Worcester Polytechnic Institute
Department of Computer Science

Lab 17: Reverse Engineering with Ghidra.

Objectives:
Students will perform activities similar to those in the last lab, but with a different environment, Ghidra, which is an open-source tool developed by the NSA and released in 2019. In addition to the above activities, students will also analyze provided binary executables to practice their reverse engineering skills and get familiar with the Ghidra environment.

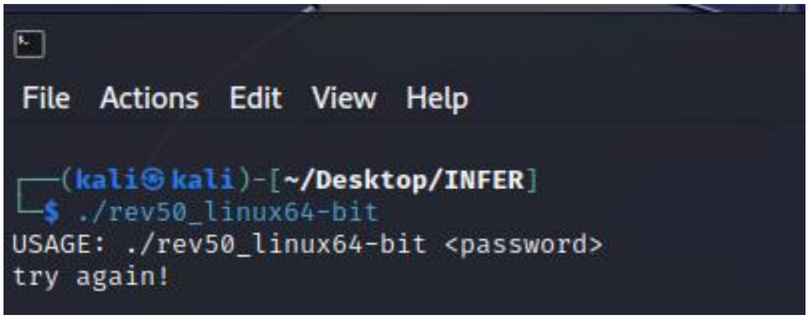
Preparation:
Download Ghidra in Linux
https://ghidra-sre.org/
Download the crackme program

Ghidra required Java 17+ in order to run the software,
To check java version in Linux
java -version

If no java installed,
sudo apt update
sudo apt install
sudo apt install openjdk-21-jdk

Task:

1. Run and test the crackme program

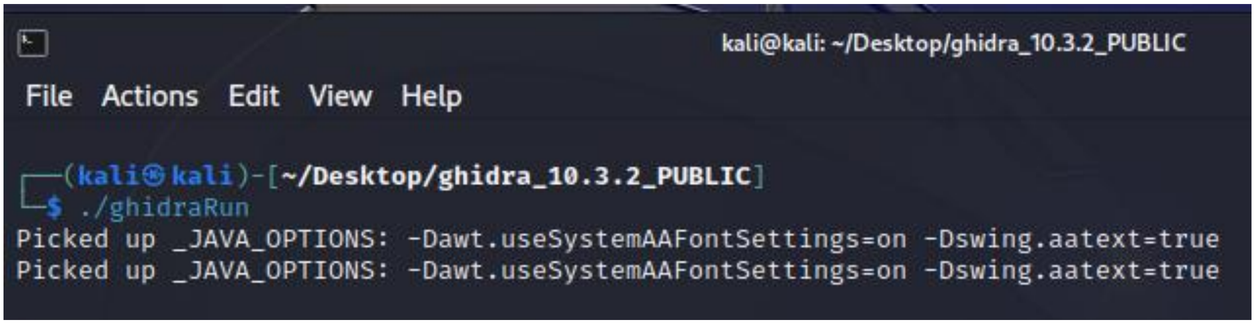


```
┌──(kali㉿kali)-[~/Desktop/INFER]
└─$ ./rev50_linux64-bit
USAGE: ./rev50_linux64-bit <password>
try again!
```

Notice program required a “password”

2. Inspect the program in Ghidra

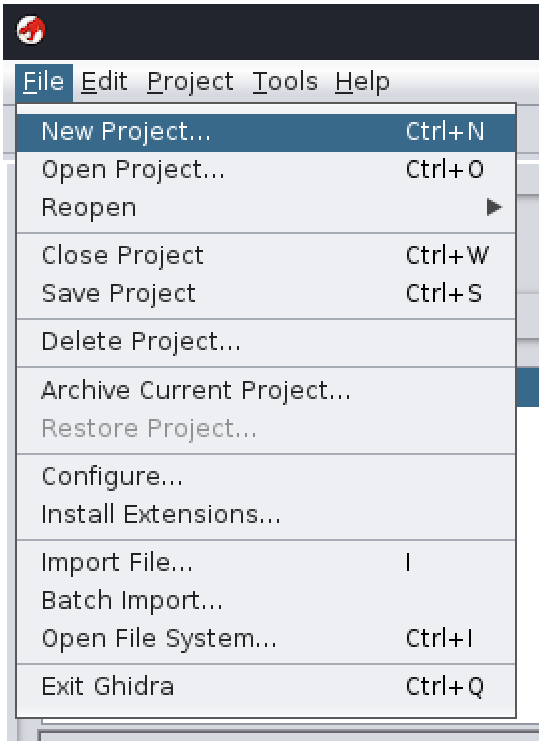
Open terminal and get into Ghidra folder, then enter ./ghidraRun


