Penetration Testing of Vulnerability in Android Linux Kernel Layer via an Open Network (Wi-Fi)

Buthaina Mohammed Al-Zadjali
Sohar University,
General Foundation Program
(Computing program)
Sohar, University Rd, 311
Sultanate of Oman

ABSTRACT

Android Smartphones, which is highly competitive smart phone in market, stores an enormous amount of data locally and remotely which sometimes cause a big challenge in security feature encouraging hackers to inject the malicious code in Android OS to steal the confidential data.

The key focus of this paper is to analyze and investigate the vulnerability in Android OS by injecting malicious code through penetration tools in the Linux kernel layer. This work will involve to selecting one type of security threats in Android system which is a Wireless access point (Wi-Fi) to evaluate the vulnerability in Android to proof if possible to attack the Linux Kernel in Android system through the open Wi-Fi network. This test will be done by using the Metasploit Framework.

General Terms

Android system, vulnerability, security.

Keywords

Android Smartphone, Linux Kernel Layer, penetration test.

1. INTRODUCTION

Smartphones have become indispensable Mobile devices for many users with different types and versions. The Android platform most widely used systems in the smartphones and it involves more security challenges. Unfortunately, it's become fertile ground for hackers to deploy different types of criminal activities. While, All Smartphones require connecting to the network through 3G, 4G and Wi-Fi instead of using the static network as the desktop computer and server the security threats in these smartphones increased [1].In addition, the new features which recently added in Android as Bluetooth, GPS and Wi-Fi make the Linux Kernel more vulnerable [2].For that reason, there is an urgent need to have a Forensic system and security Analytic which can facilitate for the forensic investigator to examine and analyze the vulnerabilities in Android system and to reduce the risk of these vulnerabilities. To detect the vulnerabilities in the Android system through the Wi-Fi connection, the penetration testing tools is the useful way to finding the security holes in Android Linux Kernel. A penetration test is a method which used to evaluating the security in any system such as computer, network and Mobile phone [3].

2. CLASSIFICATION OF PENETRATION TEST

Nowadays, many Corporations and other entities trying to defend their networks against various types of network attacks. Although, the traditional methods which they used before are firewalls and intrusion detection devices it is not enough to protect their network, so they need to utilize specialists who are having more knowledge in, how can exploit both known and unknown vulnerabilities in network to evaluate and determine the security of the network in their Corporation [4].

There are three classifications of Penetration Test: Black, White and Gray [5]:

• **White Hat:** is another name for security experts. The white box ethical hackers team uses the same tools and techniques which used by the Black Hat hackers. The security experts used those tools to foil the bad guys. In addition, they used those tools and techniques for the ethical hacking to assist the forensic investigator to find the proper solution for any security breach even in the computer, network or Mobile phone. The job of the White hat to close any security hole to protect their companies from Black Hat.

• **Black Hat:** is the name of the bad guys who used all hacking tools to send virus, worms, break into computer system, steal data and attack the network and all these types of hack are under the cybercrime and can break the law.

• **Gray Hat:** this type of hacking is a hybrid attack model and it combined elements of both Black Hat and white Hat elements. This model has two players the first, untrusted outsider who is working with trusted insider. And the second is insider feeding the outsider by important information on initiating black box reconnaissance attacks. The external scope will exploit these attacks to the areas of true vulnerability. In this experiment we will use the white box hacking model to evaluate the Android vulnerability by using penetration testing tools, just for proving if there are any vulnerabilities in Android system or not.

In this work will use the white box hacking model to evaluate the Android vulnerability by using penetration testing tools.

2.1 Penetration Test Approach and Methodology

Penetration testing is one of the decisive techniques which are required in all businesses. The rise of cyber and computer crimes in the past few years, the penetration testing has become one of the most popular and recommended techniques of network security. The penetration test can be help in keeping a business secure from internal and external threats. In addition, the penetration test can help to identify weakness and the threats which the attacker can use [6].

