Pratica S10L3

Considerando il seguente blocco di codice in assembly andiamo a spiegare le operazioni effettuate:

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 parte iniziale delle istruzioni riporta l'indirizzo di memoria in esadecimale dove viene caricata l'istruzione seguente in RAM (nel primo caso 0x00001141). Il numero tra <> indica invece l'offset, ossia la distanza in byte dall'indirizzo di memoria dell'inizio della funzione chiamante.

0x00001141 <+8>: mov EAX,0x20 → memorizzo nel registro EAX il valore decimale 32

0x00001148 <+15>: mov EDX,0x38 → memorizzo nel registro EDX il valore decimale 56

0x00001155 <+28>: add EAX,EDX → sommo i due registri precedenti e memorizzo il tutto nel registro EAX. Quindi ora EAX varrà 88.

0x00001157 <+30>: mov EBP, EAX → copio il contenuto del registro EAX nel registro EBP. Il registro EBP, Extended Base Pointer, è un puntatore che fa rifermento alla base dello stack di memoria in RAM riservata alla funzione locale

0x0000115a <+33>: cmp EBP,0xa → Viene confrontato il valore di EBP con il numero esadecimale a (in decimale 10) . In questo caso lo ZF (Zero flag) non sarà impostato, in quanto EAX vale 88 che è maggiore di 10, quindi varrà 0. Il SF (sign flag) sarà impostato, quindi varrà 1, in quanto il risultato della sottrazione 10-88 è negativo. Il CF (Carry Flag) sarà 1 dato che viene effettuato un riporto nell'operazione di sottrazione.

0x0000115e <+37>: jge 0x1176 <main+61> → Il salto condizionale jge (jump greater or equal) salterà all'indirizzo di memoria assouluto 0x1176, indirizzo relativo <main +61> (che significa 61 byte dall'indirizzo iniziale della funzione main) in base al risultato del cmp nella riga precedente. Nel nostro caso la condizione del salto è soddisfatta in quanto la destinazione EBP (che vale 88) è maggiore della sorgente che vale 10.

Nota: Le successive due istruzioni non verrebbero eseguite in quando verrano saltate dall'istruzione condizionale precedente. Il loro indirizzo di esecuzione infatti è minore di quello del salto. Riportiamo il loro significato per completezza

0x0000116a <+49>: mov eax,0x0 → Copia il valore immediato 0 nel registro EAX

0x0000116f <+54>: call 0x1030 <printf@plt> → viene chiamata la funzione print. L'indirizzo di memoria dedicata alla sua esecuzione viene specificato in 0x1030