kali@kali: ~/Desktop/ghidra_10.3.2_PUBLIC
File Actions Edit View Help

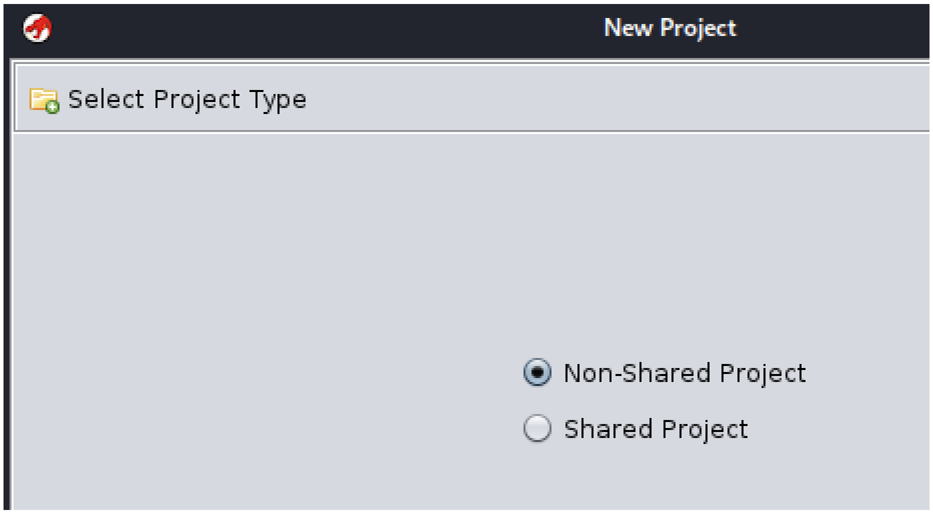
```
┌──(kali㉿kali)-[~/Desktop/ghidra_10.3.2_PUBLIC]
└─$ ./ghidraRun
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
```

If it shows no java installed, in the terminal, enter:
sudo apt update
sudo apt install
sudo apt install openjdk-21-jdk

