

Configuration Manual

MSc Internship
Cyber Security

Siddesh Ningappa
Student ID: x19141521

School of Computing
National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Siddesh Ningappa
Student ID: x19141521
Programme: Cyber Security **Year:** 2019-2020
Module: Internship
Lecturer: 17-08-2020
Submission Due Date:
Project Title: YARA based defence mechanism against NFC based attacks for Android devices
Word Count: 508 **Page Count:** 1

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: Siddesh Ningappa

Date: 17-08-2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	

Penalty Applied (if applicable):	
----------------------------------	--

Configuration Manual

Siddesh Ningappa
Student ID: x19141521

1 Overview

This document provides information about the pre-requisites required to replicate the implementation and also documents the necessary tools and scripts required for successful operation of the project. This will also assist on instructions on how to build and execute the code. The application is built in java programming language.

2 Dependencies

The user should have Java Development Kit(JDK),Android Studio and setup Android Virtual Device (AVD)with minimum API level of 29 within Android Studio. For testing the user should have any NFC enabled Android smartphone.

AWS ec2 instance(Ubuntu server-any version)

Nginx or any web server

YARA tool(any version)[4]

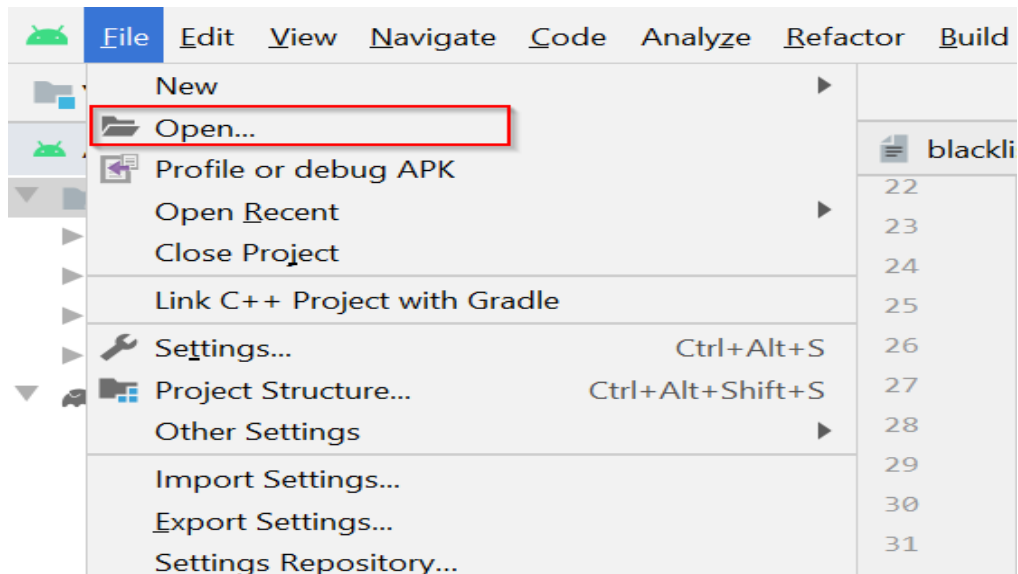
3 Installation

Install Android Studio[3]

Extract the zip file,

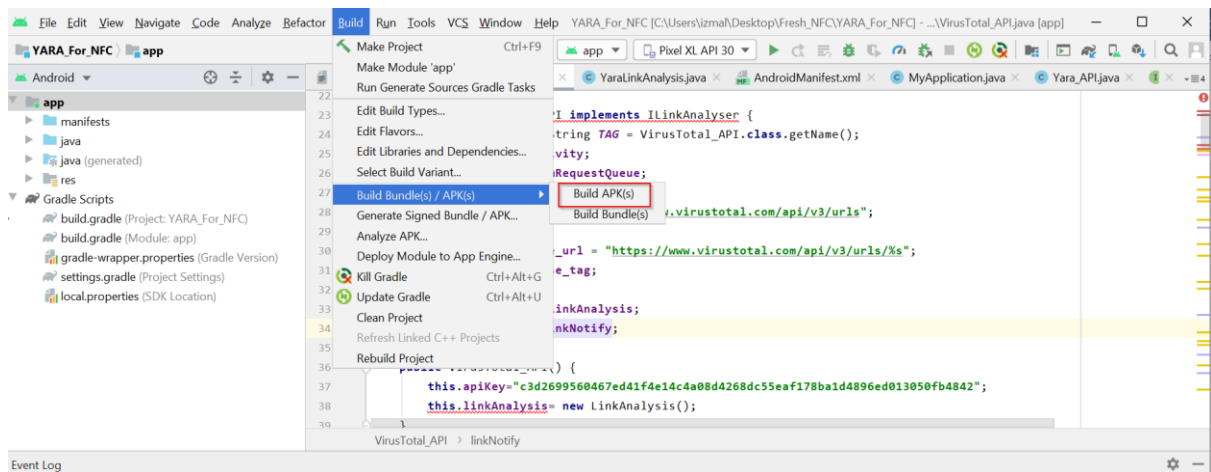
Open Android studio.

