

MATA KULIAH CYBER SECURITY

Program Studi Magister Informatika

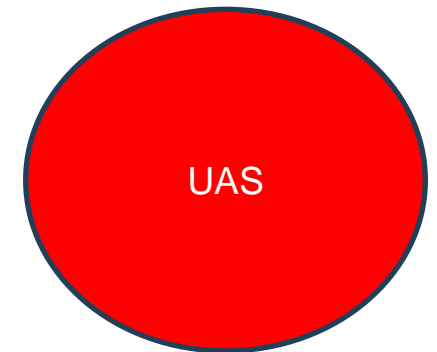
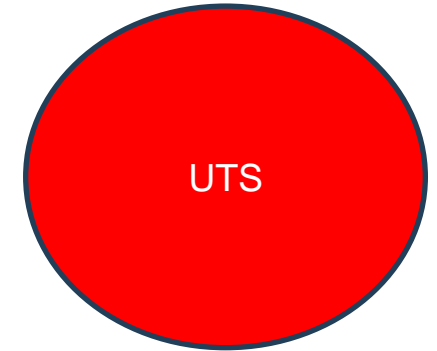
Universitas AMIKOM Yogyakarta
Tahun 2025

Creative Economy Park"



Outline Mata Kuliah Selama 1 Semester

1. Ruang lingkup keamanan cyber menurut framework Cyber Security Body of Knowledge (CyBoK)
2. Serangan infrastruktur jaringan
3. Serangan aplikasi desktop dan web
4. Social engineering
5. Solusi pengamanan data dan sistem modern
6. Regulasi dan kebijakan cyber law di Indonesia
7. Implementasi kebijakan keamanan TI
8. Penetration testing
9. Digital Forensic



Ancaman Infrastruktur

PERTEMUAN 2

Universitas AMIKOM Yogyakarta
Tahun 2025

Creative Economy Park"



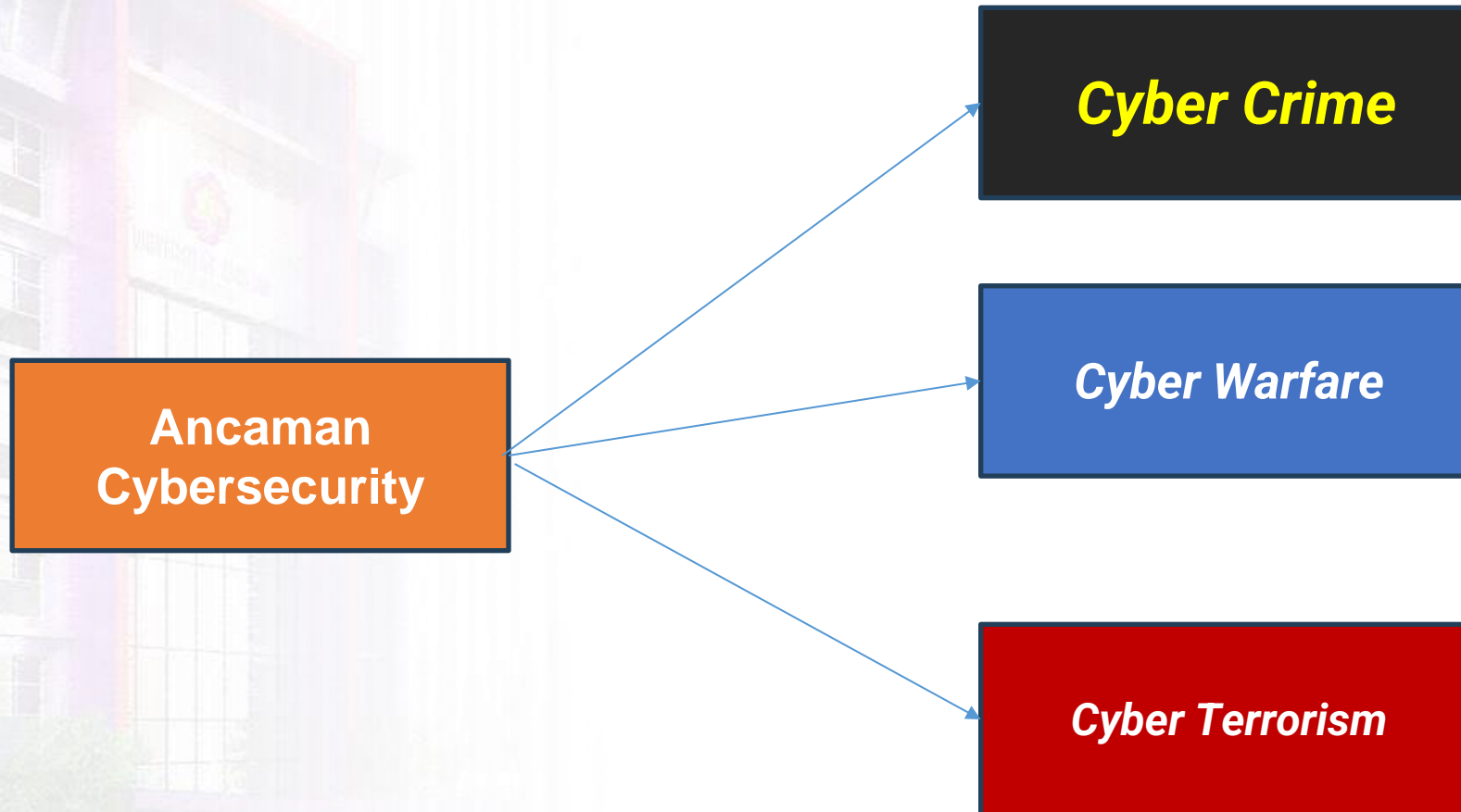
Tujuan Pembelajaran

- Mahasiswa memahami penyebab dan jenis ancaman keamanan pada jaringan
- Mahasiswa dapat mendemonstrasikan salah satu ancaman nyata di jaringan

What is Cyberscurity ?

- **Menurut ISO** (International Organization for Standardization), tepatnya ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. Cybersecurity atau cyberspace security adalah upaya yang dilakukan dalam menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) dari informasi di cyberspace. Adapun cyberspace merujuk pada lingkungan yang kompleks yang merupakan hasil dari interaksi antara orang, perangkat lunak, dan layanan di internet, yang didukung oleh perangkat teknologi informasi dan komunikasi (TIK) dan koneksi jaringan yang tersebar di seluruh dunia.
- **Sedangkan menurut CISCO, cybersecurity** adalah praktik melindungi sistem, jaringan, dan program dari serangan digital. Cybersecurity biasanya ditujukan untuk mengakses, mengubah, atau menghancurkan informasi sensitif, memeras uang dari pengguna, atau mengganggu operasional proses bisnis.
- Jadi, dapat disimpulkan **bahwa cybersecurity atau keamanan siber** sebagai tindakan untuk melindungi sistem komputer dari serangan digital atau akses ilegal. Terdapat beberapa elemen dari cybersecurity antara lain, application security, information security, cloud security, network security, disaster recovery/business continuity planning, operational security, dan end-user education. Elemen-elemen ini sangat penting guna memastikan keamanan cybersecurity secara keseluruhan, karena risiko terkena ancaman digital terus meningkat dan ancamannya pun semakin beragam. Maka dari itu, penting untuk melindungi sistem bahkan dari risiko terkecil sekalipun.

Ancaman Cybersecurity



Cyber Crime

- Berawal di periode 1960-an dan terus berkembang hingga saat ini. Terjadi pertama kali di Amerika Serikat pada tahun 1960-an. Berbagai kasus cyber crime terjadi saat itu, mulai dari **manipulasi transkrip akademik mahasiswa** di Brooklyn College New York, penggunaan komputer dalam penyelundupan narkoba, penyalahgunaan komputer oleh karyawan hingga akses tidak sah terhadap Database Security Pacific National Bank yang mengakibatkan kerugian sebesar **10.2 juta dolar AS pada tahun 1978**.
- Dalam praktik cyber crime, **pelaku melakukan akses ilegal seperti transmisi ilegal atau manipulasi data untuk tujuan tertentu, di antaranya menciptakan gangguan dan mencari keuntungan finansial**, bisa dilakukan seorang diri atau melibatkan sekelompok orang. Para pelaku cyber crime tentu adalah orang yang sudah ahli dalam berbagai teknik **hacking**, bahkan tak jarang sebuah aksi cyber crime dilakukan dari berbagai tempat berbeda di waktu bersamaan.
- Banyak contoh aksi cyber crime yang masih terjadi, **seperti pencurian identitas (identity theft), penipuan/pembobolan kartu kredit (carding), memata-matai target tertentu (cyber espionage), dan lain-lain**.

KENALI BENTUK PENIPUAN KARTU KREDIT

Semakin mudahnya transaksi online maka semakin berkembang pula metode pencurian atau penipuan. Salah satu metode penipuan yang marak adalah penipuan kartu kredit.

• Skimming

Bentuk penipuan kartu kredit paling berbahaya dengan meletakkan alat elektronik berukuran kecil di bawah mesin EDC. Secara tidak sadar para pengguna menyerahkan segala informasi di dalam kartu kredit.

• Phising

Pesan yang tidak jelas asal usulnya dikirim secara beruntun itu dinamakan. Penipu berupaya mempengaruhi korban untuk mengetahui informasi kartu kreditnya.

• Menawarkan Jasa

Jasa pembuatan kartu kredit marak terjadi. Hati-hati, karena ini bisa jadi salah satu bentuk penipuan kartu kredit.

• Menang Undian

Cara seperti ini sangat jamak dilakukan oleh penipu dengan mengirimkan informasi yaitu korban menang undian dari sebuah market-place.