After Ghidra started, click on File→New Project…



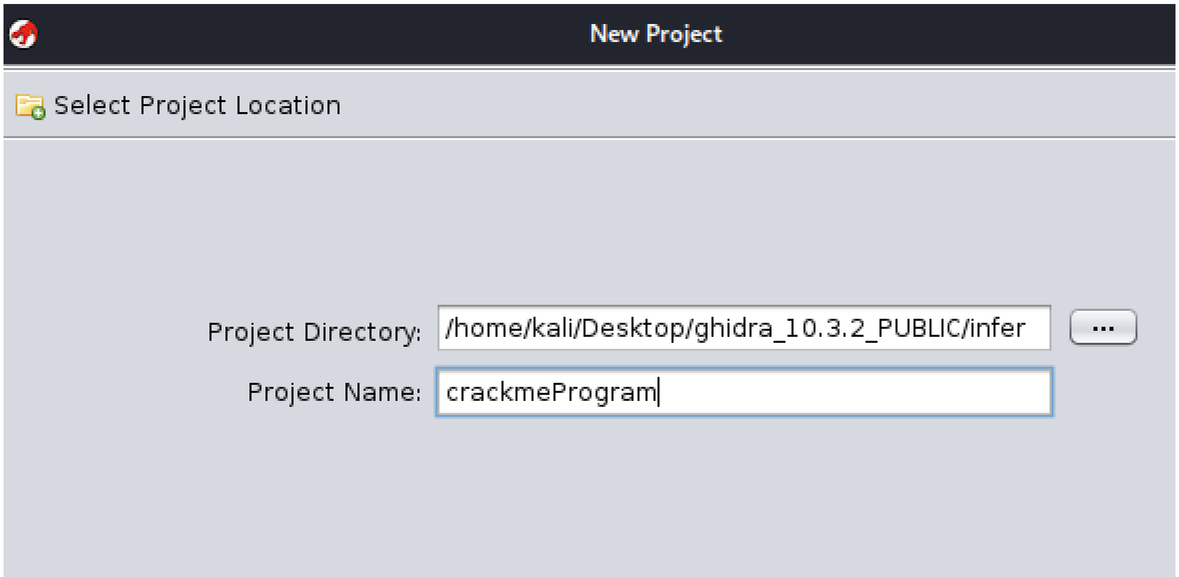
Then, select Non-Shared Project



● Non-Shared Project

○ Shared Project

Next, select a location and enter the project name

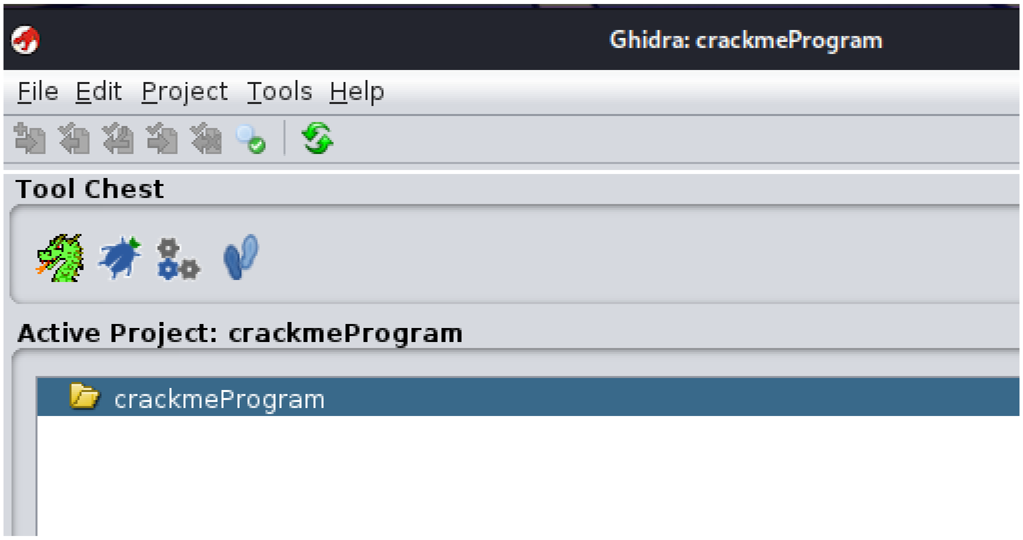


Project Directory: /home/kali/Desktop/ghidra_10.3.2_PUBLIC/infer

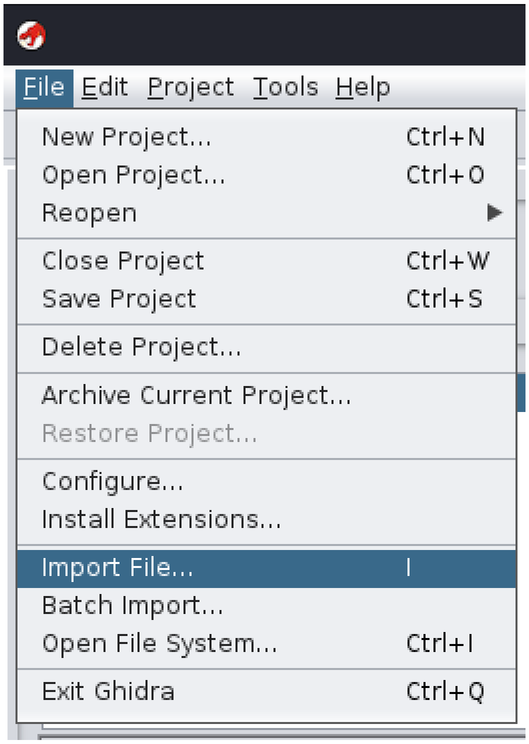
Project Name: crackmeProgram

From here, you can either

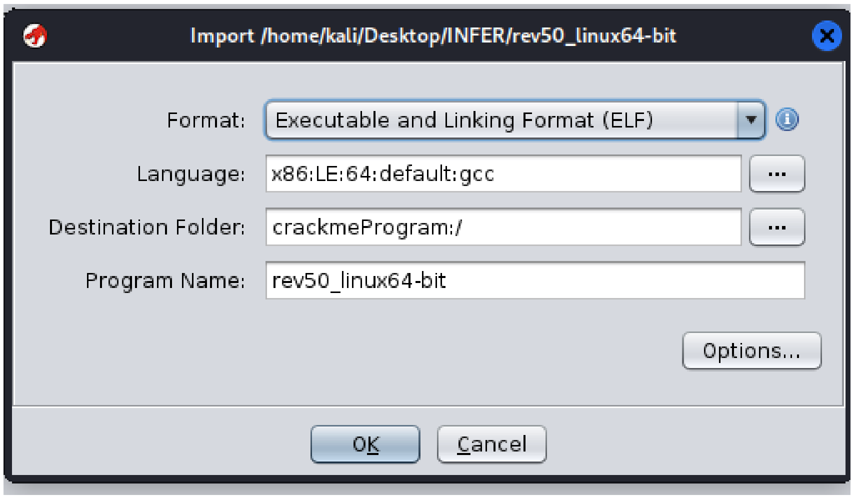
1) Drag the crackme program under this windows