The following figure Fig 1 illustrates Penetration Testing Stages:

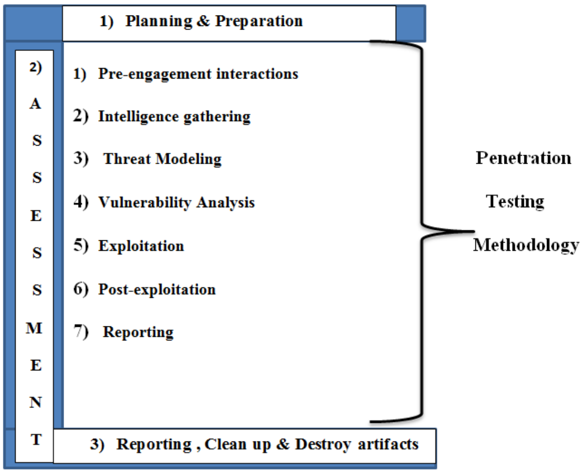

1) Planning & Preparation
2) ASSESSMENT
1) Pre-engagement interactions
2) Intelligence gathering
3) Threat Modeling
4) Vulnerability Analysis
5) Exploitation
6) Post-exploitation
7) Reporting
Penetration Testing Methodology
3) Reporting , Clean up & Destroy artifacts

Fig 1: Penetration Testing Stages.

The penetration testing can be divided into seven different phases as follows [6]:

- **Pre-engagement Interactions:** All the pre-engagement activities and scope defines in this phase and everything which you need to discuss before the penetration testing start.
- **Intelligence Gathering:** In this phase collecting all information about the target that is under test by directly connecting and passively without connecting to the target at all.
- **Threat Modeling:** This phase includes the matching of information detected to the assets in order to find the areas which has the highest level of threats.
- **Vulnerability Analysis:** This phase use in finding and identifying known and unknown vulnerabilities and validating them.
- **Exploitation:** This phase taking advantage of the vulnerabilities which found in the previous phase.
- **Post-exploitation:** The actual task which performed with target such as, downloading a file, creating a new user account on the target and shutting a system down. This phrase describes what you need to do after exploitation.
- **Reporting:** In this phase summing up the results of the test and make possible suggestions and recommendations to fix the weakness in the target.

3. IMPLEMENTATION OF PENETRATION TEST

The implementation phase of penetration test will base on the scenario of hacking Android phone through an open Wi-Fi.

3.1 Testing Scenario

There are two scenarios for the implementation phase. The First scenario is for investigation the vulnerabilities in the Android platform. The second one is about the conduct the penetration testing. To conduct the penetration testing will use the Metasploit framework with Kali Linux to exploit the Android phones through Wireless network access point (Wi-Fi).

3.1.1 Investigation of the vulnerabilities has certain steps to follow:

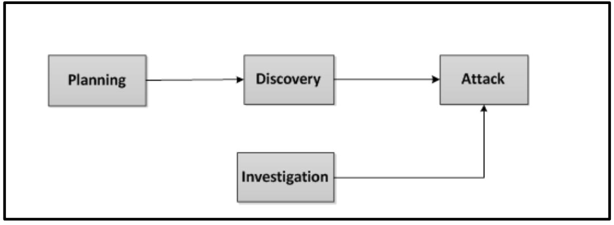


Fig 3: Steps of Investigation Vulnerabilities.

1) **Planning Stage:** set the goals of the penetration test.

2) **The discovery phase:** Identify the available IP address in the same network, Accessing the Wi-Fi and then hack the target device using hacking tools.

3) **The final stage:** will be investigated using mobile forensic tools on how the attacks performed and showing the result thereon.

This flow will work in a cycle to access the security systems of the target device and investigate the result.

3.1.2 Testing Scenario of hacking using Wi-Fi Access Point

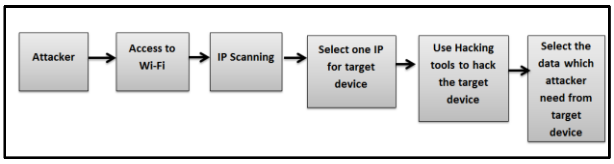

Attacker
Access to Wi-Fi
IP Scanning
Select one IP for target device
Use Hacking tools to hack the target device
Select the data which attacker need from target device

Fig 4: Steps of Hacking.

1) First the attacker will search for the available opened Wi-Fi and using the penetration tools.

2) Search and select one IP to be a target for attack.

3) The Attacker sends the malicious script to the victim mobile.

4) The pentest tools will hack the victim device by using camera, record sound and access to social networking messages from SD card database.

3.2 Penetration Testing Tools

There are many tools available in market for stealing sensitive data from Smartphones such as WhatsApp sniffer, FaceNiff, Dsploit, AndroRat, and SSL Strip which are free software's. On other hand, there are many types of penetration testing tools available to help the security experts to testing and evaluating the vulnerabilities in the Smartphones such as Metasploit Framework, Wireshark, Intercepter-NG and etc. In this experiment will use the Metasploit Framework.

