

12 Days of Ghidra

Nathan R

[Twitter](#) | [Mastodon](#)

\$whoami

Security Researcher

- Mobile devices
- Operating Systems

MSci Computer Science && PhD Student in InfoSec

Big fan of Hollow Knight and Star Wars

Day 0 – Hello, Ghidra!

Agenda

What is Reverse Engineering?

What is Ghidra

Ghidra Setup

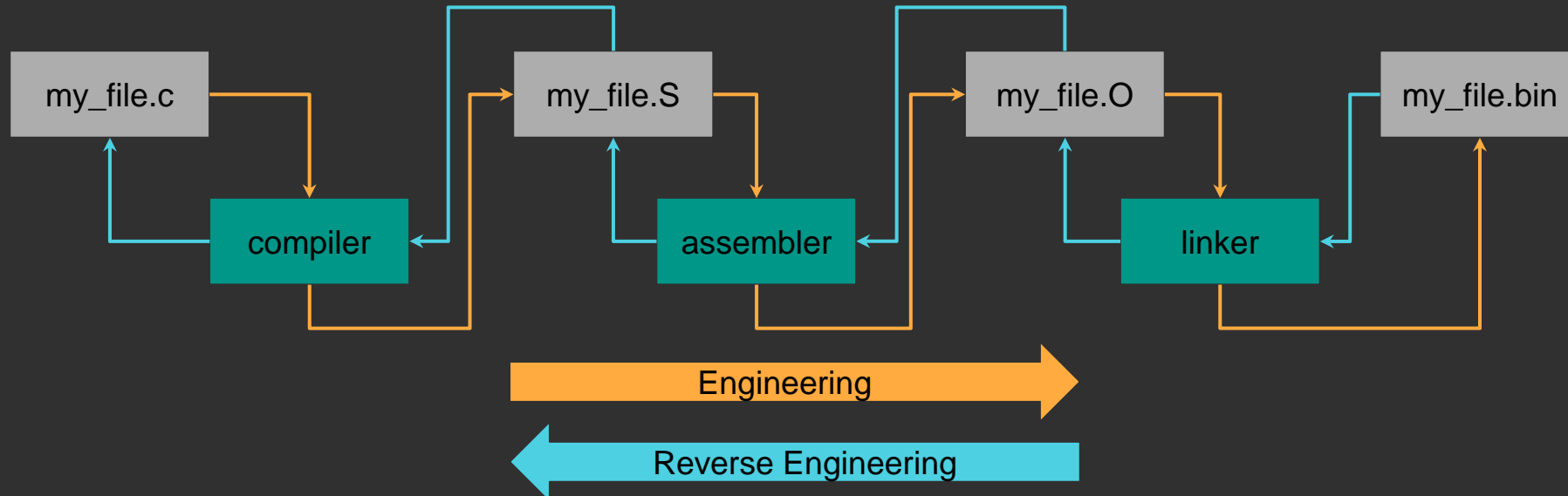
Ghidra walkthrough

Strings

What is Reverse Engineering (RE)?

Developer: source code -> binary format

Researcher: binary format -> source code



Why do we perform RE?

Understand what a binary is doing

Why?

- Malware Analysis
- Identify security issues
- Better understand undocumented features
- . . . ?

What is Ghidra?

Interactive software reverse engineering framework

Dissassembler

- Gives us a 'listing' of assembly code

Decompiler

- Attempts to present assembly code as close to source as possible

Its an investigative tool, you need to point Ghidra in the right direction :)

Ghidra Setup

Windows

Install a recent version of Java

Download Ghidra .zip from [Github](#)

Extract .zip to desktop (or any place you want)

Run **ghidraRun.bat**

Linux

Install Java JDK

- `sudo apt install openjdk-18-jdk`

Download Ghidra from Github

Run **ghidraRun.sh**

MacOS

Install [Brew](#)

- `/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"`

Install Java JDK

- `brew install --cask temurin`

Install Ghidra

- `brew install --cask ghidra`

ghidraRun

Ghidra on Apple Silicon

Need to rebuild support binaries for arm64:

Install gradle

- `brew install gradle`

Open Ghidra support directory

- `cd /opt/homebrew/Caskroom/ghidra/xx.x.x-xxxxxxx/ghidra_xx.x.x_PUBLIC/support`

Build support binaries for Arm

- `./buildNatives`

Using ghidra

Starting Ghidra

Navigate to Ghidra install directory

- `.../ghidra_<version>/`

Windows:

- `ghidraRun.bat`

Linux and MacOS

- `ghidraRun.sh`

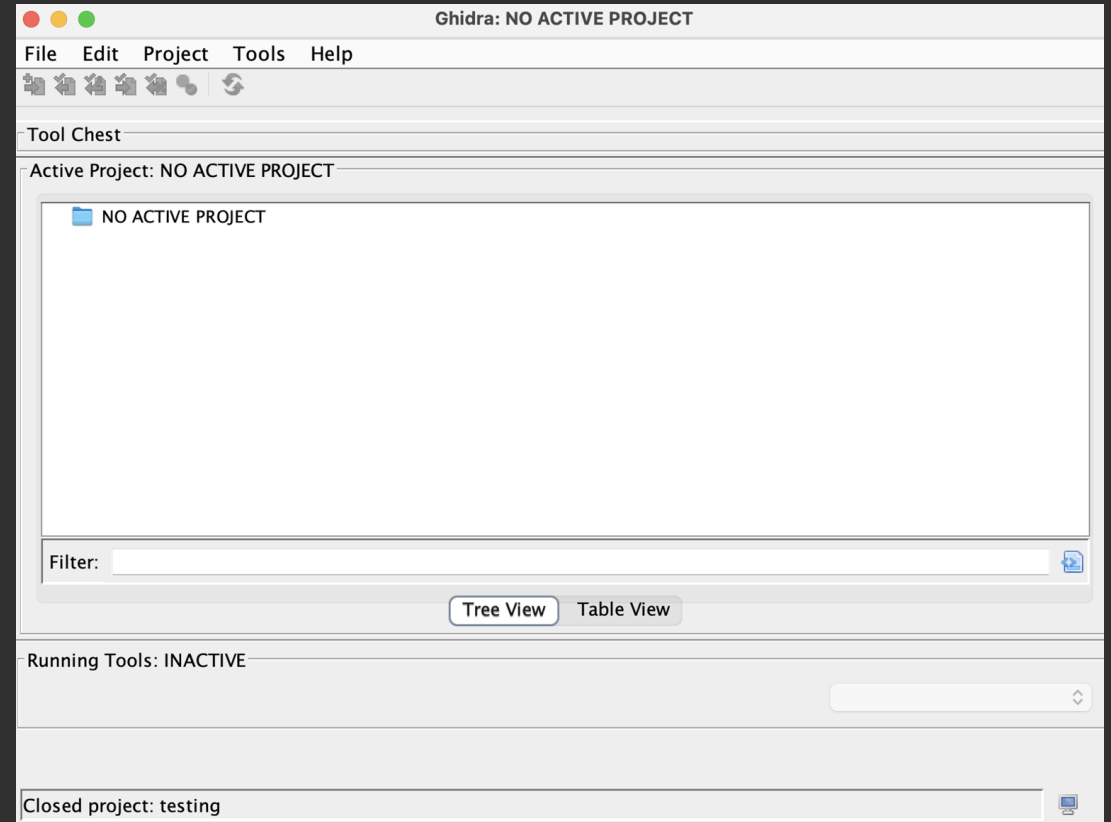
Program Manager

First window you will see in Ghidra

Hub for opening/creating projects

- Importing new files

Selecting tools



Program Manager – Creating a new Project

File -> New Project

Project Types:

- **Non-shared** for working alone
- **Shared** for working in group

Exercise 1:

- Create a new, non-shared project for 12 days of Ghidra



Tool Chest



Active Project: 12-days-of-ghidra

 12-days-of-ghidra

Filter:



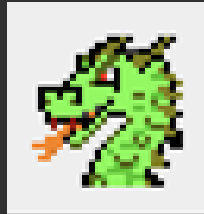
Tree View

Table View

Opening a Project in Ghidra

Select the project in the program manager

Click on the dragon button at the top



Importing a binary into Ghidra

Keybind -> I

- Or file -> import file

Select the correct compiler version

- Or make a best guess, tools like **binwalk** can be helpful

Select analysis you want to run

- Default will normally be enough

Ghidra Analysis

Aims to improve the quality of your decompilation

- Finding functions
- Finding cross-references (XRefs)
- Identifying different sections of memory
- Identifying stack variables
- Evaluating control flow

Analysis passes can take a while

- Defaults will be enough for these sessions

RE First Steps

Strings are a great first step when REing a new binary

Why?

- Can use them to identify what function is doing
- Error messages can give you good content
- Important data can be included in the binary, e.g. crypto keys

Ghidra has a built in Strings search tool

Day 0 Binary

1. Install Ghidra
2. Create a new project
3. Import day0.bin
4. Find the main function for your systems binary
5. Run the binary in a terminal to see what it does
6. See if you can find the flag in the binary
 - a. It may not be in the main function ;)

Flags are in the form vrc_flag{}

- DM me on Discord @nathanr to claim a flag :)

Prizes

We also have a couple of prizes to give away:

- Choice of book from No Starch Press
- Hoodie from @InterruptLabs

Categories:

1. For whoever completes all 12 binaries first
2. Most engaged participant
 - a. Helping on discord
 - b. Contributing to discussions
3. Best write-up