Group Name: Your Group Name  
Student Names: First (Lead), Second, Third  
Emails: Your emails for first, second and third  
Submission Date: When submitted  
Class Name and Term: CSE468 Fall 2018

Project Title

# Executive Summary

Consider your team is reporting to the c-level regarding to the project outcomes and suggestions to fix the vulnerabilities and future actions (e.g., upgrade, purchase new hardware/software, training, next-pentest schedule, etc. )

# System and Network Setup

Draw a diagraph and provide descriptions about the system network setup, include:

* topology,
* network configurations (IP addresses, etc.)
* initial reachability among network nodes

# Software

Describe major software and network services are used in this project to accomplish your goals.

# Description

## Group Formation and Strength Description

Describe the background of each group members. How you allocate the PenTest tasks among group members.

## Pentest Deployment

Provide a step by step project description. Consider a user manual style to allow others to know what you have done and your procedure should be easily reproduced. Note that the description should be illustrated based on screenshots you captured in the ThoTh Lab. You should articulate clearly the tasks are performed by which group member. Your work should have evidence and corresponding illustrations, e.g., providing configuration files if necessary as attachment in the appendix.

If you have been successfully compromised the system by exploring the vulnerabilities, please also provide description on how you do it.

## Pentest Results

Describe identified vulnerabilities including vulnerability descriptions and potential damages to the system, and suggested remedies. It will be good to provide table to summarize your findings.

# Pentest Conclusion

Provide a summary of pentest results and next step plan. Interesting discovers, tips, tricks, lesson learned from this project, etc.. Provide a self-assessment about your project and provide comments to this project.

# Appendix A: Presentation Link

Provide link such as youtube links (less than 3 minutes) of your project presentation (consider this is a reporting to c-level folks).

# Appendix B: Working Logs

Document all the activities that you team members that had investigated into developing/installation/exploiting the systems. The working logs allow you to figure out what’s wrong and how to roll back in case mistakes occur. Please use provided log template files.

# Configurations and Developed Source Codes

Provide a list of used configurations and developed source files (or gitlab/github links). In your configuration/source code file, please with well-marked comments. A good practice is to provide comments where you made changes, something like:

// Your Name: comments

# Your Name: comments

/\*

Your Name: comments

\*/

The comment format depends on your used system files and programs.

# Business Value of the Pentest

Imaging your team works on a pentest for a specific industry, e.g., bank, healthcare, public services, etc. Answer the following questions to address the business value of the project.

|  |
| --- |
| Q1 What’s the major usage of the service with identified vulnerabilities? |
|  |
| Q2 What’s the impact of security issues to a specific industry (in general)? Please use an example. |
|  |
| Q3 What’s the security issues that you identified in the Pentest? |
|  |
| Q4 What’s the executable approaches such as assumptions and issues that may impede your plan of Pentest and how to address these issues? |
|  |
| Q5 From the business aspect, what’s pros and cons for fixing these security issues? Please explain it by using an example in the identified business. |
|  |
| Q6 Have you considered one (or multiple) alternate approaches to deploy pentest? Can you address pros and cons of your current solution vs alternatives. |
|  |

# References

Reference is optional, but nice to have to allow others to read your report with additional linked source for validation and learning.

1. Wireshark, available at <https://www.wireshark.org/>, accessed by 8/31/2018.
2. Postel, Jon. "RFC 791: Internet protocol." (1981).