

Reversus Part 2: Hack the Shapes Student Instructions

Introduction

Welcome to Hack the Shapes, where you will learn about reverse engineering video games. Recall that reverse engineering in the context of software development is about figuring out what a program does without the source code. Have you ever played a game that allows you to download and use mods made from other people? Games like Minecraft or Skyrim have very active modding communities and open-source frameworks that allow people to modify the game without reverse engineering it. For other games, frameworks and tools are only created after a long period of reverse engineering and analysis.

While reverse engineering and hacking video games can have a positive, there are also negative uses as well. This is very apparent in multiplayer games. Have you ever played an online game only to see other players using a flying or infinite health hack? This is not very fun to play against if you are on the receiving end. As a solution, game companies use anti-cheat systems to try and mitigate these techniques. While not perfect, many of these systems have done a lot to prevent players from gaining unfair advantages over others.

Other applications

These skills can translate over to application security testing and help you understand what a program does without ever needing the source code. When testing applications, you could also write a proof-of-concept exploit that demonstrate how a program is vulnerable.

Tools

Cheat Engine

Hex Editor (Optional)

Controls

Arrow Keys Movement

Z Drop \$5

Enter Interact with NPC or Info

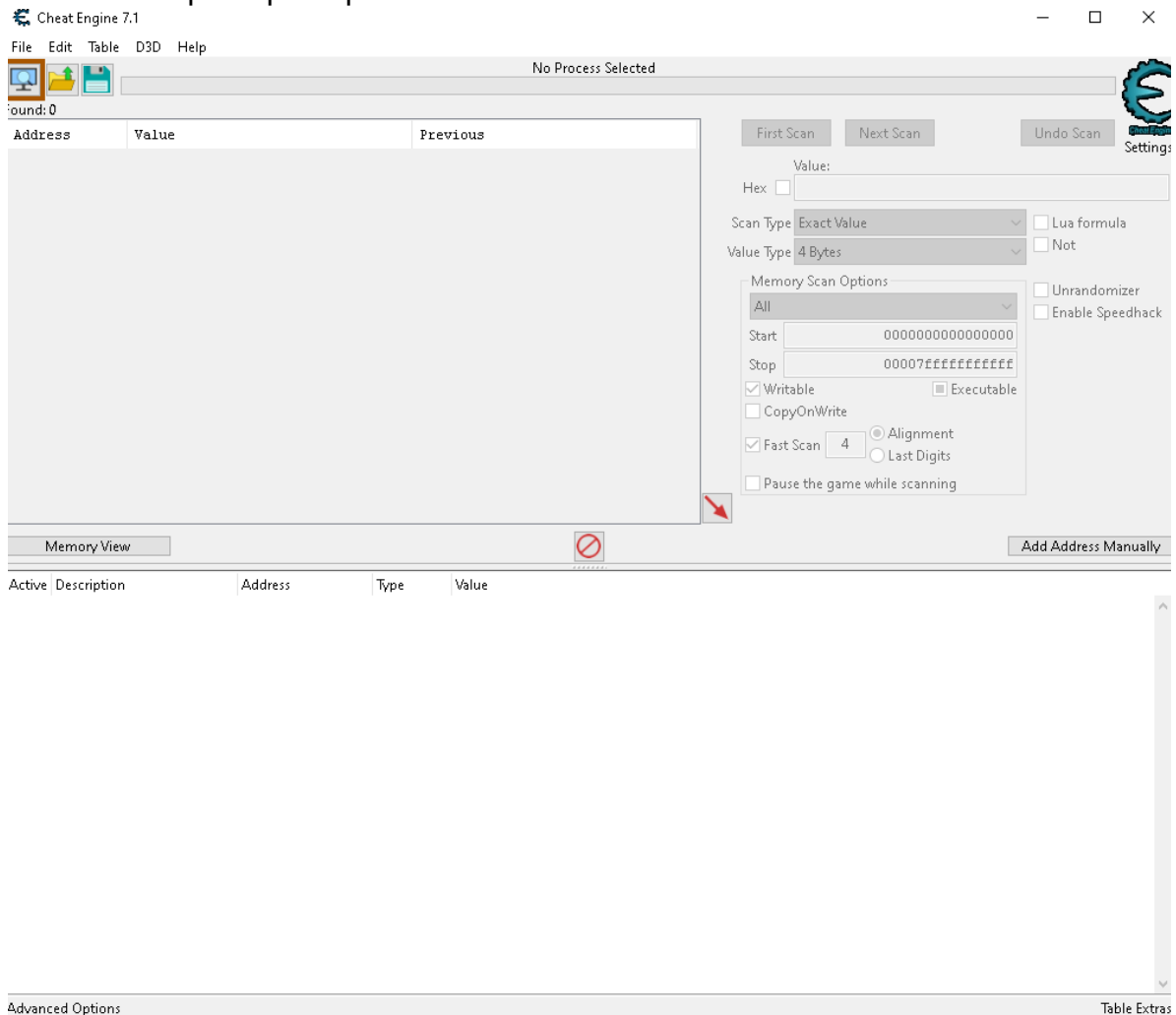
Hold Shift Run

Hold Ctrl Slow walk

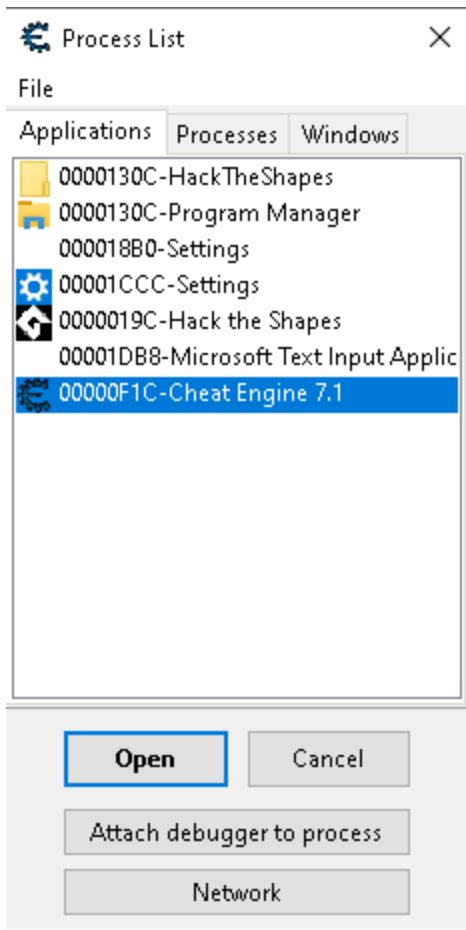
R Restart game

Setting up Cheat Engine

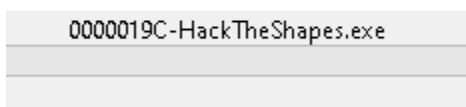
- First, make sure both Cheat Engine and the game is running.
- In Cheat Engine, click on the monitor with the magnifying glass near the top left to open up the process list.



- In the process list, find HackTheShapes.exe and click the open button.

