**Practical 12**

**Objectives: To try decompiling C and Java programs**

To do this practical, you need the C compiler and the Java JDK on Windows and Linux. Kali already has a C compiler.

**Exercise Installing a C compiler in Windows**

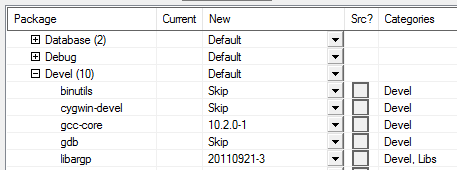
We will use Cygwin to install the C compiler on your Win10 virtual machine. You can download a prepared Cygwin-setup zip file that containing packages for the gcc compiler, perl and python interpreters and vi/nano text editors from BlackBoard or Dropbox link. You can also download the latest Cygwin and other packages from [www.cygwin.com](http://www.cygwin.com).

In Win10 VM :

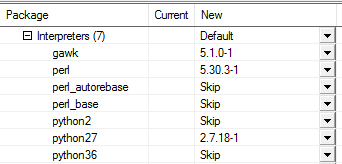
1. Create a folder “c:\cygwin-setup” on your virtual machine.
2. Download the prepared Cygwin setup zip file from BlackBoard or from the Dropbox link below, under “Files-for-Topic-12” into the cygwin-setup folder. You can also get the latest version of Cygwin from [www.cygwin.com](http://www.cygwin.com).

<https://www.dropbox.com/sh/4x22syj7ia8ppq2/AAB6fEPo2vrOxArtmHr6xU1ha>

1. Extract the contents of the Cygwin setup zip file. (the extraction may take 10 min)
2. Run the setup-x86\_64.exe to install Cygwin. Select “Install from Local Directory”.
3. For Root Directory, you can use the default C:\cygwin64 directory. Click Next.
4. For Local Package Directory, you can use the default value. Click Next.
5. In the Select Packages, expand All.
6. Under Devel category, click on the down arrow for gcc-core and select the version number.



1. Under Interpreters, select the perl and python27 package (instead of python27, you can select python36).



1. Under Editors category, select either vim or nano or both for your text editor. Click Next. Click Next. The selected packages will be installed.
2. Run Cygwin64 Terminal.
3. Create the following C program “enternumber.c” (if you are using Notepad to create the C source file, save it in C:\cygwin64\home\*<username>*).

This program asks the user to enter a number and then prints the number to the screen.

#include <stdio.h>

int main() {

int number;

printf("Enter a number: ");

scanf("%d", &number);

printf("You have entered %d\n", number);

}

1. In the Cygwin terminal, run the following command to compile the C program into an executable called “enternumber”.

gcc enternumber.c –o enternumber

1. Run “ls” to check that the file “enternumber.exe” has been created.
2. Run the executable to test it.

./enternumber.exe

**Exercise Installing the Java JDK in Windows**

In Win10 VM:

1. You can download the Java JDK from BlackBoard or from the previous Dropbox link under “Files-for-Topic12”. Java 8 has Long-Term Support which the newer versions of Java do not have.
2. Run the Java JDK setup file and install it using default options.
3. Go to My Computer. Open C drive. Open Program Files. Open the Java folder. Open the folder where the JDK is installed. Look in the bin folder to see the programs javac.exe and java.exe.

The program javac is used to compile Java programs.

The program java is used to run compiled Java classes.

1. Right-click on the Windows icon in the bottom left corner and choose System.
2. Click on Advanced system settings.
3. Click on Environment Variables.
4. Under System variables, select Path and click Edit.
5. Append the following string to the Variable value textbox so that the Java JDK is in the Path. Do not overwrite the original values.

The path may change depending on your JDK version.

;C:\Program Files\Java\jdk1.8.0\_271\bin

1. Click OK. Click OK. Click OK. You can now run “javac” or “java” without having to specify their full path names.
2. In a Command Prompt, check your Java JDK version on the Windows VM.

javac –version

**Exercise Creating a Java program and a C program in Windows and try running them in Linux**

In Win10 VM:

1. Create the following Java program called “HelloWorld.java”. You can use Notepad to create the file.

class HelloWorld {

public static void main(String[] args) {

System.out.println("Hello World");

}

}

1. In a Command Prompt, compile and run it.

javac HelloWorld.java

java HelloWorld

1. Run Cygwin.
2. Create the following C program called “HelloWorld.c”.

#include <stdio.h>

int main () {

printf("Hello World\n");

}

1. Compile and run it.

gcc HelloWorld.c –o HelloWorld

./HelloWorld

On Kali:

1. Copy the compiled HelloWorld.class file from your Win10 to your Kali.
2. Run the Java class file. You should be successful. Remember that Java programs compiled in a later version can not be run in an earlier version.

java HelloWorld

1. Copy the compiled C program c:\cygwin64\home\*<username>*\HelloWorld.exe executable file from your Win10 to your Kali.
2. In Kali, try to run the C executable. You should get an error.

sudo chmod 755 HelloWorld.exe (this is to set the executable permission)

./HelloWorld.exe

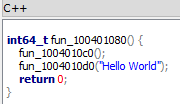
**Exercise De-compiling the C executable with Snowman Decompiler**

We will try Snowman Decompiler to try to decompile the C program.

In Win10 VM

1. Download the Snowman Decompiler 7z file from Blackboard or the Dropbox link. You can also download the latest version of the Snowman Decompiler from https://derevenets.com.
2. Download the 7-zip installer (use the x64-bit for Win10) and install it.
3. Extract the Snowman Decompiler.
4. Run the snowman.exe.
5. Go to File, Open. Open the HelloWorld C program executable c:\cygwin64\home\*<username>*\HelloWorld.exe
6. In the left hand column, the HelloWorld program is disassembled into assembly code. In the right hand column, the HelloWorld program is decompiled into C code. It is not easy to understand the decompiled code.

