Homework 4

CIS 4930 / CIS 5930
Offensive Security
Spring 2014

Due February 17, 2013, by MIDNIGHT
Worth: 100 points (4% of final grade)

Electronic turn in (Turn in via email to instructor. Email address is redwood@cs.fsu.edu)
The email must be titled in the following format:
"[OCS2014] hw4 <your last name>". (where <your last name> is your last name)
Example: [OCS2014] hw4 redwood

This homework pertains to all the topics covered during our reverse engineering week. All assembly questions are in Intel ASM format.

1) [18 points, 3 points each] Below are some single (stand-alone) x86 assembly instructions. Tell me what the instructions do (down to register details), what the variables are (whether they are local variables, global variables, static variables, or parameters for a function), the size of the variables (when applicable):

```
a) mov      DWORD PTR [ebp-0x4], 0x8
b)  mov     eax, DWORD PTR [ebp+0x8]
c) lea      eax, [ecx + eax*1]
d) call     _htons
e) cmp      [ebp+0x8], 0
f) ret
```

2) [60 points, 7.5 points each] Download the key_checker.exe file from:
the in class exercises archive (see http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/reversing/FSU_Reversing_binaries.zip)
This file checks for some file, runs a check on the data on it, and then prints out a success or failure message. Your task is to apply all the techniques we talked about in class to reverse engineer this program to answer the following:

a) What is the calling convention for main?
b) How many different sections are in the binary?
c) What permissions does the .text section have?
d) What permissions does the .data section have?
e) List all imported function that contain the substring "str" (not case sensitive)
f) At what address is the return value of fopen checked, and what value is checked against?

i) Looking at the binary, how many bytes are available on the stack for local variables?

j) In your debugger of choice, set a break point on the call to fread and show the 4 parameters being passed to the function. (screenshot, copy/paste, whatever works)

3) [**22 Points**] Turn in a file that successfully passes the key_checker.exe's checks (provide it as an attachment in the submission email).

EXTRA CREDIT [25 points = (+1% on final grade)]

Download the crackme challenge problem at this URL, http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/reversing/CRACKME2.zip

Try to crack it, to figure out the correct input to get the flag. Your solution will be the *flag*, in addition to a brief writeup on the steps you took to get the flag.