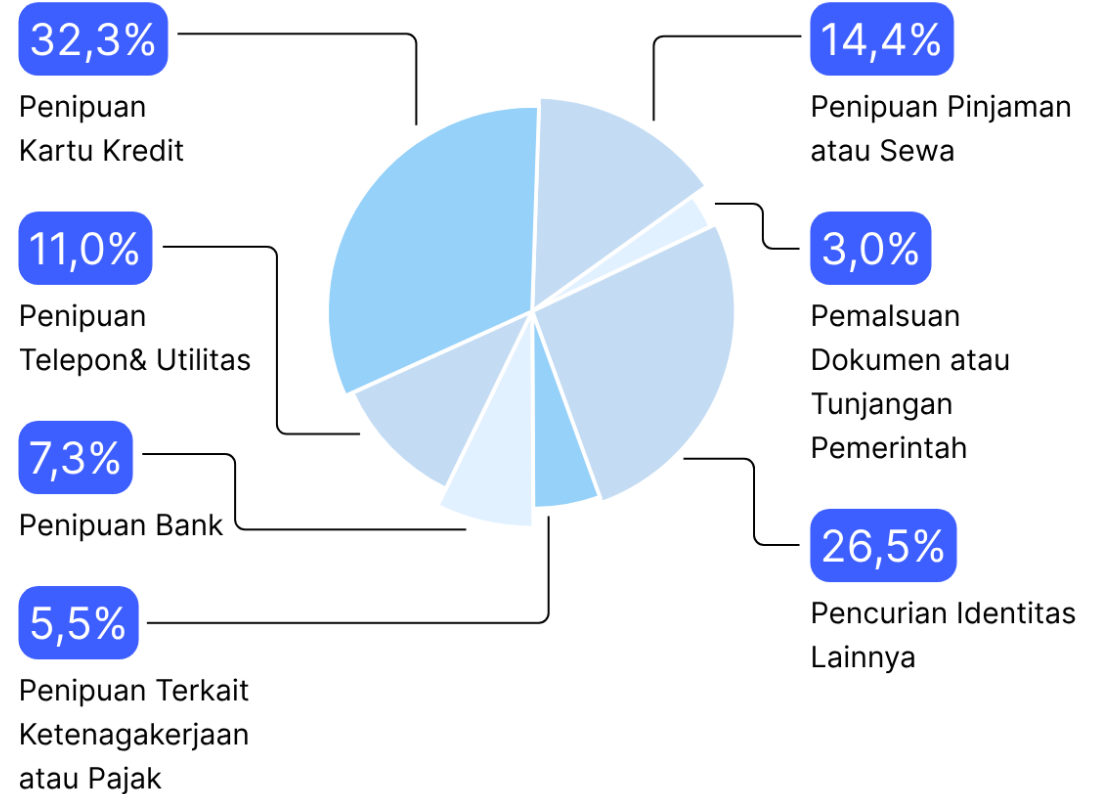
• Kirim Link Palsu

Hati-hati membuka link yang terdapat pada internet, ada kemungkinan link tersebut adalah jebakan.



• SUMBER Sindonews.com • NASKAH Danang Arradian • FOTO Ist • INFOGRAFIS Sonny Unggara

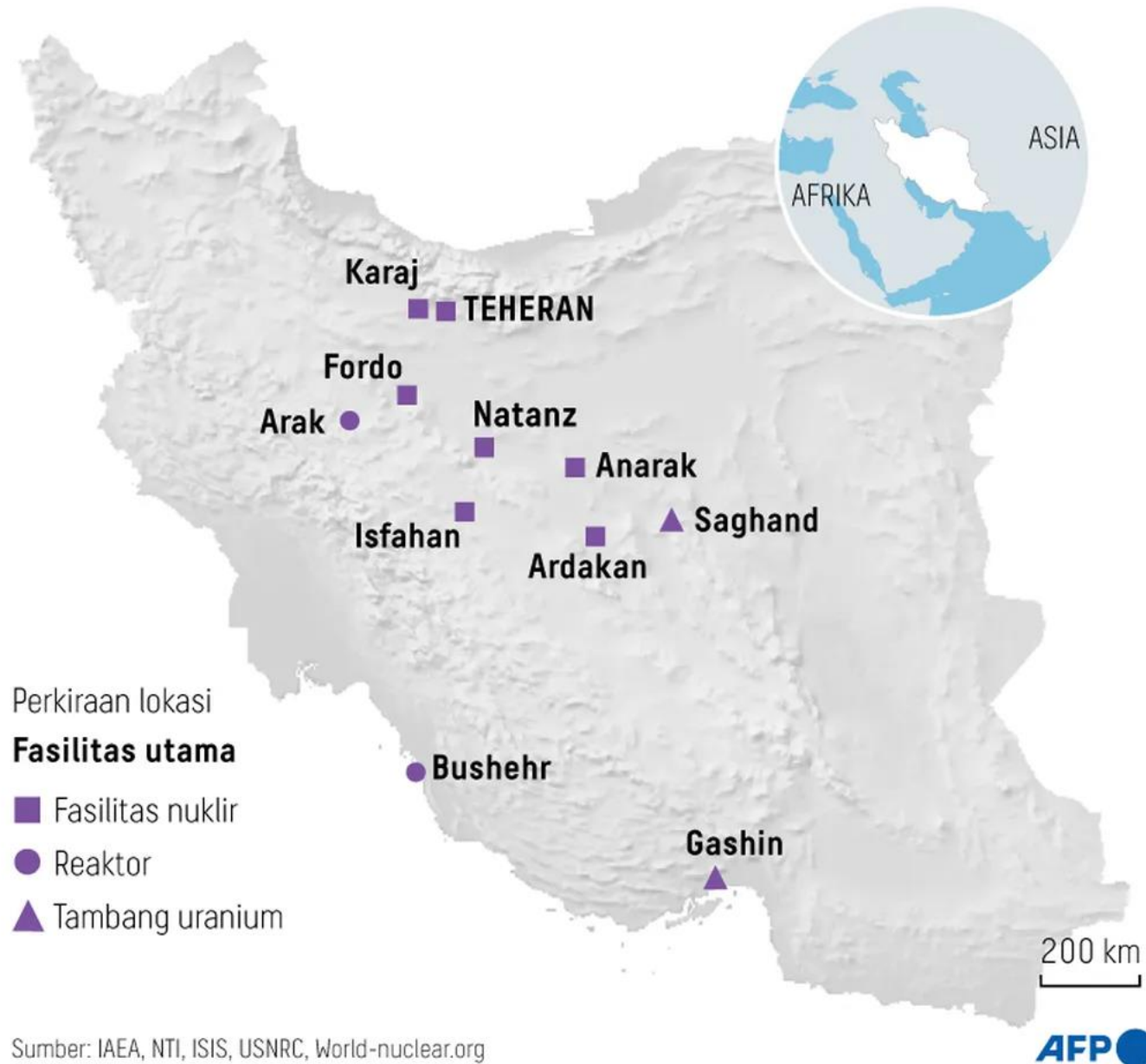
Laporan pencurian identitas berdasarkan jenisnya



Cyber Warfare

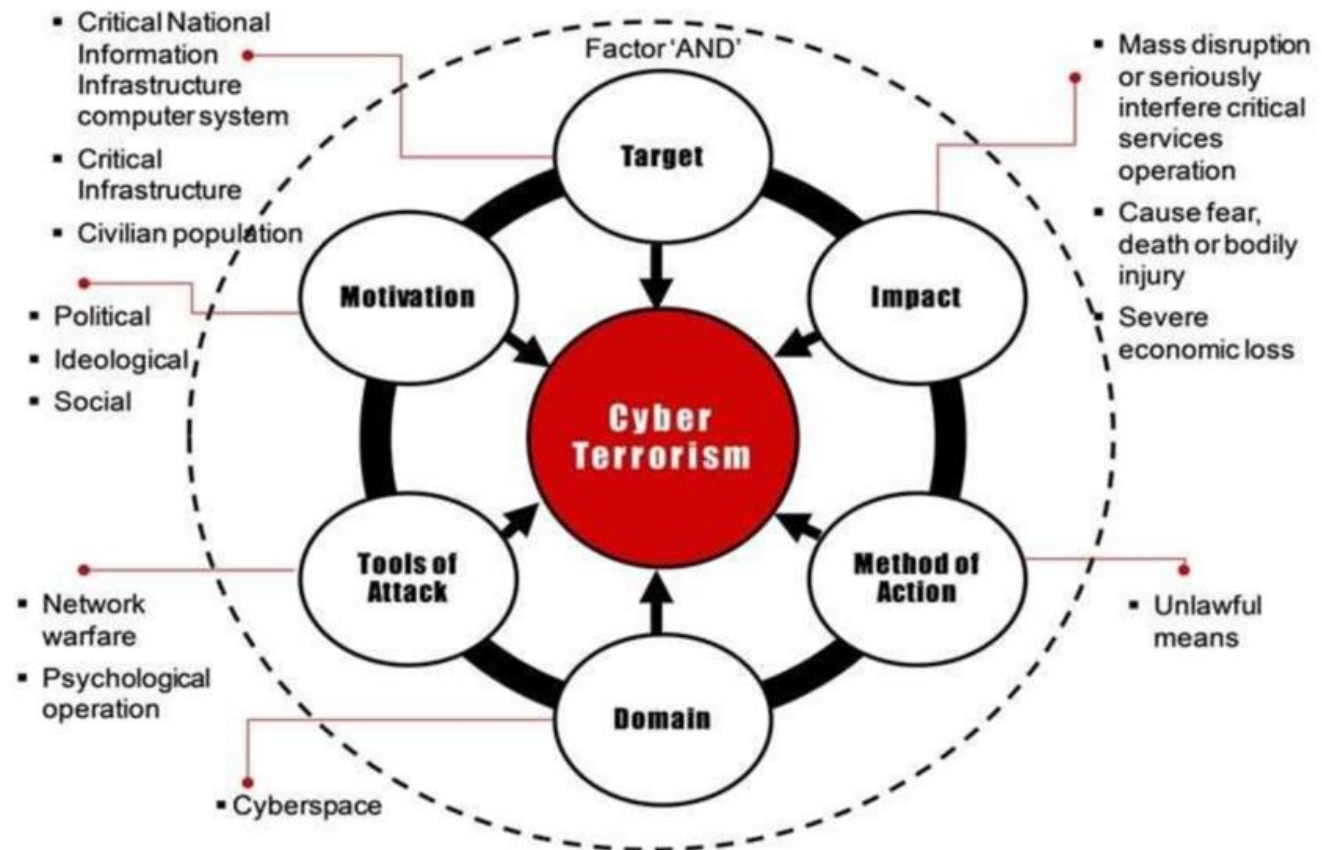
- Perkembangan teknologi informasi dan komunikasi memberi banyak kemudahan dalam menjalankan aktivitas pemerintahan, namun melahirkan ancaman baru yang berdampak bagi kestabilan kedaulatan suatu negara juga, yaitu **cyber warfare**.
- **Cyber warfare** merupakan perkembangan dari cyber attack dan cyber crime. Cyber warfare dapat diartikan **sebagai perang di dalam cyberspace, namun di dalam cyber warfare terdapat penyerangan yang berbeda dengan penyerangan dalam perang konvensional atau perang fisik lainnya**. Media utama yang digunakan di dalam cyber warfare adalah **komputer dan internet**, objek yang diserang dalam cyber warfare **bukan merupakan wilayah fisik**, wilayah teritorial ataupun wilayah geografis, namun objek dalam cyberspace yang dikuasai oleh suatu negara.
- Salah satu contoh kasus cyber warfare yaitu kasus antara Amerika Serikat dengan Iran di tahun 2008 dimana Amerika Serikat merusak sistem **sentrifugal Pembangkit Listrik Tenaga Nuklir milik Iran**.