3.2.1 Metasploit:

The most popular penetration testing framework is the Metasploit .Is an open source Penetration testing tool with various functionality and features. In addition, it provides most important information about security vulnerabilities, and it is useful in penetration testing. Furthermore, it is developed to exploit remote machines and IDS/IPS signature development. Metasploit offers a great deal of exploits, payloads, encoding techniques, and loads of post-exploitation features. It can be configured under both Windows and Linux operating system [6] .

Metasploit has various types of editions as follow:

- **Metasploit pro:** This edition is a commercial and offers great features such as a web application, scanning, exploitation and automated exploitation.
- **Metasploit community:** This is a free edition with less functionality than the pro edition. This type of edition can be used by students and small businesses.
- **Metasploit framework:** This edition is a command line with all manual tasks such as manual exploitation and third-party import.

Metasploit also offers numerous types of user interfaces, as follows:

- **The GUI interface:** In Graphical user interface all options available at a click button which can help the user to management the vulnerability.
- **The Console interface:** This interface is the most popular. This interface can provides all options which offered by Metasploit in one approach.
- **The Command –Line interface:** This interface is the most powerful and it supports the launching of exploits to activities such as payload generation.
- **Armitage:** This type is a third-party interfaces and it offers easy vulnerability management, exploit recommendations, built-in NMAP and ability to automate features using the Cortana scripting.

The following flow chart illustrates the steps of penetration testing by using the Metasploit framework:

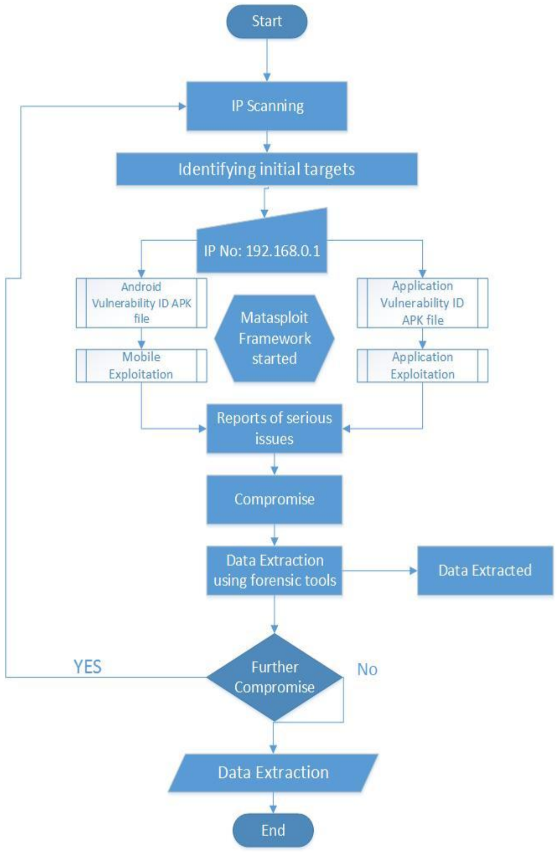

Start
IP Scanning
Identifying initial targets
IP No: 192.168.0.1
Android Vulnerability ID APK file
Metasploit Framework started
Application Vulnerability ID APK file
Mobile Exploitation
Application Exploitation
Reports of serious issues
Compromise
Data Extraction using forensic tools
Data Extracted
YES
Further Compromise
No
Data Extraction
End

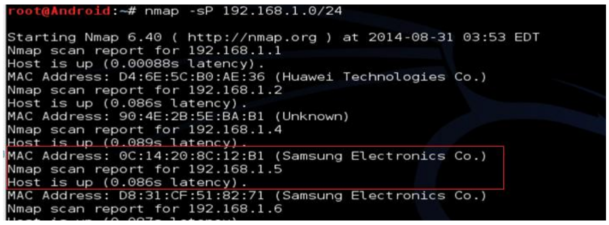
Fig 4: Metasploit Framework Scenarios.

3.2.2 *Conducting a penetration test with the Metasploit Framework:*

- **Scanning The Available IP Address In The Network**

To select the target device the attacker should scanning all available devices which use the same open network (Wi-Fi) to start his criminal activities. To Scanning and display the Available IP Address of all connected devices in the same network use the ***Nmap –sP*** command in Metasploit. ***Nmap*** is a very helpful command in Metasploit during penetration testing. It provides different types of modes for scanning target devices such as (***TCP/IP connect scan, SYN stealth scan, ACK scan and UDP scan)*** [7]. ***NMAP*** not only tells us if the system is alive or not, it can also display the ***MAC*** address of the target device by sending ***ARP*** (**Address Resolution Protocol**) request. If the target device blocks the ***ICMP*** packets the ***NMAP*** will ping scan automatically to changing from ***ICMP*** to ***TCP*** based packets.

