COFELET

Scenario: L'obiettivo è eseguire un attacco di tipo buffer overflow per redirigere il flusso di esecuzione alla funzione `win()` e ottenere la flag.

Task: Manipolare l'indirizzo di ritorno della funzione `vuln()` usando un exploit buffer overflow.

Goal: Eseguire la funzione `win()` e ottenere la flag.

Condition: Il giocatore deve saper identificare una funzione vulnerabile come `gets()` e trovare l'offset corretto per sovrascrivere l'indirizzo di ritorno.

Scenario Execution Flow (SEF):

1. Avviare il binario e verificare la presenza di funzioni rilevanti in GDB.
2. Calcolare l'offset per sovrascrivere l'indirizzo di ritorno.
3. Costruire un payload che reindirizzi `EIP` a `win`.
4. Lanciare il payload per ottenere la flag.

Knowledge Skills Ability (KSA):

- **K**: Conoscenza delle vulnerabilità buffer overflow.
- **S**: Capacità di analizzare il codice binario con GDB.
- **A**: Abilità di generare payload e manipolare registri.

Learning Objectives: Alla fine dell'esercizio, i giocatori sapranno identificare e sfruttare un buffer overflow usando un exploit `ret2win`.