You have been tasked by your instructor to perform a penetration testing engagement on both network and web application. The following is the statement of work, to breakdown the activity that needs to be done within the duration of the engagement.

# Final project PART A (20%)

Please follow the instructions below for your part A of your final project.

* Your team should identify three network vulnerabilities (two for initial foothold - and one privilege escalation technique), and two web application vulnerabilities from your metasploitable2 machine. (Totalling to 5 vulnerabilities)
  + If your group has 3 people, you will need to have three (3) web application vulnerabilities – totalling to 6 vulnerabilities (3 network, and 3 application vulnerabilities).
* ***Note that the exploit that leads directly to root does not count as “privilege escalation” but rather initial foothold.***
* Read and understand the vulnerabilities, their impacts, and ways to mitigate them.
* Use the accompanied template and populate it with your observations.
* You will have exactly two weeks to complete this task and submit it.
* Mark deduction of 10% will occur every 1 late submission day for up to three days. Submissions that are more than three days late will be marked 0.

***Note: DO NOT RE-USE ANY EXPLOITS OR VULNERABILITIES THAT WE USED IN ANY OF OUR PREVIOUS LABS***

# Final project PART B (14%)

* Taking the previous document that you created for Part A, create a full penetration testing report.
  + Please hand this in no later than one (1) day before your presentation date.
* Your team will then be presenting your observations to me (your client) – of what you have identified within my network environment.
  + You will be required to walk me through your report.
  + Each team member would need to be able to explain at least 1 network vulnerability and 1 web application vulnerability.

Presentation will be graded based on the following criteria:

* Students’ ability to communicate observations at a high level.
* Students’ ability to communicate observations at a technical level.
* Students’ ability to communicate the impact statement and recommendations/mitigation strategies.
* Students’ ability to answer questions relating to the identified observations.

Project Grade Breakdown

*Part A*

|  |  |
| --- | --- |
| **Criteria** | **Points** |
| Summary of Findings | 5 |
| Vulnerability Details:  FD1.3.1. Finding Name  FD1.3.2. Affected Resource (WHERE DID YOU FIND IT?)  FD1.3.3. Method of Finding (HOW DID YOU DISCOVER THE VULNERABILITY?)  FD1.3.4. Description (Screenshot of the vulnerability + severity rating)  FD1.3.5. Exploitation (Steps How did you identify the proper exploit and how you exploited?)  FD1.3.6. Impact  FD1.3.7. Likelihood  FD1.3.8. Risk  FD1.3.9. Recommendations to fix | 5 vulnerabilities X 3 marks each. (15 points) |
| **Total** | **20** |

*Part B*

|  |  |
| --- | --- |
| **Criteria** | **Points** |
| Executive Summary | 3 |
| Observations Summary | 3 |
| Observation details | 3 |
| Q&A | 5 |
| **Total** | **14** |