(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 získania zápočtu minimálne 6 bodov.

Text zadania:

Pre zadaný program strstr.exe nájdite s použitím nástrojov IDA a OllyDbg akceptovaný reťazec. Vypracujte pritom nasledujúce úlohy:

- Statickou analýzou pomocou nástroja IDA zistite aká je správna dĺžka akceptovaného reťazca. Odpoveď, resp. postup, zdôvodnite. (1 bod)
- Uveďte aký je tvar akceptovaného reťazca. Odpoveď aj postup podrobne zdôvodnite. (3 body)
- Stručne uveďte 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. Uveďte postup. (3,5 bodu)

Poznámka: *Pri odovzdávaní zadania môžete byť požiadaný 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:

https://www.hex-rays.com/products/ida/support/download_freeware/
http://www.ollydbg.de/

pre Linux - GHIDRA https://ghidra-sre.org