LinkedRooms : Reverse Engineering

Creator: Eddie Points: N/A

Description

LinkedRooms features a 5 node Linked-List maze that the competitor uses gdb to traverse. It allows them to figure out pointer traversal with gdb commands. They must traverse through commands like p* node->up, etc. Some nodes will point to themselves depending on the direction the user attempts to go down.

Github Path: Hack-O-Ween/LinkedRooms/

Prompt

There are rumors of a new and strange place that was in this abandoned office building. I went to check it out and was completely shocked. I don't know how I found my way out. Can you look at this simulation and figure out how to traverse the facility?

<LinkedRooms.zip>

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!

Solution

1. The user will have to get the zip files and extract the backrooms.c and LinkedRooms executable. They then can run gdb on the executable.

2. They will next have to set a breakpoint at line 10 of the program (right after the maze has been initialized) and once they hit the breakpoint they can begin traversing the maze

> l

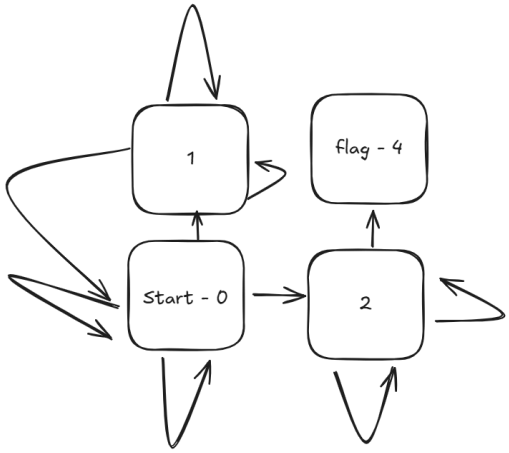
> b 10

> r

```
(gdb) l
1       #include <stdio.h>
2       #include <stdlib.h>
3
4       #include "Lists.h"
5
6       int main(){
7           //node is now the start of the maze that you can enter and evaluate
8           ListNode* node = CreateMaze();
9
10          printf("%s", "Maze Created!\n");
(gdb)
11
12          DestroyMaze(node);
13          printf("%s","Maze Destroyed\n");
14
15          return 0;
16      }
```

3. Once they have hit the breakpoint, they must print the dereferenced values of the start node that they work off of and traverse the maze using the directions (up, left, down, right)

4. Each node has a red herring for the flag however the final node is in the correct format. This will punish competitors who are too quick to jump the gun.



5. After traversing the list with pointers the correct path is:

> *node->right->up->right

The value in this node is the flag.

```
Breakpoint 1, main () at backrooms.c:10
10          printf("%s", "Maze Created!\n");
(gdb) p *node
$1 = {up = 0x555555559300, left = 0x5555555592a0, down = 0x0, right = 0x555555559360, value = "Start", '\000' <repeats 44 times>}
(gdb) p *node->right
$2 = {up = 0x5555555593c0, left = 0x5555555592a0, down = 0x555555559360, right = 0x555555559360, value = "AAAAHH", '\000' <repeats 43 times>}
(gdb) p *node->right->up
$3 = {up = 0x5555555593c0, left = 0x555555559300, down = 0x5555555593c0, right = 0x555555559420, value = "TRICK-OR-TREAT", '\000' <repeats 35 times>}
(gdb) p *node->right->up->right
$4 = {up = 0x555555559420, left = 0x555555559420, down = 0x555555559420, right = 0x555555559420, value = "flag{skin_steaker}", '\000' <repeats 31 times>}
```

Flag

flame{skin_stealer}