Lab_02-1

1. Solutions:
    a. 0x04011a0
    b. Checks for internet connection using http://reversing.rocks. If connected, calls a subroutine
        i. Uses imported function InternetCheckConnectionA
2. Solutions:
    a. The result from calling InternetOpenA(“ntoskrnl”,0,0,0,0), “reversing.rocks”, 0x4d2, 0, 0, 3, 0, 0
        i. Result from InternetOpenA is the connection handle
        ii. “reversing.rocks” is the target server to connect to
        iii. 0x4d2 is the port = 1234
        iv. Default username
        v. Default anonymous password
        vi. Use service 3 (HTTP)
        vii. No flags
        viii. No special context
    b. Opens a connection to reversing.rocks before passing execution to a subroutine. Closes the connection when subroutine returns
3. Solutions:
    a. Lots of calls are made to imported functions to find and loop through files from an internet connection
    b. FindFirstFileA, HttpOpenRequestA, HttpSendRequestExA, InternetWriteFile, FindNextFileA, HttpEndRequestA, InternetCloseHandle, and FindClose
    c. Send all files that match “*” via HTTP requests
4. Exfiltrate local files from the local machine to a remote server

Lab_02-2

1. AllocConsole, FindWindowA, ShowWindow, fopen, time, fputs, ctime, and fclose
    a. AllocConsole makes a console, FindWindow creates a window, ShowWindow shows a window, the rest are standard C functions
    b. “\\WINDOWS\\lzwindowlz.av”, “\nStarted logging: “
2. Solutions:
    a. fopen, GetAsyncKeyState, fputc, fclose, fputs, fseek, ftell, malloc, and fread
    b. Large switch statement
3. Keylogger
    a. Sending emails to “my.inbox.com”, calls to GetAsyncKeyState, the existence of the file \\WINDOWS\1zwindow1z.av
    b. The aforementioned file is used as a buffer to store keypresses in before emailing it and clearing it