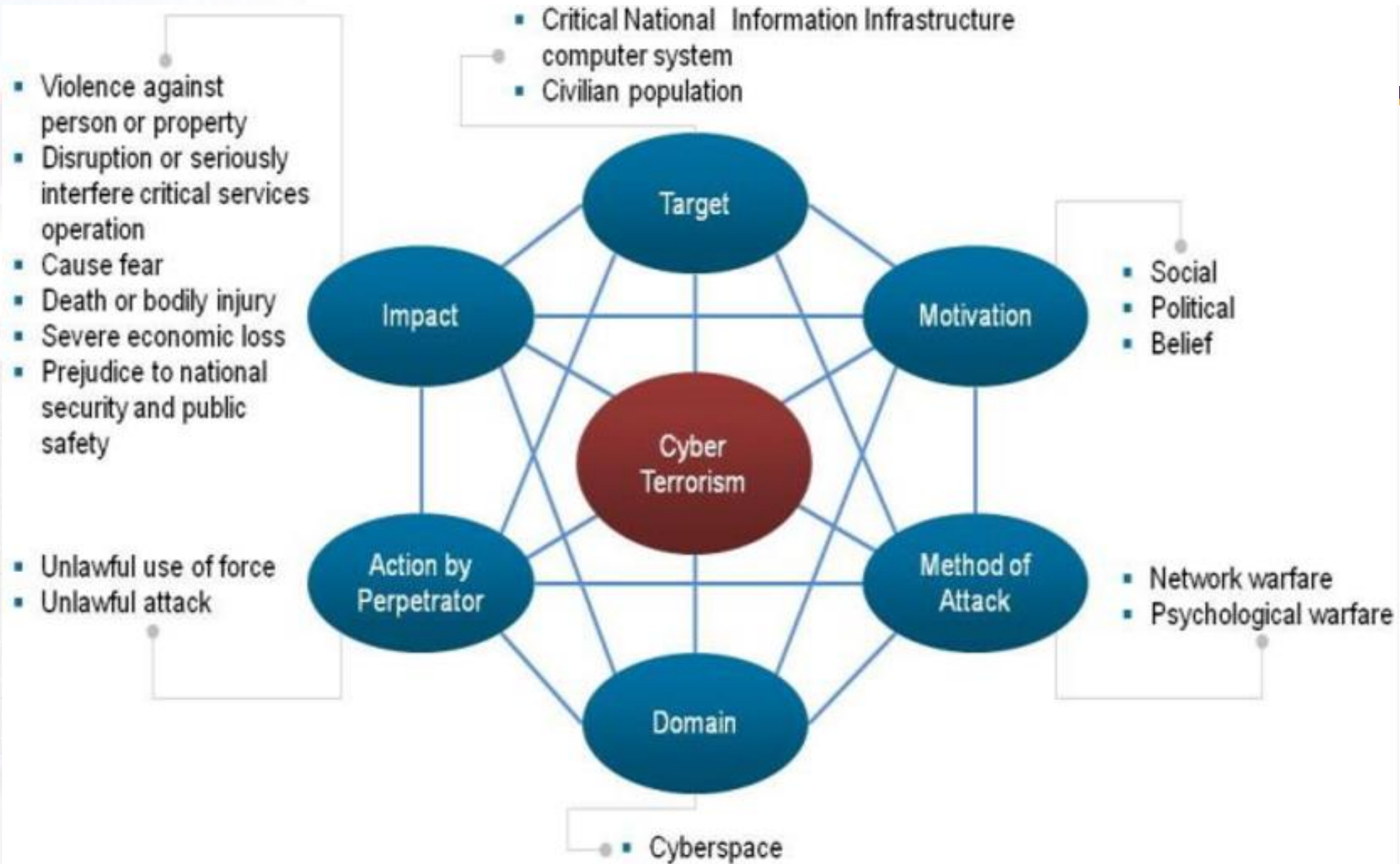
Fasilitas Nuklir Iran

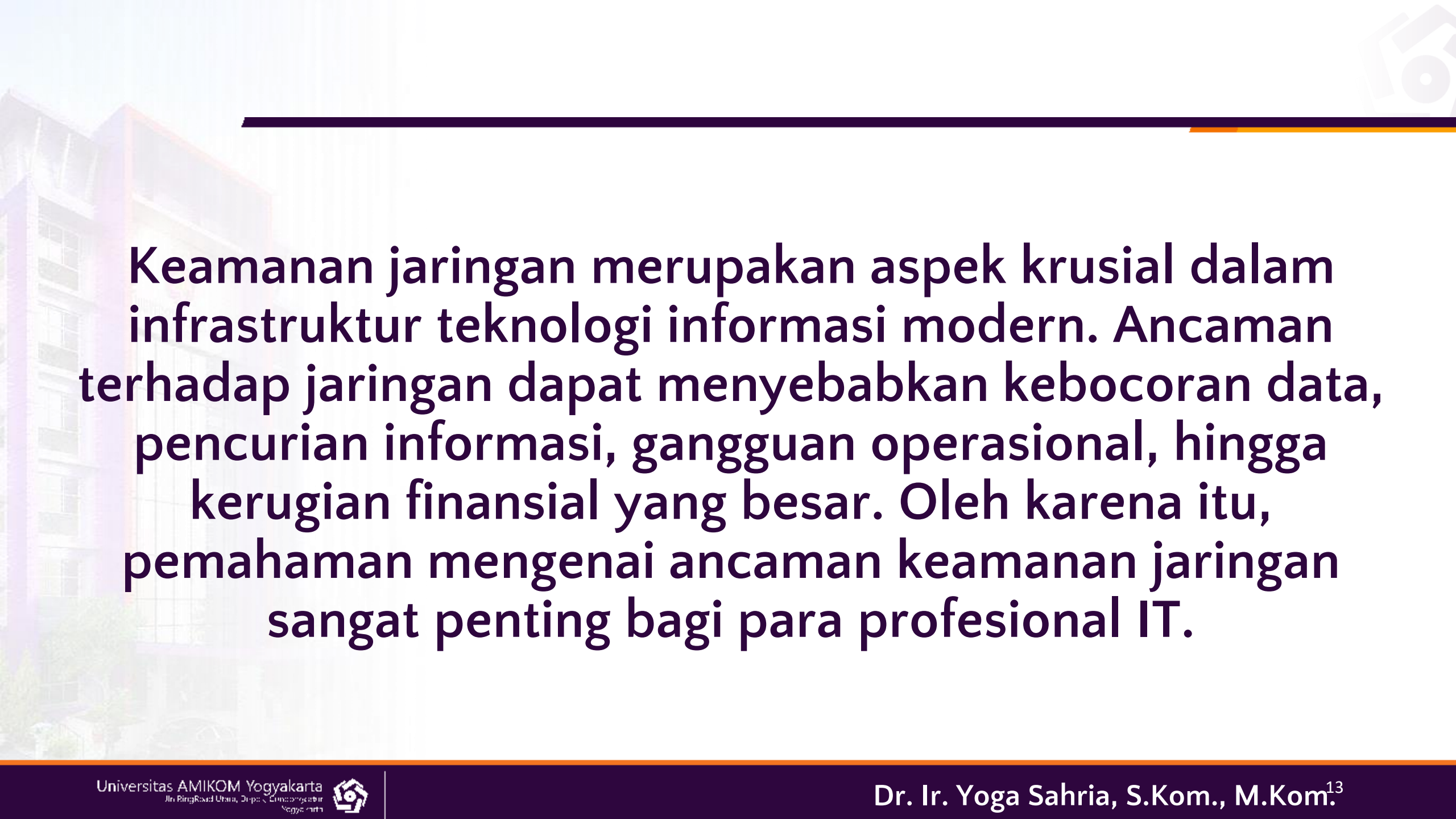


Cyber Terrorism

- Merupakan aktivitas sejumlah jaringan atau kelompok teroris yang bertujuan untuk mengganggu keamanan sosial, politik, dan ekonomi suatu negara dengan memanfaatkan kekuatan teknologi internet.
- Misalnya seperti menyerang website resmi pemerintah, melakukan sadap jaringan komunikasi strategis politik, mencuri sumber data elektronik perbankan, dan sebagainya. Aktivitas siber ini **sangat berbahaya karena dapat menyebabkan kepanikan dan ketakutan skala besar.**



