Project Two Grading Rubric

____ / 10pts - **Overview**

- Brief overview of the project, tell us about the RPISEC Nuke
  - What are some of its features?

____ / 10pts - **Key Auth One** - **Checkpoint #1 Due 1:59pm Friday, May 1st**

- What is the vulnerability? How can key auth one be bypassed?
  - Gets 'KEY CONFIRMED' for key auth one

____ / 15pts - **Key Auth Two** - **Checkpoint #2 Due 1:59pm Friday, May 8th**

- What is the vulnerability? How can key auth two be bypassed?
  - Gets 'KEY CONFIRMED' for key auth two

____ / 15pts - **Key Auth Three** - **Checkpoint #2 Due 1:59pm Friday, May 8th**

- What is the vulnerability? How can key auth three be bypassed?
  - Gets 'KEY CONFIRMED' for key auth three

____ / 20pts - **Nuke86 Programming**

- How is the nuke code checksummed?
  - Describes the algorithm
- Can you write a nuke86 program to detonate on 'GENERAL DOOM'?
- Can you exploit nuke86?
  - Gets arbitrary ROP
  - Gets the project2_priv .pass

____ / 10pts - **Exploit Automation**

- Is your exploit 100% automated?
  - Can I run a single command/script (python, bash, etc) and get the flag?
- Degree of usability and portability otherwise
- Include your final exploit script as a file separate from the writeup

____ / 20pts - **CTF Style Writeup** - **Project Due 1:59pm Friday, May 15th**

- Goes into sufficient details regarding all of the above points
- Readability - Is it fun and easy to read? Visually interesting?
  - Use of images, code snippets, or diagrams might help

____ / 5pts - **Bonus**

- Did you find any of our easter eggs?
  - Explains them / how they work

_____ / 100pts - **Final Grade**

Checkpoint #1 - **Due 1:59pm Friday, May 1st**

Since this will be your first exposure to the project and reversing it, you are only expected to complete the first key authorization. The first checkpoint is to identify the vulnerability in key authorization #1 and automate the process of exploiting it. It is only worth 10% of your final project grade as it is the simplest of all the vulnerabilities to identify and exploit.

We expect a simple explanation of what the vulnerability is, and how to exploit it much like your lab challenge descriptions. With your checkpoint #1 submission, please include an exploit script that will bypass the first key authorization. Feel free to ignore the 'Overview' part of the rubric above. You will be completing that section with your final writeup of the project, it is not due with checkpoint #1

Submit to: mbespring2015+**checkpoint1p2** [at] gmail.com

Checkpoint #2 - **Due 1:59pm Friday, May 8th**

The second checkpoint is worth 30% of your final project grade. Key authorization #2 and #3 will be a bit harder to exploit and automate than the first authorization, but you should have a feel for the project at this point and will already have your exploit script underway.

As with checkpoint #1, we expect a simple explanation of what the vulnerabilities are, and how you can exploit them. With your checkpoint #2 submission, please include an exploit script that will bypass the second and third key authorizations.

Submit to: mbespring2015+**checkpoint2p2** [at] gmail.com

Final Writeup - **Due 1:59pm Friday, May 15th**

The final writeup and any other Project #2 materials are due by the time stated above. Keep in mind that the final writeup is all encompassing, therefore you are expected to include the details regarding checkpoint #1 and checkpoint #2. It might be wise to simply start your writeup immediately, and build upon it as you progress - submitting its current state for Checkpoint #1 and Checkpoint #2.

The final writeup should be in the same form as the Project #1 writeup. It is expected to be a PDF file describing the points in the rubric above. You **MUST** include your exploit script as a **SEPARATE FILE** not embedded in the PDF.

Final course grades are due to the registrar by 9am Monday, May 18th therefore **it is imperative that you submit your project on time, otherwise you will waive your right to dispute your grade and may only receive credit for checkpoint #1 and #2.**

Submit to: mbespring2015+**project2** [at] gmail.com