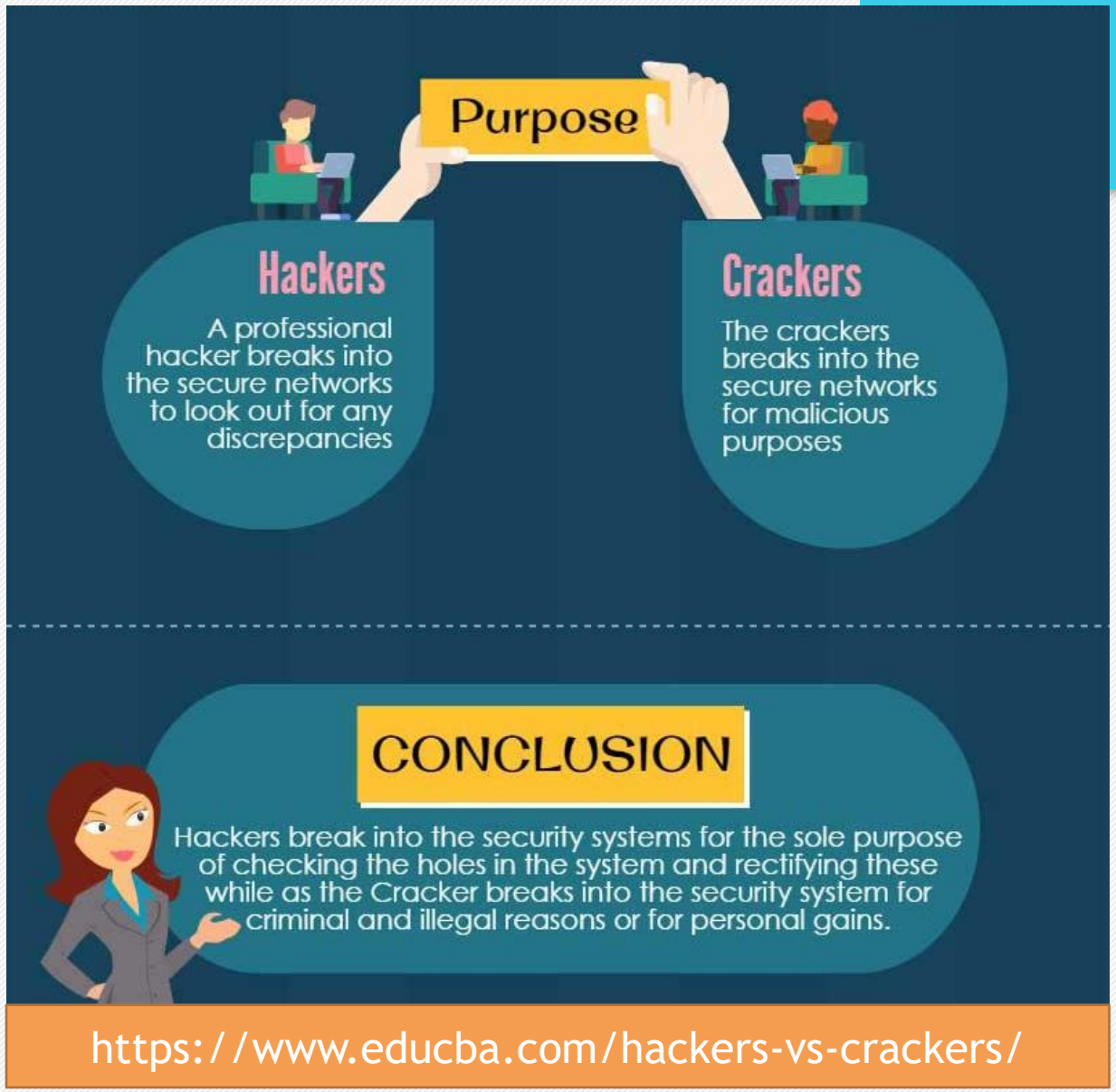
Hacker vs Cracker

Tujuan

- Hacker adalah professional yang mencari ketidakwajaran dalam sistem/jaringan untuk memperbaikinya
- Cracker memiliki tujuan masuk ke dalam sistem untuk melakukan Tindakan ilegal