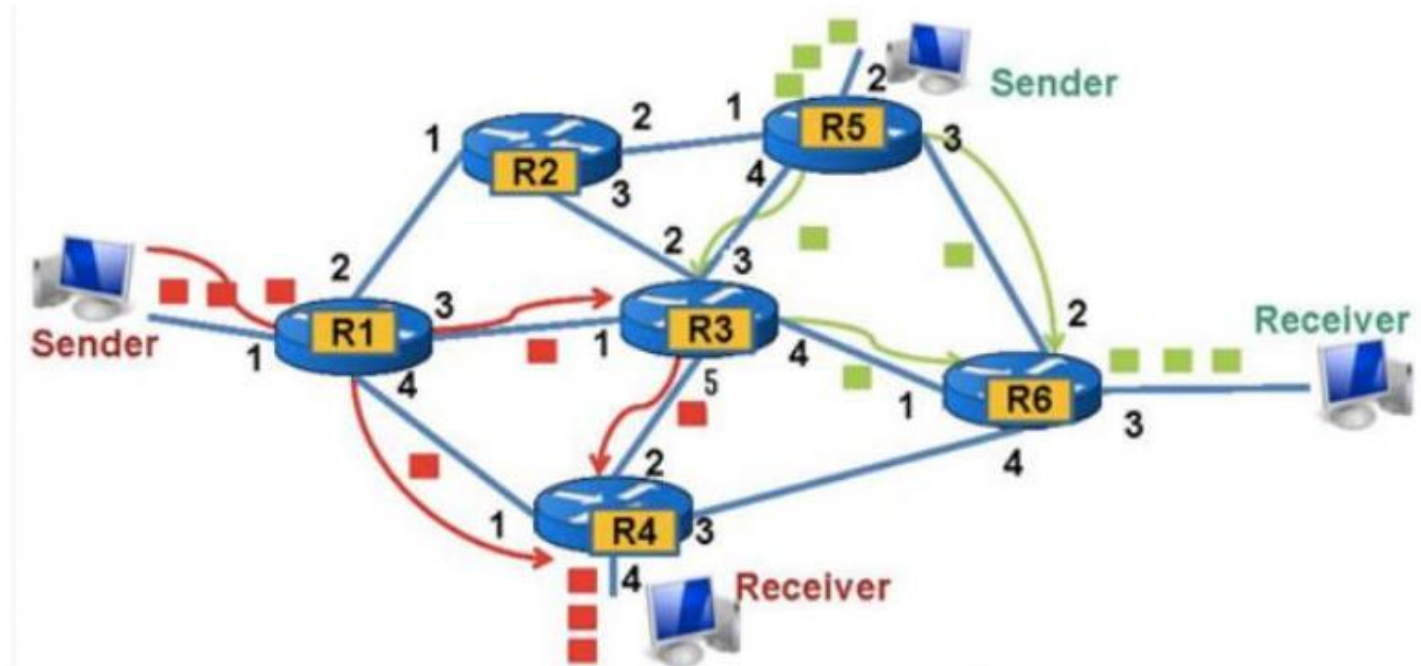




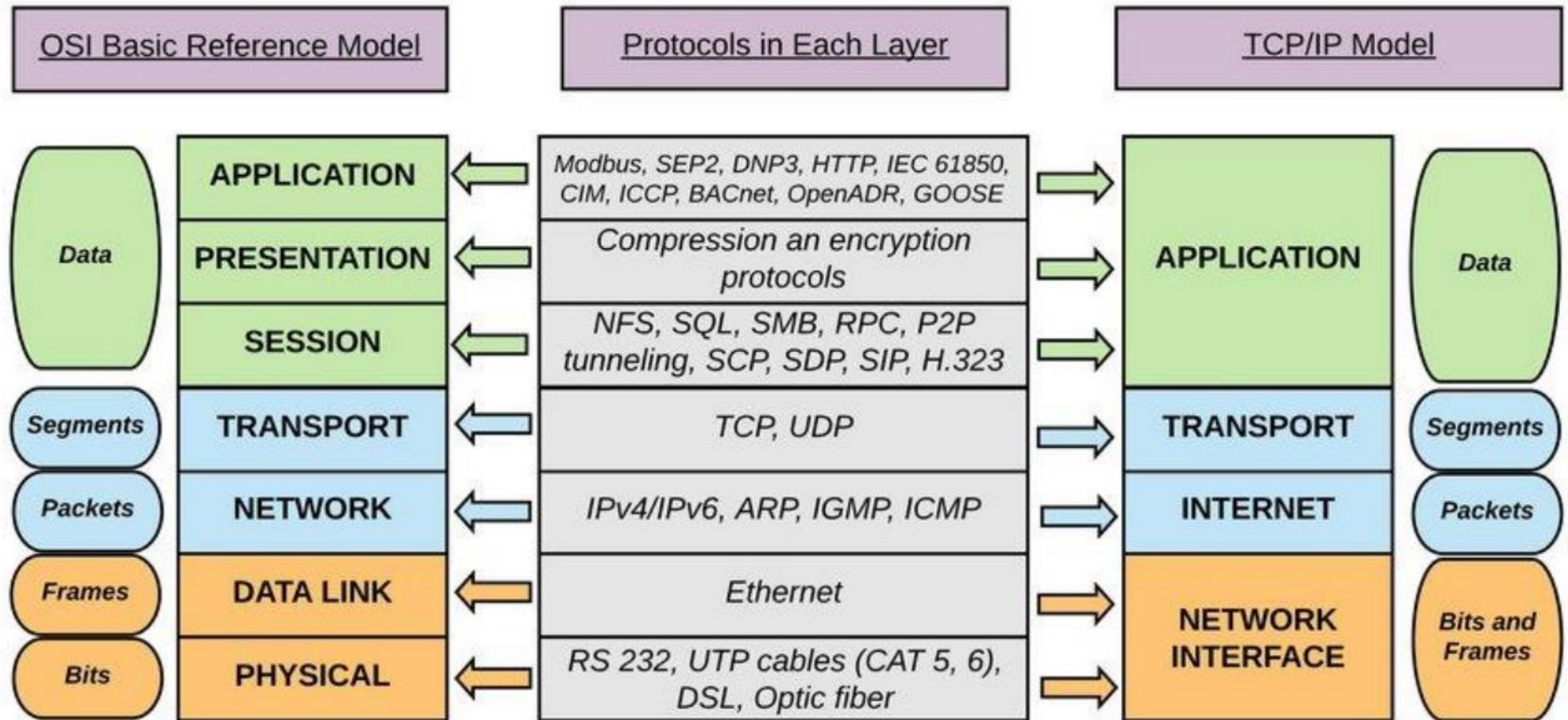
Keamanan jaringan merupakan aspek krusial dalam infrastruktur teknologi informasi modern. Ancaman terhadap jaringan dapat menyebabkan kebocoran data, pencurian informasi, gangguan operasional, hingga kerugian finansial yang besar. Oleh karena itu, pemahaman mengenai ancaman keamanan jaringan sangat penting bagi para profesional IT.

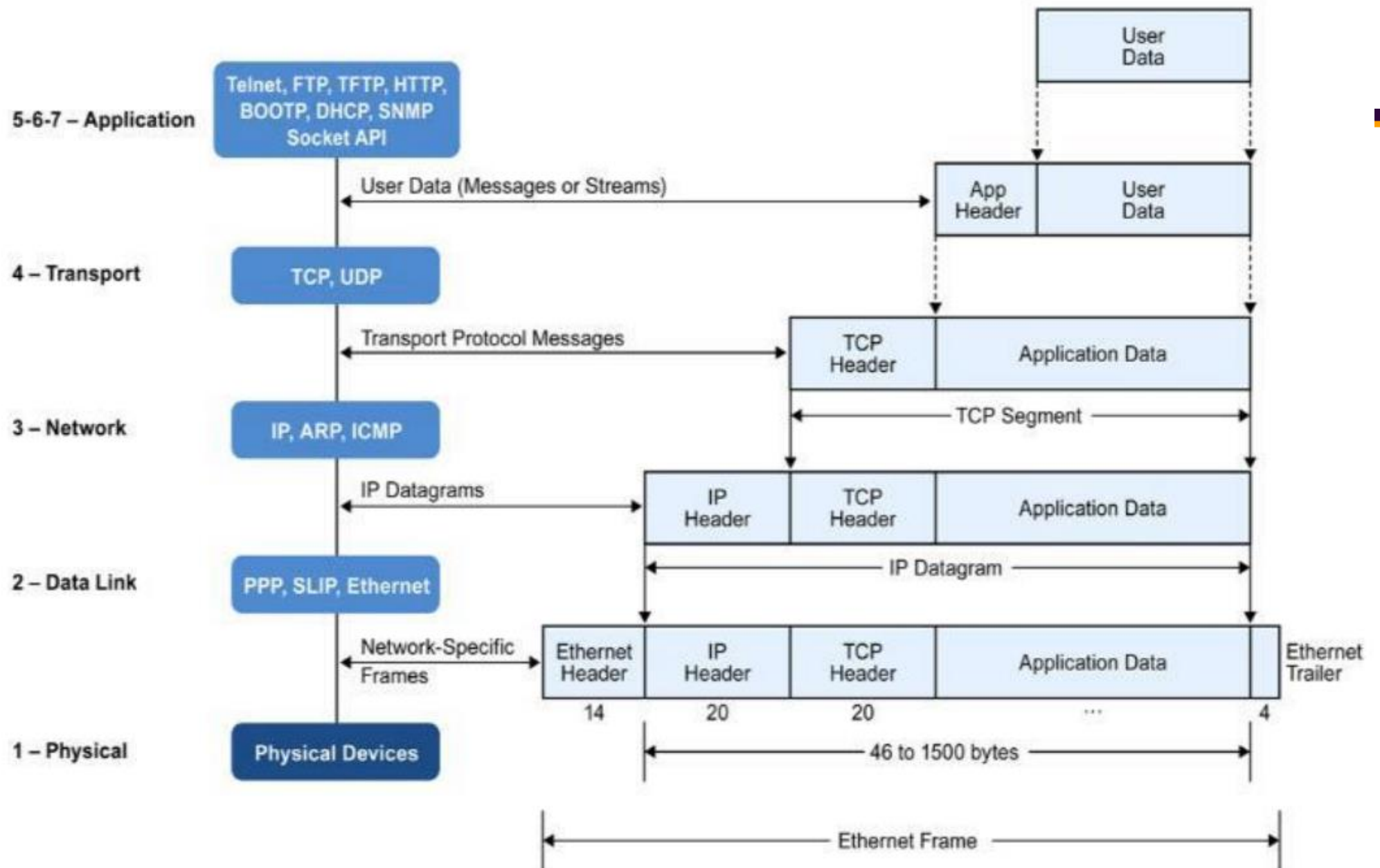
Jaringan

- Old: circuit switching
- Modern: packet-switched network
 - OSI network model
 - TCP/IP



