

Filename: howtospotahackerMOBILY.pdf

Document Name: Spotting Hackers

Publishing Date: 04/11/2009

Spotting Hackers For Dummies

How to tell if a player is really cheating

Every single day of the year here MOBILY, we ban people. We ban them for being racist; we ban them for disrespecting our servers or us. We also ban a lot of people for cheating in our servers.

We have an Anti-Cheat team of highly experienced and talented individuals whose sole purpose is to determine if a player is cheating or not. This team goes through several demos daily, taking time out of their day to make sure our servers are clean, fun, and a cheat free place to play.

Unfortunately the demos they watch are not always conclusive. Either the demo does not show the cheaters SteamID, or the person being recorded is not actually cheating. We will not blame anyone for this, as everyone makes mistakes. The reason for these mistakes is our guest admins are not trained in cheat detection as our Anti-Cheat team is. Our hope is that this document will show our admins, and players alike, the best methods for detecting cheaters.

The Cheats

There are many different forms of cheat or 'hack' for Counter-Strike and CS:S, some are easier to detect than others. In order to determine if a player is cheating, it is best to know what the different cheats actually do. Take notes!

Wall-hacks

Wall hacks are probably the most used cheat. Most cheat programs have a built in wallhack in some form, sometimes many forms. There are some cheats that simply change client variables to allow the player to view entities through walls (Such as Player Models). Some may disable key features in the map like or prop detail entities. This would be boxes, Windows in Dust/2 and so on.

Some wall-hack programs will cause the walls to be semi-transparent, in settable levels from almost solid to almost invisible.

ESP

ESP (Extra Sensory Perception) is usually bundled with other cheats. ESP basically draws a box around every player. As with a wall-hack, ESP comes in all shapes and sizes. Some of them just draw a box, red or blue depending on the team. This is a visual aid to show who to shoot at, and to see players in darker areas. ESP will normally work through walls, so it can be used to the effect of a wall-hack. In the more 'complex' hacks, ESP can be used to show a players name, their Hitboxes, what weapon they are holding, how much ammo is in their gun, if they are reloading, and so on.

No-flash/No-smoke

No-flash and no-smoke hacks do just that. They will make the cheater immune to the effect of a flashbang and smoke grenades.

Speedhacks

The easiest and most blatant form of hacking, usually used along side Aimbots or Wall-hacks.

Speedhacks will enable a player to move exponentially faster than normal speed.

Speedhacks have different modes. There is 'speed' and 'aspeed'. 'Speed' will cause the player to move at a preset or settable speed, ranging from 1x to up to (and beyond) 100x. 'Aspeed' is Attack-Speed.

This means the speedhack will only activate when the players +attack is triggered, when the player shoots. 'Aspeed' is usually used at a low setting, maybe 1.1x to minimize detection, while giving the player a slight speed advantage. This lower setting of 1.1x can easily be misinterpreted as lag, thus the hacker goes undetected.

Aimbots

Aimbots have their own section. There are many different kinds of aimbots I will cover here, so pay attention.

The one thing every aimbot has in common is its function. Aimbots are used to make aiming easier, or even completely automatic for a player. Generally used in combination with other cheats mentioned above, the aimbot is the most effective and annoying hundred lines of code ever written. Actually it's probably more like a thousand lines...anyways...

Anti-Recoil

Anti-Recoil is generally categorized separately from aimbots. It is not separate, it helps with aiming, and therefore it is an aimbot.

Anti-Recoil is the most basic form of aimbot. Usually used with Nospread and Vector aimbots (see below), anti-recoil will reduce or eliminate the recoil felt by the player. In other words, his crosshair won't move much, move downward instead of up or not at all when he shoots.

NoSpread

NoSpread is somewhat similar to Anti-Recoil. NoSpread is almost always used with Anti-Recoil, and usually used with Vector aimbots. NoSpread limits or eliminates the inaccuracy while 'spraying' an automatic weapon. The name NoSpread comes from the fact that when you use it, it has the same result as if your crosshairs did not spread apart while shooting, thus increasing accuracy.

