ForceAttack Offset

The first hack we will make in this class is an external triggerbot: a program that reads CSGO's memory, and shoots for you as soon as your crosshair is over a player. However, it's not much of a triggerbot if it's not able to shoot. Your task for this week is to figure out how to use memory hacking to make your player shoot in-game.

Luckily, there's an easy way for us to force CSGO to shoot whenever we would like it to. In Source Engine, keypress and mouse click inputs are handled via "*plus commands*". For example, the console command "+attack" will cause your player to start (and continue) shooting, and "-attack" will cause them to stop (try it!). You can think about these commands as toggle switches for certain actions in the game, such as walking forward (+forward), jumping (+jump), shooting (+attack), crouching (+duck), and so on.

The way that these commands are hooked up to actual keys and mouse buttons are through *keybinds*. For example, your spacebar key is bound to +jump and -jump, and your left mouse button is bound to +attack and -attack. Whenever your spacebar is pressed down, +jump gets executed, and whenever your spacebar is released, -jump gets executed. You can try this out yourself by executing the console command "bind x +jump". This will make the "x" key another functioning jump key in-game. Note that the spacebar will still function fine; it's still bound to +jump as well. To unbind the key, use the command "unbind x". These keybinds are also a useful way to setup in-game macros (experienced players will be familiar with "buybinds").

There happens to be a value in memory, in the module client_panorama.dll, responsible for the +attack input command. More specifically, a certain value corresponds to +attack, and another corresponds to -attack. This address is static. Find this address' offset from client_panorama.dll's module base, then plug that offset into the demo program. If done correctly, pressing spacebar will make your player shoot.

Due 1/21

Tips/tricks:

You can speed up the scan by adjusting the Start/Stop addresses to only scan client_panorama.dll's addresses.

Hints (scan to view):

If you're stuck, ask on Slack for help.