(Pre-Written) Windows Game Hack/Trainer

All Sections

Instructor's note: This is a successful student-proposed project from a previous term.

Client

Instructor / TA's

Macro-Level Explanation of Project:

Check out this video from LiveOverflow:
Windows Game Hacking with Ghidra and Cheat Engine **(https://www.youtube.com/watch?v=Pst-4NwY2is)**

(https://www.youtube.com/watch?v=Pst-4NwY2is)

This project involves learning new methods and new tools to hack various games on Windows. There are tutorials available that focus on an open-source game called Assault Cube [https://github.com/assaultcube/AC **(https://github.com/assaultcube/AC)**]. It is a lightweight (~50mb), free, online first person shooter game that does not have any anti-cheat; in other words, a perfect example to start learning with. Many published games (specifically multiplayer online games) have anti-cheat measures built into the game by the developers to either detect or deter their games from being modified. There are methods to bypass these limitations but that is beyond the scope of this project.

There are many ways to hack games. Two possibilities are external vs internal hacks. External hacks use Windows API functions like ReadProcessMemory() and WriteProcessMemory() [https://docs.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-readprocessmemory **(https://docs.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-readprocessmemory)**] to manipulate the game, where internal hacks are written as .dll's {dynamic link library}, injected into the process' memory space, and can access memory addresses directly without the use of Windows API functions.

For the end deliverable, plan to apply all the knowledge and skills that you have learned to Pwn Adventures 3: Pwnie Island [http://pwnadventure.com/ **(http://pwnadventure.com/)**] (or some other suitable game). This game is a MMORPG that was written specifically for a CTF {capture the flag} competition, Ghost in the Shellcode 2015 [http://ghostintheshellcode.com/

(http://ghostintheshellcode.com/)] for the purpose of having competitors exploit vulnerabilities for, and an example of what not to do for game developers.

Our goal is to deliver an internal .dll hack program written in C++ that has a visual menu for various cheats the user can select, to manipulate Pwn Adventures 3: Pwnie Island. Currently proposed cheats include:

- invulnerability
- additional in-game currency
- weapon effect modification (damage, ammo, recoil, etc.)
- Modifications to player (speed, jump, mana, etc.)

This list may be revised and extended as you become more familiar with the game's design and as you learn new hacks. For this project, you will need to:

- Find pointers and addresses in memory
- Analyze assembly instructions
- Decompile and reverse engineer code
- And more...

Knowledge of C/C++, OOP, and x86 assembly will be required, along with a willingness to MacGyver your way to success. This project would be ethical and educational and should be very fun!

Reference link(s) for more general information:

https://guidedhacking.com/threads/start-here-beginners-guide-to-learning-game-hacking.5911/ **(https://guidedhacking.com/threads/start-here-beginners-guide-to-learning-game-hacking.5911/)**

Assault Cube (open-source hackable game) [https://github.com/assaultcube/AC **(https://github.com/assaultcube/AC)**]

Pwn Adventures 3: Pwnie Island [http://pwnadventure.com/ **(http://pwnadventure.com/)**]

Cheat Engine [https://cheatengine.org/ **(https://cheatengine.org/)**]

Reclass.NET [https://github.com/ReClassNET/ReClass.NET **(https://github.com/ReClassNET/ReClass.NET)**]

Reverse engineering tools:

IDA [https://www.hex-rays.com/products/ida/ **(https://www.hex-rays.com/products/ida/support/download.shtml)**]

Ghidra [https://ghidra-sre.org/ **(https://ghidra-sre.org/)**]

Reply

Daniel Rivera
(https://oregonstate.instructure.com/courses/1750936/users/6209242)
2:27pm

Hello,

I would like to participate in this project and would like to know if anyone else is interested. Any takers?

Reply