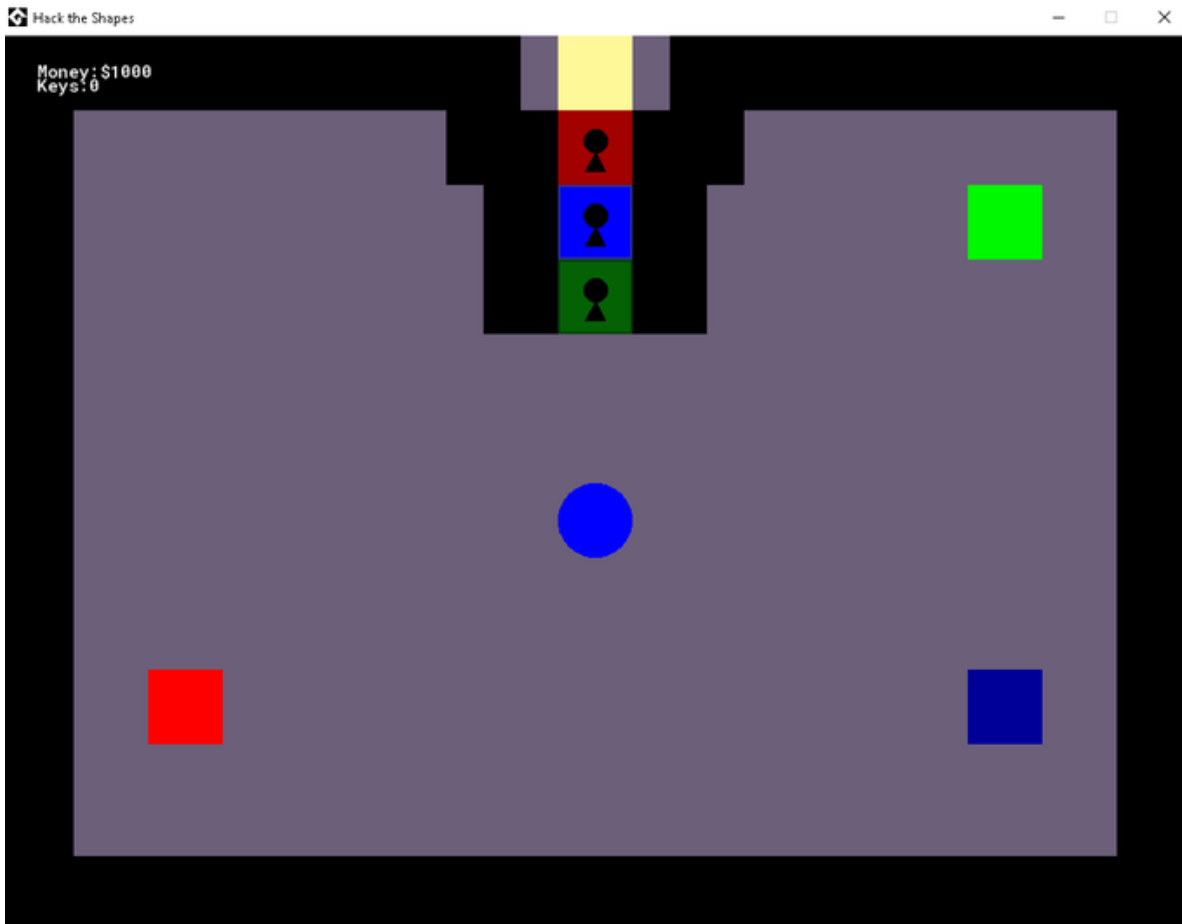


- With everything setup, you're ready to start!



The mission

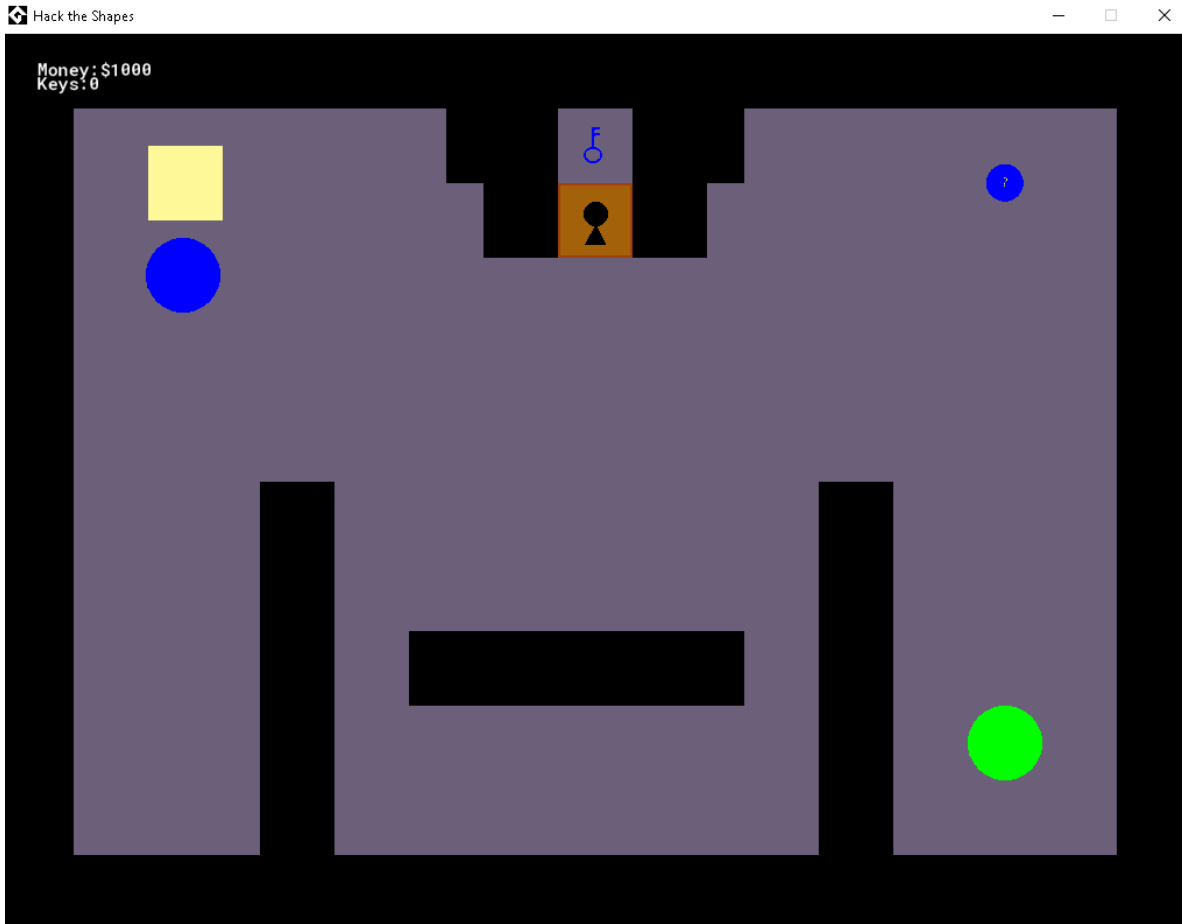
Today you will be playing a video game called Hack the Shapes. The goal is to obtain the red, green, and blue keys to remove the obstacles blocking the flag. To obtain these keys, the player must complete different levels and challenges. Each challenge cannot be completed by just playing the game and require the player to hack and reverse engineer the game.



