binScan User's Guide

A binary scanning utility

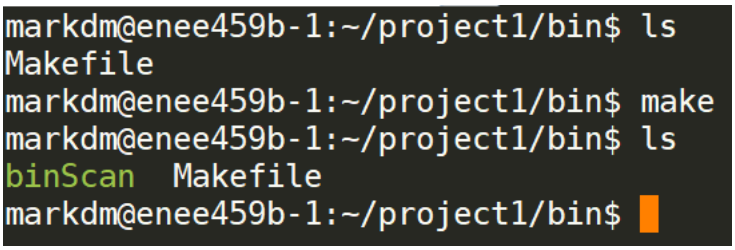
by Mark McCloskey

Table of Contents

Installation……3
Usage……4

Installation

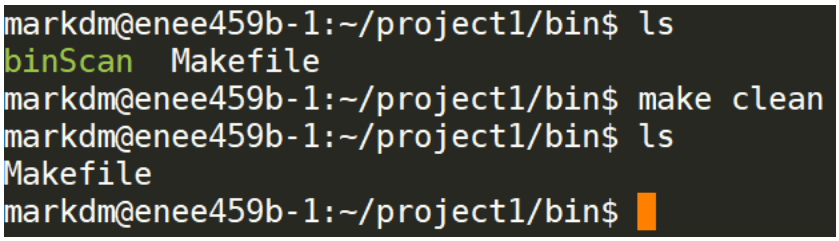
To install binScan navigate to the /bin directory, here you will find a Makefile which will build binScan for you. Type ‘make’ in the terminal and press enter. You will now see the executable in the directory.



make-ing the executable

Removal

To remove binScan navigate to the /bin directory, once again you will utilize the Makefile by typing the command ‘make clean’ and hitting enter. Once the command completes you will see that the binScan executable has been removed.



cleaning the executable

Usage

To start bin scan type ‘./binScan’ in the terminal then hit enter. Once the program is running you will be prompted to enter a username and password. Enter an acceptable username and password to gain access to the program.

```
markdm@enee459b-1:~/project1/bin$ ./binScan
Enter username: yourUsername
Enter password: yourPassword
```

Logging in

Once you’ve been authenticated you will be presented with an options menu that will allow you to choose what you want the program to do.

```
********
OPTIONS
********
1: Analyze Binary
2: Save Binary Information
3: Exit
Please choose a valid option:
```

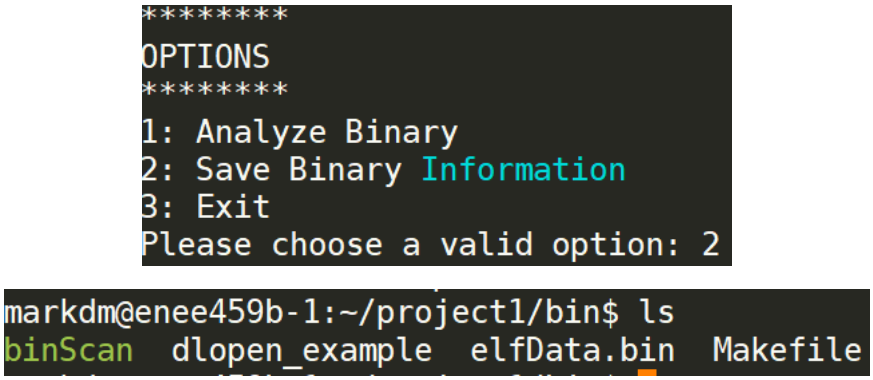
Options

To analyze a binary type ‘1’ and press enter. You will then be prompted to give the location of the binary you want analyzed. The binary’s name may be given if present in the same directory or a path to the binary may be passed. Once the binary has been analyzed the information gathered will be printed to the screen and the options menu will return.

```
Please choose a valid option: 1
Enter binary name: ../src/dlopen_example
Size of text section: 450
Number of dlopen calls: 1
Entropy of file: 0.440650
Strings passed to dlopen:
libcrypto.so
Hash of text section: 5685c4d66e53f1776594f35adc3fba
```

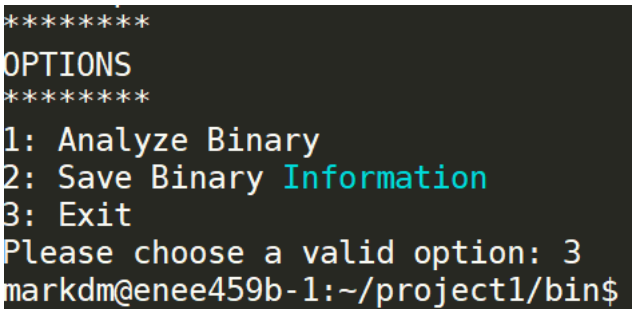
Analysis of a binary

After a binary has been analyzed you can save the information to disk by choosing option 2. This will create the file “elfData.bin” on disk.



Saving the analysis

Finally, you can exit the program by choosing option 3. This will return you to the terminal.



Exiting the program