



Marzo 2024

CYBER SECURITY SPECIALIST

S10L3

Jacopo Trovato



Assembly x86

Assembly x86 è una famiglia di linguaggi assembly usata per produrre codice macchina.

identificare lo scopo di ognuna delle seguenti istruzioni:

1. 0x00001141 <+8>: mov EAX,0x20
2. 0x00001148 <+15>: mov EDX,0x38
3. 0x00001155 <+28>: add EAX,EDX
4. 0x00001157 <+30>: mov EBP, EAX
5. 0x0000115a <+33>: cmp EBP,0xa
6. 0x0000115e <+37>: jge 0x1176 <main+61>
7. 0x0000116a <+49>: mov eax,0x0
8. 0x0000116f <+54>: call 0x1030 <printf@plt>

1. mov EAX,0x20 = **Sposta** il valore esadecimale **"0x20"** (32) nel registro **"EAX"**.
2. mov EDX,0x38 = **Sposta** il valore esadecimale **"0x38"** (56) nel registro **"EDX"**.
3. add EAX,EDX = **Somma** il valore all'interno dei registri **"EAX"**, **"EDX"**, riportando il risultato nel registro **"EAX"**, **0x20 + 0x38 = 0x58** (88).
4. mov EBP, EAX = **Sposta** il valore del registro **"EAX"** (0x58) nel registro **"EBP"**.
5. cmp EBP,0xa = **Verifica** se il valore **0xa** (10), è uguale al valore contenuto in EBP, **0x58** (88), essendo la destinazione maggiore della sorgente, non si attivano le flag, **ZF** (Zero flag) e **CF** (Carry flag).
6. jge 0x1176 <main+61> = Se il valore di destinazione **"cmp"** è maggiore o uguale al valore di confronto. **0x58** (88) > **0xa** (10), viene eseguito un **salto condizionale** nella sezione di memoria 0x1176.
7. mov eax,0x0 = **Sposta** il valore 0x0 (0) nel registro **"EAX"**.
8. call 0x1030 <printf@plt> = **Passa** l'esecuzione del programma alla funzione **"printf"**.