Exercises

01 - intro

Exercise 101 - replace `RtlMoveMemory` with `memcpy`.
Exercise 102 - replace messagebox payload with reverse shell, compile and run.
Exercise 103 - reserve and commit memory for the payload with `VirtualAlloc` with `RWX` memory protection.

02 - WINAPI

Exercise 201 - update `main()` function: get ip address and port from command line args.
Exercise 202 - use `netcat` as server, then use `metasploit` as server for reverse shell.

03 - injection

Exercise 301 - replace messagebox payload with reverse shell, compile and run.
Exercise 302 - run shellcode injection by user and try to inject to process with admin privileges.
Exercise 303 - in DLL injection example update your dll logic.

04 - evasion

Exercise 401 - update XOR encryption example - generate random key for encrypt/decrypt.
Exercise 402 - in the function call obfuscation example update code: add obfuscation trick for all WINAPI functions.
Exercise 403 - in the winapi hashing example - use example from intro and add hashing for at least one WINAPI fucntion.
Exercise 404 - in the winapi hashing example - use example from intro and add hashing for all WINAPI fucntions.

05 - persistence

PROF

Exercise 501 - try to combine any two persistence techniques in one script. Enjoy!

06 - cryptography

Exercis 601 - update payload encryption logic: try to combine XOR and base64 algo for encrypt/dynamic decrypt payload.