2) Select File→Import File…



You should then see the import option



Import /home/kali/Desktop/INFER/rev50_linux64-bit

Format: Executable and Linking Format (ELF)

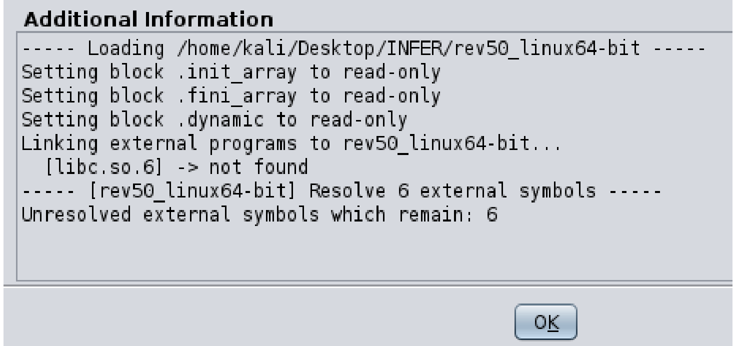
Language: x86:LE:64:default:gcc

Destination Folder: crackmeProgram:/

Program Name: rev50_linux64-bit

Leave it as default and click OK

Then, it should generate an import summary.
PS. it is fine too see libc.so.6 not found message in this example.

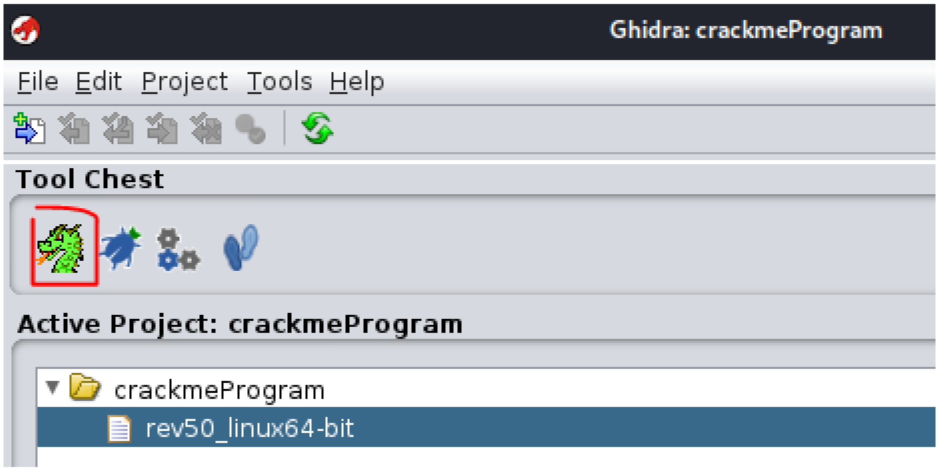


Additional Information

```
----- Loading /home/kali/Desktop/INFER/rev50_linux64-bit -----
Setting block .init_array to read-only
Setting block .fini_array to read-only
Setting block .dynamic to read-only
Linking external programs to rev50_linux64-bit...
  [libc.so.6] -> not found
----- [rev50_linux64-bit] Resolve 6 external symbols -----
Unresolved external symbols which remain: 6
```

Click OK.