At the hub, you will be greeted by three colored locks and three different warp points to other levels. Levels can be done in any order and there may be multiple solutions to a problem.

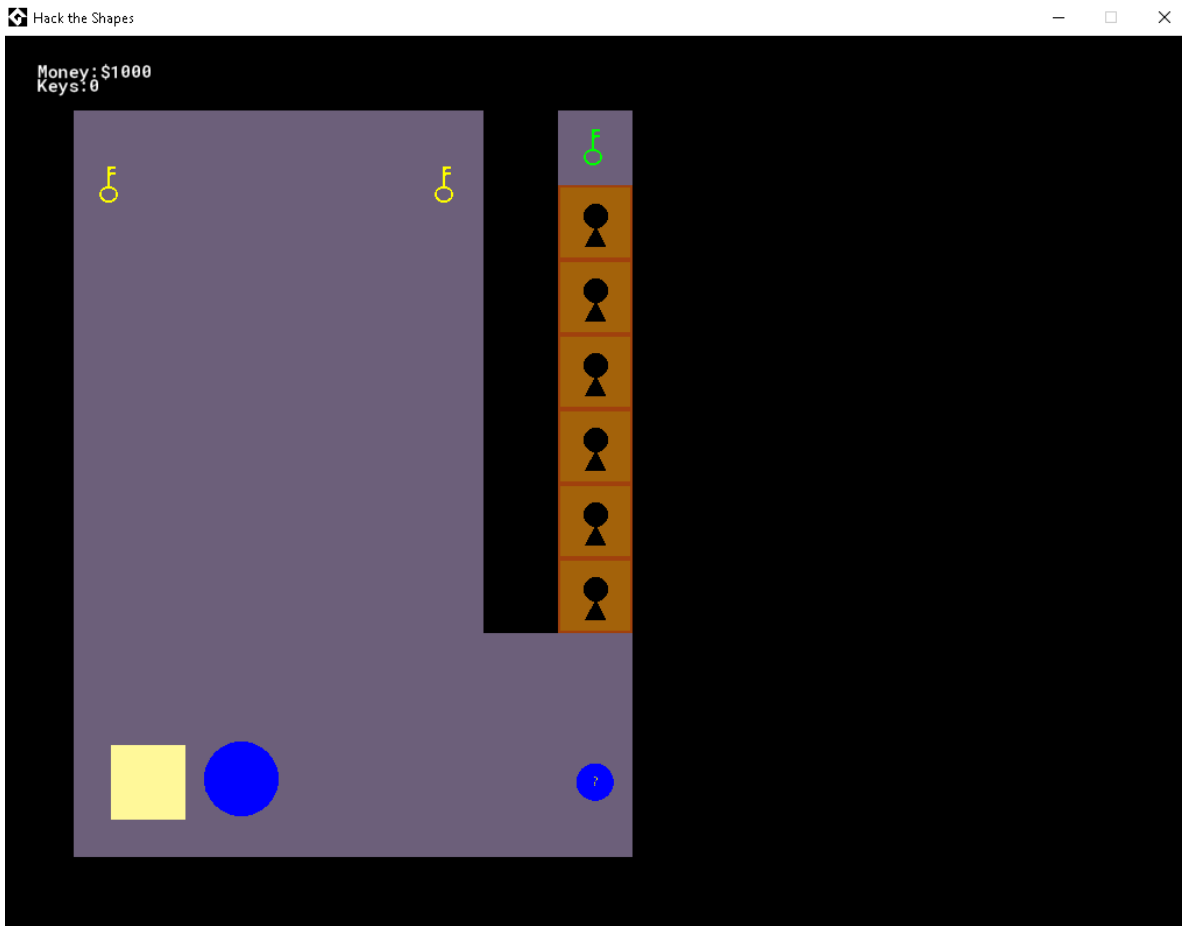
Blue Key

For this level you'll need \$10000 just to buy a key. Unfortunately, you only have a button that throws away money.



