Sig • Mal

Meeting 1

Introduction

What is SigMal?

- *“Malware Analysis”*
  - → Security, Development, and anything Malware Related

- Why this sig in particular?
  + “I have learned more in this, than some of my classes” - Random Guy

  + Summer Research → We almost did 8 weeks of work in a week

Topics

“Extremely Technical look into Computer Science”

- Reverse Engineering
- Computer Architecture
- Analysis of Computer Program and Files
- Development and General Fuckery with Programs

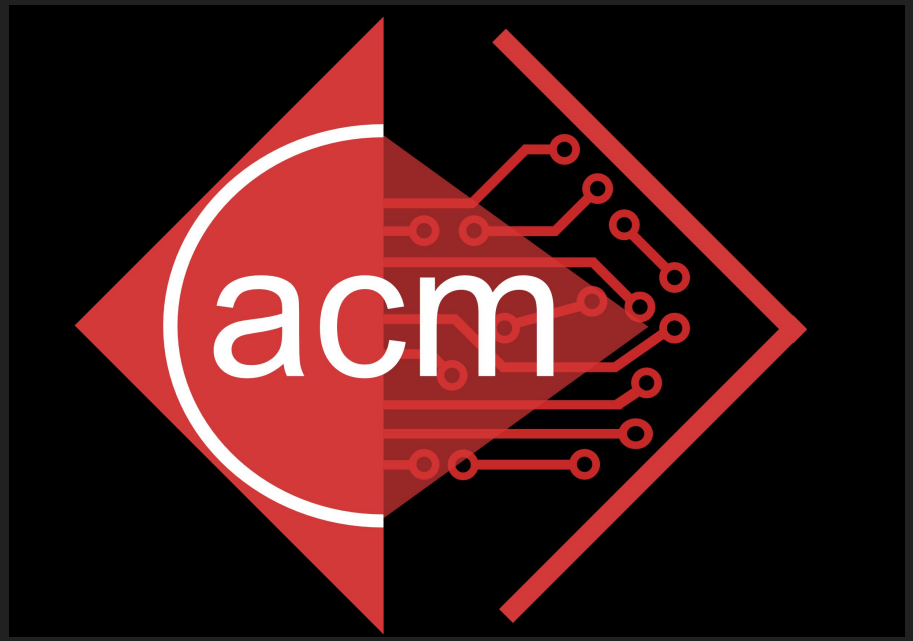
Mainly look into variants of the *nix OS

Tenets of Sig•Mal

- Big on open-source
- No one is really an expert
- The Best Hackers are often really good at coding.

  and have an ungodly amount of free time on their hands.

Thanks and personal Introductions



Andrew (missionit)

Phil (sourdough)

So, if I don’t really know something chances are these two are on the money.