The Language





El mundo es un lugar peligroso

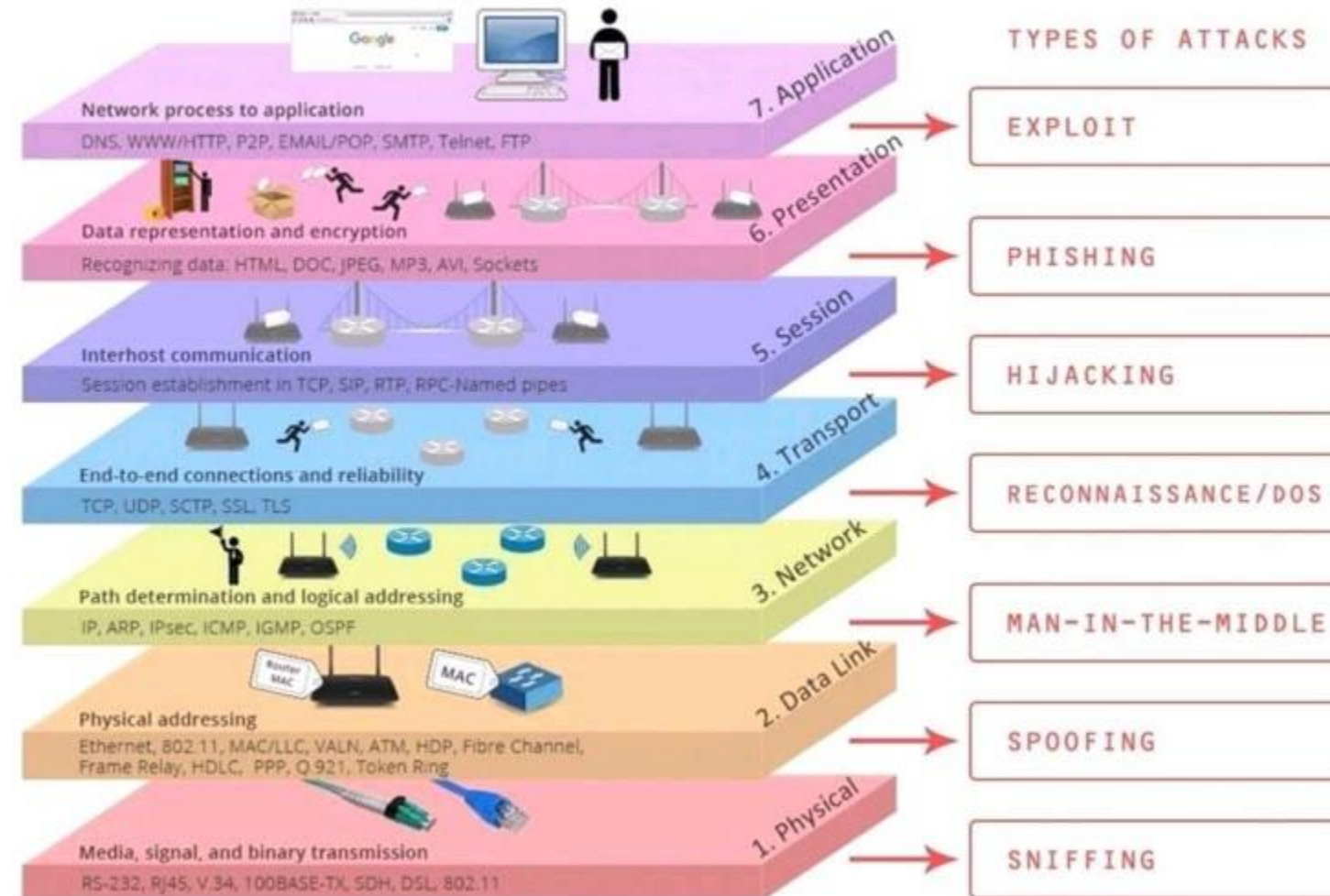


Top Network Security Cheatsheet

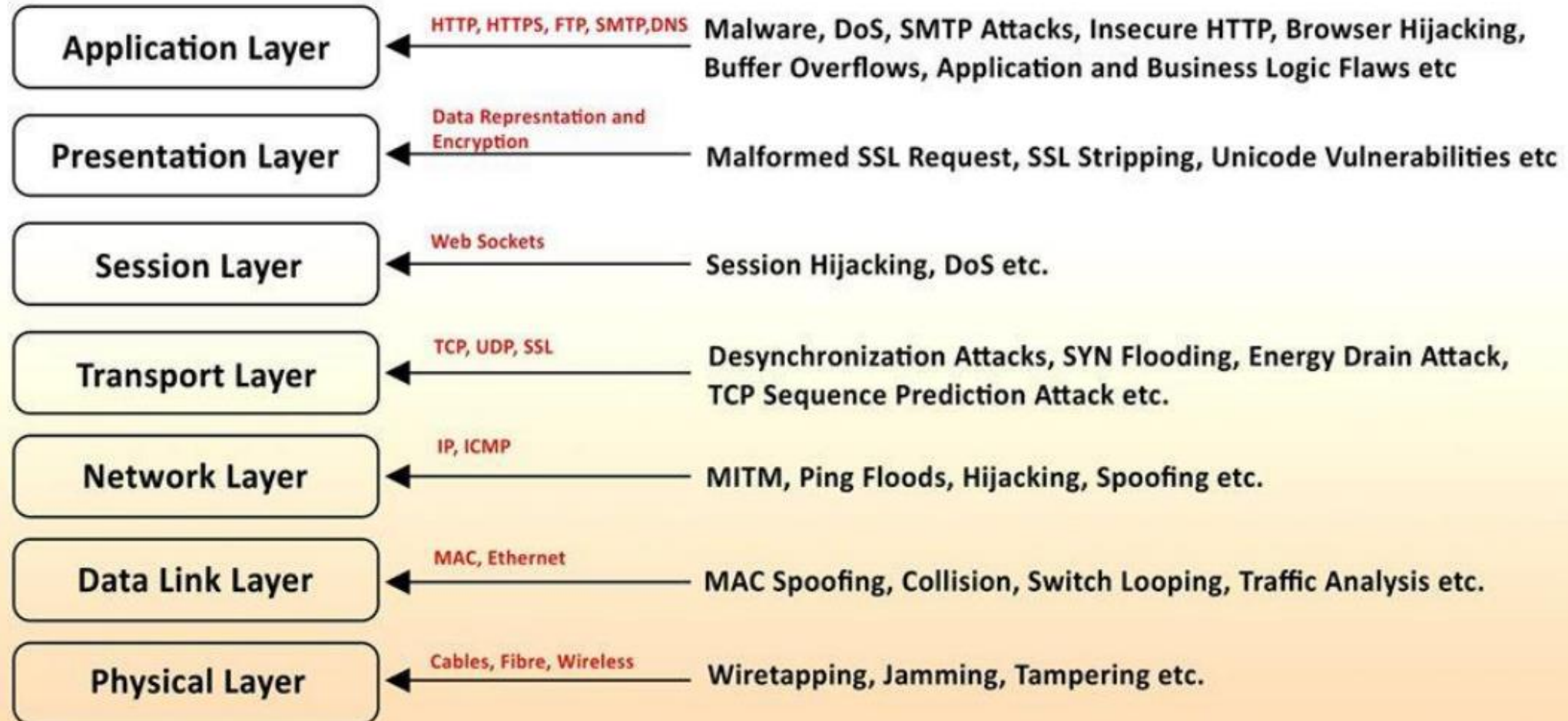
ByteByteGo

7. Application Layer	<p>request response</p> <p>HTTP, FTP, SMTP</p>	<ul style="list-style-type: none"> SQL Injection Cross-Site Scripting (XSS) DDos attacks
6. Presentation Layer	<p>compression encryption encoding</p> <p>TLS, SSL</p>	<ul style="list-style-type: none"> Character Encoding Attacks SSL Stripping Data Compression Manipulation
5. Session Layer	<p>Session</p> <p>Sockets</p>	<ul style="list-style-type: none"> Session replay Session fixation attacks Man-in-the-middle attacks
4. Transport Layer	<p>segmentation reassembly</p> <p>TCP, UDP</p>	<ul style="list-style-type: none"> UDP flood SYN flood
3. Network Layer	<p>packets packets assembly</p> <p>IP, ICMP, IGMP, IPsec</p>	<ul style="list-style-type: none"> IP spoofing Route table manipulation Smurf attack
2. Data Link Layer	<p>frames intra-network communications</p> <p>Ethernet, WiFi</p>	<ul style="list-style-type: none"> MAC address spoofing ARP spoofing Switch flooding
1. Physical Layer	<p>00100111 bitstream</p> <p>Fiber</p>	<ul style="list-style-type: none"> Eavesdropping/Tapping Physical tampering Electromagnetic interference