Bound Aimbot

Bound aimbots use a FOV and Hitboxes to aim. Normally this aimbot is bound to mouse1 (or the +attack function), and will automatically aim within a preset radius for a preset body part or hitbox. Generally the cheat will have settings to aim for the head, chest, stomach, arms, and legs. Head being most effective, it is also the most detectable. Most will set this to Chest or Stomach to avoid detection. The aimbot uses a FOV (or Field of View) to determine where to shoot. This is set in degrees from 1 to 180 in either direction (Note: Some cheats may use 1-360). If player sets the FOV to 180, and the Hitbox to head, every time he fires his weapon, the aimbot will take over and lock onto the heads of any enemy within that radius of 180 degrees (in any direction).

Most cheaters scared of being detected will use a low FOV setting of 1-15 degrees, and set the Hitbox to anything but head. This means that when the cheater sees an enemy, he can

point in the general direction and let the aimbot do its work. This generally will look like lag from a spectators' point of view.

Automatic Aimbots

Same effects as the Bound aimbot, only the aimbot will go to work no matter what button is pressed. Because of this, this aimbot is much easier to detect.

Vector Based Aimbot

Vector aimbots are the most complex, and most effective form of aimbot when used properly. Usually characterized by a seemingly random shake, this is the easiest aimbot to detect.

Vector based aimbots use a series of algorithms, different for each weapon, which are designed to produce "Perfect accuracy". Though few people can get this result, that was this aimbots original intention. Vector based aimbots almost always use a FOV Hitbox aimbot, NoSpread, and Anti-Recoil.

The cheat calculates and predicts where bullets will go at any given time in a game, and moves the crosshairs accordingly. For example, if a player shoots a two round burst with an M4A1, the first bullet may hit dead on, but the second bullet might up 1 inch and left one inch.

In the exact same situation, the Vector based aimbot would go down 1 inch, and right one inch for the second shot, causing it to hit the same place as the first. This is why these aimbots shake as they do.

You will notice that the shake is different for each gun and situation. If the cheater holds an M4 and crouches, there will be almost no shake at all, because if he shoots only once, that bullet will hit almost dead on anyway. However if that player were to spray his weapon, the Vectors would take over and he would shake like crazy to counter the recoil and spread. The cheater himself does not see this shake, it can only be seen by the other players in the server.

The Vectors themselves are defined by a line of numbers in a config file bundled with the cheat. This config file can sometimes contain several different vectors for each weapon, designed for different purposes. Some for 'spraying' M4 headshots, some for noscoping scout headshots, and so on.

Other Hacks

There are a few other random hacks out there which are not worth going into depth with, but I will mention some of them.

Fullbright – Removed lighting from the map, so every texture is super bright. No dark corners.

Whitewalls – Turns every texture in the map solid white, for easily spotting the enemy.

VEC Dodger – Used to avoid the Vector aimbot, characterized by the player spinning rapidly.

OK Great! Now...how do I spot them??

This is a tough subject, so you will be reading for a while here. Detecting cheats is not an exact science. If it were, we wouldn't need an Anti-Cheat team.

Detecting Wall-hacks

Wall-hacks can be easily hidden, but are almost always detectable. It takes a trained eye, and a lot of watching to spot a 'good' wall-hacker. Look for signs and clues as to his movement, and listen to the sounds in the game, as most wall-hackers will claim to have 503.1 surround sound headphones.