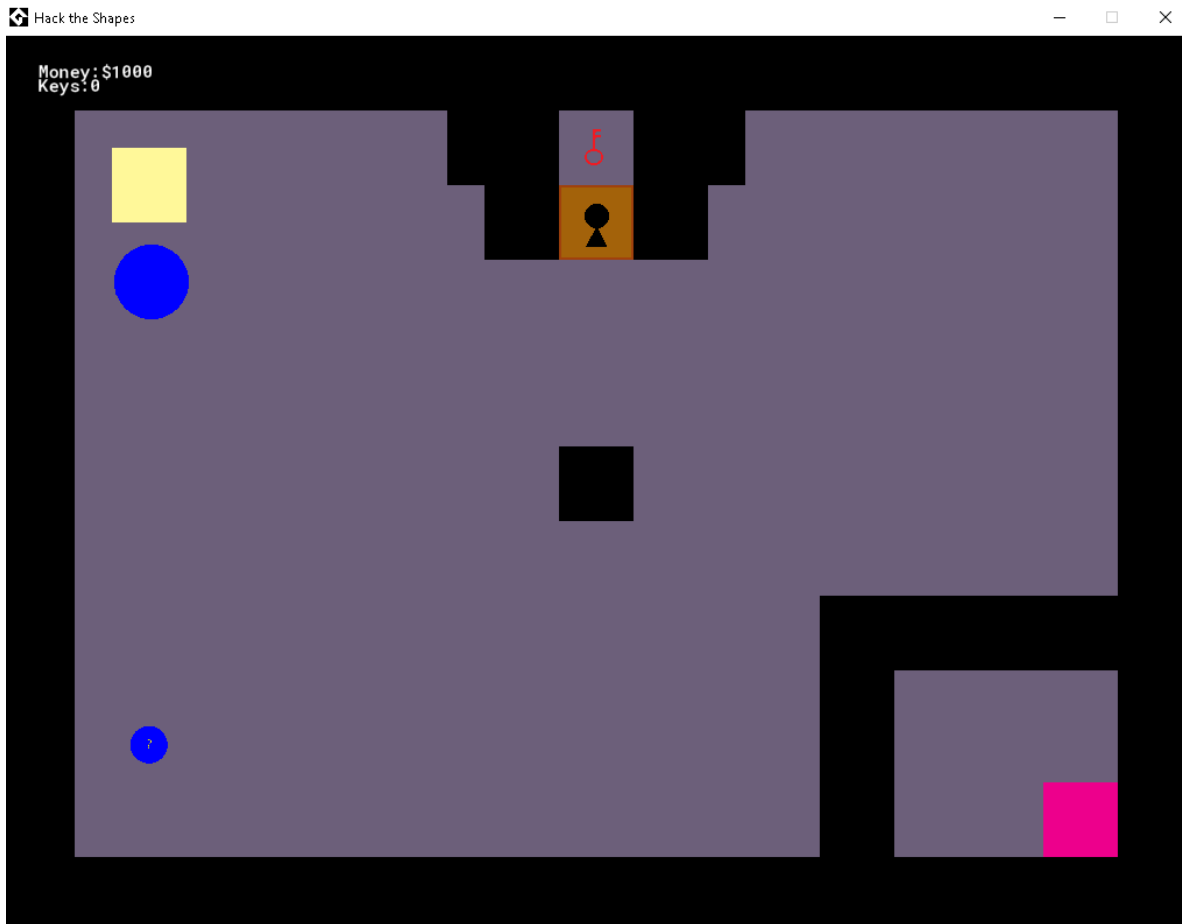
Green Key

This level has multiple locks but not enough keys. If only there was a way to give yourself more keys.



Red Key

This level requires a block to be placed on a pink square to remove the lock. Unfortunately, there is a solid wall that prevents you from progressing through normal means. Maybe there's a way to move it over there without pushing it?



Once you have gained all the special keys, you will be able to obtain the flag.

NOTES:

- When going through narrow spaces, you may not be able to go through at first due to the collision mechanics. Use the slow walk (**Hold CTRL**) to have an easier time going through it.
- When looking for the X and Y coordinates in the Red Key room, messing with certain addresses may make you go through the block. If the player starts to pass through, do not go all the way or you might get stuck and have to restart the game.
- When choosing a scan type, make sure you are set to Double as number values for this game are stored that way.
- https://wiki.cheatengine.org/index.php?title=Tutorials:Finding_values:Integers
This link might help when doing some of the game.
- If you need some extra help starting out, try out the Cheat Engine tutorial that's provided within the program.