The following figure Fig 5 displays the available IP Address, MAC Address and the Type of device. The target device which the attacker selected was Samsung with MAC address (0c:14:20:8c:12:B1) and the IP address was 192.168.1.5.



```
root@Android:~# nmap -sP 192.168.1.0/24

Starting Nmap 6.40 ( http://nmap.org ) at 2014-08-31 03:53 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00088s latency).
MAC Address: D4:6E:5C:B0:AE:36 (Huawei Technologies Co.)
Nmap scan report for 192.168.1.2
Host is up (0.086s latency).
MAC Address: 90:4E:2B:5E:BA:B1 (Unknown)
Nmap scan report for 192.168.1.4
Host is up (0.089s latency).
MAC Address: 0C:14:20:8C:12:B1 (Samsung Electronics Co.)
Nmap scan report for 192.168.1.5
Host is up (0.086s latency).
MAC Address: D8:31:CF:51:82:71 (Samsung Electronics Co.)
Nmap scan report for 192.168.1.6
```

Fig 5: Scanning IP Address.

- **Starting Metasploit Framework And Injecting Malicious Code (APK File) In Victim Device:**

After selecting the target device the attacker should start the Metasploit framework to implement the steps of hacking. To Start the Metasploit Framework use the ***msfconsole*** command. The ***msfconsole*** use to set up the console interface of Metasploit and support way to access most of features in Metasploit [8].

After selecting the target device the attacker will inject the malicious code **(APK file). APK** is an (Application Package file) which needs to distribute to the victim device by using the ***msfpayload***. ***Msfpayload*** is a Metasploit command use to generate shell code which use in manual exploits and it is used to create payloads such as (exe, Java, apk etc.) [9]. The attacker can use different ways to distribute the **APK** file to the victim device, such as uploading the file and sending the link to the victim, dropping the file on a USB stick, or in a compressed zip format into E-mail. The Successful execution of ***msfpayload*** will create the apk file which involves the Application of Metasploit reverses TCP backdoor. After injecting this malicious file in the victim device it required from victim to install the Main Activity application which is the Metasploit reverse TCP backdoor. When the victim opens and install the APK file, the ***meterpreter*** shell will start connection between the victim and attacker device. ***Meterpreter*** command is an advanced multi-function payload which can use to display running process, printing working directory, search for a file, take photo using the device camera, record sound and access to Sdcard database in target device [10]. The following figure Fig 6 display the APK file application and the reverse TCP:

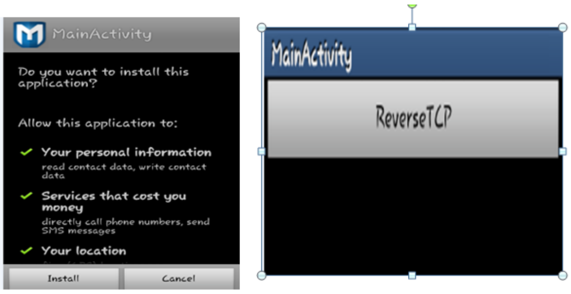
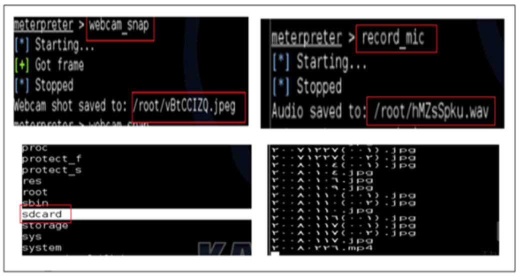

MainActivity
Do you want to install this application?
Allow this application to:
✓ Your personal information
read contact data, write contact data
✓ Services that cost you money
directly call phone numbers, send SMS messages
✓ Your location
Install
Cancel
MainActivity
ReverseTCP

Fig 6: Metasploit Reverses TCP backdoor.

After the ***meterpreter*** open the session between the attacker and victim device. There are lists of commands the attacker can use to access to all data's in victim device such as **(webcam, record_mic, SD card, etc.)**. The following figures Fig 7 and Fig 7.1 show the commands and the result of each command which was used to conducting penetration tests on Android devices. The **webcam_snap** command allows using the front or backing camera in the victim device to capture some photo and the **record _mic** allow recording the conversations. And also, can access to all data on the SD card such as WhatsApp databases and some other database by using **Sdcard** command.



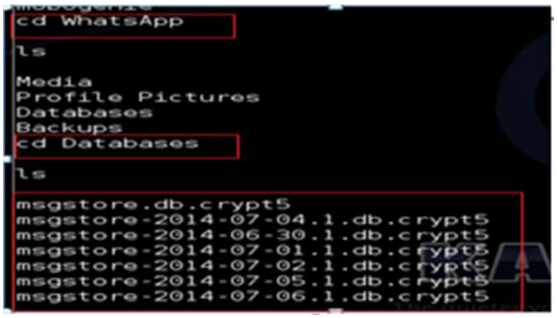
```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/vBtCCIZQ.jpeg
```

```
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /root/hMZsSpku.wav
```

```
proc
protect_f
protect_s
res
root
sbin
sdcard
storage
sys
system
```

```
٢٠٠٧١٢٢٧(٠٠١).jpg
٢٠٠٧١٢٢٧(٠٠٢).jpg
٢٠٠٨٠١٠٤(٠٠١).jpg
٢٠٠٨٠١٠٤.jpg
٢٠٠٨٠١٠٦.jpg
٢٠٠٨٠١٠٩.jpg
٢٠٠٨٠١١٠(٠٠١).jpg
٢٠٠٨٠١١٠(٠٠٢).jpg
٢٠٠٨٠١١٠.jpg
٢٠٠٨٠١١٦(٠٠١).jpg
٢٠٠٨٠١١٧(٠٠١).jpg
٢٠٠٨٠١١٧(٠٠٢).jpg
٢٠٠٨٠١١٧.jpg
٢٠٠٨٠٢٢٦.mp4
```

Fig 7: Display how can access to camera and record sound



```
cd WhatsApp
ls

Media
Profile Pictures
Databases
Backups
cd Databases
ls

msgstore.db.crypt5
msgstore-2014-07-04.1.db.crypt5
msgstore-2014-06-30.1.db.crypt5
msgstore-2014-07-01.1.db.crypt5
msgstore-2014-07-02.1.db.crypt5
msgstore-2014-07-05.1.db.crypt5
msgstore-2014-07-06.1.db.crypt5
```

Fig 7: Display WhatsApp Database from Sdcard.

.

4. CONCLUSION

After conducting the penetration test on Android phone by Metasploit Framework, can be summarized the findings of this tool which are the Android system is a vulnerable and can be hacked through Wi-Fi. The attacker can access to sensitive data and use webcam to take pictures also can use record-mic to record conversations of victims. Thus it was found that Linux kernel layer is the most sensitive part of Android Operating system and the hackers can easily access to data of this layer.

5. FUTURE WORK

The forensic investigators can examination and extraction of data from Smartphones by using different types of Mobile forensic tools. The future work will involve the extraction of data from Android platform by using forensic open source tools to find the proper evidences.

6. REFERENCES

[1] A. Alonso-Parrizas, "Securely deploying Android devices," Dublin, Ireland, 2011.

[2] V. VIJITH, "Android Forensic Capability and Evaluation of Extraction Tools," 2012.

[3] Naresh Kumar & Muhammad Ehtsham Ul Haq, "Penetration Testing of Android-based Smartphones," p. 5, 2011.

[4] D. M. Hafele, "Three Different Shades of Ethical Hacking Black, White and Gray," SANS Institute InfoSec Reading Room, 2004.

[5] Linda McCarthy and Denise Weldon-Siviy, Hackers and Crackers, D. Weldon-Siviy, Ed., Linda McCarthy, 2010.

[6] N. Jaswal, Mastering Metasploit, First Edition ed., BIRMINGHAM - MUMBAI: Packt Publishing Ltd., 2014, p. 22.

[7] A. Singh, Metasploit Penetration Testing Cookbook, Birmingham: Packt Publishing Ltd, 2012, p. 34.

[8] Mati Aharoni,William Coppola,Devon Kearns,David KennedyMatteo Memelli,Max Moser,Jim O'Gorman,David Ovitz and Carlos Perez , "https://www.offensive-security.com/metasploit-unleashed/," JUNE 2011. [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/.

[9] David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni, Metasploit The Penetration Tester's Guide, San Francisco: William Pollock, 2011.

[10] S. Sleuth, "http://www.security-sleuth.com/sleuth-blog/2015/1/11/using-metasploit-to-hack-an-android-phone," 12 JANUARY 2015. [Online]. Available: http://www.security-sleuth.com/sleuth-blog/2015/1/11/using-metasploit-to-hack-an-android-phone. [Accessed 2015].