Mason Competitive Cyber

[Intro to Game Hacking]

Why?

-Builds and practices skills that a security researcher needs

-Like a CTF, but with no flags

-Makes for a nice project to add to a resume

-Get to work in a group on something fun on anyone’s schedule

-Teaches you to create/analyze malware

Resume

Really bad example:

I epically pwned fortnight with my 1337 skillz

More reasonable (but still bad) example:

Hacked into online multiplayer game and gave myself infinite ammo

Good example:

Reverse engineered a game binary and utilized DLL injection to force a win condition using Ghidra, x64dbg, and C.

- Focus more on the techniques and tools than the exploit or game

-Be sure to mention if you worked in a group.

Tips/Advice

-Work in groups (You can’t divide knowledge)

-Keep it legal (I’m serious on this one)

-Gather evidence of your process and write a report about your project

-Don’t be frustrated if you fail at first or don’t understand things, this takes months/years to learn and longer to master

-Don’t touch anti cheat (especially kernel-level)

-This isn’t a job, it’s just used to refine and build skills

The Basics

- Learning the Hexadecimal system, assembly, and how memory works is important
- You will learn most of these as you go, no need to study beforehand
- Assembly follows the 80-20 rule
- Hex/file editing is a good starting point for those with no experience
- Cons to file editing:
    - Incredibly easy to detect
    - Doesn’t work on most games
    - Mostly guesswork and chance

External Hacks

-Utilizing the windows API to latch onto a game

-Allows access to pre-allocated memory

-Demands prior analysis of addresses

-Must learn how pointers (multi and single-level) work

-Normally requires a script (C, C++, C#)

-This technique is used by some malware

-Cons to external hacks:

- Also easy to detect (though not nearly as much as file editing)

- Not much room to grow

Internal / DLL Injection

-The big one

-More advanced technique, but is used by all kinds of malware (not always on disk, but still)

-Need to create both a loader to add the path and the malicious DLL

-Far more control and power than external

-If you learn game hacking for one reason it should be to learn DLL Injection

-Cons to DLL Injection:

- Decently high learning curve
- Can be overkill

Anticheat

What does it do?

- File Integrity Checks
- String Detection for cheat tools
- AntiDebug
- Obfuscation detection
- Signature Based Detection
- Memory Integrity Checks
- Virtualization Detection
- Kernel Drivers which block process access token creation & more

If you couldn’t make it

Summary for those who couldn’t make it:

- Work in groups
- Build up to DLL injection, then make/analyze malware
- Used to refine and build skills, not an actual profession

Proud Sponsors