Pratica W22D1

Traccia:

EPICODE

Esercizio
Linguaggio Assembly

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).

```
0×00001141 <+8>:    mov   EAX,0×20
0×00001148 <+15>:   mov   EDX,0×38
0×00001155 <+28>:   add   EAX,EDX
0×00001157 <+30>:   mov   EBP, EAX
0×0000115a <+33>:   cmp   EBP,0xa
0×0000115e <+37>:   jge    0×1176 <main+61>
0×0000116a <+49>:   mov   eax,0×0
0×0000116f <+54>:   call   0×1030 <printf@plt>
```

3

Soluzione:

1. **mov EAX, 0x20**: Carica il valore esadecimale 0x20 (32 in decimale) nel registro EAX.
2. **mov EDX, 0x38**: Carica il valore esadecimale 0x38 (56 in decimale) nel registro EDX.
3. **add EAX, EDX**: Aggiunge il contenuto del registro EDX al registro EAX e memorizza il risultato in EAX.
4. **mov EBP, EAX**: Copia il contenuto del registro EAX nel registro EBP.
5. **cmp EBP, 0xa**: Compara il valore del registro EBP con il valore esadecimale 0xa (10 in decimale).
6. **jge 0x1176 <main+61>**: Salta all'indirizzo 0x1176 (offset di 61 rispetto all'inizio della funzione main) se il flag di "greater than or equal" (indicato dalla istruzione **cmp**) è impostato.
7. **mov eax, 0x0**: Carica il valore esadecimale 0x0 (0 in decimale) nel registro EAX.
8. **call 0x1030 <printf@plt>**: Esegue una chiamata alla funzione **printf** (presumibilmente) all'indirizzo 0x1030.

- **Movimento dei dati nei registri:** Le istruzioni **mov** vengono utilizzate per spostare dati. Ad esempio, **mov EAX, 0x20** sposta il valore esadecimale 0x20 nel registro EAX.

- **Operazioni aritmetiche:** L'istruzione **add** viene utilizzata per eseguire l'addizione. In questo caso, **add EAX, EDX** aggiunge il contenuto del registro EDX al registro EAX e memorizza il risultato in EAX.
- **Confronto e salto condizionale:** Le istruzioni **cmp** e **jge** vengono utilizzate insieme per confrontare valori e decidere il flusso del programma. **cmp EBP, 0xa** confronta il contenuto del registro EBP con il valore esadecimale 0xa. **jge** è un salto condizionale che salta a un certo indirizzo se il confronto soddisfa una condizione specifica, in questo caso se EBP è maggiore o uguale a 10.
- **Chiamata di funzione:** L'istruzione **call** viene utilizzata per chiamare una funzione. In questo caso, **call 0x1030** chiama la funzione situata all'indirizzo 0x1030.