

# 12 Days of Ghidra

Nathan R

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

# Day 5 – Structs

# Structs

You may have noticed an AES struct in the previous binary

Structs are how variables are group in C / C++

They form a composite data type

- A type composed of different variables

# How to know if it is a struct or an array?

**Arrays** are made up of elements of the same types

- Therefore, offset calculations can be consistent
  - `mov r0, array_base + (idx * sizeof(type))`

**Structs** are composed of many different types

- Therefore, offset calculations are going to be relative to each of the fields in the struct
  - `mov r0, struct_base + 0x4 // char (1 byte)`
  - `mov r1, struct_base + 0x8 // int (4 bytes)`
  - `mov r0, struct_base + 0x1E`

# Ghidra Autostruct

Right-click on a variable and select 'create autostruct'

Can edit the variable type to update fields in the struct

# Day 5 Binary

## Suggestions:

- Use ghidra's autostruct feature to generate astruct types for a variable
- malloc() can be a good way to check that the array size is correct
- Check how each of the struct fields are used in the program logic
- Try and identify what file the application is expecting