**Game hacking – LS (TSS)**

Game hacking, focusing on the intentionally vulnerable MMORPG: PwnAdventure3

Pwn Adventure 3: Pwnie Island is a limited-release, first-person, true open-world MMORPG set on a beautiful island where anything could happen. That's because this game is intentionally vulnerable to all kinds of silly hacks! -- <http://www.pwnadventure.com/>

The resources, including the assignments and projects: <https://github.com/CSeCIITB/LS-2024-Intro-To-Game-Hacking>

Background on Game Hacking and setting up the game client and server for future weeks.

* **Timeline:**  
  Week 1: 27 June - 7 July   
  Week 2: 8 July - 14 July  
  Week 3: 15 July - 21 July  
  Week 4: 22 July - 28 July
* Week 1-3: Weekly content will be released along with corresponding assignments.
* Project statement will be released in 2 parts:
  + Part 1 will be released along with Week 2
  + Part 2 will be released after Week 3

**Week 1:**  
Set up a Private Docker Server and explore the game in its original form.

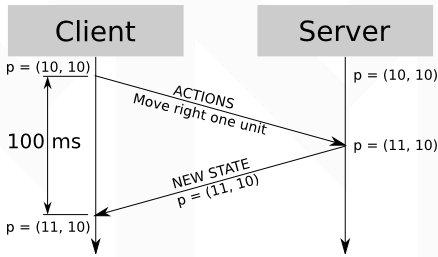
**Week 2:**  
Disassemble the game binary and examine internal structures using GDB. Set up a template LD\_PRELOAD script.

**Week 3:**  
Write an LD\_PRELOAD script to modify player attributes for fun and advantage.

**Week 4:**  
Project: "Golden Eggs" - Disassemble the binary to uncover all coordinates and develop a teleportation feature to collect those golden eggs.

# Definitions :

* Client-Server model:
  + There is a server somewhere in the world that has a database of all player credentials and the player has to download a Client of the game and register with the server to get some identification, which is then used to later connect to the server to enable gameplay.
  + Even during the gameplay, a lot of the player attributes are stored on the server side and are constantly updated by communicating with the server either after every Game Tick or when an input button is pressed by the player.
  + For this reason, you can't just attach Cheat Engine to Fortnite and expect to be invincible, because the player health is calculated and stored on the server and not on the client.
  + The exact mechanism of how the server actually handles the requests and what does the client do while it waits for the server's response is quite complex and varies from game to game. You can read this [link](https://www.cnblogs.com/cuizhf/p/3417195.html) to understand how the communication is handled in Fast-paced Multiplayer games.



# Notes :

* "A game is a description of strategic interaction that includes the constraints on the actions that the players can take and the players’ interests, but does not specify the actions that the players do take."
* "Game hacking" refers to modifying the working of a game by exploiting certain functionalities or actively changing the game's flow.
* There are many classifications of video games :
  + basis of platforms, basis of genres etc.
  + We are interested in is the following classification: Offline games and Online games.
* Online Games:
  + typically follow a Client-Server model.
* Offline Games:
  + rely entirely on the device they're played on.
  + All computations, graphics rendering, and logic processing occur locally. This means the game's performance and capabilities are directly tied to the hardware of the device.
  + For this reason, we can freely modify any and all player attributes in any way we want. But, usually offline games are stripped before release to improve the performance which makes it difficult to decompile and understand the Game Logic.
* Most common methods of game hacking :
  + Memory Editing: modifying the memory values where the game keeps its status information.
  + Botting: Developing an automated script to perform actions without direct player input.
  + **Code Injection**: modification of the game's executable code while it is running.
  + **Network Traffic Forgery**: editing packets to modify outbound network traffic.
* Refer to Docker Server for instructions to set up the game client and server.