Architettura 32bit:

sudo dpkg --add-architecture i386

sudo dpkg --print-foreign-architectures

sudo apt update

sudo apt upgrade

sudo apt install libc6:i386 libncurses5:i386 libstdc++6:i386

sudo apt install vim

sudo apt install tmux

(

per avviarlo -->

nuova sessione: tmux new -s nome\_sessione

per splittare in orizzontale: ctrl+B+sift+2

per splittare in verticale: ctrl+B+sift+5

per spostarsi

)

sudo apt install gcc-multilib g++-multilib

sudo apt install gdb

sudo apt install curl

bash -c "$(curl -fsSL https://gef.blah.cat/sh)"

(

per verificare se gef è installato correttamente -->

sudo apt install checksec

sudo apt install python3

sudo apt install python3-pip

pip install pwntools

objdump -d nome\_eseguibile --> restituisce il codice in formato assembly

per vedere il file main.c: vim main.c

per salvare --> :w + enter

per uscire --> :wq + enter

per modificare --> nano nome\_file

per lanciare gdb: gdb nome\_file

per creare un file in 32 bit: gcc -m32 -o nome\_eseguibile nome\_file

per lanciare un file gdb: gdb nome\_file

**GEF**

Per inserire un breakpoint --> b + punto in cui inserire il breakpoint {facoltativo}



per eseguire --> r (esegue tutto l'eseguibile ma se c'è un breakpoint si ferma là)

per scorrere le istruzioni durante il debug --> c

per uscire da gef --> q {oppure quit}

**CHECKSEC**

Per vedere i livelli di protezione di un eseguibile -->   
checksec –-file=nome\_eseguibile

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente

Verdi attive e rosse non attive.

**Cos’è il Canary?**

**File crackme**

<https://book.rada.re/crackmes/ioli/intro.html#ioli-crackmes>