Sig•Mal

Meeting 1

Intros

What is Sig•Mal?

Intros

What is Sig•Mal?

↳ “Malware Analysis”

>> Security, Development, and anything “Malware” related

Intros

What is Sig•Mal?

↳ “Malware Analysis”

>> Security, Development, and anything “Malware” related

Why this SIG in particular?

↳ Building security skills / knowledge + CTF practices

>> Increased proficiency within security

>> General knowledge and CTF specific practicals

Topics

- Reverse Engineering
- Binary Exploitation
- Malware Analysis
- Exploit Development + Analysis
- Development + General “Fuckery” with Programs
- Security within Github Projects

❖ Mainly look into variants of the *nix OS.

Topics

- Reverse Engineering
- Binary Exploitation
- Malware Analysis
- Exploit Development + Analysis
- Development + General “Fuckery” with Programs
- Security within Github Projects

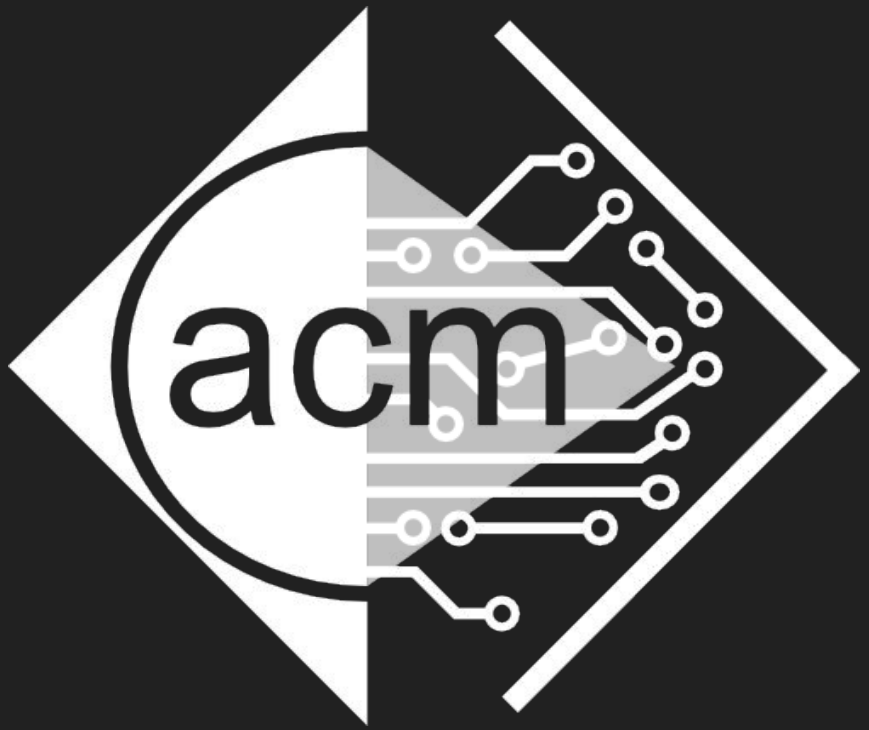
Defensive / Forensics Semester

❖ Mainly look into variants of the *nix OS.

Tenets of Sig•Mal

- Big on open-source
- Do not completely reinvent the wheel
- NO one is really an expert
- You don’t ‘need’ coding for security, but it makes you better

Thanks + Personal Introductions



Andrew (missioninit)

Phil (sourdough)

Justin (wuteztrain)

If I don’t know something, these legends might. They are also really helpful with leading Sig•Mal!

OS and their Executables

Windows	ELF (Executable and Linkage Format)
Linux	PE File (Portable Executable)
MacOS	Mach-O Executable

Types of Malware Analysis

- Static

- Dynamic

Types of Malware Analysis

- Static

  → Not running the program

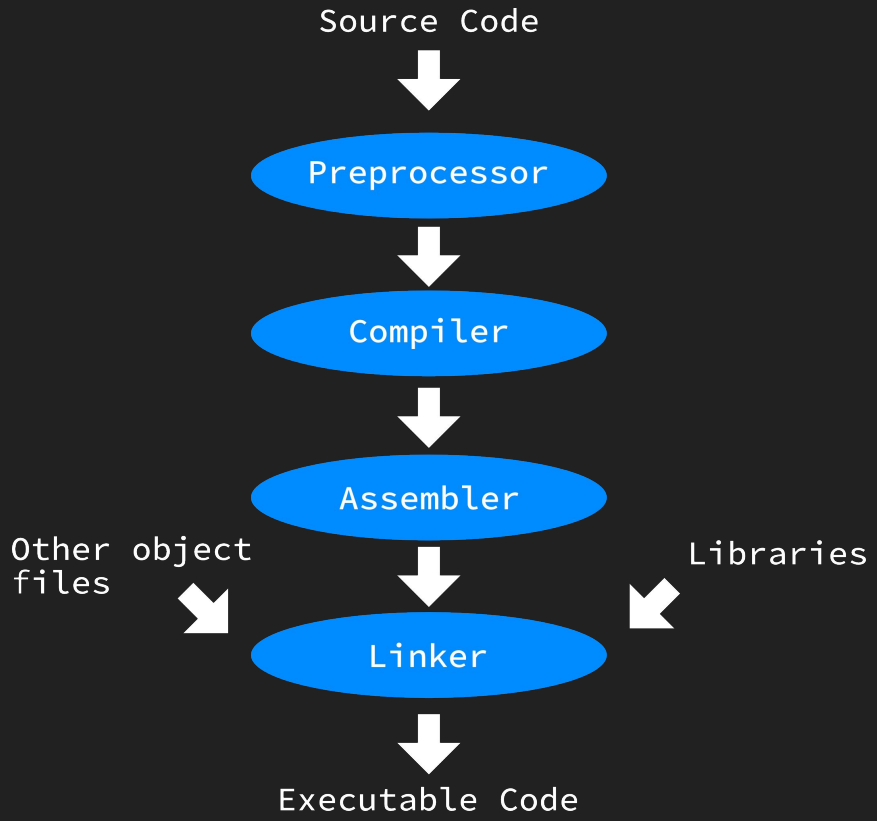
  >> Looking at the code and the metadata of the file