For those wall-hackers that hide it well, try recording a demo of the player for several rounds, and watching it yourself in Wireframe mode. To do this, follow these directions..;

1. Open Console [~] (**while not connected to a server**)
2. Type "Demoui" and load the demo you recorded (**or shift + F2 while CSS is open**)
3. Wait for the demo to load...can take a couple seconds for long demos
4. In console, type "sv_cheats 1"
5. In console, type "mat_wireframe 1" OR "r_drawothermodels 2"

This will enable wireframe mode. This command will **only** work if SV_CHEATS is set to 1 in the server. You cannot set SV_CHEATS to 1 in any server you do not own/have RCON to. **Do not attempt to turn on wireframe in a public server, it won't work!**

Anyways, now that you are watching the demo with wall-hacks, you will be able to see what the player was pointing at when he/she looks at walls. If you notice the player looked directly at another player through the walls, several times, or following the other player when he/she moved around, then he may have been using wallhacks. Submit the demo to <http://www.reachgaming/reportHacker.php>

Sometimes it's much easier, sometimes much harder. For example you may have someone blatantly follow someone else's head through the wall and shoot it off the very instant he comes around the corner, but in other cases it is almost impossible to tell if the player is walling. If a player is lining up shots before going round a corner then this can indicate that a player is using a wallhack. If the target player is in a regular camping spot, then it may just be the player knows the map well, if the target player is in a more open or unusual position then it is a strong indicator that wallhacks may be being used.

For those super-hard to detect wall-hackers, you must listen very carefully to what he can hear. See if he reacts to grenades thrown from the other side of a wall before he can see/hear them. Watch which corners and camping spots he checks, sometimes wall-hackers will only check the spots that people are in, and ignore the rest. If you see a lot of behavior like this, the player is likely wall-hacking.

Please note...not all players who shoot through walls and get kills are wall-hackers! I shoot through walls all the time, I get a kill from it once in a while, no big deal. If you get killed through a door once, there is no need to demo and ban right away.

Use your radar! The radar can be extremely useful when try to decide if someone is wallhacking. If you are spectating a player who is firing through a wall you can use your radar map to tell whether there is an opposition player on the other side and whether they are being hit.

Switching to freeview and moving your view through the wall is ok, but remember that in the time it takes you to do that, the target player may have moved, or another player moved to that location.

Detecting NoSmoke/NoFlash hacks

Unfortunately it is pretty hard to detect no-flash hacks these days. The flash effect is not the same on all computers. I have tested this by putting two computers next to each other, loading them both into a server, and using one to spectator the other while I flashed myself. Both screens went white, but the one in spectator stayed white for a good 7 seconds longer.

If you notice a player getting a lot of blind kills, try to determine how blind he *should* be by the position and distance of the flash. If the player turned away last second, there is a good chance the SPECTATOR would be completely blind, while he was only partial. This difference is caused by Latency. The flash effect is not calculated by the server, it is done by the players computer. If he turned away really quick 30 ms before the flashbang went off, and his ping is more than 30, you would get completely blinded, but he would be half blinded. Take this into account when accusing a player of noflash hacking.

No-Smoke is also pretty tricky, since many people use different video settings. It is easier to see through smoke grenades with certain adjustments made in video settings. Resolution, AA, AF, shading...it will all have an effect on just how transparent smoke seems. Fortunately the smoke is never completely transparent, and at a certain point within the cloud your screen will almost always go solid gray. Watch for multiple kills with bursted fire through smoke. A player with a no-smoke hack will usually try to kill everyone on the other side of the smoke before it dissipates, giving him the upper hand. If he truly has a nosmoke hack, his shots will be (for the most part) on target. You can use the same demo+wireframe method here to determine this.

Detecting Speedhacks

Speedhacks are almost always easy to spot. If the player gets from his spawn the enemy spawn before the enemy has bought grenades...he is probably speedhacking...or using Mole if it is a WarCraft server.

Any speedhack set higher than 1.3x is easy to detect, and most speedhack users will set their hacks for complete domination by setting it to 40x or something.

