LinkedRooms

Introduction

LinkedRooms is our reverse engineering challenge. Reverse engineering is all about going into the code of a program and finding vulnerabilities.

Rather than conducting an exploit, reverse engineering is all about investigation. Pay close attention to what the program is doing and see if there are any similarities to what you have done in the past.

Tips

Try running the program to see what you can do without any tools.

Some tools that you might find helpful are

GDB (GNU DeBugger) - Step through code line at a time and follow where your code changes using breakpoints and print statements for analysis

VALGRIND - LOOK FOR MEMORY LEAKAGES AND PAIRS WITH GDB TO GIVE YOU EXACT LOCATIONS IN CODE FOR A POWERFUL ANALYSIS COMBO

GHIDRA - BUILD YOUR ASSEMBLY CODE BACK INTO READABLE PSEUDOCODE FOR EASY ANALYSIS. CAN RECONSTRUCT CODE AND SIMPLIFY CHALLENGES BY A LONGSHOT

HINTS

1. IS THERE A DEBUGGING TOOL THAT YOU CAN USE TO FIND OUT ATTRIBUTES OF VARIABLES DURING RUNTIME?
2. COMMAND: P
3. DON'T FORGET POINTER NOMENCLATURE!