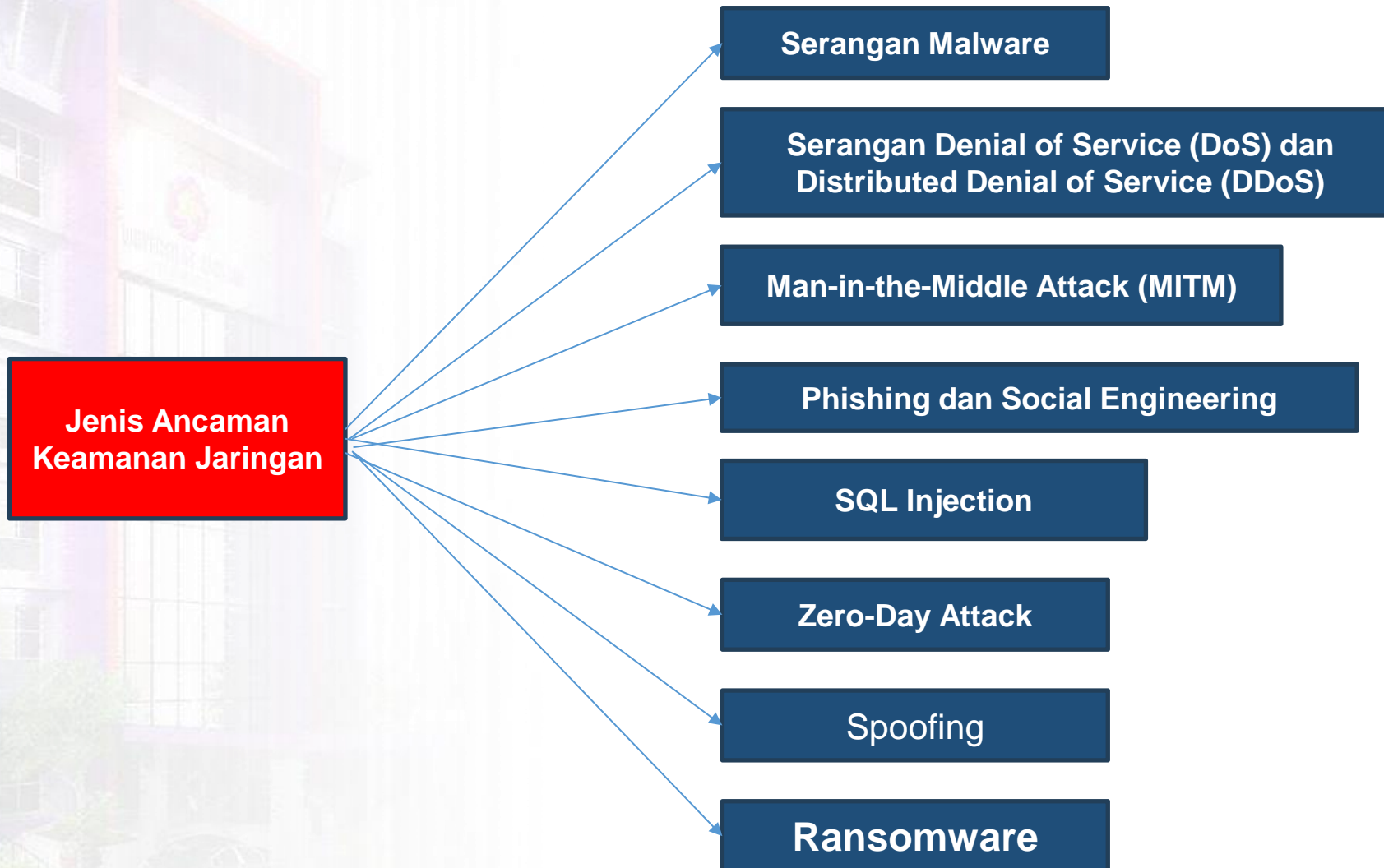
Types of Attacks in OSI Layer



ATTACKS ON OSI LAYERS



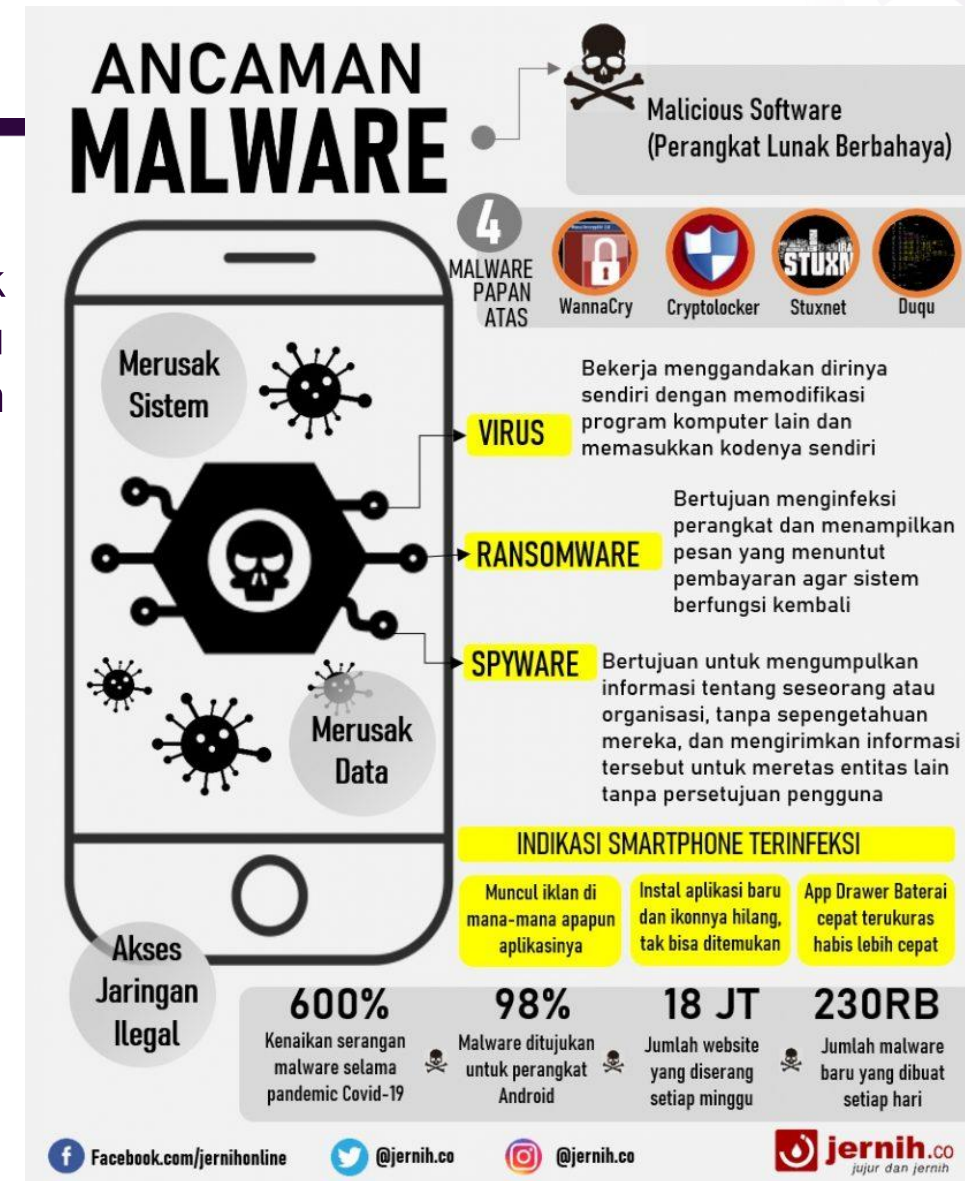
Jenis Ancaman Keamanan Jaringan



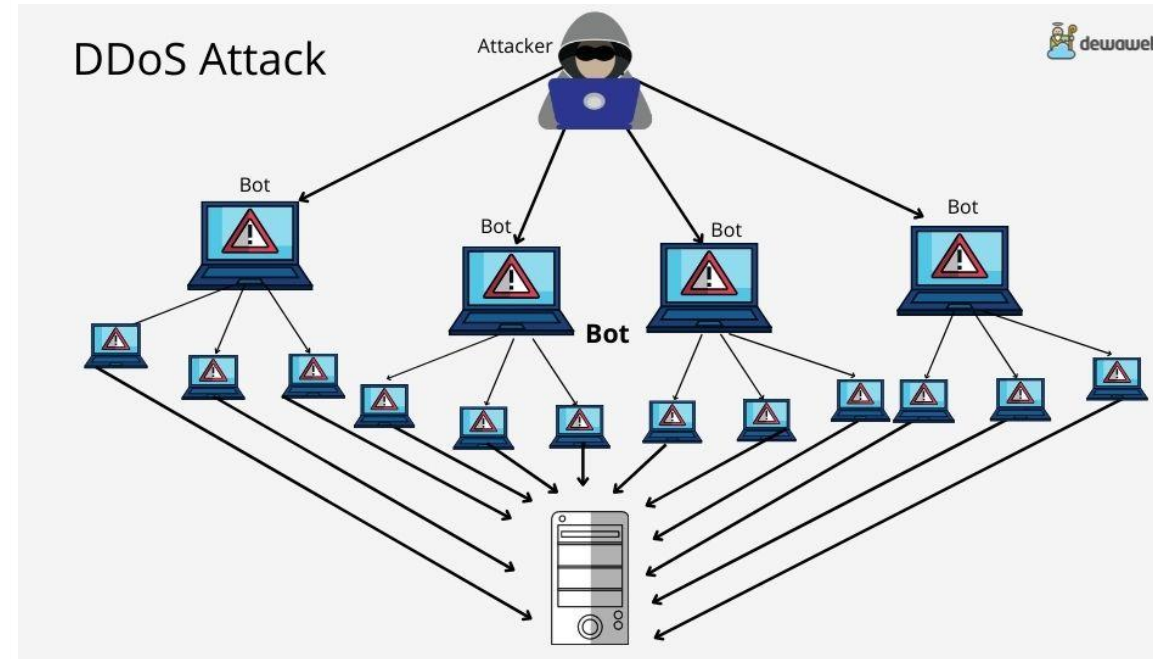
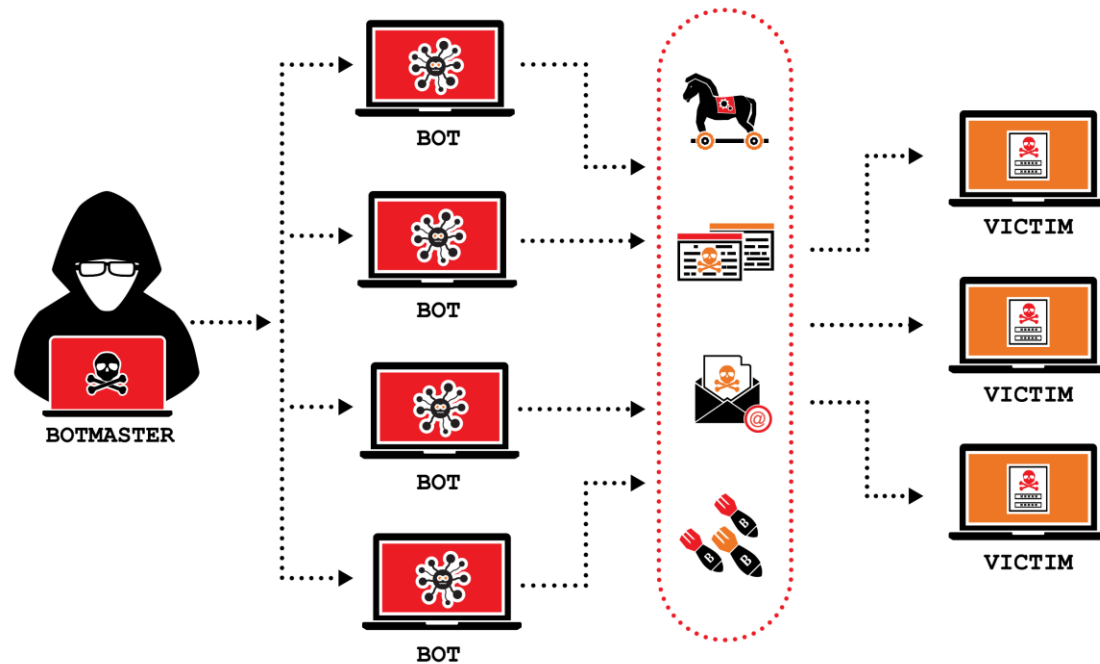
Serangan Malware

Malware (malicious software) adalah perangkat lunak berbahaya yang dirancang untuk merusak atau mengeksploitasi sistem komputer dan jaringan. Beberapa jenis malware meliputi:

- **Virus** Program yang dapat mereplikasi diri dan menyebar ke sistem lain.
- **Worms** Malware yang dapat menyebar tanpa memerlukan interaksi pengguna.
- **Trojan Horse** Program yang tampak sah tetapi memiliki fungsi tersembunyi yang berbahaya.
- **Ransomware** Malware yang mengenkripsi data korban dan meminta tebusan untuk pemulihannya



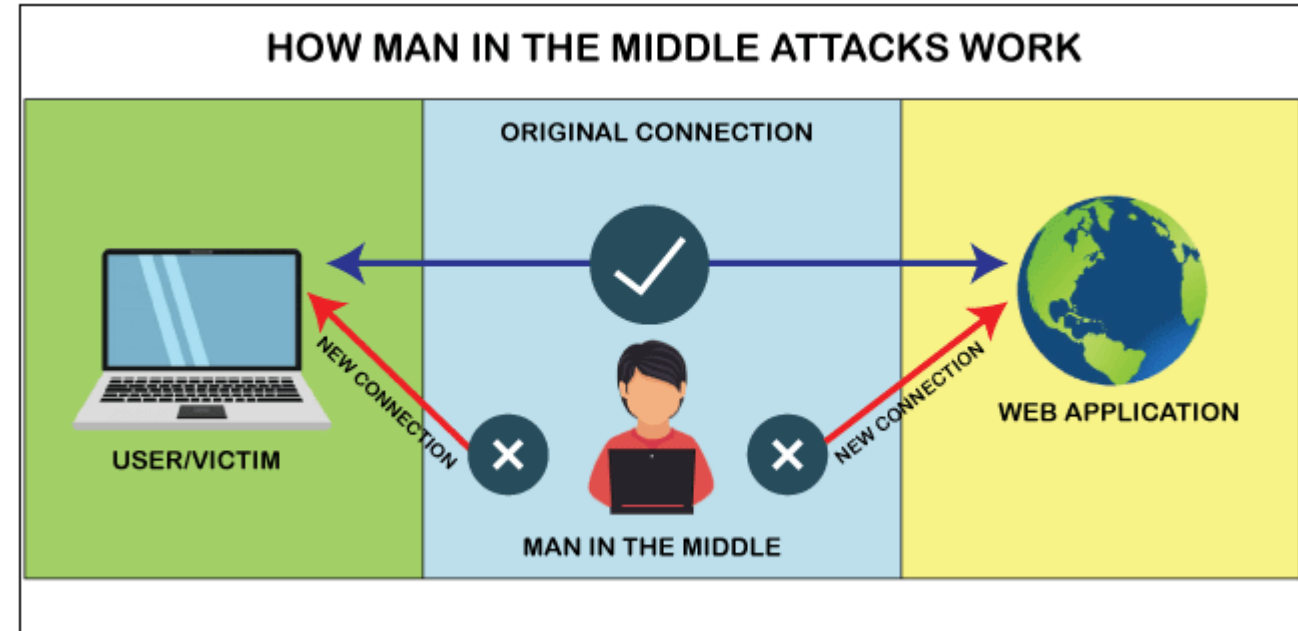
Serangan Denial of Service (DoS) dan Distributed Denial of Service (DDoS)



