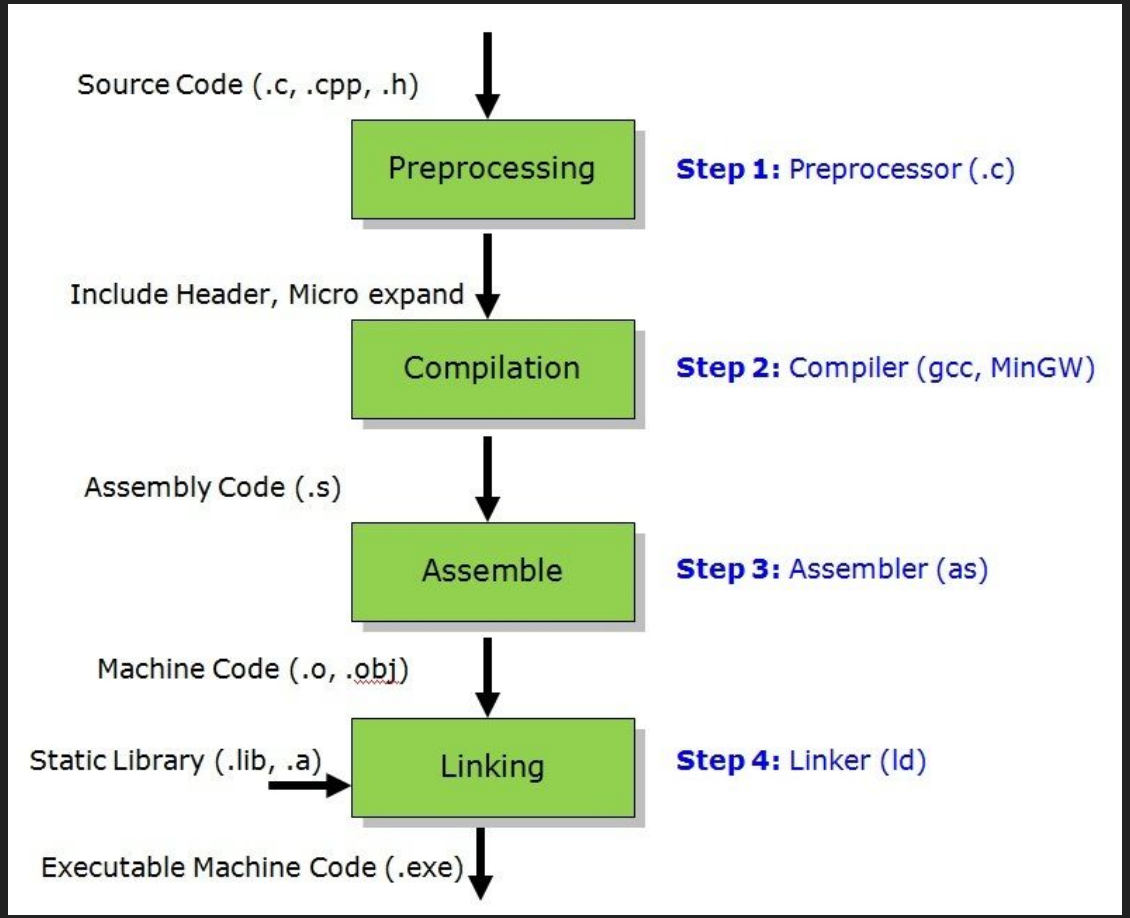
HSGS Sec Day 06

Reverse Engineering

Compilation



Dịch ngược mã là gì?

- Từ một chương trình đã được biên dịch, không có mã nguồn, tìm ra cách hoạt động của chương trình đó
- Thường bao gồm quá trình dịch chương trình đó sang Assembly

Tại sao lại dùng hợp ngữ Assembly

- Khi bạn code một chương trình bằng ngôn ngữ bậc cao, bạn chỉ thấy được toàn cảnh chứ không thấy được hết từng điều máy tính thực hiện
- Nằm ẩn trong Assembly sẽ là những behavior kì lạ.
- Do Assembly tương ứng 1:1 với mã máy, việc disassemble (chuyển từ mã máy sang Assembly) là điều gần như luôn thực hiện được
- Tại sao không đọc thẳng mã máy: coz your brain is bigger than mine.
    - Máy tính hoạt động qua những con số, việc nhớ những con số tương ứng với chỉ dẫn gì là tương đối khó đối với con người.

Decompilation

- Chuyển mã Assembly sang mã giả (có thể là C)
- Có thể thực hiện được, cho dù độ chính xác không quá cao do có thể dùng thuật toán để khảo sát sự di chuyển của các giá trị, flow analysis….

Tại sao cần dịch ngược mã

- Không phải phần mềm nào cũng có mã nguồn mở đi kèm
- Khi cần vá các lỗi phần mềm mà không muốn biên dịch lại từ đầu
- Phân tích mã độc
- Dịch ngược cho vui ?? :D ??
  - Dịch ngược game (pwn adventure)
  - **KHÔNG KHUYẾN KHÍCH CÁC HÀNH VI PHẠM PHÁP**
    - **Chép code (không khuyến khích)**
    - **Vui thôi đừng vui quá**

Các phương pháp phân tích phần mềm

- Phân tích tĩnh
  - Dịch chương trình ra ngôn ngữ bậc thấp
  - Đọc chương trình bằng ngôn ngữ bậc thấp và xây dựng lại logic của chương trình
- Phân tích động
  - Chạy chương trình và quan sát hành vi của chương trình đó, sử dụng một số công cụ hỗ trợ
  - Nếu không biết chương trình mình đang phân tích có độc hại hay không thì tốt nhất nên chạy trong máy ảo
  - E.g: dynamic instrumentation(frida), symbolic execution, ltrace, strace
- Trên thực tế thì khi kết hợp 2 phương pháp này sẽ cho hiệu quả tốt nhất

Các loại công cụ

- Disassemble
  - Radare2(Cutter)
  - IDA (Interactive Dissassembler)
  - Ghidra by NSA
  - Hopper
  - Binary Ninja (cloud)
  - Objdump
- Decompile
  - Hex-Rays Decompiler plugin cho IDA ($$$$$$$$$$$$$$$$$$$$$$$$) (SOTA)
  - Ghidra (NSA boiz)
  - Cutter (radare2 + Ghidra) (GSoC + NSA = ?)
  - Hopper
- Debugger
  - gdb - GNU debugger + plugin (pwndbg, gef)
  - lldb - LLVM debugger

Demo Crackme