Select the program and click on the dragon icon as shown in below

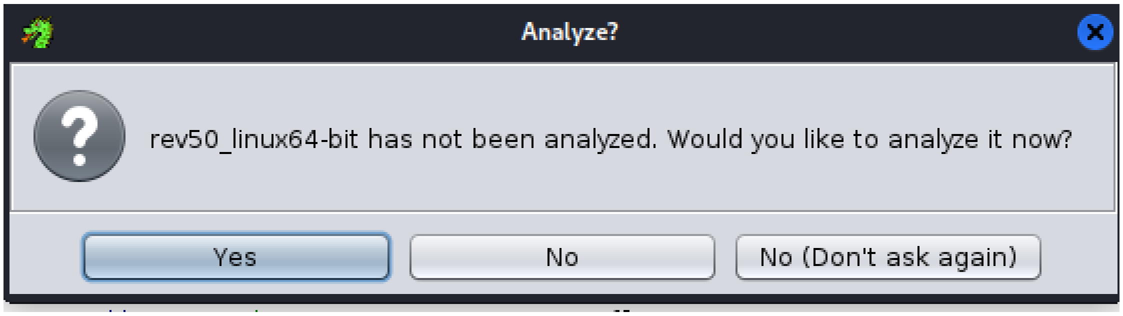


Ghidra: crackmeProgram

Active Project: crackmeProgram

- crackmeProgram
  - rev50_linux64-bit

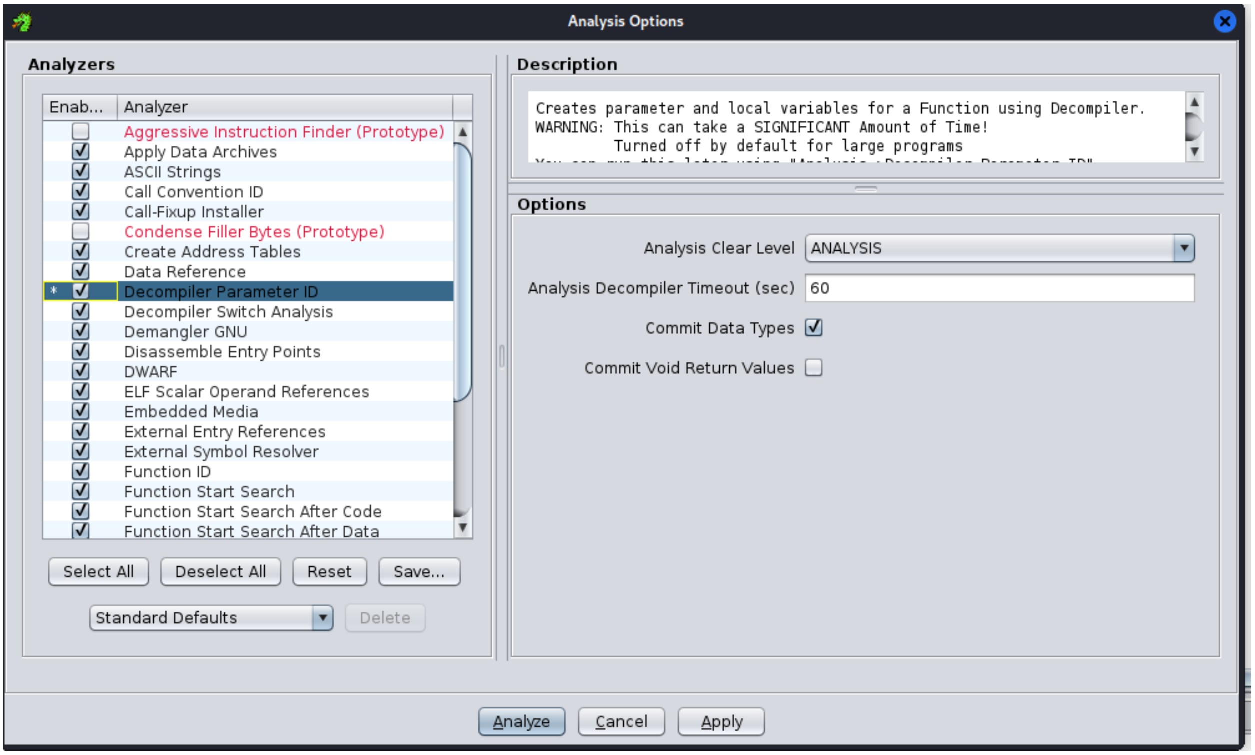
Click on Yes when the Analyze message shows up



Analyze?

rev50_linux64-bit has not been analyzed. Would you like to analyze it now?

Check the Decompiler Parameter ID and click Analyze



Analysis Options

Analyzers

Enab...	Analyzer
☐	Aggressive Instruction Finder (Prototype)
☑	Apply Data Archives
☑	ASCII Strings
☑	Call Convention ID
☑	Call-Fixup Installer
☐	Condense Filler Bytes (Prototype)
☑	Create Address Tables
☑	Data Reference
* ☑	Decompiler Parameter ID
☑	Decompiler Switch Analysis
☑	Demangler GNU
☑	Disassemble Entry Points
☑	DWARF
☑	ELF Scalar Operand References
☑	Embedded Media
☑	External Entry References
☑	External Symbol Resolver
☑	Function ID
☑	Function Start Search
☑	Function Start Search After Code
☑	Function Start Search After Data

Description

```
Creates parameter and local variables for a Function using Decompiler.
WARNING: This can take a SIGNIFICANT Amount of Time!
         Turned off by default for large programs
You can run this later using "Analysis->Decompiler Parameter ID"
```

Options

Analysis Clear Level: ANALYSIS

Analysis Decompiler Timeout (sec): 60

Commit Data Types ☑

Commit Void Return Values ☐

Task 2: Explore Ghidra Interface

Code browser
Listing window
Hax window

Task 3: Reverse engineering

(Follow this video and complete the lab)
https://www.youtube.com/watch?v=fTGTnrgjuGA&ab_channel=stacksmashing