

# (SPaASM) Statická a dynamická analýza programu - zadanie 3

## Téma:

Statická a dynamická analýza neznámeho programu, spätný preklad (disassembling).

## Platforma:

OS Windows, Intel x86.

**Termín odovzdania:** 11. cvičenie.

**Hodnotenie:** 10 bodov. V zmysle podmienok udelenia predpokladu na vykonanie skúšky minimálne 6 bodov.

## Text zadania:

Pre zadaný program `strstra.exe` nájdite s použitím nástrojov IDA, Ghidra alebo OllyDbg akceptovaný reťazec. Vypracujte pritom nasledujúce úlohy:

- Statickou analýzou pomocou nástroja IDA (Ghidra, OllyDbg) zistíte aká je správna dĺžka akceptovaného reťazca. Odpoveď, resp. postup, zdôvodnite. (1 bod)
- Uvedte aký je tvar akceptovaného reťazca. Odpoveď aj postup podrobne zdôvodnite. (2.5 bodu)
- Stručne uvedte aké argumenty a návratové hodnoty majú nasledujúce funkcie z Windows API: `DialogBoxParam`, `GetDlgItemText`, `MessageBox` a aký je ich účel. (1 bod)
- Na akých adresách sa volá `GetDlgItemText` a aký je jej význam (čo spôsobí)? (0.5 bodu)
- Na akých adresách sa volá `DialogBoxParam` a aký je jej význam (čo spôsobí)? (0.5 bodu)
- Na akej adrese sa volá `MessageBox` v prípade správne zadaného reťazca a s akým textom? (0.5 bodu)
- Vytvorte upravený program (nový `exe` súbor) ktorý akceptuje reťazec vytvorený z vášho mena (v prípade potreby skráteného alebo doplneného o ďalšie znaky, napríklad z priezviska). Zmeny robte v texte (kóde) programu, v dátach len v nevyhnutnom prípade. Uvedte postup. (4 body)

Poznámka: Pri odovzdávaní zadania môžete byť požiadaní o zmenu akceptovaného reťazca.

Riešenie odovzdajte v jednom textovom súbore s príponou `.txt` (ASCII, môže byť diakritika, žiadne `.doc/.ods` a pod.) a modifikovaný spustiteľný súbor s príponou `.exe`.

## **Linky:**

IDA [https://www.hex-rays.com/products/ida/support/download\\_freeware/](https://www.hex-rays.com/products/ida/support/download_freeware/)

Ghidra <https://ghidra-sre.org>

OllyDbg <http://www.ollydbg.de/>

Problematika reverzného inžinierstva (použitie, výhody, ochrana aj právne aspekty)  
<https://www.tme.eu/sk/news/library-articles/page/56932/reverzne-inzinierstvo-v-com-spociva-tato-reverzna-technika-a-je-legalna/>