Click on File→ open

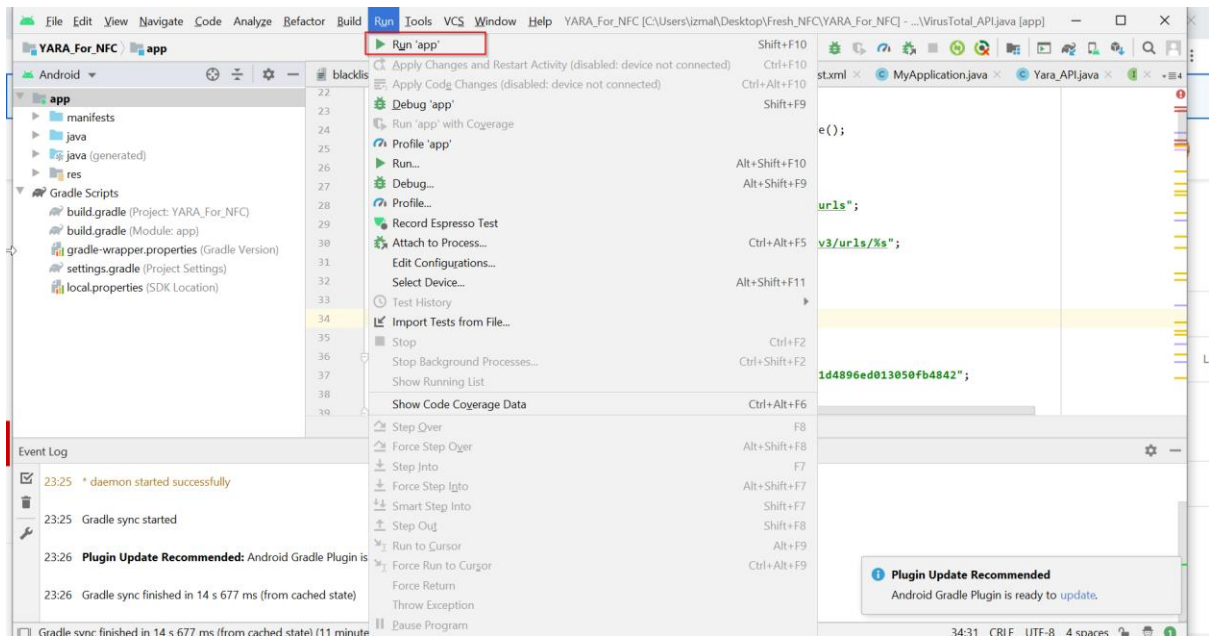


Navigate to the extracted directory and select the directory

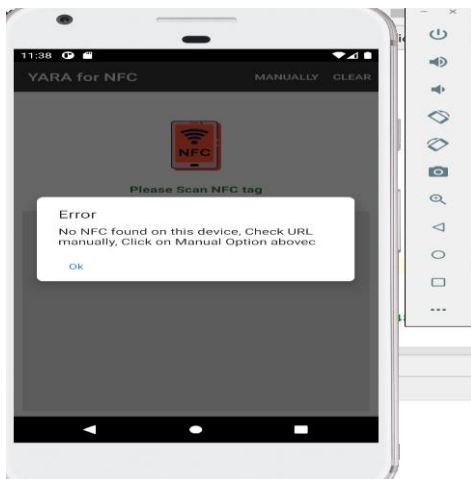
Once done, Click on Build, Build Bundle/APK → Build APK



Once the Build is complete, Click on Run →



This will trigger the AVD and the application will run



Server Side

AWS ec2 instance minimum of 2GB RAM and 40 GB HDD/SSD

```
root@kali:~/nfc# ssh -i "nfc.pem" ubuntu@ec2-54-204-6-177.compute-1.amazonaws.com
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1111-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Are you ready for Kubernetes 1.19? It's nearly here! Try RC3 with
   sudo snap install microk8s --channel=1.19/candidate --classic
   https://microk8s.io/ has docs and details.

18 packages can be updated.
0 updates are security updates.

Last login: Sun Aug 16 22:20:28 2020 from 37.228.254.129
ubuntu@ip-172-31-42-94:~$ id
uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),110(lxd)
```

Install Nginx server (`sudo apt install nginx`)[1]

```
ubuntu@ip-172-31-42-94:~$ sudo apt install nginx
Reading package lists... Done
Building dependency tree
Reading state information... Done
nginx is already the newest version (1.10.3-0ubuntu0.16.04.5).
0 upgraded, 0 newly installed, 0 to remove and 14 not upgraded.
ubuntu@ip-172-31-42-94:~$
```

Install YARA tool(`sudo apt install yara`)

```
ubuntu@ip-172-31-42-94:~$ sudo apt install yara
Reading package lists... Done
Building dependency tree
Reading state information... Done
yara is already the newest version (3.4.0+dfsg-2build1).
0 upgraded, 0 newly installed, 0 to remove and 14 not upgraded.
ubuntu@ip-172-31-42-94:~$
```

4 Installation of built APK On Android Device

Once the build is completed from the above step,
Navigate to `app\build\outputs\apk\debug` directory
You will be able to identify `app-debug.apk`.
Copy the file to Android device,
On the Android device, enable install application from untrusted sources from settings
Once done click on the copied APK file.
Application will be installed

5 Testing

Once the application is installed, enable NFC on your smartphone, open the app “YARA for NFC” and scan any NFC tag. If the tag contains malicious URL, you will get a response stating malicious URL in red else the URL will be displayed in Green

6 References

- [1] Ubuntu. 2020. *Install and Configure Nginx | Ubuntu*. [online] Available at: <<https://ubuntu.com/tutorials/install-and-configure-nginx>> [Accessed 16 August 2020].
- [2] Amazon Web Services, Inc. 2020. *Amazon EC2 Instance Types - Amazon Web Services*. [online] Available at: <<https://aws.amazon.com/ec2/instance-types/>> [Accessed 16 August 2020].
- [3] Android Developers. 2020. *Download Android Studio and SDK Tools | Android Developers*. [online] Available at: <<https://developer.android.com/studio>> [Accessed 16 August 2020].
- [4] Virustotal.github.io. 2020. *YARA - The Pattern Matching Swiss Knife for Malware Researchers*. [online] Available at: <<https://virustotal.github.io/yara/>> [Accessed 16 August 2020].