

**Information Security:**

TITLE: ASSIGNMENT 02

NAMES:

ADBUL REHMAN QASIM (20I-0946)

SHEIR MUHAMMAD (20I-0958)

INSTRUCTOR:

Dr. Zainab Abid

SUBMISSION:

<SUBMISSION DATE>

# **PART 01:**

The task here is to download the apk file for the mobile app to be used for the repackaging attack, and to establish a connection with the android virtual machine being hosted on the same device over the same network!

**<honestly we weren’t able to establish a connection between both vm’s ah well it is what it is!>**

Commands:

1. adb connect <ip address of android vm>
2. adb install <application\_name>.apk

# PART 02:

The objective of this phase is to extract the source code from the application and then re-package the source code with our ever so trusty totally not malicious code**. ONLY THE DISASSEMBLY WAS DONE HERE FOR THIS PHASE.**

This would help convert the code to samli code. <don’t know what this means either>

Commands:

1. apktool d <application\_name>.apk

# PART 03:

Here, we had to now add the malicious code file into the source code folder of the application to be targeted.

# PART 04:

Commands:

1. Apktool b <application\_folder\_name>
2. keytool -alias <alias\_name> -genkey -v -keystore mykey.keystore
3. jarsigner -keystore mykey.keystore app\_name.apk <alias\_name>

Tasks:

1. Now repackage the application after adding the code.
2. Generate the public and private keys:
3. Sign the apk file.

# PART 05:

Install the repackaged application and then trigger your creation of destruction.

# PART 06: