Reversus: Hack the Shapes Student Instructions

✓ **The Big Idea: System Security**

Software and hardware work in complex ways to achieve an overall objective: This workout focuses on the complexity of software translated to memory instructions. Using reverse engineering tools and techniques, you will better understand the nature of software interacting with the system.

Describe Common Security-Related Vulnerabilities: The vulnerabilities you encounter in this lab have to do with the integrity of the software. Malicious software will often hide by injecting itself into commonly run software on a system. In this workout, you modify the software to fix an impossible game, but you could also modify the software to perform some malicious action as well.

Introduction

Welcome to Hack the Shapes, where you will learn about reverse engineering video games. Recall that reverse engineering in 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 modifications made by other people? Games like Minecraft or Skyrim have active modding communities and open-source frameworks that allow people to modify the game without reverse engineering. For other games, frameworks and tools are only created after a long period of reverse engineering and analysis.

Reverse engineering games can be helpful in better understanding systems, but there may be negative consequences. This is very apparent in multiplayer games. Have you ever played an online game and seen other players using a flying or infinite health hack? This is not 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.

⊗ Reverse engineering may be restricted in the software license you accept when installing the software. When in doubt, make sure you have permission to reverse engineer the software, and if you find any vulnerabilities, coordinate with the software provider to let them know.

Other applications

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

Tools

Cheat Engine

Hex Editor (Optional)

Controls

Arrow Keys Movement

Z Drop $5

Enter Interact with NPC or Info

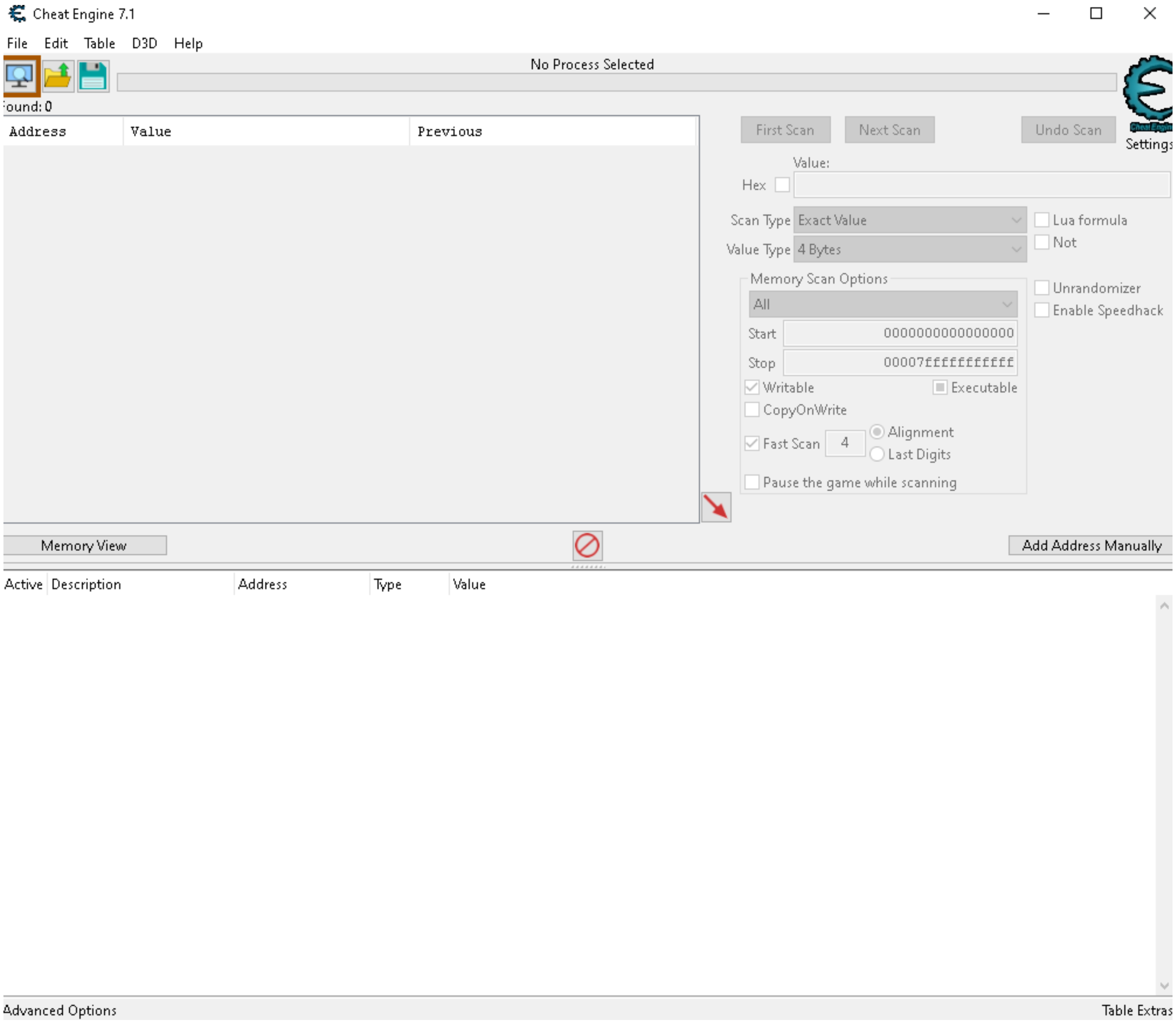
Hold Shift Run

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.



No Process Selected

Found: 0

Value:

Hex □

Scan Type: Exact Value

Value Type: 4 Bytes

□ Lua formula

□ Not

Memory Scan Options: All

Start: 0000000000000000

Stop: 00007fffffffffff

☑ Writable

▣ Executable

□ CopyOnWrite

☑ Fast Scan: 4

● Alignment

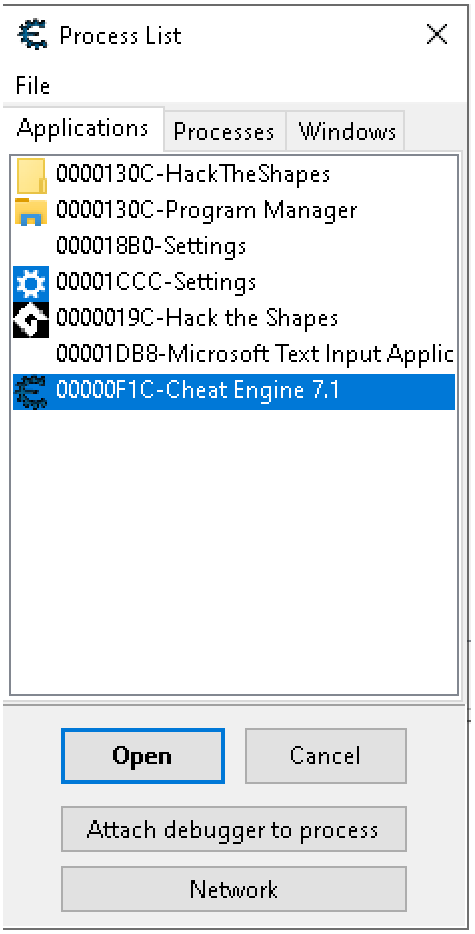
○ Last Digits

□ Pause the game while scanning

□ Unrandomizer

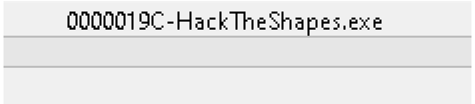
□ Enable Speedhack

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



0000130C-HackTheShapes
0000130C-Program Manager
000018B0-Settings
00001CCC-Settings
0000019C-Hack the Shapes
00001DB8-Microsoft Text Input Applic
00000F1C-Cheat Engine 7.1

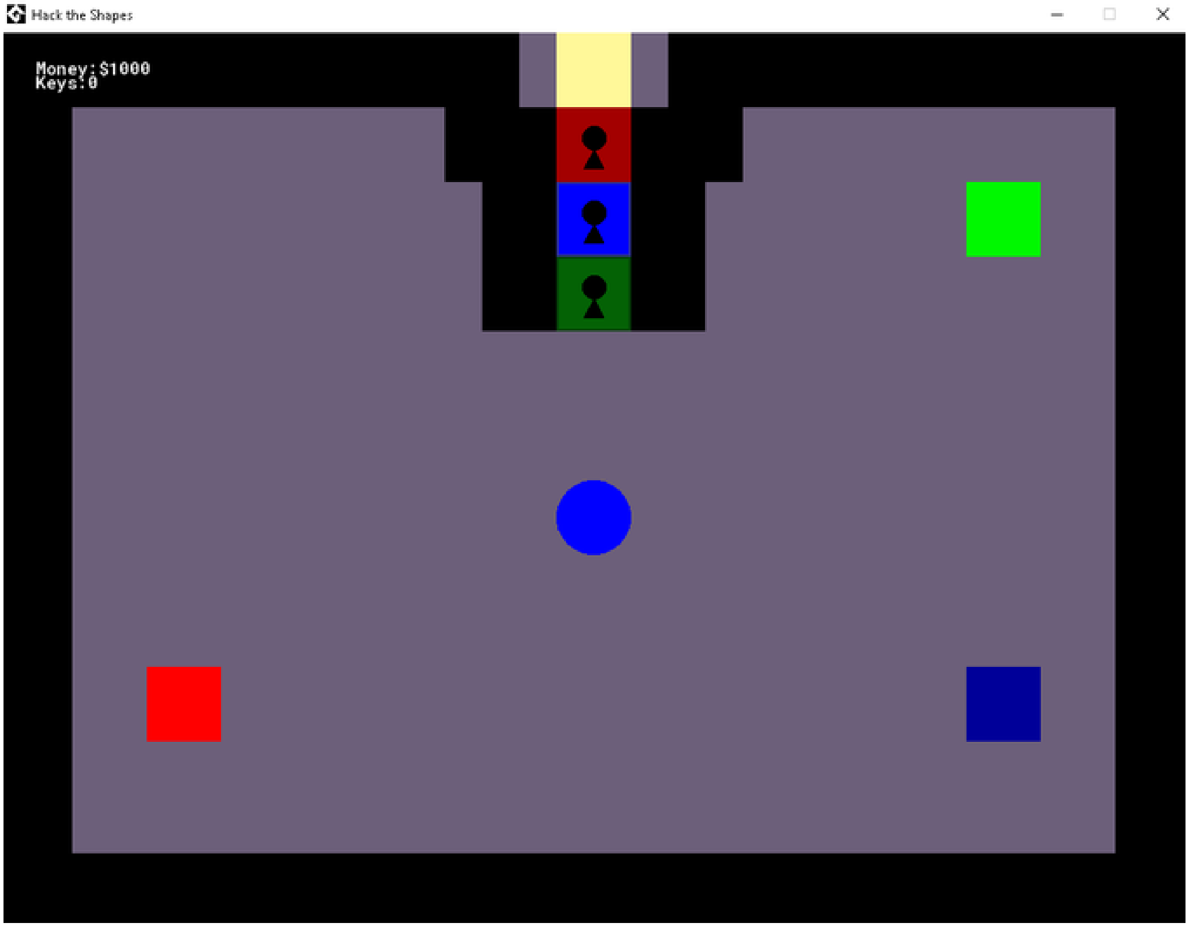
- With everything setup, you're ready to start!



0000019C-HackTheShapes.exe

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.

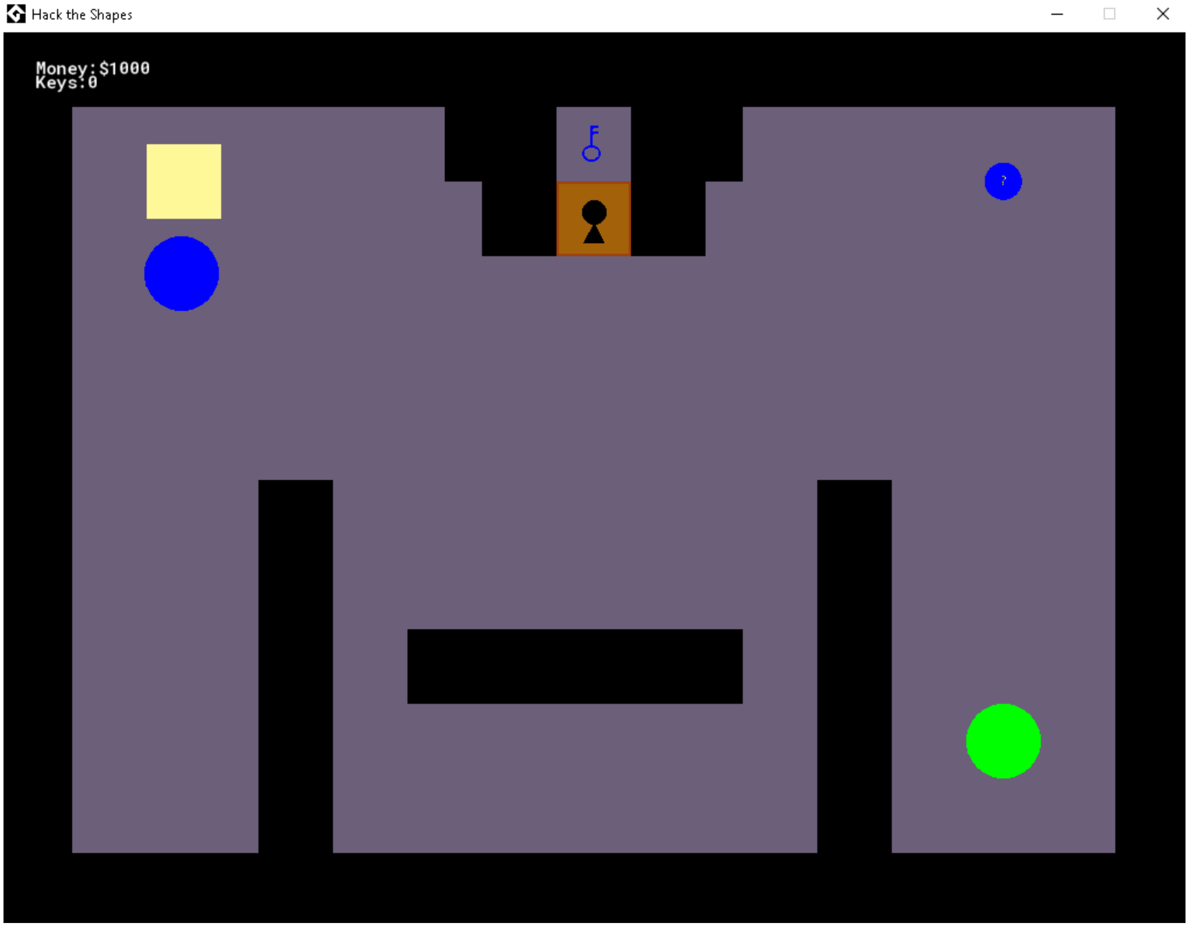


```
Money:$1000
Keys:0
```

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.

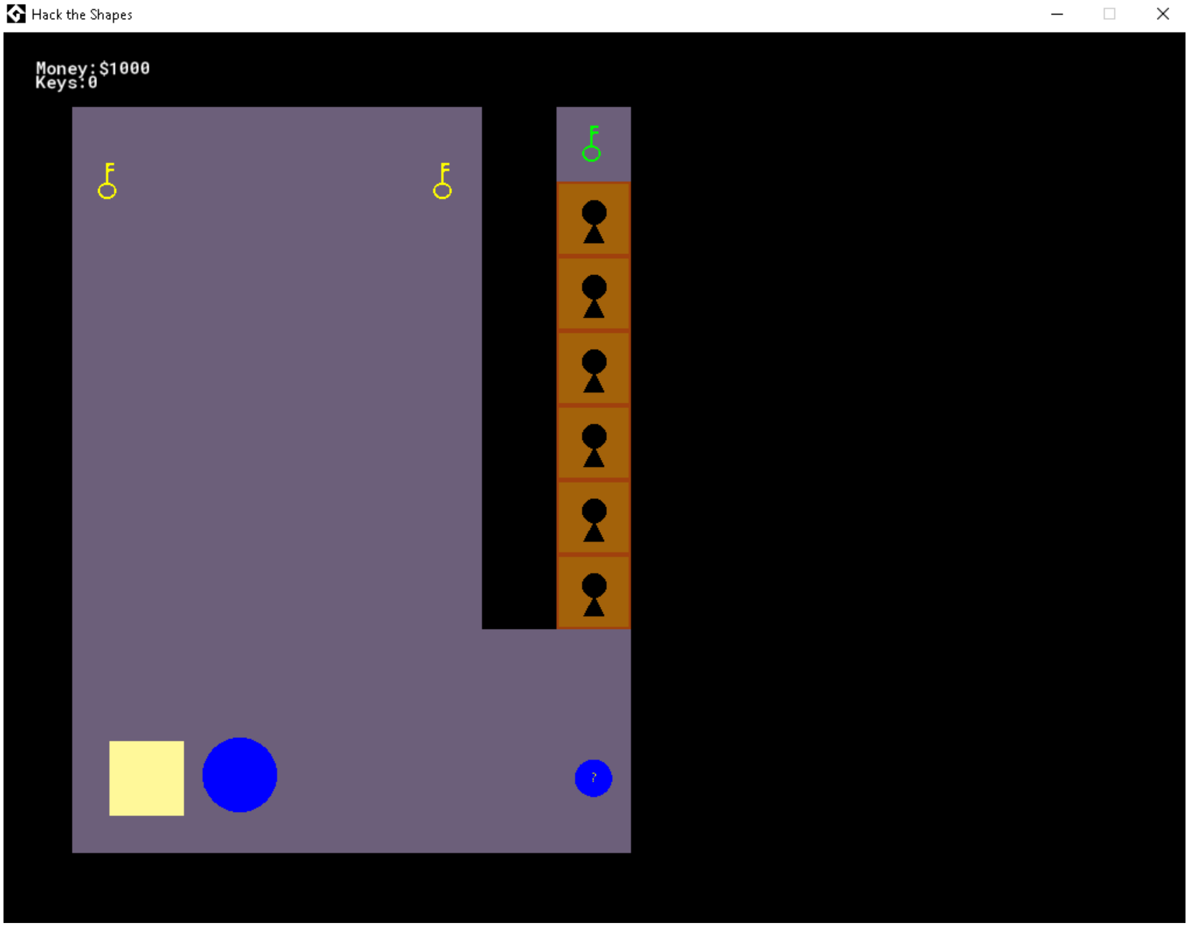
Blue Key

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



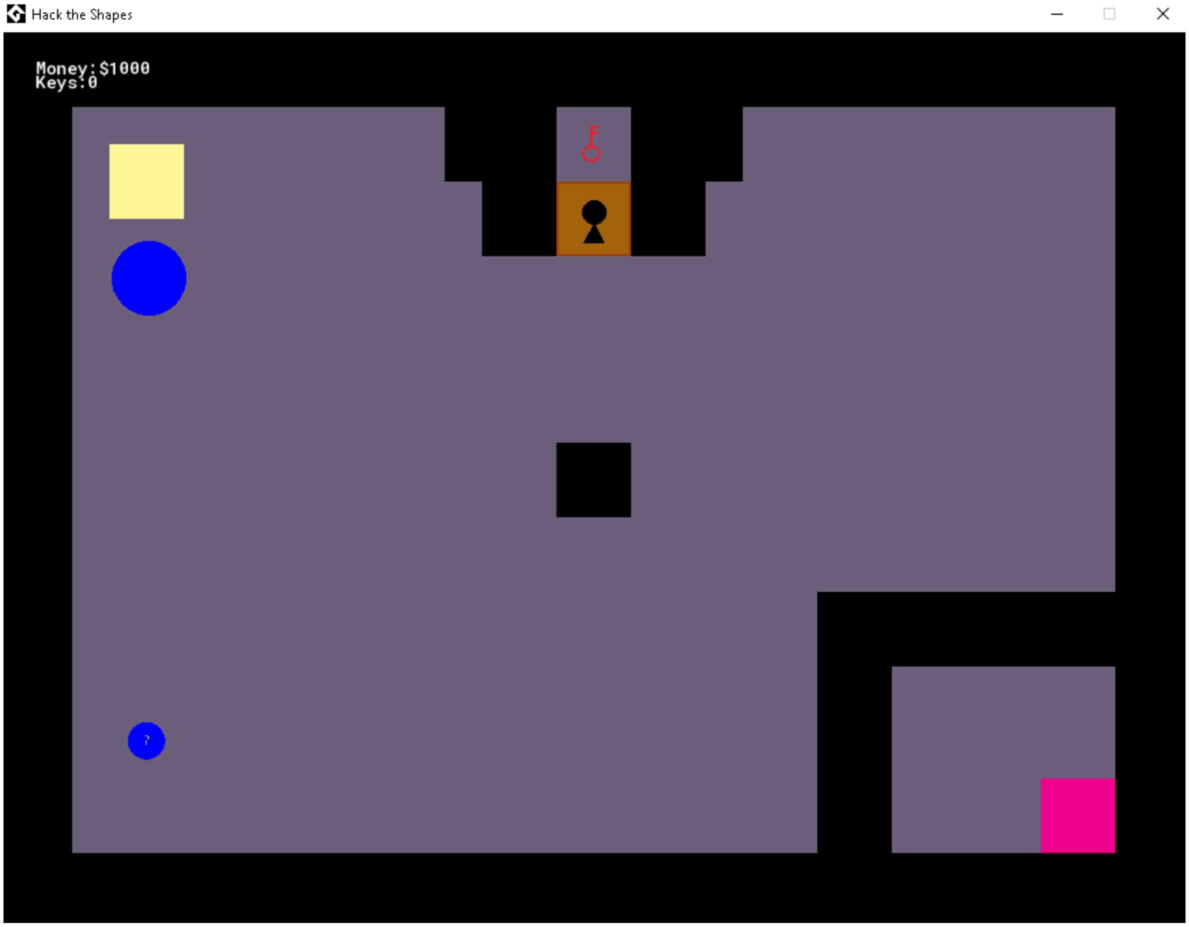
Green Key

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.