

# 12 Days of Ghidra

Nathan R

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

# Day 7 – Ghidra Script

# Introduction

Allows you to extend the functionality of ghidra

- E.g. -> [VTgrepGhidra](#)

Written in Python(2) or Java

- Python3 is available using third party extensions (not covered here)

API for interacting with core Ghidra components

- Program database -> var info, addr info

# Setup

Can be open within Ghidra itself

- Window -> script manager || Window -> python

Ghidra integrates with Eclipse for better IDE support

- [Download Eclipse](#)
- On Ubuntu can use snap -> `snap install --classic eclipse`
- On MacOS use brew -> `brew install --cask eclipse-java eclipse-cpp`

# Python Example

```
fm = currentProgram.getFunctionManager()  
  
funcs = fm.getFunctions(True) # True means 'forward'  
  
for func in funcs:  
    print("Function: {} @ 0x{}".format(func.getName(),  
func.getEntryPoint()))
```

Print the names of every function in the program

# Day 7 Binary

You need to construct a key using GhidraScript

- Concatenate function names based on forward CFG

Suggestions:

- Demangle the function name to remove noise
- Open the binary in ghidra to find a good entry point function
- A recursive algorithm could be useful