Somewhere near the bottom of the C decompiled code output in Snowman, you can see the printf(“Hello World”)



**Exercise De-compiling the Java class file with Jad**

In Kali:

1. Download the Jad for Linux zip file from Blackboard or the Dropbox link.
2. Extract the Jad for Linux zip file.
3. Use Jad to decompile the Java class file HelloWorld.class.

./jad HelloWorld.class

1. Use a text editor to view the generated HelloWorld.jad. Is it similar to the original Java source file?

Java programs are easier to decompile than C programs.

**Exercise Obfuscating a Java Program (STOP HERE)**

Programmers of commercial software may not wish to have their products reverse-engineered so easily. So they would try to obfuscate their software to prevent others from decompiling it.

**Decompiling a sample class file**

In Kali:

1. Create the following 2 directories.

* proguard-in
* proguard-out

1. Download the sample CalculateArea.class from BlackBoard or Dropbox link.
2. Try running the CalculateArea.class.

java CalculateArea

1. Use Jad to decompile the class file.

./jad CalculateArea.class

1. View the decompiled file CalculateArea.jad to see the generated source. Can you more or less understand the decompiled code?

**Using ProGuard to obfuscate a program**

1. Copy the CalculateArea.class to the proguard-in directory.

cp CalculateArea.class proguard-in

1. Download the ProGuard zip file from BlackBoard or the Dropbox link. (You can also download from https://github.com/Guardsquare/proguard but the latest version is more for Android platforms)
2. Extract out the contents of the downloaded ProGuard file.

tar –xvf proguard6.2.0.tar.gz

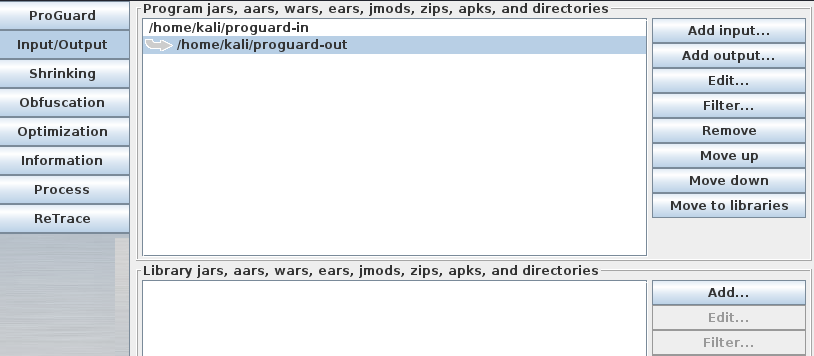
1. Change directory to the proguard/lib directory.

cd proguard6.2.0/lib

1. Run the ProGuard GUI.

java -jar proguardgui.jar

1. Click on Input/Output button.
2. Click on Add input and select the proguard-in directory that you just created.
3. Click on Add output and select the proguard-out directory that you just created.
4. Under the Library jars section, select the /usr/lib/jvm/java-11-openjdk-amd64/lib/rt.jar entry and click Remove (see following diagram).



Remove the rt.jar entry

1. Click on Shrink button and uncheck the Shrinking option.
2. Click on Obfuscation button and check Overload aggressively.
3. Click on Information button and check Ignore warnings about possibly erroneous input.
4. Click on Process button and click Process! to start the obfuscating.
5. In a terminal, view the file created in proguard-out directory. This is the obfuscated version of the CalculateArea.class.
6. Change directory to the proguard-out directory.
7. Try running the obfuscated CalculateArea.class. It should run the same way as before.

java CalculateArea

1. Use Jad to decompile the class file (remember to specify the path to the jad program)

jad CalculateArea.class

1. View the decompiled file CalculateArea.jad to see the generated source.

Because the CalculateArea is a simple program, the difference in the obfuscated decompiled code is not much. But you can see some lines of code are more difficult to understand.

**Exercise Decompiling Java Applets**

In Win10 (or any Windows system):

1. Download the Jad for Windows from BlackBoard or Dropbox link.
2. Unzip the contents of the Jad zip file. There is a jad.exe and a Readme.txt.
3. View the contents of the unzipped file.
4. Let’s find a Java Applet to decompile. Browse to the following webpage for a sample Java applet.

http://www.cs.rit.edu/~ncs/color/a\_spaces.html

1. The applet may not be able to run due to web browser security restrictions.
2. Right-click in the web page and choose View Source.
3. Look for the APPLET tag in the source. The code attribute indicates the name of the class file and the codebase attribute indicates the directory where the class file can be found.

The code file is in “.” (current directory)

The code is found in “F.class”



1. As the F.class is located in the current directory, change the URL in the Web Browser to the following :

http://www.cs.rit.edu/~ncs/color/F.class

1. Download the F.class.
2. Run the jad.exe in a Command Prompt to decompile the Java applet.

You may have to specify the path to the jad and F.class files

jad F.class

1. Use a text editor to open the F.jad file to see the decompiled Java code.

**Decompiler Quiz**

Try the Decompiler Quiz on BlackBoard (to help in your General Performance marks).

**Activity 1**

Download the HelloWorldHacked.class from BlackBoard to either your Windows or Linux and run it to see the output. Using your knowledge of decompilation, try to find a security loophole in the Java program. Run the HelloWorldHacked to cause the security loophole to be activated (if you are successful, a message about reaching the backdoor will be displayed).

Activity 1 Quiz

Answer the question in Activity 1 Quiz, If you answer the question correctly, you will be able to see and proceed to Activity 2. There are 3 Activities in total.

*End of Practical*