International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-5, Issue-2, February 2019 Pages 06-09

An Open Source Android Applications Penetration Testing Lab

Sawan Bhan, Nisha TN

***Abstract*— Today, the majority of people have become completely dependent on mobileapplications. These applications could be a gateway to sensitive data that attract more hackers. The Android penetration testing process helps to address security weaknesses or vulnerabilities in the Android platform. In this paper, we present different penetration tests (or pentests) for Android-based mobile applications in a very comprehensive manner. First, we explain how to set up a pentesting environment, including hardware/software requirements, USB debugging, and configuring a proxy.Next, weperform some of the most popular pen testing tools such as AFLogical, Dex2jar, JD-GUI, Apktool and Drozer by using Santoku Linux distribution. Finally, we conduct an Android repackaging attack on selected apps byusing Santoku Linux distribution and then demonstrate the attack on our Android VM. This work attempts to give developers and security professionals a step-by-step guide for Android mobile application pen testing.**

***Index Terms*— Vulnerability, Penetration, Testing, Assessment, Security.**

I. INTRODUCTION

A. *Android PenetrationTesting*

In the present day, people use their smartphones in almost every aspect of their life, social interactions, career,finance,learning,and even health. According to Statista[1],"allofthe non-gaming app publishers in the Google Play Store had double-digit download figures without any signs of slowing down." The rapidly increasing number of mobileapplication users has attracted more hackers. This not only increases the possibility and number of smartphones that hackers could target, but it also increases the possibility to hack any system or device that connects to the same network. Smartphone penetration testing is one of the most essential kinds of security pentesting that demonstrate what exploitable vulnerabilities exist within application and the level of damage that could occur if the application is hacked. In general, penetration testing or (ethical hacking) is the process of discovering security weaknesses and raising the security level of systems, networks, or applications as performed by a penetration tester or auditor.Also, it is important to point out that penetration testing (often shortened as pentesting) is commonly mistaken as vulnerability testing. In fact, vulnerability testing is to identify potential problems, where penetration testing is meant to analyze those problems as well as attack the system to determine vulnerabilities. Among the mobile Oss ,Android is one of the most popular and the fastest growing mobile operating system. However, during application development, sometimes developers make security mistakes or ignore the secure coding practices. So, Android apps often contain security weaknesses that need to be discovered before a successful hack. Application vulnerabilities, insecure password storage, information disclosure, manifest privileges, insecure file permissions, and DDoS attacks are all common vulnerabilities foundamongpentesting applications. The more protection the application needs, the more often pentesting should be implemented to decrease the possibility of any attack.There is a large amount of resources of mobile application pentesting tools that are available on the Internet. In this paper, we use Santoku Linux distribution [2] that is designed specifically for mobile forensics, mobile malware analysis, and mobile security testing. Basically, we cover the main steps that needed to conduct Android application pentesting such as setting up the environment, configuring proxy, and performing some security tools required for Android pentesting. Also, we conduct Android mobile application repackaging at tackasasimulation of how an attacker could repack an Android application.

Sawan Bhan, Symbiosis Centre for Information Technology,Pune,India
Nisha TN, Symbiosis Centre for Information Technology,Pune,India

B. *The Basics of Android*

Android is Linux-based open source software which is divided into five main layers as shown in the architecture diagram below, Figure 1. Basically, it is designed in the form of a software stack architecture that contains four core layers:

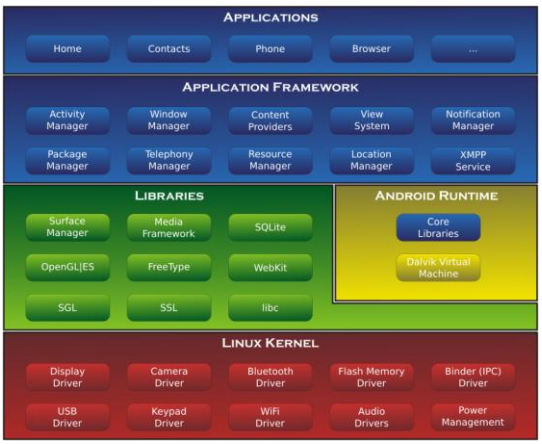

Figure 1 Five core layers of Android [3]

1. Applicationlayer:
The application layer is the top layer of the stack. It contains native applications and third- party applications

that are installed by a user such as (WhatsApp and Snapchat).

2. Application Framework layer:

The application Framework layer provides many upper level services to applications that manage and control the application layer. In this layer, the developers of the application are the only people who are allowed to control installed applications. The Android framework includes four types of Android application components:

Activities: It controls all tasks through graphical user interface performed by a user. *a)*
Content:It provides access to the installed applications to share information with other applications.

Services: Provides access to non-code embedded services which allow the user to execute multiple application during one time such as listing to music while using the internet.

Notifications orBroadcast:

It displays alerts and notifications.

3. Libraries

This layer controls and accesses applications data. Android provides a lot of C/C++ libraries for different uses. Here some of the most useful libraries:

- ***System C Library***: It allows developers to createapplications.
- ***Media framework:*** It is useful to program video and audio files.
- ***Android.content:*** It allows messaging between applications and application components.
- ***Android.webkit***: It provides access to the internet within anapplication

4. Android runtime
This layer consists of Dalvik Virtual Machine (DVM) and a set of core java programming libraries. Before running any java applications, java files are converted into Dalvikformat (dex) to be optimized for a minimum memory.

5. LinuxKernel
This layer is the most important layer because it controls core services such as hardware, memory management, power controls, security, and rest of the software stack.

II. OBJECTIVE

The objective of this thesis is to understand android security architecture and analyze the android application security using an applied Android mobile application penetration-testing framework**.**

III. SYSTEM ANALYSIS

A. Penetration Testingis the process of testing the security of the application, network, and system etc. It is performed with the prior permission from the authority. Penetration testing is a systematic approach to find out the vulnerability/Vulnerabilities present in the given target. The target can be web application, mobile application, system, server, ornetwork.

The findings are documented in a standard document structure.The documentisre-checked for the correctness of the details mentioned in the document. Document consists of 3 mainparts, the yare–Executive summary, Vulnerabilities report, & Annexure – Areport This report is submitted to the authority of the target.

B. TOPMobileapplicationThreats:

1. ***Weak Server Side Controls***
2. ***Lack of Binary Protections***
3. ***Insecure Data Storage***
4. ***Insufficient Transport Layer Protection***
5. ***Unintended Data Leakage***
6. ***Poor Authorization and Authentication***
7. ***Broken Cryptography***
8. ***Client Side Injection***
9. ***Security Decisions via Untrusted Inputs***
10. ***Improper Session Handling***

IV. USEFUL TOOLS

Below are some of the important tools used while performingSecurityAssessmentofandroidapplication:

1. **ADB**: It is a CLI based interface that is used to interact with the Android Device.
2. **DBBrowserforSQLite**–Thistoolisusedtoviewthe database file extracted throughADB.
3. **Apktool** – This tool is used to reverse engineer the androidapplication.Thistooldecodestoitsalmostoriginal form.
4. **Dex2jar**–This tool is used to convert the .dex file to .jar file to View the source code of the application.
5. **Drozer** – This tool provides huge collection of public exploitsfortestingthesecurityoftheapplication.

6. **MobSF**– This tool is a powerful framework for performing static analysis, dynamic analysis of android application.

7. **Logcat**–This tool dumps the all the system logs.

V. PENETRATION TESTING PHASES

Gathering information – This is the first stage in Penetration testing where the basic information and functionalities of the application is gathered.

1. **Analysis and Planning –** This is the second stage in penetration testing. In this stage the planning is made to carry out the test. This involves deciding the flow of execution.

2. **VulnerabilityDiscovery**–In this stage vulnerabilities are discovered either using tool or manually.This stage finds out thevulnerabilities present in the application.

3. **Exploitation**-In this stage the actual attack is done on the application.In this stage the attack is performed to find out level of severity of the vulnerabilities.

4. **Risk Analysis and Recommendation**–In this stage the analysis of risk is performed to find out the impact.

5. **Reporting –** This is the post stage of testing the application.In this stage a detailed report is prepared on the findings and submitted to the person concerned.

VI. SETTING UP THE TESTINGENVIRONMENT

Download and installSantoku OS - Linux distro,Genymotion - Android emulator and Virtual Boxfromrespectiveofficialwebsites.

Virtual box and Genymotion installation and Setup process is straight forward. However, after installing Genymotion, we need to perform the following steps:

- Click on "Add". This will show us the list of android virtual devices you can add.
- Choose the one with which you like to work. I have used"Google Galaxy Nexus - 4.1.1- API 16 - 720x1280".
- Follow the next screens. This will download and install the virtual device.

Now Start the Android virtual device from the genymotion as shown.

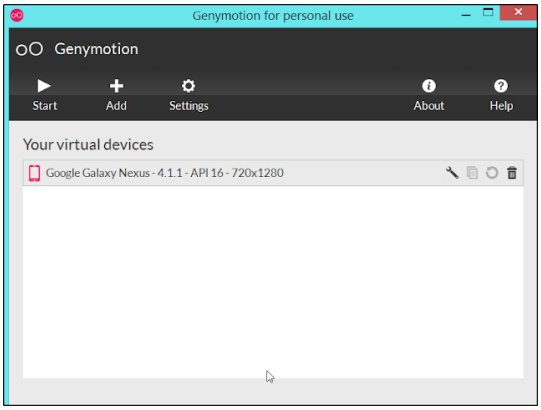

Figure 2(Genymotion setup page)

The virtual mobile device will boot up and appear on the screen like this:

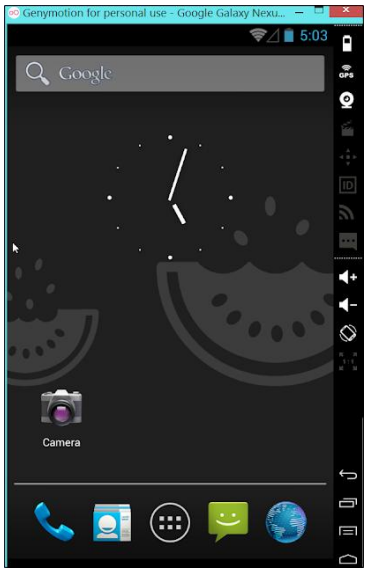

Figure 3 (Virtual android Device)

Now, we can proceed with the installation of Santoku OS in the virtual box, and provide around 30 GB space for the Santoku virtual hard drive. The final setting in the virtual box looks like as shown below:

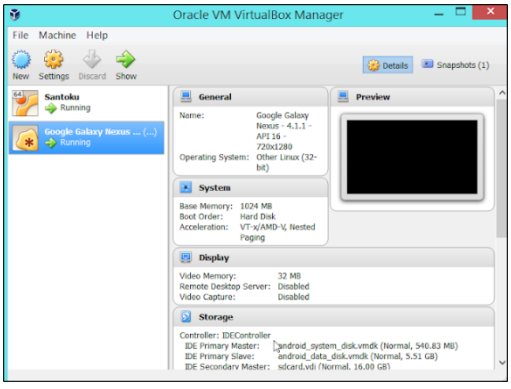

Figure 4(Installation settings for Saktoku Linux installation on virtual machine)

Then ,launch Santoku VM within VirtualBox.

Since each vulnerability analysis area requires different tools to examine the security configuration of the application, the tools of Santoku is categorized intofour areas:

1. Device Forensics tools,
2. Penetration testing tools,
3. Reverse engineering tools,
4. Wireless analyzers tools

Figure 5 Santoku Linux distribution desktop

Connecting Virtual Genimotion Device with Santoku linux:

Open the terminal in Santoku (under accessories-->lxTerminal). Connect the Santoku terminal with the adb device by using the following command: adb connect ip address emulator

Example:***adb connect 192.168.1.2***

If the connection is successful, verify that the emulator is connected by typing the following command on the terminal:

adb devices

Figure6 (adb connection)

So, we are ready to go and will be getting our hands dirty.

VII. CONCLUSION

Although developers care about security, not all of them have enough knowledge to diagnose or address security issues. It may be impossible to create a fullysecure environment, but there are some ways that help to identify threats and preventdata disclosure. Mobile penetration testing helps to address security weaknesses or vulnerabilities that exist within the mobile infrastructure.

Usage of android application is increasing exponentially. Android apps are being developed and used to carry out everyoperation.VAPTonandroidapplicationswillhelpto find out the vulnerabilities present in the application. By knowingthevulnerabilities, the developer can patch those vulnerabilities.

REFERENCES

[1] Statista, “Annual number of mobile app downloads worldwide 2022 | Statistic,”2018, *Statista*. [Online]. Available: https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobileapp- store-downloads/. [Accessed:07-Jun-2018].

[2] Santoku-Linux. Retrieved from https://santoku-linux.com/.

[3] Android App Development Tutorial. (n.d.). Retrieved fromhttp://android-app-tutorial.blogspot.com/2012/08/architecture-system-application-stack.html#.WxenJPZFzRM

[4] Guarda, Teresa, et al. “Penetration Testing on Virtual Environments.” *Proceedingsof the 4th International Conference on Information and Network Security - ICINS 16*, 2016,doi:10.1145/3026724.3026728.

[5] Denis, Matthew, et al. “Penetration testing: Concepts, attack methods, anddefense strategies.” *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2016, doi:10.1109/lisat.2016.7494156.

[6] KoopariRoopkumar and Bharath Kumar, "Ethical Hacking UsingPenetration Testing" (2014). *LSU*

[7] Dawson, Joel, and J. Todd Mcdonald. “Improving Penetration TestingMethodologies for Security-Based Risk Assessment.” *2016 Cybersecurity Symposium (CYBERSEC)*, 2016,doi:10.1109/cybersec.2016.016.

[8] Android Studio. Retrieved from https://developer.android.com/studio/install