For those few 1.1x users, there is one way to see it. In your console type "**cl_showpos 1**". This will show your (or who you are specing) current real-time position, as well as your velocity. If this number goes above 260 sustained while walking forward, there is a chance the user is speedhacking. Normal speed with a knife or pistol is 240, the fastest is the scout at 250

(Yes, you go faster with a scout than you do a knife!).

Other than that, you can watch for lag spikes from the player. **Lag spikes don't mean someone is speedhacking.** What I am saying is, when a player speedhacks, sometimes they will spike once every second, for about 1/4 of a second. His ping will stay steady, but his player will spike. This is one side effect of speedhacking. If you notice this when he is running, he *might* be speedhacking.

Detecting Aimbots

A lot goes into detecting aimbots in some cases. There are a lot of factors to consider, mainly Latency, Mouse, and Sensitivity.

If you have a friend record a demo of you, while you record a demo of yourself, you may be surprised how different those two demos will be. In the one you record, you will see what you say while playing, you point at a player and fire. In the other demo however, your movement will appear smoother (if you are a 'twitchy' player), and you will appear to shoot before your crosshairs are on the target. This difference is caused by latency. The higher your ping, the more time difference you will see in the person you are spectating, and in your demo.

High mouse sensitivity can cause a shaky look on another player. Personally I use a sensitivity of 9 with a simple optical mouse, so when I use a scoped weapon, my crosshairs appear to shake when I move my mouse.

To determine if this shake is because of a mouse, instead of an aimbot, you can watch

how the shake reacts to certain movements and weapons. If the shake increases when the player walks or jumps, it is possibly an aimbot. Vector based aimbots will shake extremely violently when the player jumps. However, if it does not increase...the player is not using a vector aimbot.

The mouse-shake is most noticeable when watching a player with a scoped weapon such as an AWP. The shake is only shown when the player is scoped in, and moving his mouse. AWP is the easiest though. Because the AWP will always hit dead on if you stand still, a vector aimbot does *not* need to compensate or move at all. If you see shaking while a player is scoped with an AWP and standing perfectly still other than mouse movements, he is not likely aimbotting.

If you notice a player appears to miss the enemy after a swing-shot, but registers as a kill, keep in mind the latency differences.

A word on Recoil; If you see a player with no recoil at all, that does not automatically mean the player is hacking. Sometimes, depending on rates and ping, recoil will not show up at all. This is not grounds for a ban alone, the player must show more than a lack of recoil for our Anti-Cheat team to take actions.

On the other hand though, if a player shoots once, gets a headshot, but his mouse didn't even move until after the shot was fired, I would be suspicious of a Bound Aimbot. If this happens multiple times, where he gets a headshot before even moving the mouse, start up a demo and submit it to <http://www.reachgaming.com/reportHacker.php>. Since the player moved before he shot, it *should* move at least a little before his/her shot goes off. Either he/she has the fastest hands in the west, or there is foul play at hand.

Note: You may notice with scoped weapons, a lot of the time players will get a hit or kill without the scope being on target. This is a result of latency on both sides. The higher the ping, the more of a delay there will be.

Other methods

Observe the players overall skill in the game to help you determine if the player is cheating. Watch how they move around the map and handle their weapons. If they jump around the map easily, switch weapons well and make good use of grenades then they are most likely a good player. Although that does not mean that they do not cheat.

Always remember, if you are uncertain of a player cheating, record a demo, **do not ban**. Let the professionals in our Anti-Cheat department handle it. We don't like seeing good players get banned three or four times a week because they got skillz. We would advise you all to view demos yourself, watch them and learn from them. Practice makes perfect, so if you have 15 minutes to kill, load up one of those demos!

Ok, well I hope everyone learned something from this. Sure, half of it was me explaining what hacks are, but that's what you need to know. If you know how the hacks work, what exactly they do, you will be able to spot them more accurately, and not ban the good players. I hope you all use this information to help keep MOBILY game servers the cleanest in the business.

Contributing Editors: MOBILY Anti-Cheat Task Force