TEORI

1. CIA Triad adalah konsep fundamental dalam dunia **cyber security** yang terdiri dari tiga pilar utama:

1. **Confidentiality (Kerahasiaan)**
   Tujuan: Menjaga informasi agar hanya dapat diakses oleh pihak yang berwenang atau bisa disebut sebagai pemberian hak akses. di dalamnya terdapat kontrol akses, otentikasi, enkripsi.
   - 2 model authentikasi = fisik dan digital. Digital seperti OTP, Capthca dan Fisik seperti sidik jari, retina mata, kartu identitas.
   - enkripsi -> data plain text menjadi chiper text
   - dekripsi -> data chiper text menjadi plain text

   Contoh confidentiality: Enkripsi data, penggunaan password, otentikasi.

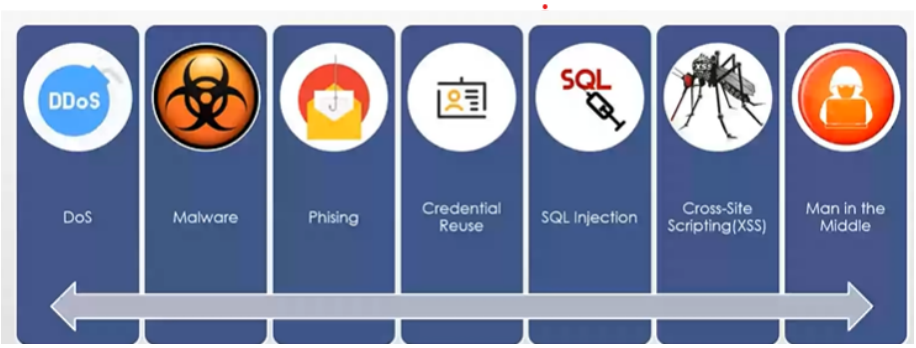
2. **Integrity (Integritas)**
   Tujuan: Menjamin bahwa data tidak diubah secara tidak sah, baik disengaja maupun tidak disengaja, dibawah integrity adalah authenticity (data bersumber dari tempat yang sah), validity(informasi sesuai dengan fakta/keabsahan) dan data yang diberikan akurat.

3. **Availability (Ketersediaan)**
   Tujuan: Memastikan bahwa sistem dan data selalu tersedia saat dibutuhkan oleh pengguna yang sah (authority).

   Contoh availability: Backup, sistem redundan(backup dengan double server dimana jika satu server down server lainnya akan melayani). server mirror (membuat backup, dimana jika data diubah hanya tampilan saja tetapi data di database tetap utuh).

2. TERMINOLOGI KEAMANAN : Kondisi dimana ada potensi terjadi serangan keamanan dengan tingkat ancaman dan prioritas yang berbeda.

THREAT (ANCAMAN)



DoS (Denial of Service)

- Serangan yang membuat sistem, layanan, atau jaringan tidak dapat diakses oleh pengguna sah dengan membanjiri server dengan lalu lintas palsu.
- Versi lebih berbahaya: **DDoS (Distributed DoS)** dilakukan dari banyak perangkat sekaligus.

Malware (Malicious Software)

- Perangkat lunak berbahaya yang dirancang untuk merusak, menyusup, atau mencuri data dari sistem komputer.
- Contohnya: virus, worm, ransomware(mencuri data dengan meminta tebusan), trojan.

Phishing

- Teknik rekayasa sosial untuk menipu korban agar memberikan informasi sensitif seperti kata sandi atau data kartu kredit.
- Biasanya dilakukan melalui email atau situs palsu seperti undangan berbentuk apk pada whatsapp.

Credential Reuse

- Ketika pengguna memakai ulang kombinasi username dan password yang sama di berbagai layanan.
- Jika satu layanan bocor, akun di layanan lain juga bisa diretas.

SQL Injection

- Serangan yang menyisipkan perintah SQL berbahaya ke dalam input pengguna, biasanya pada formulir web, untuk mengakses atau memanipulasi database.

Cross-Site Scripting (XSS)

- Serangan di mana penyerang menyisipkan skrip berbahaya ke dalam situs web yang dilihat oleh pengguna lain.
- Bisa digunakan untuk mencuri data seperti cookie(jejak digital login) sesi pengguna.

Man in the Middle (MitM)

- Serangan di mana penyerang menyadap komunikasi antara dua pihak tanpa sepengetahuan mereka.
- Bisa mencuri atau memanipulasi informasi yang dikirimkan.
- protokol hacking handphone ss7

3. Analisis Kerentanan (Vulnerability Analysis) adalah proses untuk **mengidentifikasi, mengevaluasi, dan mengklasifikasikan kelemahan** dalam sistem, aplikasi, jaringan, atau perangkat yang bisa dieksploitasi oleh pihak tidak berwenang (threat actor).

