LEMBAR KERJA MAHASISWA (WORKSHEET 14)

TOPIK: PROTEKSI, BUFFER OVERFLOW, & MITIGASI KEAMANAN

Mata Kuliah: Sistem Operasi (INF-201) – Semester Ganjil 2026/2027

Nama Mahasiswa	:	.....
NPM	:	.....
Kelas / Kelompok	:	.....

Tugas Membaca Acuan (Prasyarat Pengerjaan):
Mahasiswa wajib membaca: [**OSTEP**] Ch. 54; [**TLCL**] Ch. 9; [**Think OS**] Ch. 5 sebelum mengerjakan worksheet ini.

A. ANALISIS BUFFER OVERFLOW (C3 – C4)

Perhatikan potongan kode C yang rentan (vulnerable) berikut ini:

```c
#include <stdio.h>
#include <string.h>

void login(char *password) {
    char buffer[16];
    strcpy(buffer, password); // Fungsi rentan!
    if (strcmp(buffer, "rahasia") == 0) {
        printf("Akses␣Diberikan.\n");
    } else {
        printf("Akses␣Ditolak.\n");
    }
}

int main(int argc, char *argv[]) {
    if (argc > 1) login(argv[1]);
    return 0;
}
```

1. Apa yang akan terjadi pada struktur memori (*Stack Frame*) dari fungsi `login()` jika argumen `password` yang diinputkan memiliki panjang 40 karakter?

2. Bagaimana seorang penyerang dapat memanfaatkan kerentanan ini untuk menjalankan kode berbahaya (*shellcode*) miliknya?

B. EVALUASI TEKNIK MITIGASI (C4 – C5)

1. Jelaskan bagaimana **Stack Canaries** dapat menggagalkan serangan *buffer overflow* pada program di atas! Mengapa disebut "canary"?

2. Pada OS modern dengan **ASLR** aktif, alamat basis memori selalu berubah setiap kali program dieksekusi. Mengapa fitur ini menyulitkan serangan *Return-to-libc*?