Kesimpulan

- Perbedaan paling kentara dan mudah dikenali antara kedua istilah ini adalah dari sisi **TUJUAN** dan **ETIKA**
- Dalam istilah lain
  - Hacker = White Hat
  - Cracker = Black Hat
- Namun, saat ini istilah perusakan sistem sudah terlanjur dikonotasikan kepada Hacker



https://www.educba.com/hackers-vs-crackers/

Beberapa Hacker Dunia

Kevin Mitnick

- Kevin pertama kali melakukan hacking menggunakan teknik *Social Engineering* dan *Dumpster Diving* pada saat umur 12 tahun untuk mendapatkan semua akses tiket bis LA. Menggunakan Teknik yang sama, ia membobol banyak computer milik perusahaan terkemuka. Kini ia menjadi Security Consultant setelah masuk penjara selama 5-8 tahun

Julian Assagne

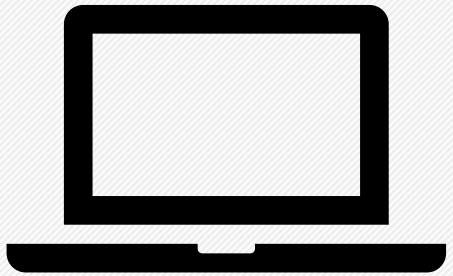
- Founder Wikileaks, situs yang banyak membuka dokumen rahasia negara. Pada usia 16, Assange melakukan hacking kepada NASA. 4 tahun kemudian, dia ditangkap oleh Polisi Federal Australia dan dituntut atas 31 kasus Hacking.

Edward Snowden

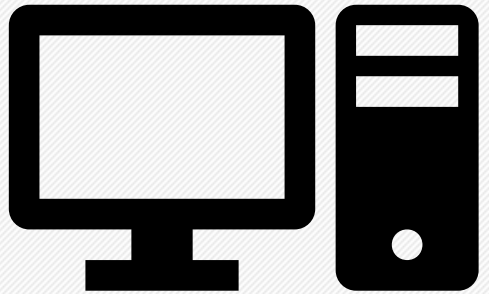
- Whistleblower yang membocorkan dokumen NSA sewaktu masih menjadi pegawai kontrak CIA tahun 2013. Dokumen tersebut berisi tentang Global Surveillance Program yang dijalankan oleh NSA dan Beberapa Agensi Intelligence.

PC vs Workstation vs Server

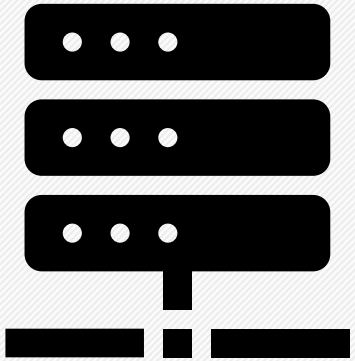
- **Personal Computer** (PC) dapat berupa PC Desktop maupun Laptop yang digunakan untuk keperluan pribadi



- Workstation adalah perangkat **komputer khusus** yang digunakan secara **spesifik** untuk melakukan kerja tertentu.



- Sedangkan Server adalah jenis komputer yang **terhubung ke internet** untuk menjalankan **beragam layanan** dalam **jumlah besar**



Penggunaan dan Nilai Data pada PC

KARAKTERISTIK PC:

- Keperluan pribadi
- Memiliki GUI
- Spesifikasi bervariasi sesuai penggunaan
- Bisa digunakan dengan atau tanpa internet

DATA & NILAI YANG TERSIMPAN:

- Data Pribadi: dokumentasi (foto/video/dokumen) pribadi
- Akun aplikasi/game online: Game, Email, Rekening, E-wallet
- Reputasi dan Hubungan dengan Relasi
- Riwayat pencarian online

Ancaman terhadap PC

IDENTITY THEFT
(Pencurian Identitas)

MALWARE

Information Leakage
(Kebocoran Informasi)

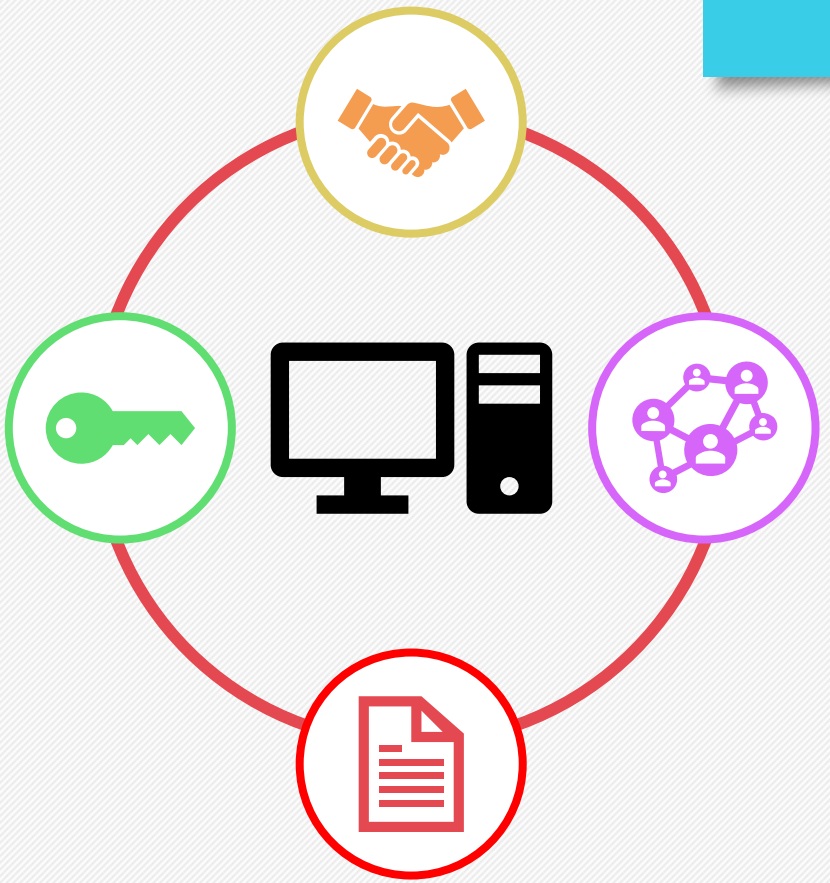
Penggunaan dan Nilai Data pada Workstation

KARAKTERISTIK:

- Keperluan pekerjaan yang spesifik
- Memiliki GUI
- Spesifikasi yang tinggi
- Umumnya digunakan dengan internet

DATA & NILAI YANG TERSIMPAN:

- Data internal perusahaan
- Akun aplikasi perusahaan
- Credential/akses ke jaringan perusahaan
- Nilai bisnis



Ancaman terhadap Workstation

IDENTITY THEFT
(Pencurian Identitas)

MALWARE

Information Leakage
(Kebocoran Informasi)

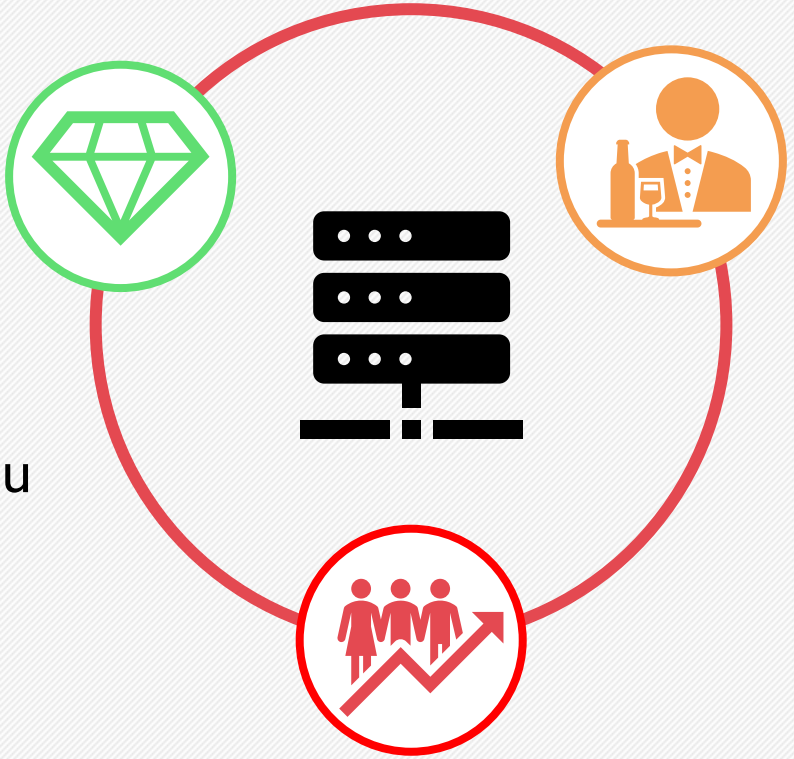
Ancaman terhadap Server

KARAKTERISTIK:

- Keperluan orang banyak secara online/cloud
- Sebagian berbasis GUI dan banyak pula yang tidak
- Spesifikasi sangat tinggi
- Digunakan harus dengan internet

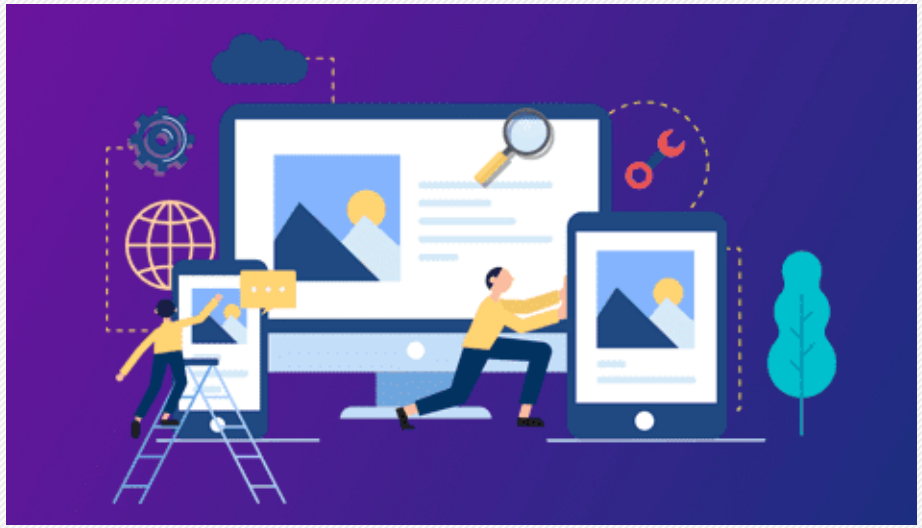
DATA & NILAI YANG TERSIMPAN:

- Data orang banyak yang dipercayakan kepada pemilik atau data internal perusahaan
- Layanan yang harus terus berjalan
- Reputasi dan valuasi perusahaan



Ancaman terhadap Server

MALWARE



Serangan ke
Web Aplikasi

DDoS
(Serangan Terdistribusi)

Information Leakage
(Kebocoran Informasi)

Attack (Serangan)

"An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information"

- NIST -

- Cyber Attack (Serangan Siber) secara sederhana adalah upaya destruktif yang dilakukan pada cyberspace (internet)
- Cyber Attack yang bertemu dengan Vulnerability yang tepat akan menghasilkan dampak destruktif yang besar
- Diperlukan beragam multi layer defence mechanism untuk mengurangi peluang berhasilnya serangan
- Serangan adalah Resiko Eksternal sistem

Vulnerability (Kerentanan)

"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)"

- CVE -

- Vulnerability atau Kerentanan pada dasarnya adalah kelemahan yang tercipta pada sebuah sistem
- Vulnerability yang tidak diperbaiki (patch) akan dapat dieksploitasi oleh hacker untuk masuk ke dalam sebuah sistem
- Untuk melihat apakah suatu sistem memiliki Vulnerability, perlu dilakukan Vulnerability Assessment (VA) secara berkala setiap pengembangan/update/patch dilakukan
- VA Tools yang populer adalah Acunetix, NESSUS, VEX, BurpSuite, OpenVAS, Nikto, dll
- Vulnerability adalah Resiko internal suatu sistem

Vulnerability (Kerentanan)

Beberapa referensi yang dapat digunakan untuk melihat penemuan Vulnerability terbaru:

- OWASP
  - https://owasp.org/
- CVE - MITRE
  - https://cve.mitre.org/
- Exploit DB
  - https://www.exploit-db.com/
- NIST
  - https://nvd.nist.gov/vuln/search