🔍 Tujuan Utama Analisis Kerentanan

1. Mendeteksi celah keamanan yang dapat dimanfaatkan hacker.
2. Mencegah serangan siber sebelum terjadi.
3. Membantu memperkuat sistem melalui patching atau konfigurasi ulang.

🛠️ Langkah-Langkah Umum dalam Analisis Kerentanan

1. Identifikasi Aset
    - Menentukan perangkat keras, perangkat lunak, jaringan, dan data penting.
2. Pindai Kerentanan (Vulnerability Scanning)
    - Menggunakan tools seperti Nessus, OpenVAS, atau Qualys untuk mendeteksi kelemahan.
3. Analisis Hasil
    - Menilai tingkat keparahan kerentanan berdasarkan CVSS (Common Vulnerability Scoring System).
4. Klasifikasi dan Prioritasi
    - Menentukan kerentanan mana yang paling kritis dan harus segera diperbaiki.
5. Remediasi
    - Menutup celah dengan patch, update sistem, konfigurasi ulang, atau segmentasi jaringan.
6. Verifikasi Ulang
    - Setelah perbaikan, dilakukan pemindaian ulang untuk memastikan celah sudah tertutup.

📌 Contoh Kerentanan Umum

- Port terbuka yang tidak digunakan
- Sistem belum di-update (banyak bug yang ditemukan dan dapat menjadi celah)
- Password default atau lemah
- Aplikasi rentan terhadap SQL Injection atau XSS

Kerentanan menimbulkan sebuah ancaman, tanpa ada kerentanan tidak akan ada ancaman.

4. Eksploitasi

Tujuan exploitasi = pemanfataan kelemahan atau celah untuk mendapat keuntungan. bisa menggunakan protocol ssh/telnet untuk mengendalikan perangkat tujuan dari perangkat kita dan menjadikan kita sebagai super user /root.

5. Target Evaluasi

simulasi serangan untuk menemukan kelemahan pada sistem jaringan tertentu (penetration tester).

6. Serangan/Attack

indikasi penyerangan sistem aplikasi dan jaringan baik jarak jauh maupun lokal.

Jenis Manuver ofensive digunakan oleh negara/individu yang menargetkan sebuah informasi yang biasanya terdeteksi sebagai anonim atau nama samaran.

Contoh = 1. serangan cyber di negara estonia yang melumpuhkan negara

2. stucknet - > mengakui kepemilikan instalasi nuklir (Amerika)

Tingkatan serangan siber ada 3 = low, medium, high.

- Low = misal serangan hanya mengubah tampilan saja dan sistem kita masih beraktifitas seperti biasa maka dikategorikan low.
- Medium = tipe serangan jika aktifitas sistem kita menjadi terganggu.
- High = tipe serangan jika kita benar-benar tidak bisa melakukan aktifitas di sistem.

7. Pelaksanaan Kebijakan keamanan infromasi

Output = Kebijakan menghasilkan pelaksanaan dan pengendalian

pelaksanaan pengendalian dibagi 3 =

1. Kendali Teknis =
    - pengguna harus di identifikasi, otentikasi, otorisasi.
    - deteksi gangguan seperti pemasangan antivirus dan penggunaan protocol tertentu
    - firewall/penyaringan
    - kriptografi
    - Mengunci ruangan / membatasi ruangan server
2. Kendali Formal =
    - SOP (laptop hanya digunakan untuk bekerja, tidak boleh digunakan untuk kegunaan lain)
    - Peraturan (Peraturan adalah bagian dari SOP)
    - Pengawasan (Proses pengawasan dari SOP dan Peraturan)
3. Kendali Informal =
    - Workshop
    - Seminar (mengetahui update pada bidang keamanan informasi)
    - Sosialisasi

TOOLS/WEB

CATATAN TOOLS/WEB DAY 2 :

1. archive.org = Internet Archive: Digital Library of Free & Borrowable Texts, Movies, Music & Wayback Machine (digunakan untuk mengecek website untuk melihat tampilan terakhir sebelum website terkena serangan, berisi log data pertanggal tampilan website)
2. blackop.id = Dashboard Pentest (Digunakan untuk melakukan simulasi penetration testing)
3. sql injection = SQL Injection Demo (Digunakan untuk simulasi injeksi sql)