Costrutti C - Assembly X86

Traccia

Prendendo in considerazione il codice seguente elaborare le seguenti tracce:

- Identificare i costrutti noti
- Ipotizzare la funzionalità
- BONUS: studiare e spiegare ogni singola riga di codice

```
.text:00401000                push    ebp
.text:00401001                mov     ebp, esp
.text:00401003                push    ecx
.text:00401004                push    0               ; dwReserved
.text:00401006                push    0               ; lpdwFlags
.text:00401008                call    ds:InternetGetConnectedState
.text:0040100E                mov     [ebp+var_4], eax
.text:00401011                cmp     [ebp+var_4], 0
.text:00401015                jz      short loc_40102B
.text:00401017                push    offset aSuccessInterne ; "Success: Internet Connection\n"
.text:0040101C                call    sub_40105F
.text:00401021                add     esp, 4
.text:00401024                mov     eax, 1
.text:00401029                jmp     short loc_40103A
.text:0040102B ; ---------------------------------------------------------------------------
.text:0040102B
```

Identificare i costrutti noti

```
.text:00401000                push    ebp
.text:00401001                mov     ebp, esp
.text:00401003                push    ecx
.text:00401004                push    0               ; dwReserved
.text:00401006                push    0               ; lpdwFlags
.text:00401008                call    ds:InternetGetConnectedState
.text:0040100E                mov     [ebp+var_4], eax
.text:00401011          IF →  cmp     [ebp+var_4], 0
.text:00401015                jz      short loc_40102B
.text:00401017                push    offset aSuccessInterne ; "Success: Internet Connection\n"
.text:0040101C                call    sub_40105F
.text:00401021                add     esp, 4
.text:00401024                mov     eax, 1
.text:00401029        Else →  jmp     short loc_40103A
.text:0040102B ; ---------------------------------------------------------------------------
.text:0040102B
```

Ipotizzare la funzionalità

Il codice sembra controllare se una macchina ha accesso a Internet utilizzando la funzione InternetGetConnectedState. Se la connessione è disponibile, viene visualizzato un messaggio di successo

BONUS: studiare e spiegare ogni singola riga di codice

push ebp = Mette il valore del registro ebp nello stack

mov ebp, esp = Copia il valore di esp nel registro ebp, creando un nuovo frame di stack

push ecx = Mette il valore del registro ecx nello stack

push 0 ; dwReserved = Mette il valore 0 nello stack preparando il parametro dwReserved per la chiamata a InternetGetConnectedState

push 0 ; lpwdFlags = Mette il valore 0 nello stack preparando il parametro lpdwFlags per la chiamata a InternetGetConnectedState

call ds:InternetGetConnectedState = Chiama la funzione InternetGetConnectedState

mov [ebp+var_4], eax = Copia il valore di eax nella variable locale [ebp+var_4]

cmp [ebp+var_4], 0 = Compara [ebp+var_4] con 0

jz short loc_40102B = Salta a loc_40102B se il risultato della comparazione precedente è 0 (Zero Flag)

push offset aSuccessInterne ; "Success: Internet Connection\n" = Mette l'offset della stringa "Success: Internet Connection\n" nello stack

call sub_40105F = Chiama la funzione sub_40105F

add esp, 4 = Aggiunge 4 a esp

mov eax, 1 = Imposta il valore di eax a 1

jmp short loc_40103A = Salta a loc_40103A senza considerare alcuna condizione