Pretest CJ

1. Tuliskan 5 kasus *data breach* baik di dalam dan luar negeri beserta penyebabnya (*root cause analysis* secara singkat).

    - Xiaomi -> *zero-day vulnerability in* Xiaomi website
    - Capital One -> *Misconfiguration at* Capital One's *Cloud Server*
    - Joomla -> *Joomla Resources Directory team stored a full unencrypted backup of the JRD website on an Amazon Web Services S3 bucket owned by the third-party company*
    - Digital Ocean -> *internal document accessible to the internet without requiring any password*
    - Razer -> misconfiguration of elasticsearch

2. Jelaskan apa yang dimaksud dengan PII (Personally Identifiable Information) beserta bagaimana seharusnya pengelola layanan teknologi informasi mengamankan PII yang dipercaya oleh pengguna.
    - PII adalah data diri pengguna yang bisa digunakan untuk mengidentifikasi siapa orang tersebut di dunia nyata. PII bisa dalam banyak bentuk seperti email, password, nomor telepon, nomor KTP, nomor BPJS, alamat rumah, nama lengkap, dll.
    - Untuk mengamankannya bisa dengan cara hashing password dan harus dilakukan edukasi terhadap pegawai di perusahaan pengelola layanan teknologi informasi tersebut agar tidak mudah terkena praktek social engineering.

3. Tuliskan 5 kesalahan umum terkait keamanan yang biasa dilakukan oleh penyedia layanan teknologi informasi yang menggunakan komputasi awan (seperti AWS dan Google Cloud).
    - Tidak menyiapkan RBAC yang benar, sehingga unauthorized user bisa mengakses data penting
    - Tidak menyiapkan backup / disaster recovery plan
    - Menentukan bandwith yang sesuai terhadap masing masing perusahaan client
    - Sistem wipe data yang menyeluruh jika terjadi perubahan kenggunaan / client pada rack server tertentu
    - Menutup port yang tidak digunakan

4. Jelaskan risiko dari *zero day vulnerability* terkait *memory corruption* pada web browser dan tuliskan contoh skenario peretesan yang bisa terjadi pada sisi pengguna biasa dan pada jaringan perusahaan.

Attacker yang memanfaatkan *zero day vulnerability* terkait *memory corruption* dapat memanfaatkan *current memory* dari *user* yang mengakses di saat itu, bila misalkan *user* itu merupakan *administrator* maka *attacker* itu punya permission *administrator* juga yang menandakan *attacker* bisa *well… basicly take control the affected system*, *attacker* itu bisa

menginstall *program*, melihat, memodifikasi, atau menghapus *sensitive data,* atau juga bisa meng*create new account* lainnya untuk *attacker*nya sendiri. contoh nya : CVE-2019-1367

5. Jelaskan risiko tertinggi yang mungkin bisa terjadi dengan adanya celah open redirection pada aplikasi web (jika Anda ingin menjelaskan mengenai eksploitasi berantai, Anda dapat mengasumsikan celah lain yang mungkin ada pada aplikasi web yang sama).
    - Open redirect membuka kemungkinan penyerang untuk melakukan redirect user ke website / konten di domain yang sama yang di kontrol oleh attacker. Hal ini bisa berakibat pencurian kredensial login dengan cara phising ke website yang di kontrol attacker atau juga di chaining dengan reflected XSS untuk mencuri session cookie user agar attacker bisa login sebagai user.

6. Tuliskan langkah-langkah yang bisa dilakukan oleh penyerang secara manual untuk mengkesploitasi celah time-based blind sql injection untuk melakukan database *exfiltration* tanpa menggunakan tools tambahan seperti sqlmap.

- Check beneran ada ga celah SQLi nya
- Setelah mengetahui celahnya dimana dan bagaimana, check response time nya saat kondisi yang diberikan seharusnya mengeluarkan value True atau False
- Check perbedaan time nya seberapa banyak (biasanya yang mengeluarkan value True itu lebih lama)
- Sisanya tinggal lakukan satu persatu untuk semua kondisi di databasenya
- Mulai lah simpan hasil output yang diinginkan dan lakukan sampai… sampai selesai .-. (Sampai semua data yang diinginkan yang ada di databasenya keluar)

7. Tuliskan contoh karir yang bisa dieksplorasi oleh orang yang memiliki minat/bakat di:
    a. Web hacking : Web Pentester
    b. Cryptography : Cryptographer, Source Code auditor
    c. Digital forensics : Digital Forensic Analyst in DFIR
    d. Reverse engineering : Malware Analyst / Researcher
    e. Binary exploitation : Exploit Developer