Lab 05: Random War

Turn in a Word or PDF document to D2L

Notes

The lab is available in the Learn org of Dakota State University's Information Assurance Lab within the vApp <username>_CSC234_Zwach_Base. It's accessible at https://ialab.dsu.edu. You can start the vApp by double clicking on it and then clicking the play button in the Flash client or clicking Actions and Start in the HTML5 client.

The code that comprises the entire application is available within the ~/course_files/_assignments/crypto_and_random_numbers directory. Make your changes there using a text editor of your choosing. Remember, you can permanently revert your changes to the codebase at any time with the command `revertall`.

The username of the Kali VM is `student` and the password is `Password1!`.

Your goal is to defeat the game by determining the seed **without** printing it at game runtime.

Discovery

This program has one or more flaws. Identify changes you'd make and why.

1. *(6 points)* Review the source code for the application of interest (war.c).
    a. **Provide screenshots** of vulnerable or otherwise flawed code segments. Be specific.
    b. Explain each issue in your own words.
2. *(4 points)* Write a program to determine the seed and another program to let you know how to win the game. Printing the seed within war.c is **not a valid solution.**
    a. **Provide screenshots** of your code
    b. **Provide screenshots** of the execution of your code showing the generation of card numbers that will be dealt.

Remediation

After finding the flaws, use your knowledge and available resources to modify the source to follow best practices and remediate any vulnerabilities.

1. *(6 points)* Modify the source code to remediate the flaws.
    a. Document your resulting source code with **a screenshot of each** of the flaws you remediated.
    b. Explain how each of your changes fixes the flaw
2. *(4 point)* Test your changes
    a. **Provide screenshots** documenting the proper operation of the application without vulnerabilities.

Bonus

For one bonus point, completely automate playing more than 990 rounds of the game. Complete automation in this case can exclude seed discovery and up to 5 hands played at the beginning. Upload your source code screenshots, and an example of the last 10 rounds of a

1000 round game to the dropbox titled War-Bonus for up to 1 bonus point (1% impact on your grade)