Ethical Student Hackers

Game Hacking

SHEFFIELD | Ethical Student Hackers

Breaking into security.

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

SHEFFIELD Ethical Student Hackers
Breaking into security.

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

SHEFFIELD Ethical Student Hackers
Breaking into security.

Legality of making game hacks

- Copyright
  - Most copyright for games does not allow you to reverse-engineer or modify the original games code
  - https://pwnadventure.com/ - This allows you to reverse engineer their game
  - For example - https://www.terraria.org/terms disallows reverse-engineering of any sort
- Terms of Service
- Online games
  - Not to different from penetration testing a web application - It is likely ILLEGAL!
  - Generally it's best to avoid online games
- https://law.stackexchange.com/questions/25825/is-creating-and-selling-cheats-or-hacks-for-games-illegal - This is for USA law, however some applies to the UK

What sort of game hacks are there?

- DLL (Dynamic Linked Library) injection
  - This is when we inject a hack into the memory of the game
- DLL hijacking
  - Similar to DLL injection, but we take over an existing DLL file and add our own code to that
  - We add code in “code caves” - Areas in the DLL that don’t contain any useful code
  - We can also use a “proxy dll” - A dll we own to get called before the original dll
- Memory editing
  - Directly changing values in the process memory
- Network traffic forgery
  - Analysing the packets sent by the game to the server
  - Change the packets to modify the users activity

So, where to start?

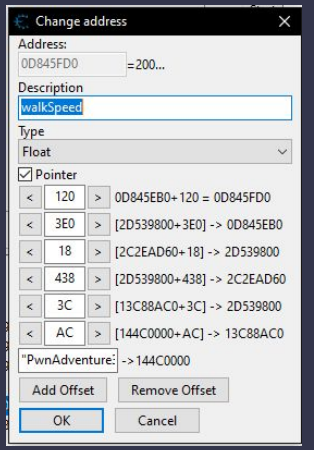
- Cheat Engine is an incredibly useful tool for both looking at the games instructions as well as allowing us to change them during execution
- It has features that make it easy for very simple game cheats, such as changing health values
- It also has advanced capabilities that allow us to look and edit the assembly code of the game, therefore allowing us to change how the game runs!
- It has multiple incredibly useful features that will save you a lot of time, while also being relatively easy to use

- https://guidedhacking.com/ - Some great resources and code snippets
- https://www.youtube.com/user/seowhistleblower - Stephen Chapman

SHEFFIELD | Ethical Student Hackers
Breaking into security.

Pointers

- Chances are incredibly high that you will be using pointers when reverse engineering games or applications, so they're a really useful skill to learn!
- Pointers are locations in memory that 'point' to another memory address. They store the address of another value.
    - You'll see a lot of pointers pointing to other pointers with an offset
- More generally, we will be using pointers to find useful values in our application that we want to access frequently, such as health, money …
- Fortunately cheat engine does quite a bit of heavy lifting for us when it comes to Pointers, so learning them shouldn't be too complicated (hopefully :P)



SHEFFIELD Ethical Student Hackers
Breaking into security.

Nops and Nop slides

- A nop is simply an instruction that does nothing. The computer sees the nop and just moves onto the next instruction to execute
- The assembly hex for a nop is 90
- Therefore, a nop slide or nop sled is a chain of nops that follow on from one another
  - 90 90 90 90 90 90 90
- Nop slides are often used to overwrite code that we don't want the game to execute. This allows us to remove functionality from the application
  - For example nopping code that edits our health or our ammo count

Internal vs External

- External
  - External cheats use a handle given by the kernel to allow them to read and write to the process' memory - This can be blocked if there is a kernel level anti-cheat
  - Uses an external process to read/write values to the game process, this is easier to detect
  - Generally poor performance due to kernel calls

- Internal
  - Has direct access to game memory as it's being run as the game process
  - Faster performance than external cheats
  - A lot more versatile as you have access to more
  - Can be better for anti-cheat (Not that you should be bypassing it :P)

Demo time!

Resources

- https://guidedhacking.com/
- https://guidedhacking.com/forums/the-game-hacking-bible-learn-how-to-hack-games.469/
- https://guidedhacking.com/threads/how-to-hack-any-game-tutorial-c-trainer-3-first-internal.12142/
- https://guidedhacking.com/threads/internal-vs-external-hacks-whats-the-difference.8808/
- https://guidedhacking.com/threads/guide-on-how-to-call-game-functions.11116/
- https://guidedhacking.com/threads/c-mid-function-hooking-codecaving-tutorial.4061/
- https://youtu.be/8Z1D64qfrxM?list=PLhixgUqwRTjzzBeFSHXrw9DnQtssdAwgG - LiveOverflow
- https://www.youtube.com/user/seowhistleblower - Stephen Chapman
- https://guidedhacking.com/threads/dll-hijacking-vulkan-hook-tutorial-quake-2-hack.13518/ - DLL Hijacking
-

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

19th April - Guest talk & AGM

26th April - Mike Jones (ex Anonymous) Talk

3rd May - Binary Exploitation - Jack

10th May - Wifi Sniffing - Brooks

15-17th May - Raspberry Pi CTF - Mac

Any Questions?

www.shefesh.com

Thanks for coming!

SHEFFIELD Ethical Student Hackers

Breaking into security.