PROBLEM SET 14: KEAMANAN KERNEL (C1–C6)

BERBASIS TAKSONOMI BLOOM (LEVEL C1 S.D. C6)

Mata Kuliah: Sistem Operasi (INF-201) – Program Studi Informatika UNIB

SOAL LEVEL C1 – C3: KONSEP DASAR KEAMANAN

1. Jelaskan perbedaan konseptual antara perlindungan menggunakan *Access Control List* (ACL) dan *Capability Lists*!

2. Apa fungsi dari bit `SetUID` (`suid`) pada sistem berkas Unix, dan sebutkan satu contoh program umum yang memerlukannya!

SOAL LEVEL C4 – C5: ANALISIS MITIGASI (CASE STUDY)

1. **Case Study**: Sebuah *web server* ditulis dalam bahasa C dan mengalami *Stack Buffer Overflow*. Namun, sistem operasi memiliki fitur **NX Bit (No-Execute)** yang diaktifkan. Penyerang mengubah strategi menjadi serangan *Return-to-libc*. Analisis perbedaan fundamental antara eksekusi *shellcode* tradisional dengan serangan *Return-to-libc* di bawah mitigasi NX Bit!

2. Evaluasi mengapa kebijakan W^X (*Write XOR Execute*) sangat penting diterapkan secara ketat oleh sistem operasi yang memprioritaskan keamanan (seperti OpenBSD).

SOAL LEVEL C6: DESAIN ARSITEKTUR KEAMANAN

1. Anda ditugaskan merancang pembaruan keamanan untuk sebuah aplikasi daemon pemroses teks sederhana (`text-processor`) di sistem operasi mirip-Unix. Aplikasi ini hanya perlu membaca dari berkas di `/tmp/input.txt`, memproses, lalu menulis hasil ke `/tmp/output.txt`, dan mencetak status ke `stdout`. Rancanglah struktur perlindungan menggunakan pendekatan API mirip OpenBSD (`pledge` dan `unveil`). Tuliskan urutan panggilannya (secara konseptual atau pseudocode) dan jelaskan analisis ancaman (threat model) apa saja yang berhasil dicegah dengan desain Anda tersebut, bahkan jika `text-processor` memiliki kelemahan *buffer overflow*!