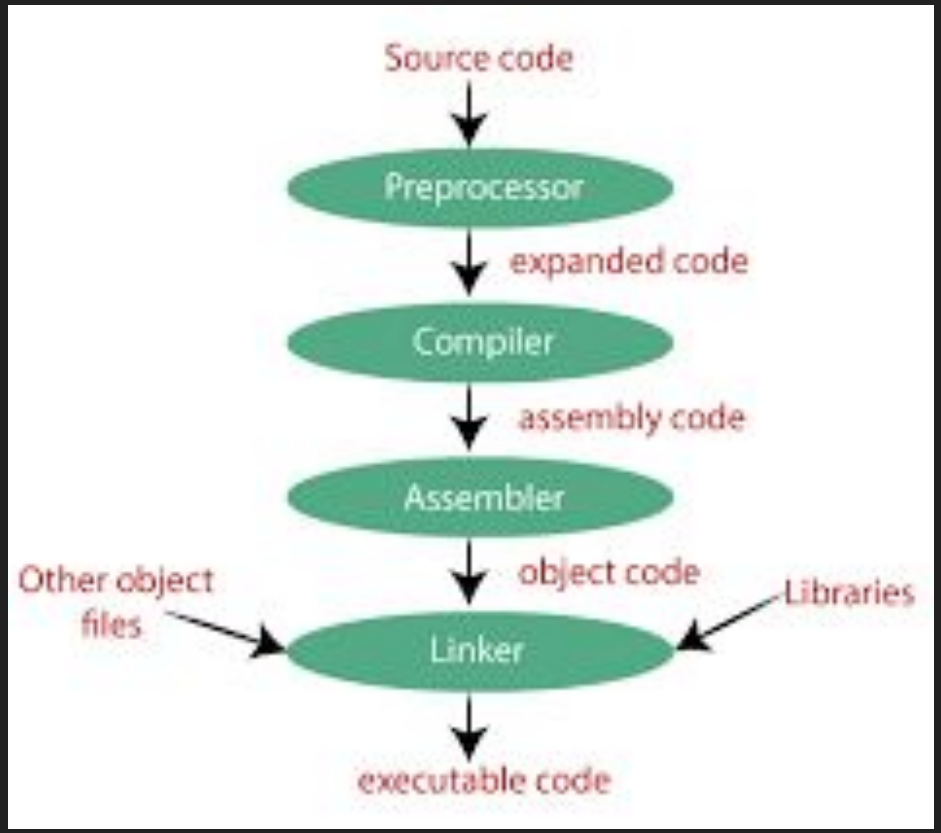
OS and their Executables

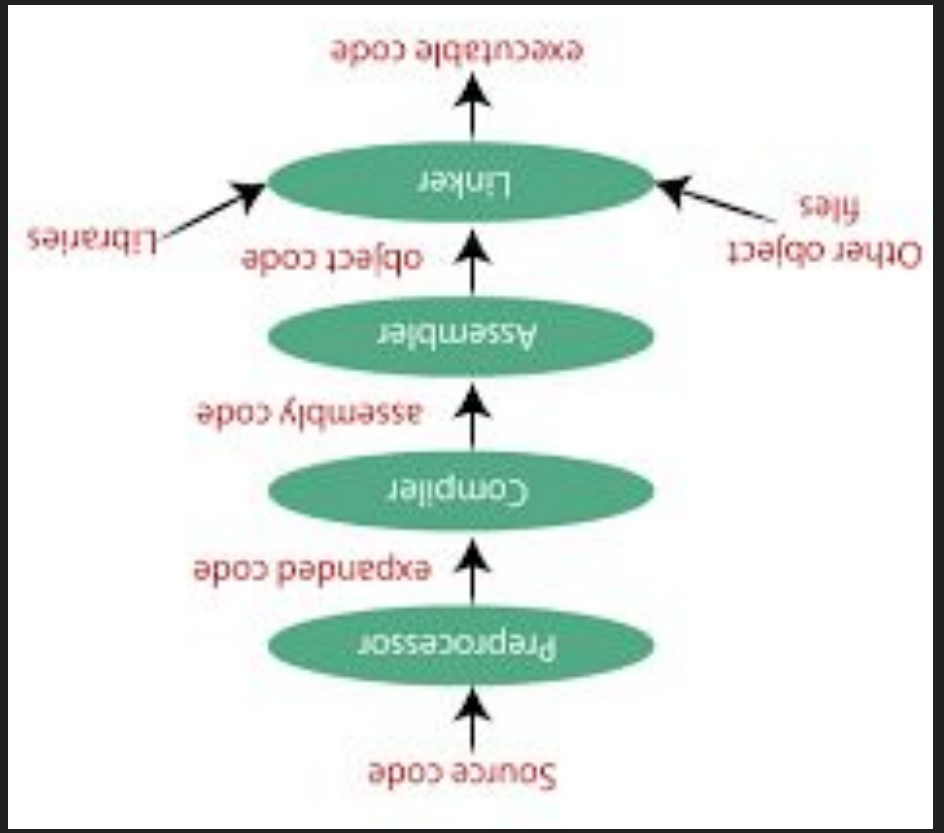
Linux → ELF (Executable and Linkage format)

Windows → PE file (Portable executable)

Mac (Disgusting ik) → Mach-O executable (~it belongs to mac)

Compilation and Decompilation





LIVE DEMO TIME

If there's a takeaway from just doing one meeting of crackme's it should be that: Any program can be cracked given enough time, hence any form of client side validation (like client-side game anti-cheats) are breakabl