CAPTURE THE FLAG REPORT

Author or Team: [Insert the names of all people who worked to get the report finished]

EXECUTIVE SUMMARY:

The target file was named [insert file name] downloaded from [web page or repository].

The file was actually [describe the file, was it renamed or compressed or otherwise obfuscated to hide its true purpose].

It appeared the file was supposed to [insert what it appears the intent was] but actually [insert what the file appeared to actually do].

INTRODUCTION:

I/we had the opportunity to reverse engineer a file and edit it to perform a modified task.

This was done through [name the tools used] which [describe what features of the tools were used].

I/We then proceeded by [for example, trial and error … describe the methods used] to modify the file to [specify the achieved outcome here] by employing methods detailed in the next section.

The Findings section details how I/we successfully gained access to hidden information and the significance of this information.

TOOLS AND METHODS:

The tools used to attack analyse the file are common tools that are free…

[Use this section to briefly describe the tools. Add screen grabs of the tools if this is appropriate]

FINDINGS:

From Steps 3 and 4 of the “Capture the Flag Report” instructions in the Word document, briefly document the following items that were identified while analysing the binary file:

1. What address does the Portable Executable Signature start at?
2. What is the value of the Portable Executable Signature?
3. What is the target Machine value?
4. How many sections does the binary say it has?
5. What is the Time Date Stamp in hex and the human readable value?
6. Where is the Symbol Table?
7. How many symbols are in the symbol table?
8. What is the Optional header size?
9. What are the Characteristics flags that were set?
10. What is the Magic number?
11. What is the Linker Version?
12. What is the Target Subsystem?
13. What else can be determined from the binary file, such as information about the machine that did the compiling?
14. Describe what the code actually does

CONCLUSION:

[This is the place to reflect on the exercise. Below is just suggested text. Replace it with anything that needs to be said]

This exercise was beneficial due to [insert reasons here].

It is one thing to learn in a class how to utilize scanning programs.

It is a completely different thing to be able to apply our skills in a real-ish world scenario.

The tools that I/we learned the most from were [insert tools and reasons here].

These were programs I/we had not gone over that extensively until this report.

It was also an exercise in teaching ourselves how to interpret program documentation.

The largest take away from the project was [insert the one or more important things you learned]**.**

Q: If you had to do this challenge again, what would you differently?

A: [Insert answer here]