Esame Software Security Febbraio 2023
Docente: Andrea Lanzi
(Tempo: 2 ore e mezza)

Dato il programma vuln.c, scrivere un exploit in python con tecnica ROP che effettua la seguente operazioni:

1) Exploitare la funzione vuln ed eseguire una shell di sistema, senza usare uno shellcode.

Dati i programmi bof1 e bof2 explitarli utilizzando le funzioni vulnerabili attraverso l'esecuzione dello shellcode.

Per ogni exploit descrivere la metodologia utilizzata. Mostrare come sono stati estratti i vari indirizzi di memoria, riportare lo script in python che contiene l'exploit e la prova in screenshot della sua esecuzione che mostra con quali parametri vengono lanciati gli exploit.

Shellcode da utilizzare:

shellcode=(b"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80")