- Dynamic

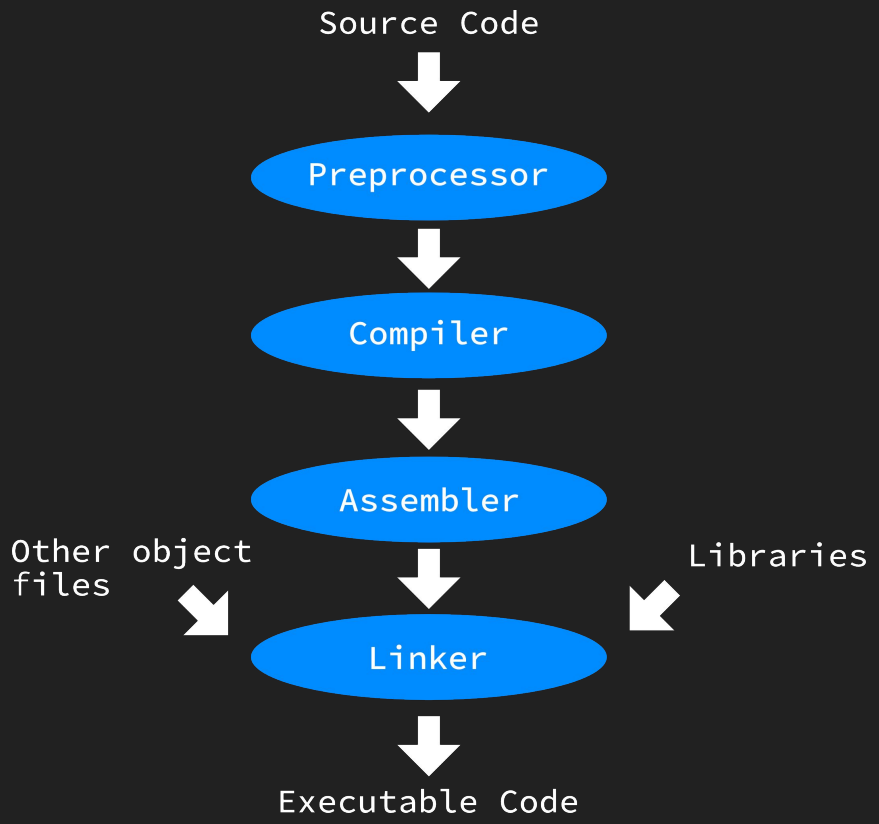
  → Running the program

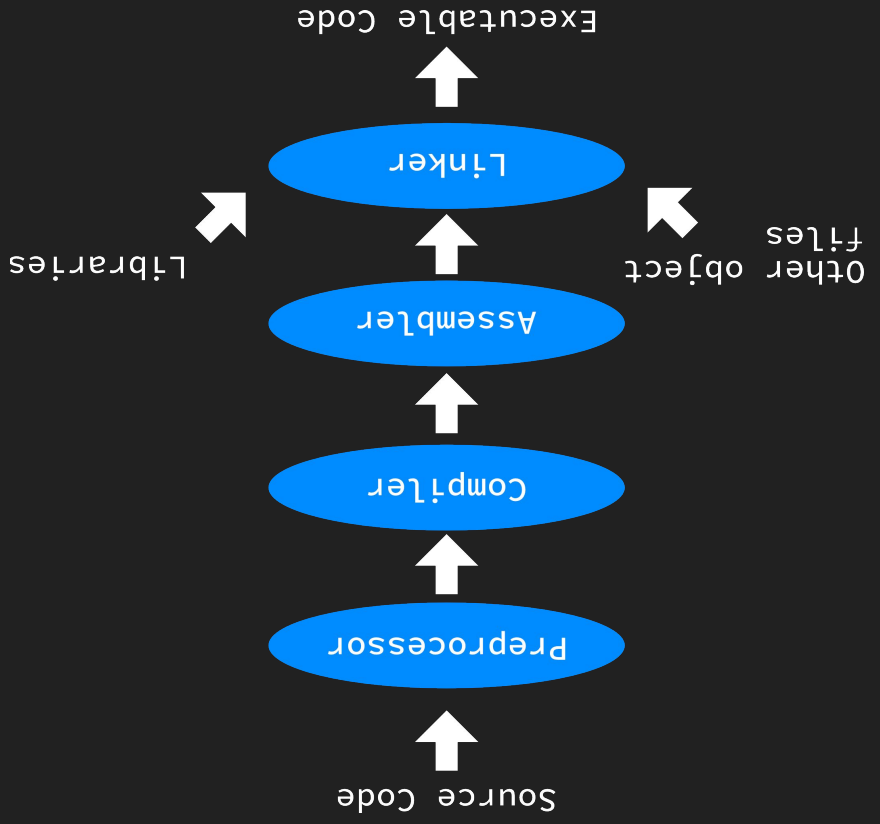
  >> “Letting it run loose and see what it does (or doesn’t do)”

Compilation and Decompilation



Compilation and Decompilation





Sources

- https://enterprise.comodo.com/forensic-analysis/malware-analysis-types.php
  - Be weary that normally, static analysis does really get into debuggers since that is more dynamic. Because debuggers normally require running a program.

LIVE DEMO TIME