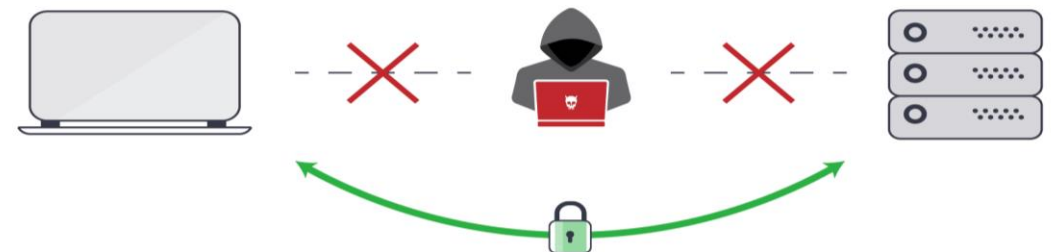
Serangan ini bertujuan untuk melumpuhkan sistem atau jaringan dengan membanjiri server target dengan lalu lintas berlebih sehingga layanan menjadi tidak tersedia.

Man-in-the-Middle Attack (MITM)

- **Man in the Middle Attack (MitM)** adalah jenis serangan siber di mana penyerang secara diam-diam menyusup dan memantau atau mengubah komunikasi antara dua pihak yang percaya bahwa mereka berkomunikasi langsung satu sama lain.
- Penyerang dapat mencuri informasi sensitif seperti kata sandi, nomor kartu kredit, atau informasi pribadi lainnya, atau dapat juga menyuntikkan data yang berbahaya ke dalam komunikasi tersebut.

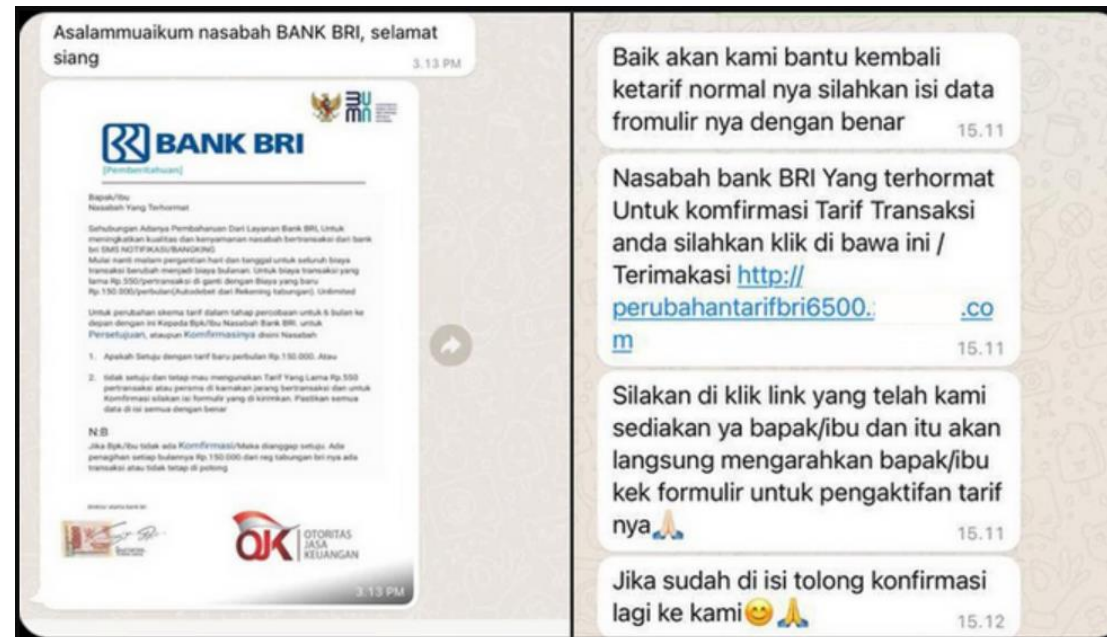


Avoiding **Man-in-the-Middle** Attacks

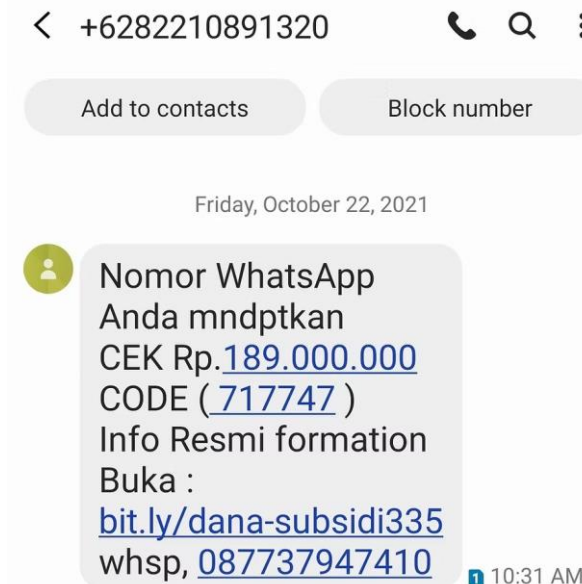


Phishing dan Social Engineering

- **Phishing** adalah upaya untuk mendapatkan informasi sensitif seperti kata sandi dan data kartu kredit dengan menyamar sebagai entitas terpercaya.
- **Teknik social engineering** memanipulasi korban untuk memberikan akses ke sistem.



1



2



CSIRT
Badan Meteorologi Klimatologi dan Geofisika



9 CARA UNTUK MELINDUNGI DIRI DARI PHISING

Phising adalah Upaya untuk mendapatkan Informasi data seseorang dengan teknik pengelabuan. Berikut cara agar terhindar dari penipuan online tersebut.

Pusat Jaringan Komunikasi



ISO 9001
Quality Management
System
CERTIFIED

ISO/IEC
20000-1
Service Management
CERTIFIED

ISO/IEC
27001
Information Security
Management
CERTIFIED

PAS 99
Integrated Management
System
CERTIFIED

- DATA PRIBADI: NAMA, USIA, ALAMAT
- DATA AKUN: USERNAME & PASSWORD
- DATA FINANSIAL

DATA YANG BIASA JADI SASARAN



InfoBMKG



InfoBMKG



InfoBMKG



InfoBMKG

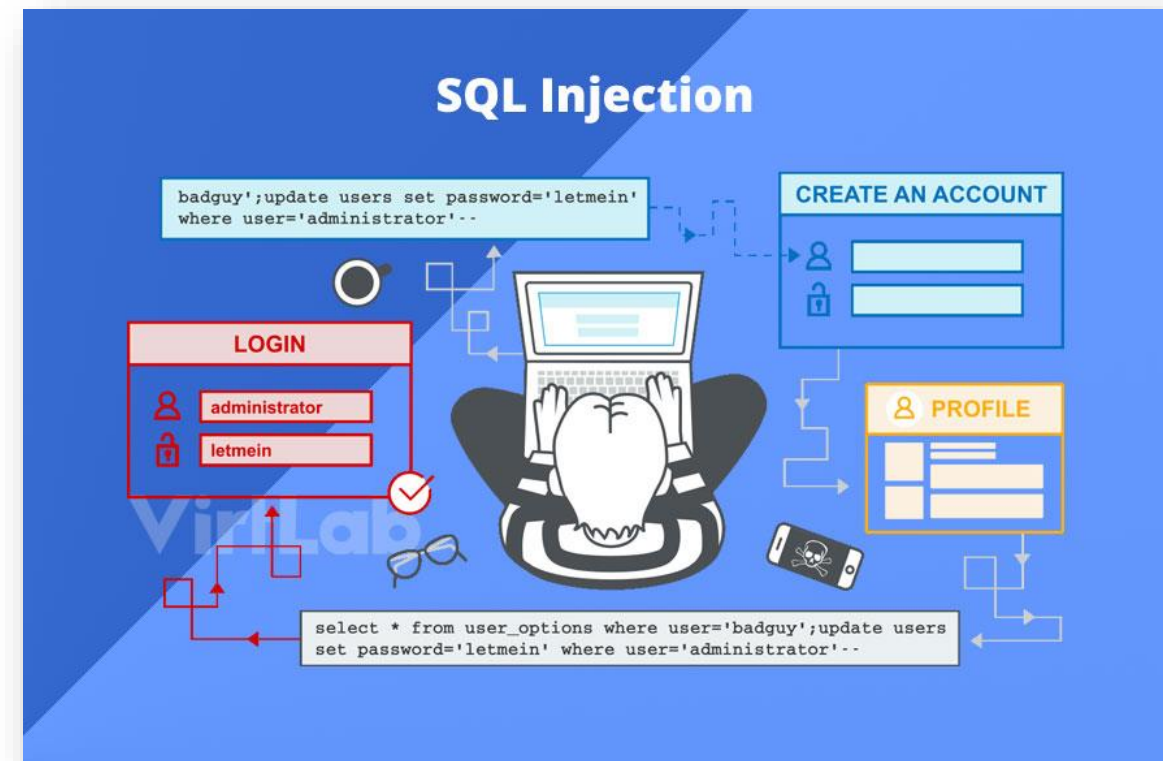
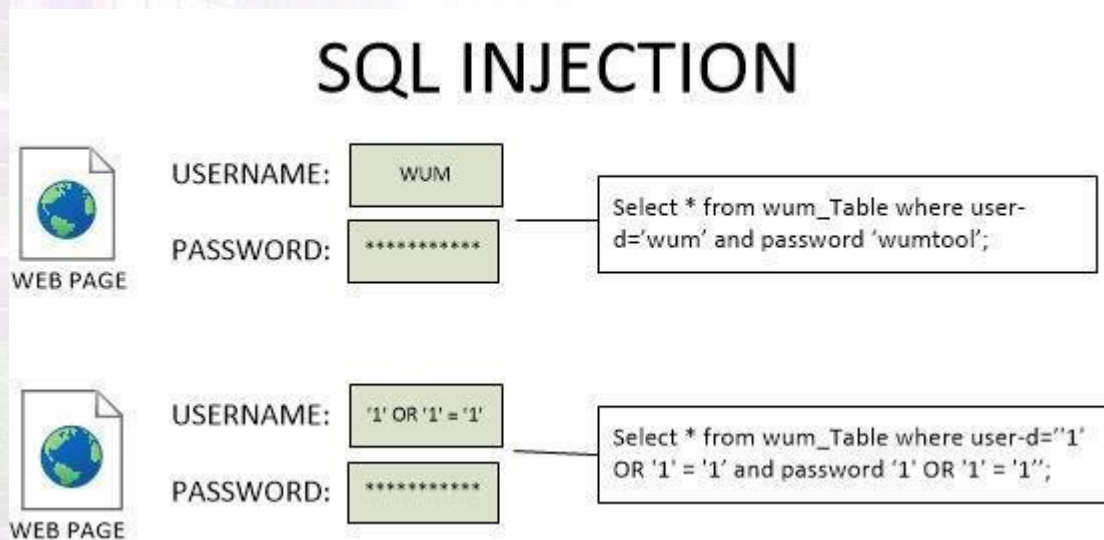


