Introduction:

We are not expecting a full penetration test report from you. Please don't get scared or overwhelmed. If anything, you can just follow exact steps providing a response per each question down below, and write the report. That being said, we still want to provide you a full experience of what a penetration testing is; testing, **and** reporting. Down below is a sample template of penetration test report. It is intentionally shortened, as we do not expect a full blown penetration test, because we understand you all have schoolwork as well. We will expect an executive summary of the test as well as technical details.

After writing the report, please send the report to Mr. Hunter. huntergosu123@gmail.com

* If you are really interested in penetration reporting, please check out the link!. If you don't have much time, read the example template; starting from page 18. Another link that is good is this list of public reports hosted on github, which can be found here.

<TITLE PAGE>

Name, company name, dates of the test, etc. Make it look nice.

<TABLE OF CONTENTS>

Google docs can auto generate table of contents. Please do that, like so:

1. Executive Summary - No more than 7 sentences!

a. Who - Who did the testing? For whom? ***a,b,c can be summarized to 1 line**
b. What - What was the scope of the testing?
c. When - When was the testing performed?
d. Why - What was the objective?

e. Vulnerability summary - Provide a high level view. No technical details are required.
   i. What did you find? How many? In which areas?
   ii. Small Tables/Graphics would be nice
      1. Probably not applicable in this test
f. Potential Risk (csec101) / Impact of these vulnerabilities
   i. If an attacker were to gain knowledge of these vulnerabilities, what could've happened?
g. Solution recommendation - High level
   i. Note that solutions have been included with findings and findings have been rated on some scale to note severity, but also note its up to internal auditors to diagnose the threat of each vulnerability depending on the criticality of the infrastructure involved.

2. Detailed Findings

a. Target Summary **Table**
   i. IP, System Type, OS Information, Open Ports (number, protocol, service name)

b. Detailed Findings of each service
   i. Summary of vulnerability (service name, vulnerability name, severity)
   ii. Details
      1. Service Name
      2. Risk Level - Low, Medium, High, Critical
      3. Source / root cause of vulnerability
      4. Vulnerability description + Ways to exploit them
      5. Solution recommendation

3. [Optional] External References and links, if there are any