S10L3

Traccia:

Nella lezione teorica del mattino, abbiamo visto i fondamenti del linguaggio Assembly. Dato il codice in Assembly per la CPU x86 allegato qui di seguito, identificare lo scopo di ogni istruzione, inserendo una descrizione per ogni riga di codice. Ricordate che i numeri nel formato 0xYY sono numeri esadecimali. Per convertirli in numeri decimali utilizzate pure un convertitore online, oppure la calcolatrice del vostro computer (per programmatori).

```
0x00001141 <+8>:     mov    EAX,0x20
0x00001148 <+15>:    mov    EDX,0x38
0x00001155 <+28>:    add    EAX,EDX
0x00001157 <+30>:    mov    EBP, EAX
0x0000115a <+33>:    cmp    EBP,0xa
0x0000115e <+37>:    jge    0x1176 <main+61>
0x0000116a <+49>:    mov    eax,0x0
0x0000116f <+54>:    call   0x1030 <printf@plt>
```

- La riga di codice "mov EAX, 0x20" assegna il valore esadecimale "0x20" al registro EAX su una CPU x86 o x86-64. In questo caso, "0x20" rappresenta il numero 32 in decimale. Quindi, questa istruzione muove il valore 32 nel registro EAX.

- La riga di codice "mov EDX, 0x38" assegna il valore esadecimale "0x38" al registro EDX su una CPU x86 o x86-64. In questo caso, "0x38" rappresenta il numero 56 in decimale. Quindi, questa istruzione muove il valore 56 nel registro EAX.

- La riga di codice “add EAX, EDX” esegue un’addizione fra i contenuti dei registri EAX e EDX. In breve, questa istruzione somma il valore contenuto nel registro EDX al valore contenuto nel registro EAX e memorizza il risultato nel registro EAX.

- La riga di codice "mov EBP, EAX" copia il contenuto del registro EAX nel registro EBP. Questo significa che il valore attuale presente nel registro EAX viene memorizzato anche nel registro EBP.

- L'istruzione "cmp EBP, 0xa" confronta il valore contenuto nel registro EBP con il valore immediato 0xA (che è 10 in decimale). Questo confronto imposta dei flag nel registro dei flag della CPU (come il registro EFLAGS) in base al risultato della comparazione. Se il valore in EBP è inferiore a 10, il flag di Carry (CF) verrà impostato a 1. Se il valore in EBP è uguale a 10, il flag di Zero (ZF) verrà impostato a 1. Se il valore in EBP è maggiore di 10, il flag di Carry verrà impostato a 0 e il flag di Zero sarà impostato a 0
- l'istruzione "jge 0x1176 <main+61>" fa sì che il flusso di esecuzione del programma salterà alla posizione di memoria 0x1176 solo se la condizione "maggiore o uguale" è soddisfatta. Altrimenti, il programma continuerà l'esecuzione normalmente.
- L'istruzione "mov eax, 0x0" assegna il valore immediato "0x0" al registro EAX. In altre parole, imposta il valore del registro EAX a zero.
- L'istruzione "call 0x1030 printf@plt" effettua una chiamata di funzione alla posizione di memoria 0x1030, che nel caso specifico sembra essere l'indirizzo di printf dalla Procedure Linkage Table (PLT), una tabella usata per la risoluzione dinamica dei simboli durante l'esecuzione di un programma compilato dinamicamente.