www.bmkg.go.id



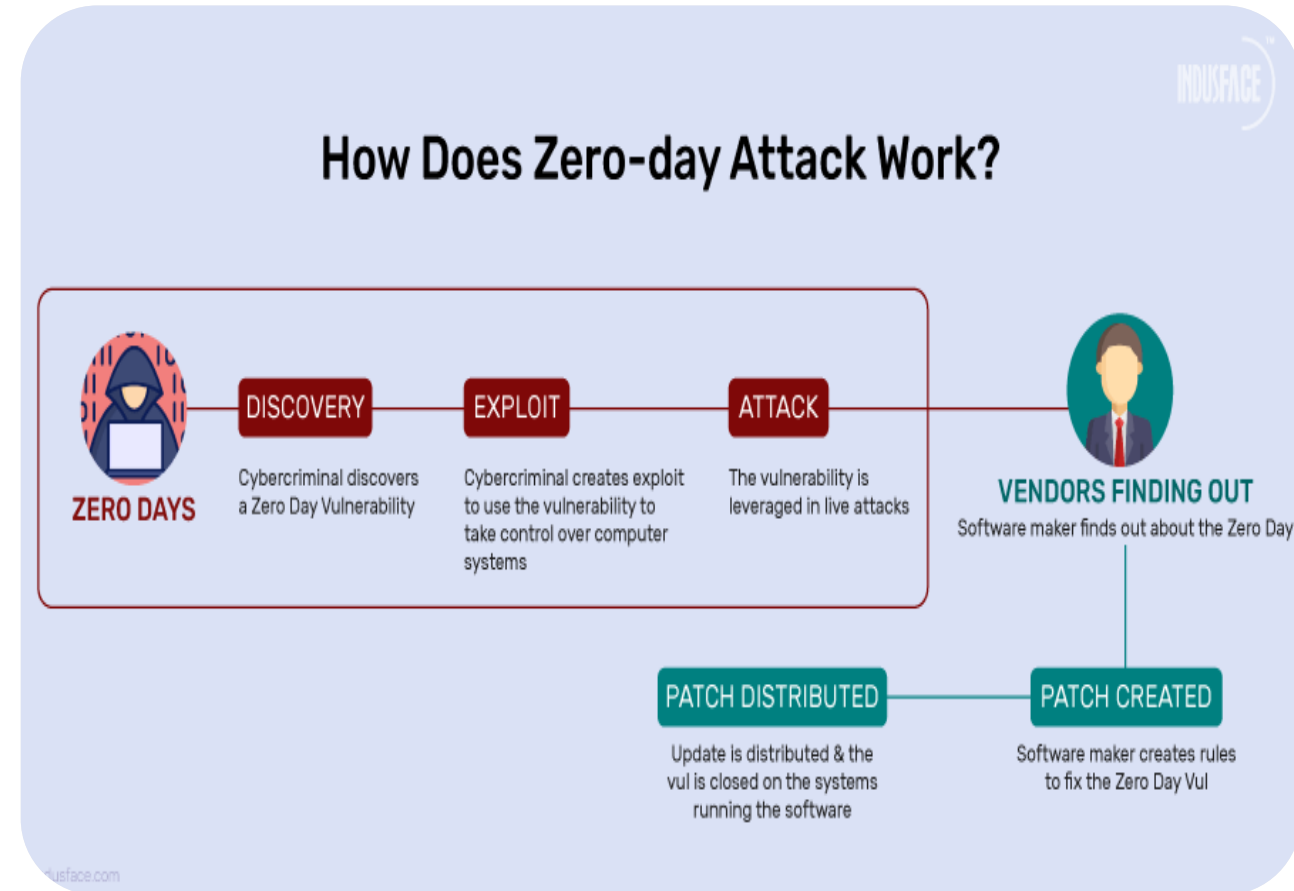
SQL Injection

Serangan yang memanfaatkan celah keamanan dalam database dengan menyisipkan kode SQL berbahaya untuk mengakses atau merusak data.

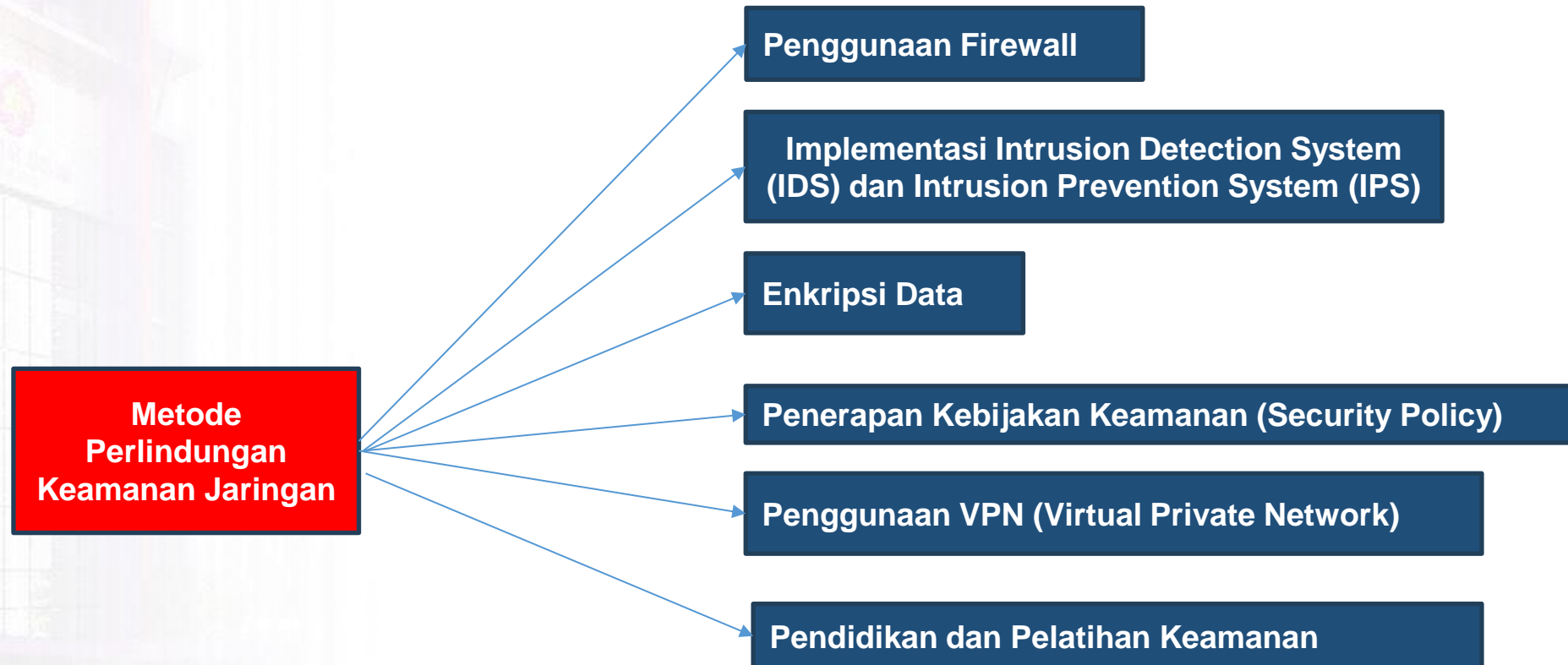


Zero-Day Attack

- Serangan yang mengeksploitasi kerentanan perangkat lunak yang belum diketahui atau belum diperbaiki oleh pengembang.
- **Zero day attack atau zero day exploit** adalah serangan yang mengeksploitasi kerentanan perangkat lunak (software) atau sistem yang belum diketahui oleh pihak software beserta pengembangnya. Kerentanan yang tidak terdeteksi ini membuat serangan dapat berlangsung tanpa hambatan hingga ditemukan dan diperbaiki oleh pemilik aplikasi/software. Serangan ini bisa terjadi pada berbagai jenis software, mulai dari sistem operasi, aplikasi browser, hingga hardware. Setelah memahami definisi dari zero-day attack, penting untuk mengeksplorasi jenis-jenis serangan zero day attack.



Metode Perlindungan Keamanan Jaringan



a. Penggunaan Firewall

Firewall berfungsi sebagai penghalang antara jaringan internal dan eksternal, mencegah lalu lintas yang mencurigakan.

b. Implementasi Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS)

IDS mendeteksi ancaman dalam jaringan, sementara IPS mengambil tindakan untuk mencegah serangan lebih lanjut.

c. Enkripsi Data

- Penggunaan enkripsi untuk melindungi data selama penyimpanan dan transmisi sangat penting untuk mencegah pencurian informasi.

d. Penerapan Kebijakan Keamanan (Security Policy)

Organisasi harus menerapkan kebijakan keamanan seperti autentikasi dua faktor (2FA), manajemen akses berbasis peran (RBAC), dan pembaruan sistem secara berkala.

e. Penggunaan VPN (Virtual Private Network)

VPN membantu mengamankan komunikasi dengan mengenkripsi data yang dikirim melalui jaringan publik.

f. Pendidikan dan Pelatihan Keamanan

- Kesadaran pengguna terhadap ancaman keamanan sangat penting. Pelatihan dan edukasi rutin dapat membantu mencegah serangan berbasis social engineering.

Kesimpulan

- Ancaman keamanan jaringan terus berkembang seiring dengan kemajuan teknologi. Oleh karena itu, penting bagi organisasi dan individu untuk selalu memperbarui sistem keamanan mereka, menerapkan praktik keamanan terbaik, serta meningkatkan kesadaran terhadap ancaman yang ada. Dengan demikian, sistem jaringan dapat lebih terlindungi dari berbagai serangan siber yang berpotensi merugikan.

Quotes Of The Day

“Winners continue working while others have stopped, losers stop working before others.”

Orang-orang yang sukses terus bekerja sebelum orang lain berhenti, orang-orang yang gagal berhenti sebelum orang lain



UNIVERSITAS
AMIKOM
YOGYAKARTA

